СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(10–24.08)

2015 № 14

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(10–24.08)
№ 14

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

Відповідальний редактор
Л. Чуприна, канд. соц. ком.

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Два месяца назад был запущен проект Profebook – профессиональная социальная сеть для бизнеса. И уже в октябре состоится первое масштабное обновление: будет внедрена инновационная технология – самообучающаяся умная система релевантных рекомендаций. Все, кто успеет зарегистрироваться до этого, бесплатно и навсегда получат премиум-аккаунт, пишет AIN.UA (http://ain.ua/2015/08/10/594413?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ainua+%28AIN.UA%29).

Profebook – это социальная сеть, предназначенная для предпринимателей, стартаперов, поставщиков, специалистов и других участников бизнес-коммуникации. Здесь можно найти полезные контакты, стартаперам – команду для воплощения своих идей, специалистам – работу, предпринимателям – сотрудников, партнеров и поставщиков, а также продвигать свои продукты, компании, следить за конкурентами, черпать идеи и многое другое.

При этом Profebook, по определению, остается социальной сетью, а это значит, что площадка предоставляет инструменты не только для ведения бизнеса, но и для любой другой мультимедийной коммуникации между пользователями. В настоящее время сайт доступен на английском, польском и русском. В скором времени добавятся испанский, португальский, французский и немецкий языки.

По словам создателей проекта, новая технология будет работать по принципам, приближенным к искусственному интеллекту. Самообучающаяся система будет собирать из аккаунта пользователя данные, позволяющие создать картину о его интересах, и на их основании будет рекомендовать подходящие контакты и компании.

Основная идея этого механизма в том, чтобы анализировать все обновления аккаунта, вплоть до лайков, репостов и новых друзей, поддерживая актуальный, «живой» образ пользователя. Машина будет постоянно обучаться и оттачивать свои формулы. И все это будет происходить автоматически в фоновом режиме, без непосредственного участия пользователя. Таким образом, юзеры будут получать самые релевантные предложения и рекомендации, даже не утруждаясь целенаправленным поиском. И чем больше будет пользователей и контента, тем точнее и умнее Profebook будет помогать людям решать их задачи.

«Скажем, если вы менеджер по продаже стройматериалов, а интересуетесь производством скоростных лодок, то в Profebook вы рано или поздно найдете отличную работу, партнеров или единомышленников, связанных с вашими истинными интересами. Profebook будет подталкивать пользователей осуществлять их мечту и находить возможности для самореализации именно в той сфере, в которой они хотят», – говорит один из основателей проекта А. Бауэр.

Эта система станет главным отличием Profebook от всех предшественников, которые в большинстве своем являются по сути справочниками. После внедрения этой технологии премиум-аккаунт, дающий доступ ко всем функциям портала, будет платным, но пока есть шанс зарегистрироваться бесплатно и получить его навсегда. Для этого необходимо обзавестись аккаунтом на Profebook до 1 октября 2015 г.

Тем временем уже сейчас зарегистрировавшимся пользователям Profebook доступны все ключевые возможности соцсетей. Пользователи могут общаться друг с другом, формировать свою новостную ленту из подписок на страницы пользователей и компаний, создавать группы, ставить лайки, делать репосты, загружать все виды файлов, создавать именные ссылки для своих аккаунтов, делиться контентом в социальных сетях и т. д. Кстати, авторизоваться в Profebook также можно с помощью других соцсетей, что предполагает синхронизацию аккаунтов.

Но, как специализированная соцсеть, Profebook предлагает пользователям также уникальные возможности для профессионального и бизнес-развития. Например, система генерирует красиво оформленное резюме пользователя, собирая данные о его опыте, навыках и профессиональных интересах, и предлагает его потенциальным работодателям. Когда пользователь указывает сферу своего бизнеса – система предлагает ему круг полезных контактов: поставщиков, партнеров, потенциальных сотрудников, клиентов. Таким образом, Profebook – это площадка не только для персонального роста, но и для продвижения своего продукта в сети.

Profebook предлагает много инструментов для кастомизации – как дизайна страницы, так и пользовательских настроек. Также можно установить свои правила приватности. В зависимости от геолокации, юзеры видят текущий курс валют и погоду в определенном регионе.

Кроме внедрения умных технологий, к октябрю команда проекта запланировала еще ряд обновлений. Во-первых, в соцсети будет создан собственный мессенджер, также с инновационными функциями: автоматически анализируя вашу деловую переписку, система будет составлять для вас список задач и напоминаний. Эти списки можно будет просматривать и редактировать совместно с другими участниками переписки. Что касается групповых чатов, то в них, в отличие от большинства других мессенджеров, не будет никаких ограничений по количеству участников. Во-вторых, выйдут два мобильных приложения – для iOS и Android – с полным набором функций портала, которые также можно получить бесплатно.

В 2016 г. Profebook планирует создать свою платформу для видеоконференций, которая будет интегрирована в соцсеть и доступна по платной подписке. Также она будет функционировать и продаваться как отдельный продукт. Среди особенностей этой платформы – полная поддержка iOS, потоковая передача видео в высоком разрешении, а также возможность объединить до 20 тыс. человек в онлайн-трансляции.

Profebook – это проект одноименной польской компании. Бета-версия была запущена в мае 2015 г. под руководством сооснователя Profebook А. Корнийчука. Проект был запущен инвестициями создателей. Со временем командой планируется проведение IPO на одной из европейских площадок.

С момента запуска в соцсети зарегистрировались пользователи из 102 стран мира. Создатели обещают, что 95 % функционала всегда будут доступны бесплатно. Премиум-аккаунт, который с октября будет платным, будет включать ряд дополнительных возможностей.

«Сейчас мы полностью открыты к советам и пожеланиям пользователей, чтобы сделать соцсеть максимально удобной и полезной. Для нас важен любой фидбек», – заявляет команда Profebook ***(Profebook: социальная сеть, которая помогает воплощать мечты // AIN.UA (http://ain.ua/2015/08/10/594413?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ainua+%28AIN.UA%29). – 2015. – 10.08).***

***

Twitter зняв обмеження в 140 символів в особистих повідомленнях. Тепер користувачі можуть обмінюватися між собою текстами будь-якої довжини. Про це йдеться на порталі Yahoo News.

«Сьогоднішня зміна – це ще один великий крок до того, щоб зробити приватний сегмент Twitter ще більш потужним і розважальним», – прокоментував на своїй сторінці в соцмережі керівник проекту Direct Messages в Twitter Inc С. Агарвал.

Зміна почала діяти з 12 серпня для всіх мобільних додатків Twitter для програми Tweetdeck, а також для користувачів, які пишуть із сайту соцмережі.

Для того щоб почати писати довгі особисті повідомлення у Twitter, користувачам потрібно оновити свої додатки до останньої версії.

Обмеження на стандартні публічні повідомлення в 140 символів зберігається.

Раніше сервіс мікроблогів Twitter запустив функцію, яка дає змогу прокоментувати додатковими 116 знаками пост, який користувач ретвітнув і розмістив у себе на сторінці ***(Twitter зняв ліміт у 140 знаків в особистих повідомленнях // Media Sapiens (http://osvita.mediasapiens.ua/web/social/twitter_znyav_limit_u_140_znakiv_v_osobistikh_povidomlennyakh). – 2015. – 13.08).***

***

Социальная сеть Facebook работает над новым приложением для чтения новостей, которое будет оповещать пользователей о важных событиях. Такой информацией располагает британское издание Business Insider UK.

Как сообщает источник, при первом запуске программы пользователь может подписаться на любимые новостные сайты, а также выбрать интересующие темы (Facebook называет их «станциями»). Чтобы держать читателей в курсе событий, издания получат возможность рассылки

уведомлений о горячих новостях. Такие сообщения будут включать ссылку на интернет-ресурс и краткое описание с ограничением в 100 символов. Отсюда и сравнение с микроблогами в Twitter.

В настоящее время Facebook тестирует альфа-версию, и говорить о каких-либо сроках запуска проекта пока рано. Также непонятно, почему разработчики просто не добавили функцию оповещений в уже существующий новостной агрегатор Paper ***(Facebook решил ворваться на территорию Twitter // ITBusiness.com.ua (http://itbusiness.com.ua/social-networks/3020-facebook-reshil-vorvatsya-na-territoriyu-twitter.html). – 2015. – 13.08).***

***

Социальная сеть «ВКонтакте» обновила приложение Snapster, позволяющее выкладывать фотографии с наложенными фильтрами, пишет «Телеграф» (http://telegraf.com.ua/tehnologii/2017151-snapster-ot-vkontakte-podderzhivaet-gorizontalnyie-snimki.html).

В новой версии для iPhone пользователи получили возможность публиковать снимки в горизонтальной ориентации, в том числе с возможностью кадрирования готовых изображений. Помимо этого были исправлены ошибки на некоторых устройствах и повышена стабильность и скорость работы приложения.

Snapster состоит из пяти основных разделов: лента новостей, рекомендации, съемка и публикация, уведомления и профиль. По функционалу приложение частично напоминает соцсеть Instagram и дает примерно те же возможности – создавать снимки; просматривать ленту, в которую попадают фотографии из «ВКонтакте», а также создавать собственные фильтры. Есть возможность добавлять хэштеги и указывать геометку места, где фотография была сделана.

На основную вкладку попадают все фотографии, загруженные друзьями пользователя. Снимки можно отметить как понравившиеся и прокомментировать (текстом или снимком). На вкладке с рекомендациями доступны три раздела: «Популярное», «Друзья друзей» и «Рекомендации» – снимки, которые понравились друзьям. На вкладке с уведомлениями пользователь видит, кто добавил его в друзья, лайкнул или прокомментировал фотографию, а также прислал фотографию личным сообщением.

Из Snapster можно отправлять самоуничтожающиеся фотографии, что делает его похожим на популярный на западе сервис Snapchat. Снимок пропадает через указанное время (до 20 с). Приложение уведомляет пользователя, если собеседник успел сделать скриншот сообщения.

«Мы создали Snapster, чтобы люди могли обрабатывать фотографии на профессиональном уровне и делиться ими со своими друзьями и подписчиками, – говорит А. Рогозов, операционный директор “ВКонтакте”. – Это первый мобильный продукт “ВКонтакте”, существующий отдельно от социальной сети, но тесно интегрированный с ее социальным графом. Таким образом мы создаем глобальный проект, не ограниченный аудиторией сайта».

Особенности новой версии Snapster для iOS:

– добавлена возможность публиковать фотографии в горизонтальной ориентации (через кадрирование или при создании снимка в горизонтальном положении устройства);

– исправлены ошибки и вылеты на некоторых устройствах;

– повышена стабильность и скорость работы приложения ***(Snapster от «ВКонтакте» поддерживает горизонтальные снимки // Телеграф (http://telegraf.com.ua/tehnologii/2017151-snapster-ot-vkontakte-podderzhivaet-gorizontalnyie-snimki.html). – 2015. – 12.08).***

***

На платформе «Одноклассников» стали доступны групповые видеоканалы. Это нововведение позволит производителям контента в разы увеличить количество просмотров ролика и попасть в витрину лучших видео, сообщили CNews в Mail.Ru Group. По данным компании, ежедневно в «Одноклассниках» видео просматривает более 220 млн человек, пишет cnews.ru.

Новый инструмент обеспечивает возможность подписаться на видеоканал без подписки на группу и анонимный просмотр видео без регистрации на портале. Каналы, созданные в группах, можно найти в поиске видео, на витрине и в тематических разделах. Подписчик группового канала сможет получать уведомления о новых видео с помощью системы оповещений и в списке подписок.

Помимо этого, администратору стал доступен новый раздел «Загрузка видео», с помощью которого можно следить за ходом выполнения загрузки, редактировать название видео, описание, добавлять теги и выбирать канал. Администратор при этом может осуществлять загрузку в фоновом режиме, рассказали в Mail.Ru.

Создание видеоканала пока доступно только для веб-версии «Одноклассников». В ближайшее время вести видеоканалы можно будет и в нативных приложениях на Android/iOS, и в мобильной версии ***(«Одноклассники» запустили групповые видеоканалы // МедиаБизнес (http://www.mediabusiness.com.ua/?option=com_content&task=view&id=44286&Itemid). – 2015. – 11.08).***

***

Внутри социальной сети «Одноклассники» (в том числе в мобильной версии и мобильных приложениях) начал работу сервис онлайн-стриминга телеканалов на базе собственного видеоплеера. Первым каналом, который начал вещать в «Одноклассниках» в прямом эфире, стал LifeNews. Трансляция доступна в официальной группе и пользователи могут делиться ею и комментировать эфир. В настоящее время ведутся переговоры о старте трансляции в «Одноклассниках» других российских телеканалов: «Первого» и «России» ***(Одноклассники запустили стриминг телеканалов внутри сети //***

Marketing Media Review (http://mmr.ua/show/odnoklassniki_zapustili_striming_telekanalov_vnutri_seti). – 2015. – 24.08).

***

Российская социальная сеть «ВКонтакте» заключила соглашение с ВГТРК о легальном размещении видеоконтента телекомпании на страницах сети. Информацию об этом подтвердил пресс-секретарь «ВКонтакте» Г. Лобушкин, сообщает «Обозреватель» со ссылкой на Газета.Ru.

Реализацией соглашения займется сеть онлайн-дистрибуции видео Pladform. В сети «ВКонтакте» будут размещены видео программ «Вести», «Вечер с Владимиром Соловьевым», «Прямой эфир», «Специальный корреспондент», «Главная сцена», «Танцы со звездами», «О самом главном» и др.

«ВКонтакте» будет получать как архивные записи передач, так и новые выпуски сразу после эфиров ***(«ВКонтакте» будет размещать российскую пропаганду // Обозреватель (http://tech.obozrevatel.com/news/10682-vkontakte-budet-razmeschat-rossijskuyu-propagandu.htm). – 2015. – 18.08).***

***

Twitter тестирует отдельную вкладку для новостей. Она содержит в себе список самых обсуждаемых новостей из различных источников. При нажатии на новость пользователи увидят краткое содержание новости, изображение, а также список твитов, посвященных этой теме.

Социальная сеть также проводит эксперимент под названием Project Lightning, цель которого – сбор твитов, посвященных какой-то теме, в коллекции.

Предполагается, что новостная вкладка поможет пользователям, только зарегистрировавшимся в соцсети, быстрее там освоиться ***(Twitter тестирует отдельную вкладку для новостей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_testiruet_otdelnuyu_vkladku_dlya_novostey). – 2015. – 10.08).***

***

Во «ВКонтакте» появилась возможность размещать любое изображение в сниппете – блоке, который прикрепляется к записи при добавлении ссылки. То есть теперь можно размещать в записи кликабельную иллюстрацию на любую страницу. Например, на карточку товара в интернет-магазине.

Нововведение поможет увеличить количество переходов из ленты «ВКонтакте» на сайт компании, а также пригодится всем, кто активно делится ссылками в сообществах ***(В сниппеты «ВКонтакте» можно добавлять любые изображения // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/v_snippety_vkontakte_mozhno_dobavlyat_lyubye_izobrazheniya). – 2015. – 14.08).***

***

Twitter открыл доступ к архиву всех проиндексированных твитов с помощью нового поискового функционала под названием Full-Archive Search API. Анализ архивных твитов призван помочь брендам в разработке новых рекламных кампаний, продуктов, аналитических решений и т. д.

В разработке инструмента приняли участие специалисты Gnip – компании, приобретенной Twitter в прошлом году.

Новый функционал эффективно использует существующее 30-дневное поисковое решение и расширяет доступ к твитам давностью более девяти лет. Full-Archive Search API позволят клиентам Gnip мгновенно найти публичный твит любой давности.

В прошлом году Twitter обновил функцию поиска, чтобы пользователи могли найти все когда-либо написанные твиты.

В конце января 2014 г. специалисты сервиса микроблогов запустили ряд новых поисковых фильтров по контенту, публикуемому на сайте. Новые поисковые фильтры позволили искать твиты, содержащие видео или фото, а также ограничить поиск определенным местоположением.

В апреле того же года Twitter добавил дополнительный фильтр поиска по контенту, публикуемому на сайте. Основной фильтр получил название Timelines («Хроники») ***(Twitter запустил API поиска по архиву // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_zapustil_api_poiska_po_arhivu). – 2015. – 18.08).***

***

Facebook запустил сервис видеотрансляций, недоступный для обычных пользователей

Знаменитости, у которых есть аккаунт в Facebook, теперь смогут вести прямые видеотрансляции при помощи нового сервиса Live. Live – это одна из функций приложения Facebook Mentions, которое было создано для общения знаменитостей со своей аудиторией. Однако видеотрансляции может посмотреть любой пользователь, подписанный на страницу публичной персоны в Facebook.

Трансляции будут сохраняться на странице знаменитости и останутся доступными для повторного просмотра. Первыми, кто опробовал новый функционал, стали Дуэйн «Скала» Джонсон, теннисистка С. Уильямс, футболист Р. Кака и др. ***(Facebook запустил сервис видеотрансляций, недоступный для обычных пользователей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_zapustil_servis_videotranslyatsiy_nedostupnyy_dlya_obychnyh_polzovateley). – 2015. – 10.08).***

***

Инвалиды тоже хотят проводить время в социальных сетях, но некоторые не могут сидеть в обычных соцсетях из-за ограниченных возможностей, передает издание Supreme2.ru. Именно поэтому в Кемеровской области заработала специальная соцсеть для людей с ограниченными возможностями.

Сайт доступен по адресу s-voi.ru.

С 18 августа сайт стал официально функционировать. По словам авторов проекта, это первый подобный опыт для России. Несмотря на то что социальная сеть предназначена для инвалидов, любой желающий может с легкостью зарегистрироваться там.

Сайт создан с учетом потребностей аудитории и со специальным интерфейсом, в котором имеется режим «цветовой слепоты».

В целом, соцсеть предоставляет такие же возможности, как и обычные, популярные на сегодняшний день социальные сети. Разработчики планируют в скором времени создать версию сайта для дальтоников и слабовидящих людей.

Также в планах имеется создание специальных приложений в соцсети, по которым люди с ограниченными возможностями смогут обучаться различным профессиям в сфере информационных технологий.

Разработчики сообщили, что в качестве почетного гостя пригласили знаменитого ученого С. Хокинга. По мнению авторов, он сможет стать для всех пользователей соцсети символом надежды и исполнения мечты ***(Создана социальная сеть для инвалидов // Supreme2.Ru (http://supreme2.ru/15310-sozdana-socialnaya-set-dlya-invalidov). – 2015. – 20.08).***

***

Аналитическая компания Pew Research опросила интернет-пользователей на предмет использования мобильных мессенджеров, приложений, социальных сетей и блог-платформ.

Эксперты из Pew Research выяснили, что 36 % опрошенных владельцев смартфонов используют мессенджеры, подобные Kik или iMessage, а 17 % предпочитают приложения, в которых сообщения автоматически удаляются, например Snapchat or Wickr.

Кроме того, опрос показал, что количество взрослых онлайн-пользователей, заходящих в Pinterest и Instagram, удвоилось за период 2012–2015 гг. В частности, 31 % респондентов используют Pinterest (по сравнению с 15 % в 2012 г.), 28 % – Instagram (в 2012 г. – 13 %).

Помимо прочего выяснилось, что ни одна из социальных платформ, упомянутых в исследовании, не показала существенного роста аудитории за период с сентября 2014 по апрель 2015 г. Тем не менее, некоторые сайты обнаружили значительное увеличение ежедневных посетителей: Instagram ежедневно используется 59 % опрошенных против 49 % осенью прошлого года; для Pinterest эти показатели составляют 27 и 17 % соответственно. Количество ежедневных пользователей LinkedIn среди участников опроса увеличилось с 13 до 22 % за упомянутый период.

В Pew Research также сообщают, что Facebook остается самым популярным у респондентов social media: 72 % опрошенных используют его, при этом ежедневно авторизовываются в социальной сети 70 %, включая 43 % делающих это несколько раз в день.

Блог-платформы показали результат в 15 % пользователей, участвовавших в исследовании Pew Research, читающих топики на таких площадках, как Reddit, Digg или Slashdot. При этом 10 % респондентов используют Tumblr ***(Как онлайн-пользователи относятся к мессенджерам, приложениям и соцсетям // ReklaMaster.com (http://reklamaster.com/marketing-and-advertising/kak-onlajn-polzovateli-otnosjatsja-knbspmessendzheram-prilozhenijam-i-socsetjam). – 2015. – 21.08).***

***

Главный исполнительный директор Foursquare Д. Кроули на конференции GrowthBeat в Сан-Франциско рассказал, что количество зарегистрированных пользователей сервиса за 10 месяцев увеличилось на 5 млн и в настоящее время превысило 60 млн, при этом количество ежемесячно активных пользователей достигло 50 млн. Об этом пишет searchengines.ru

Необычное соотношение показателей объясняется тем, что не все активные пользователи Foursquare зарегистрированы в сервисе.

Количество подсказок Foursquare превысило 75 млн, в то время как в октябре этот показатель составлял всего 50 млн.

Кроме того, Foursquare является поставщиком данных о том, куда люди ходят со своими телефонами. «Мы строим сервис, который призван узнать о местах, в которые вы ходите», – говорит Д. Кроули. Этот сервис называется Pinpoint.

Twitter использует данные Foursquare для информации о местоположении. Microsoft использует их для Windows Phone и Cortana. Сервис также используют AT&T, Jaguar и Land Rover ***(Количество зарегистрированных пользователей Foursquare превысило 60 миллионов // МедиаБизнес (http://www.mediabusiness.com.ua/?option=com_content&task=view&id=44386&Itemid=). – 2015. – 20.08).***

***

Что будет, если Google и Facebook захватят мир

Мессенджер Google Hangouts превратился в независимое веб-приложение. Сам же Google уже давно стал лидером в картографии. Facebook, в свою очередь, отвоевывает позиции на информационном пространстве.

Atlantico: *Что может грозить нам, если какая-то компания получит монополию на онлайн-карты?*

В. Пент-Деренокур: Google получил настоящую монополию в геолокализациии среди граждан западных стран. Кроме того, принадлежащий ему Android тоже повсеместно устанавливает местоположение пользователей.

Это в высшей степени ценная информация. Сегодня она служит для рекламы, а завтра может использоваться для алгоритма прогнозирования ваших передвижений или установления ваших привычек. Наконец, она придает Google немалый вес в отношениях с государствами и их широкомасштабным аппаратом слежения.

Изначально картография была государственной и даже военной областью, однако она далеко не первая правительственная прерогатива, которую отдали на откуп частному сектору. В прошлом столетии главным по картам почти целый век был Michelin, пока Google не отобрал у него этот титул. Во Франции карту пытались сделать формой государственного имущества, но нельзя не признать, что изменение самой концепции карты в связи с ее переходом в цифровое пространство вывело государство из игры.

С расширением монополии в борьбе за контроль над картами все далеко не так просто. Хотя лозунг Google и звучит «Не будь злом» (Don’t be evil), компания собирает о вас все больше данных, увеличивая тем самым добавленную стоимость. Конкуренты же постепенно сдают: кто-то еще пользуется картами от Apple? Получается, что новичкам на рынке нужно преодолеть все более высокую планку. Купив два года назад за миллиард долларов Waze с его 50 млн пользователей и добавив его в свои карты, Google получил монополию в динамической картографии (Waze), статической картографии (Карты + спутниковые снимки), а также режиме просмотра (Google Earth).

Кроме того, ни для кого не секрет, что все это имеет смысл в подготовке к созданию автомобиля без водителя: если Google известны транспортные предпочтения сотен миллионов человек, он сможет напрямую сделать им чрезвычайно привлекательное предложение. Будет ему прекрасно известно и о том, где разместить свои машины, если он захочет запустить в Париже услугу вроде AutoLib.

– Facebook, в свою очередь, все больше укрепляет позиции в информационной сфере. Компания М. Цукерберга постепенно уничтожает всех своих конкурентов? Если да, как это происходит?

– Об уничтожении конкурентов говорить пока рано, хотя все к этому идет. Сейчас на Facebook приходится четверть всего трафика политических информационных ресурсов при том, что в прошлом году речь шла всего о 10 %. Он вряд ли остановится на достигнутом, и пусть даже до 100 % дело явно не дойдет, он вполне вероятно может стать главным источником посетителей для значительной части интернет-сайтов.

Недавно в ситуации возник новый виток, когда банки la Banque Populaire и les Caisses d’Epargne сообщили о намерении открыть виртуальные отделения в Facebook, то есть перевести часть клиентской программы на платформу соцсети. Это говорит о том, что способность Facebook поглощать Интернет не ограничивается одной информацией и теперь касается связей с клиентами.

Все это является отражением перехода от информационной сети (ее символом является Google), которая нужна нам для поиска ответов на вопросы,

к развлекательной сети (ее прекрасно сумели реализовать в Facebook), чья социальная функция ближе к той, которую вчера играло телевидение.

Переходу на Facebook также способствуют пробелы в предлагаемой сегодня прессой информационной модели, которые отчасти компенсируются алгоритмами соцсети. Если прессе (будь то традиционный киоск или Google News) не достает разнообразия, Facebook наоборот блещет плюрализмом мнений и точек зрения. Люди жаждут демократии, а французскую прессу демократической никак не назвать. Некоторые сюжеты для нее под запретом, а в других допускается лишь одна точка зрения: Украина является прекрасным тому примером. Facebook же куда проще сблизить непохожие взгляды, потому что порождаемые этим споры служат его главной пищей. Предлагаемое французской прессой разнообразие – лишь тонкий слой внешнего лака, тогда как в Facebook оно вполне реально и куда лучше отражает существующее многообразие людей. В результате соцсеть становится информационным сервисом, который люди хотят получить от СМИ.

Наконец, в достижении своей главной цели (получение прибыли) Facebook опирается на пристрастие, которое возникает в связи присутствием в социальной сети (не быть там, значит, отдалиться от общества) и ожиданием новой информации от друзей и страниц, на которые подписан пользователь (здесь, кстати, отбирается наиболее достойная внимания или же способная породить дискуссию информация: заметьте, что в записях ленты практически нет одних лишь статусов, и почти все они сопровождаются хотя бы одной фотографией). Цель здесь, разумеется, в том, чтобы максимально увеличить присутствие человека в сети: это приносит прибыль от рекламы и целевого продвижения тех или иных страниц.

– *На основании каких критериев алгоритм Facebook выбирает публикуемые записи? Может ли это как-то ограничивать плюрализм?*

– Как раз таки наоборот, перед нами предстает всплеск плюрализма мнений. Если у вас много друзей, которые придерживаются непохожих взглядов, в результате вы получите настоящий информационный коктейль, который сегодня не в состоянии предложить вам пресса.

Опасность заключается скорее в способности Facebook заключить пользователя в информационный пузырь, потому что алгоритм платформы нацелен на то, чтобы доставить ему удовольствие и продлить время пребывания в сети. Кроме того, было доказано, что Facebook в большей степени предлагает вам материалы с близкими к вашим политическими взглядами. Противоположные встречаются реже, хотя и это все равно просто невероятное информационное богатство и разнообразие по сравнению с традиционными СМИ. Поколение назад люди получали всю информацию из одной-двух газет и вечерних новостей по телевидению. Печатная пресса (с тех пор она так и не смогла по-настоящему эволюционировать) предлагала информацию для отражения той или иной идеологической позиции в форме ориентированных в какую-либо сторону статей. О плюрализме тут говорить не приходится. Google

и Facebook постепенно подрывают эту модель, которая в силу контраста все больше воспринимается людьми как устарелая машина пропаганды.

У прессы больше не осталось прежнего воздействия на общественное мнение, Интернет полностью разрушил эту прежнюю функцию СМИ. Это наблюдалось на референдуме 2005 г., когда почти вся пресса агитировала за «да», оставив «нет» на откуп Интернету. Десять лет спустя все изменилось еще больше, и теперь единственная задача прессы – давать топливо социальным сетям. Рычаги влияния перешли в руки самих людей, которые используют статьи для воздействия на других. Речь идет о кардинальной смене парадигмы, которая может привести к переустройству общественного порядка.

– Что конкретно в настоящий момент контролируют Google и Facebook?

– Google принадлежит доступ к информации, что, по сути, является развитием прошлых функций библиотеки, а также, в перспективе, мыслительной функции, памяти и ориентации в пространстве. Это открывает путь для широкого спектра возможностей. Самая очевидная из них – удовлетворение ваших желаний и его монетизация.

Facebook осуществляет переход социального полотна в виртуальную среду и передачу вытекающей из этого информации.

Оба они заняли в высшей степени политические позиции, которые в прошлом принадлежали государству, прессе (то есть промышленникам XX в.) и школе. Что касается отхода от вчерашних СМИ, тут мы имеем дело со своего рода экономическим дарвинизмом. Касательно школы же все выглядит несколько тревожнее.

В результате мы видим потерю контроля централизованными структурами (обычно это государство и ряд лобби) и переход к экономическим образованиям, которые, в свою очередь, уступают немалую его часть пользователям. Все это ведет к небывалому в прошлом плюрализму. Достаточно взглянуть на то, как трудно сейчас государствам навязать населению новый менталитет с врагами в лице России и Китая, хотя еще в прошлом столетии для этого не потребовалось бы особых усилий.

Подвести этому итог можно следующим образом: Google отвечает за ваши связи с миром, а Facebook – за связи с обществом. С одной стороны, это – контроль над информацией и смежными с ней областями (здравоохранение, автомобиль без водителя), с другой – выстраиваемый вокруг вас мир.

В конечном итоге подходы Google и Facebook, несмотря на все различия, дополняют друг друга. Один опирается на отношения в группе, другой – на ваше присутствие в группе.

– Сегодня два этих гиганта ведут войну. Какие в ней стоят экономические, политические и философские цели?

– Экономическая цель весьма проста: это поиск прибыли. Сегодня она поступает через рекламу, но завтра найдется множество иных средств монетизации.

Политические цели стали для них относительно новым фактором. В Google поняли это довольно давно, начав политику «вертушки» между собой и американским государством, примерно как в крупных банках, руководители которых работают то в одном, то в другом учреждении. Осознание политического веса Facebook пришло с «арабской весной», и он очень значителен.

Facebook дает пользователю возможность передать политическую власть населению в обход государства и предприятий. Это ведет к изменению равновесия сил с пока еще труднопредсказуемыми последствиями. Модель на основе самоорганизации (или, по крайней мере, передачи значительной части организации на откуп широкой базе) может привести к возникновению разрушительных социальных явлений. «Подемос» является хорошим тому примером, хотя организация партии выходит за рамки предлагаемой Facebook модели.

Google предлагает всем прямую связь со знанием, что в некотором роде сравнимо с появлением протестантизма, то есть прямой связи человека с Богом там, где старая модель (католицизм) насаждала посредника (священника) и контроль над этой связью. Тогда возникший разрыв спровоцировал долгую гражданскую войну. Сейчас же действия Facebook и Google могут привести к слому схожих масштабов, хотя он и примет совершенно иную форму.

В конечном итоге, Facebook и Google преследуют одну цель, но идут к ней разными путями.

Facebook делает вас частью своей нематериальной вселенной: на facebook.com есть все.

Google формирует материальную вселенную, где ваше присутствие становится одним из параметров: Интернет вещей, автомобиль без водителя, робототехника, ИИ, здравоохранение, Google Glass и т. д.

– Чем может грозить нам то, что мы отдаем мир на откуп технологическим гигантам?

– Речь идет примерно о том, что грозило предыдущим поколениям, которые отдали мир на откуп промышленным гигантам XX в. Если подвести итог, положительным его никак не назвать. Так, несмотря на колоссальный рост в некоторых областях в США, им не удалось избежать катастрофы: за прошлый год на американском континенте погибла половина пчел. Без пчел не будет опыления, а без него расти смогут только бобовые, травы и зерновые. Деревья же и кустарники обречены на смерть…

Если мы отдаем на откуп технологическим гигантам то, что позволяет обществу двигаться вперед, мы зайдем в точно такой же тупик. Хотя все, конечно, будет складываться иначе по сравнению с тем, что творят компании вроде Monsanto.

В повседневной жизни человек может столкнуться с синдромом изоляции: ваша вселенная сводится к тому, что вы видите, и вы попадаете в ситуацию полной зависимости, потому что система стремится доставить вам наибольшее удовольствие, чтобы не дать вам уйти. А развитие ИИ поднимает

вопрос, не случится ли однажды так, что созданное нами нас же и поработит. И разве процесс уже не начался? ***(Что будет, если Google и Facebook захватят мир // News UA (http://nua.in.ua/novosti/mir/chto-budet-esli-goog2015le-i-facebook-zaxvatyat-mir). – 2015. – 21.08).***

***

Несколько лет назад разработчики популярных социальных сетей решали, как этичнее всего поступить с аккаунтами умерших пользователей. В соцсети Eter9 поступили по-своему, гарантируя людям так называемое цифровое бессмертие: аккаунт будет имитировать действия пользователя даже после его смерти.

По словам португальских разработчиков, Eter9 тщательно анализирует интересы и поведение своих подписчиков. Со временем соцсеть сама размещает аналогичную информацию от имени пользователя, даже если он умрет. Например, если человека интересуют новости о Т. Свифт, соцсеть будет подбирать соответствующую информацию и публиковать ее в ленте новостей аккаунта. Утверждается, что боты могут общаться как между собой, так и с настоящими людьми ***(Открылась соцсеть, гарантирующая людям цифровое бессмертие // InternetUA (http://internetua.com/otkrilas-socset--garantiruuasxaya-luadyam-cifrovoe-bessmertie). – 2015. – 23.08).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Украинские министерства и ведомства часто спрашивают мнение пользователей соцсетей о тех или иных законопроектах. Чиновники считают это элементом демократии. Социологи – пиаром.

Украинские чиновники берут на вооружение популярный и бесплатный инструмент влияния на людей – социальные сети. В пятницу, 7 августа, правительство Украины обратилось к своим подписчикам в микроблоге Twitter с вопросом, не упростила бы им жизнь отмена трудовых книжек? «Хотим знать ваше мнение о новой инициативе @mineconomdev отказаться от бумажных монстров», – стояло в твите правительства.

На это сообщение отреагировали около 100 пользователей. Но уже через несколько часов правительственный аккаунт торжественно известил о народной поддержке: «Большинство комментариев – 94 % – за реформирование. Ваше мнение важно! Подробности позже». В тот же день Министерство экономического развития и торговли опубликовало в сети сообщение с призывом отменить трудовые книжки и аргументацией, почему это следует сделать. То есть меньше чем за сутки министерство поставило

вопрос на голосование, определило его результаты и представило свою позицию.

Лишь бы спросить

С таким подходом категорически не согласна социолог и директор Фонда «Демократические инициативы» И. Бекешкина. Такой «опрос» представляет мнение не всех слоев населения, а только активных пользователей социальных сетей, объясняет DW-эксперт. И добавляет, что данный метод никоим образом не может быть репрезентативным.

«Если Кабмин действительно написал, что 94 % поддерживают отмену трудовых книжек, то это просто ерунда. Точно так же мы могли бы выйти на улицу и опросить всех прохожих, которых мы бы встретили. Кого они представляют? Только тех, кого мы встретили. Количество здесь не имеет никакого значения!» – возмущается И. Бекешкина. Эксперт считает интернет-голосование скорее популизмом политиков.

Зато в Министерстве экономразвития опросы в социальных сетях называют хорошим каналом быстрой обратной связи. «Времени на проведение общественных обсуждений у меня нет, а людям неудобно ехать в общественную приемную, чтобы пожаловаться или высказать свое мнение», – объясняет заместитель министра М. Нефедов.

Спросить Facebook – как подбросить монету

Известный украинский блогер Р. Шрайк, у которого только в Facebook около 50 тыс. подписчиков, сам часто проводит опросы на разные темы. Начиная от того, за кого люди проголосуют на ближайших выборах, и заканчивая экономической тематикой. На проводимые им опросы пользователи соцсетей реагируют активно, даже активнее, чем на правительственные.

Однако сам Р. Шрайк, хоть и любит проводить такие голосования, принимать решение на основании их результатов не советует. «Провести опрос в Facebook – это как подбросить монету. Можешь получить любой результат. Для законодательной деятельности такой инструмент малополезен», – говорит блогер.

По его мнению, в социальных сетях политики часто добиваются народной поддержки своих инициатив. Например, грузинский реформатор и заместитель Генпрокурора Д. Сакварелидзе опросов в Интернете не проводит, но на своей странице в Facebook часто прямо призывает распространять его информацию и приобщаться к его инициативам.

М. Нефедов из Министерства экономического развития также не скрывает, что, подавая в парламент новый законопроект, для него важно чувствовать народную поддержку. «Тогда мы можем сказать и депутатам, и чиновникам, что мы получили положительные отзывы. Пусть они спросят людей на улицах и убедятся сами», – аргументирует М. Нефедов.

Манипуляция сознанием?

Если в Украине политики обычно сами пишут в социальных сетях, то, например, в США над общением с людьми работают целые команды. Никто из известных чиновников сам не ведет свой аккаунт. Докторант Университета

Мэриленд и редактор проекта Global Voices Т. Локоть отмечает: «Если политик решил выставлять в Интернете какие-то вопросы и мониторить время от времени ответы, то этого явно недостаточно. Нужно, чтобы была логика общения с народом, чтобы люди видели, что есть какая-то обратная связь. Это требует усилий и времени».

К сожалению, в украинском сегменте Facebook дискуссии часто происходят иначе, отмечает она. Например, министр внутренних дел и активный пользователь соцсетей А. Аваков тоже часто апеллирует к людям через Интернет. В частности, интересуется их мнением относительно дизайна новой патрульной машины полиции и положительно отзывается в случае поддержки. Однако, когда большое количество пользователей Facebook возмущено его инициативами, реакции на это от чиновника не следует.

Во время обсуждения отмены трудовой книжки Министерство экономического развития также отвечало в основном лишь тем пользователям, которые одобрительно отзывались об инициативе ведомства. По словам Т. Локоть, при обсуждении программы ObamaCare в США, пользователи социальных сетей часто делали критические замечания и ставили жесткие вопросы. Почти все эти комментарии были обработаны, а пользователи получили разъяснения. Это была довольно успешная и прозрачная кампания по изучению общественного мнения, считает эксперт.

По мнению Я. Юрчишина, эксперта инициативы «Реанимационный пакет реформ», украинские чиновники, напротив, часто манипулируют аудиторией и навязывают ей свое мнение, вместо того чтобы обсуждать с ней все аспекты вопроса. «Например, когда твит министра экономического развития и торговли А. Абромавичуса о трудовой книжке начинается со слов “хороним совковое наследство”», – отмечает Я. Юрчишин ***(Как украинские чиновники используют социальные сети // Deutsche Welle (http://www.dw.com/ru/как-украинские-чиновники-используют-социальные-сети/a-18641355?maca=rus-rss_rus_UkrNet_All-4190-xml). – 2015. – 13.08).***

***

Украинские женщины-политики в соцсетях: о чем пишут Е. Згуладзе, Н. Яресько и другие

Социальные сети – неотъемлемая часть современной жизни. Ними охвачено более половины интернет-пользователей, и с каждым годом их количество только увеличивается, пишет «Обозреватель» (http://obozrevatel.com/chronics/05274-ukrainskie-zhenschinyi-politiki-v-sotssetyah-o-chem-pishut-zguladze-yaresko-i-drugie.htm).

Поэтому для политиков социальная сеть – удачная платформа для пропаганды своих убеждений и агитации. Это и не удивительно. Ведь количество пользователей в социальной сети не сравнится ни с одной самой популярной газетой или ТВ-каналом.

Практически все политики – пользователи Twitter или Facebook. Издание АиФ.ua проанализировало, как же ведут себя украинские женщины-политики в социальных сетях.

О. Богомолец, народный депутат Украины, советник Президента Украины по гуманитарным вопросам

Социальная сеть: Facebook – 53,479 тыс. подписчиков

#всеофициально

Свою страницу в Facebook О. Богомолец ведет не сама, а ее помощники. Данный вывод был сделан из информации на странице, которая обновляется ежедневно и оперативно, подается четко, без орфографических ошибок. Стилистика постов исключительно официальна. Поэтому соцсеть для О. Богомолец – не платформа для общения, а «помощник» в профессиональной деятельности. Наверное, именно поэтому ее посты напоминают политические листовки.

Если подписчики хотят послушать эфир какой-либо передачи с ее участием – на странице можно найти всю информацию о том, где и как это можно сделать.

Под каждым постом О. Богомолец есть комментарии единомышленников или противников. Первые, кстати, показывают свою поддержку нардепу в основном при помощи лайков. Под постами среди подписчиков не ведутся ярые споры или восторженные возгласы. Возможно, это связано с тем, что сама О. Богомолец или ее помощник не общаются и не отвечают в комментариях.

Н. Королевская, украинский политик и общественный деятель, экс-депутат от «Партии регионов»

Социальная сеть: Twitter – 1369 тыс., Facebook – 20 тыс. подписчиков

#душевно

В обеих социальных сетях Н. Королевская ведет активную деятельность. Несмотря на небольшое количество подписчиков, она использует социальные платформы по назначению. Twitter и Facebook Н. Королевской взаимосвязаны: практически в каждом посте в Twitter она делает ссылку на Facebook. Ежедневно Н. Королевская делится с подписчиками своими мыслями или событиями. Судя по изложению информации, Н. Королевская лично ведет социальные странички. Там можно увидеть поздравления, призывы, отчеты о проделанной работе, соболезнования и даже смайлики в конце предложений.

Н. Королевская активно зазывает подписчиков к дискуссиям и рассуждениям в комментариях. Например, пост 17 августа 2015 г.: «Друзья, а сколько газа потребляет ваш котик или песик?» Но, несмотря на это, читатели не спешат лайкать или репостить Н. Королевскую, а в комментариях отписываются единицы.

И. Бережная, народный депутат Украины, «Партия регионов»

Социальная сеть: «ВКонтакте» – 14,2 тыс., Facebook – 17,543 тыс. подписчиков

#общительная

Свою страничку во «ВКонтакте» и Facebook И. Бережная ведет лично. В отличие от других женщин-политиков, И. Бережная активно общается со своими подписчиками. Ставит смайлики, хештеги, смело заявляет о своих позициях и мнении на счет настоящей власти. Например, пост 7 августа 2015 г.: «В Киеве в рамках декоммунизации планируют создать мост Рейгана и проспект Бандеры. Предлагаю не мелочиться и сразу переименовать Майдан в Нуланд-square, Банковую – в Обама street, Грушевского – в Керри avenue, Красноармейскую – в Байден prospect, Сырец (р-н Киева, где находится Бабий Яр) – в Шухевич garden; ну, а мордорский Московский мост переименовать в “демократический” – American bridge!».

Регулярно выкладывает видео программ, в которых она участвовала и личные фотографии.

Подписчики более активны в Facebook. Там они лайкают, делают репосты и с удовольствием вступают в дискуссии в комментариях. Можно сделать вывод, что И. Бережная – активный пользователь социальной сети и четко знает, для чего и в каких целях можно ее использовать.

А. Кужель, народный депутат Украины, партия «За єдину Україну»

Социальная сеть: Twitter – 24,3 тыс., Facebook – 43,179 тыс. подписчиков

#наэмоциях

А. Кужель – одна из самых читаемых и популярных украинских женщин-политиков в социальной сети. На нее подписываются, ее комментируют и активно делают репосты. И это не смотря на то, что Twitter она не обновляет уже практически год, а в Facebook пишет редко, но много.

Сложно сказать, лично ли она ведет свою страницу. Ведь неоднократно и Twitter, и Facebook взламывали. Но, по заявлениям самого нардепа, Facebook она обновляет сама. Ее посты в основном обращены к женской половине аудитории, они понятны и наполнены эмоциями. Личных фотографий практически нет, но зато полным-полно официальных документов и различных протоколов. Графы с личной информацией заполнены очень коротко и неинформативно. Но снова-таки, ее страница среди украинских женщин-политиков самая посещаемая, несмотря на то что сама А. Кужель – не активный пользователь соцсети.

И. Геращенко, народный депутат Украины, партия «УДАР»

Социальная сеть: Facebook – 43,828 тыс. подписчиков

#информативно

Читая ленту И. Геращенко, чувствуется образование журналиста. Она интересна, увлекательна и познавательна. Нардеп делится личными мыслями и наблюдениями, которые органично смотрятся наряду с ее политической деятельностью. Посты обновляются регулярно, при этом не теряют свою информативность. Многие записи подкреплены фотографиями (как личными, так и официальными), которых на странице И. Геращенко очень много.

Подписчики И. Геращенко не часто оставляют свои комментарии или делают репосты, но регулярно лайкают записи, показывая свою активность.

Е. Згуладзе, заместитель министра внутренних дел Украины
Социальная сеть: Facebook – 24 тыс. подписчиков
#любительрепостов

Судя по странице Е. Згуладзе, сложно сказать, что она активный пользователь социальной сети. Она не пишет личные посты, не общается с подписчиками и не высказывает своего мнения на странице в Facebook. Информация в основном состоит из ее репостов с сообществ, новостных сайтов и со страниц других политических деятелей. Скорее всего, это связано с тем, что вместо нее страницу в Facebook ведут помощники.

Страница напоминает политический блог, где собраны актуальные и обсуждаемые материалы. Личных фотографий Е. Згуладзе не выкладывает, а графа с информацией о себе и вовсе не заполнена.

Чаще всего Е. Згуладзе репостит записи М. Саакашвили, А. Авакова и И. Геращенко.

Н. Яресько, министр финансов Украины
Социальная сеть: Twitter – 13,1 тыс., Facebook – 19 тыс. подписчиков
#поделу

Н. Яресько точно знает, для чего нужен Twitter и Facebook. Она активный пользователь обеих соцсетей, где обновляет информацию несколько раз в день. Н. Яресько пишет на украинском языке и в основном о себе. Куда поедет, что получила, с кем увиделась – все это вы можете найти в ее постах. Стиль изложения информации официально-деловой. Ни тебе эмоций, ни смайликов, ни хештегов. Сухая констатация фактов и распространение новостей. Даже пожелания и поздравления в преддверии праздников выглядят так, как будто речь идет о сложных экономических процессах.

Подписчики ее записи лайкают, но практически не комментируют и не делают репосты ***(Украинские женщины-политики в соцсетях: о чем пишут Згуладзе, Яресько и другие // Обозреватель (http://obozrevatel.com/chronics/05274-ukrainskie-zhenschinyi-politiki-v-sotssetyah-o-chem-pishut-zguladze-yaresko-i-drugie.htm). – 2015. – 19.08).***

***

Кабинет Министров Украины решил осваивать YouTube. В микроблоге анонсирован не только запуск отдельного канала украинского правительства, но и проведение прямых трансляций с заседаний. Можно также ознакомиться с короткими видеовыпусками о планируемых действиях правительства, проведении реформ по децентрализации и другими подобными материалами.

Работа с пользователями соцсетей для чиновников правительства в Украине уже становится привычным делом. Ранее украинский МИД организовал встречу с подписчиками министра иностранных дел в Twitter ***(Украинское правительство запустило прямые трансляции и видеоблоги в YouTube // Блог Imena.UA (http://www.imena.ua/blog/youtube-government). – 2015. – 10.08).***

***

У рамках спільного проекту з Реанімаційним пакетом реформ Platfor.ma вирішила подивитися, як представники української влади спілкуються зі своїми читачами в соцмережах. …Перевірили Міноборони, Мінкульт, Укрзалізницю, Київпастранс і КМДА.

Міноборони: сталеві чоловіки й котики

Це міністерство чи не найбільш активно висвітлює свою діяльність у соцмережах – веде офіційні аккаунти у Facebook, Twitter, Instagram та YouTube-канал.

Аккаунти Міноборони в Facebook і Twitter існують уже давно, проте лише нещодавно перестали виконувати винятково формальну функцію. Тепер у Twitter з'являються записи на зразок: «У нас спекотно не тільки на навчаннях! Наші десантники також дають жару!» або «Ми не бачили, як гартується сталь. Але спостерігали за тим, як гартують сталевих чоловіків». На Facebook модератори розчулюють учасників дитячими листами на фронт, а на критику з боку читачів відповідають жартома, наприклад фотографією котиків.

Раніше разом з україномовною існувала й англомовна Facebook-сторінка Міноборони – до травня минулого року там публікували новини із зони АТО для іноземців. «Вибачте за те, що ми закрили цей проект. Ми не знаємо, чи відновимо його коли-небудь і коли це буде», – написали модератори свій прощальний пост аж у березні 2015 р. – через рік після початку мовчання.

Якою мовою ведуть нещодавно створену сторінку міністерства в Instagram незрозуміло. Варіантів тут три: підписи під фото з'являються або українською, або англійською, або взагалі відсутні. Деякі фоловери попросили модераторів робити двомовні, тобто українсько-англійські описи. Кілька разів таке зустрічалося, але у звичку, схоже, ще не увійшло.

На YouTube-каналі Міноборони, як і належить, можна знайти всі відео, що стосуються діяльності установи. Особливої уваги заслуговує головний ролик каналу. Це – коротенький мультфільм 11-річного Т. Ландрієва про Україну. «Дивитись усім, хто вірить у нашу перемогу», – написали адміністратори каналу.

Мінкульт: до і після

Місяць тому навколо Twitter Мінкульту розгорівся скандал. Тоді SMM-менеджер установи агресивно відреагувала на зауваження учасника, що переросло у 18-годинну перепалку з образами та докорами в обидва боки. Співробітниця міністерства почала банити всіх підряд, а розлючені користувачі роздули проблему до нечуваних масштабів.

Уже через кілька днів новим модератором стала 23-річна Ю. Решітько. «Доброго дня усім! І перепрошую. Мене звати Юлія, і тепер я наповнюватиму Mincult_ua. Готова до критики, але сподіваюсь на дружню пораду», – таким був її перший твіт з офіційного акаунту Мінкульту. За місяць її роботи скандал вщух, а твіти стали стриманими та доволі привітними. Тепер на сторінці з'являються посилання на чимало українських та закордонних медіа: BBC, телеканал «Дождь», «Левый берег», Hromadske.TV, Cultprostir і Platfor.ma.

І хоча Twitter Мінкульта виправився, сторінка міністерства в Facebook досі залишається формальністю. Повідомлення повністю дублюють новини на офіційному сайті та, у найкращому випадку, збирають з десяток лайків. На поодинокі запитання та коментарі читачів представники міністерства не реагують.

Київпастранс: романтика і почуття гумору

«Без трамваїв і Київ – не Київ. Трамвайні маршрути – це не лише відстань від початкової до кінцевої зупинки, нерідко це ще й захоплююча екскурсія мальовничими вуличками столиці та її околиць», – це частина одного з останніх повідомлень комунального підприємства «Київпастранс» у Facebook.

Так чутливо вони пишуть про трамвай № 12, який їде до Пущі-Водиці. Але і це ще не все, адже його маршрут «пролягає через ліс, який захоплює своєю красою і влітку, коли всюди зелено й сонячно, і взимку, коли величні дерева згинаються під вагою лапатого снігу, милує око восени, коли листя пофарбоване в жовто-червоні відтінки, і навесні – пори, коли бруньки от-от готові розпуститися, щоб знову вкрити дерева густою зеленою кроною».

Попри свою романтичну натуру, представники Київпастрансу дозволяють собі й пожартувати. Востаннє, наприклад, про ціну тролейбуса й автомобіля BMW. Цей запис побив усі рекорди й зібрав більше 200 уподобань.

До речі, ще у квітні 2014 р. цю сторінку вели російською мовою. Зараз на неї переходять тільки тоді, коли відповідають на коментарі російськомовних користувачів. Утім, перехід на українську мову не зміг гарантувати грамотності – час від часу читачі скаржаться на граматичні та лексичні помилки в постах підприємства.

Київпастранс також має аккаунти в Twitter та Instagram, проте вони, скоріше, мертві, аніж живі – перший не оновлювався більше місяця, а другий має лише одну публікацію.

КМДА: переадресація і Кличко

Офіційна сторінка Київської міської державної адміністрації у Facebook видається доволі активною – принаймні записи там з'являються по кілька разів на день. Більше того, представники КМДА хай і не завжди, але відповідають на запитання читачів. Зазвичай це виглядає приблизно так: скаргу зареєстрували, чекайте, зверніться за таким телефоном. Стримано і ввічливо – як і належить держустановам.

Найактивніші обговорення виникають на сторінці тоді, коли в Києві щось іде не так. Так сталося кілька днів тому, коли в деяких районах міста відключили воду. На шквал незадоволених коментарів представники КМДА відповіли, що «розуміють обурення і ще раз просять вибачення за завдані незручності». І порадили звертатися до Київводоканалу, а воду набирати в кранах для поливання. Далі кияни дискутували самі із собою.

Набагато більше бажання спілкуватися з власними підписниками мають адміністратори сторінки Kyiv Smart City – проекту з розвитку столиці, який реалізовують громадські активісти разом із КМДА. Крім новин, модератори публікують цікаві факти про «розумні міста» в інших країнах та охоче

відповідають на запитання читачів. Окремі Facebook-представництва мають і деякі підрозділи адміністрації, як, наприклад, департамент суспільних комунікацій. Проте його сторінка говорить скоріше про відсутність комунікації, аніж про її наявність.

На відміну від Facebook, з Twitter у КМДА не склалося взагалі. Читати там можна хіба акаунт В. Кличка з гучними заявами на кшталт «Київ буде містом парків і скверів, а не містом МАФів!» або «Я підпишу розпорядження перевірити усі нафтобази та автозаправки». Проте офіційність цієї сторінки не підтверджена. Ті ж, кому хочеться розважитися, можуть підписатися на жартівливу сторінку-пародію київського мера.

Укрзалізниця: лаконічність і селфі стажерів

«Ми прагнемо конструктивного діалогу з усіма нашими клієнтами, та всіма, хто відвідує нашу сторінку у Facebook, тому всі коментарі є дуже важливими для нас», – зазначено в описі офіційної сторінки Укрзалізниці. Насправді комунікація з читачами відбувається зовсім інакше – і про увагу до клієнтів тут не йдеться. За останні місяці адміністратори відповіли лише на три запитання, але й на ті – без особливого ентузіазму. Навіть один з найбільш обговорюваних дописів, який стосувався появи мережі Wi-Fi у потягах «Інтерсіті», не змусив представників Укрзалізниці долучитися до дискусії. На питання, хто ж буде провайдером, вони відповіли коротко і ясно: «ТОВ “Інтертелеком”». І самоусунулися з коментарів. Решту користувачі соцмережі намагалися з’ясувати самотужки.

Чи не єдині ознаки людяності цієї сторінки – два повідомлення із сумного та радісного приводів. Це прохання допомогти хворій співробітниці Укрзалізниці та фотографії дівчат-касирів у вишиванках. До останнього навіть підпис не такий офіційний: «Звична метушня на ескалаторі, сотні валіз і заклопотаність не завадили створенню особливої атмосфери – піднесеної, доброзичливої й теплої».

Схожим на Facebook-сторінку є і Twitter-акаунт організації. Проте, наскільки Укрзалізниця цікавиться справами своїх клієнтів, говорить кількість користувачів, на яких вона підписана, – один. І це – Міністерство інфраструктури, тобто орган, до якого входить установа. До речі, у міністерстві Facebook використовують за призначенням: там розміщують селфі стажерів і відгуки «чарівних розумниць» про нову роботу ***(Коваленко К. Засоби масової інтернетизації: як держава веде себе у соцмережах // Телекритика (http://www.telekritika.ua/daidzhest/2015-08-13/110074). – 2015. – 13.08).***

***

Недавно назначенный на должность начальника милиции Одесской области соратник М. Саакашвили Г. Лорткипанидзе применяет креативный подход к усовершенствованию системы борьбы с нарушителями. Он предлагает одесситам выкладывать на его «стене» в Facebook фото нарушений ПДД и неправильной парковки для последующего реагирования на эти материалы

правоохранителей, пишет NovostiUA.net (http://novostiua.net/main/70832-novyy-nachalnik-odesskoy-milicii-vzryvaet-socseti-stenoy-pozora.html).

«В связи с тем что на улицах Одессы очень часто можно наблюдать нарушения правил дорожного движения, а также беспорядочную парковку транспортных средств в не предназначенных для этого местах (на пешеходных переходах, перекрестках, трамвайных путях и в местах, где остановка и стоянка запрещена действующим законодательством), я призываю одесситов не быть равнодушными, фиксировать правонарушения и выкладывать фото на стену моей официальной странички Facebook. Мы, в свою очередь, будем реагировать и принимать соответствующие меры», – сообщил Г. Лорткипанидзе своим подписчикам на Facebook.

Одесситы уже отреагировали на обращение и начали публиковать фото дорожных хамов ***(Новый начальник Одесской милиции взрывает соцсети «стеной позора» // NovostiUA.net (http://novostiua.net/main/70832-novyy-nachalnik-odesskoy-milicii-vzryvaet-socseti-stenoy-pozora.html). – 2015. – 10.08).***

***

У час неоголошеної війни всі засоби придатні. Івано-франківських чоловіків запрошують до військомату через соцмережі.

Відповідний список днями з'явився в соціальних мережах та на сайті міста. На 117 сторінках прізвища понад 400 військовозобов'язаних. Усі вони перебувають на обліку у військовому комісаріаті ***(Франківських чоловіків запрошують до військомату через соціальні мережі // Galka.if.ua (http://www.galka.if.ua/frankivskih-cholovikiv-zaproshuyut-do-viyskomatu-cherez-sotsialni-merezhi-video). – 2015. – 12.08).***

***

Google, Facebook и Twitter присоединились к инициативе британской благотворительной организации Internet Watch Foundation (IWF), которая борется с распространением детской порнографии в Интернете. Об этом сообщил официальный сайт организации.

Компании-участницы IWF создадут базу данных «хешей» – уникальных цифровых отпечатков фото и видеоматериалов, эксплуатирующих образы детей. В результате это поможет социальным сетям, дата-центрам и интернет-провайдерам быстрее выявлять и удалять запрещенный взрослый контент из интернет-ресурсов по всему миру.

«Хеши» будут создаваться только из изображений, отобранных экспертами вручную, в трех основных форматах: MD5, SHA-1 и PhotoDNA. По прогнозам IWF, в ближайшем будущем их число превысит несколько миллионов.

Кроме Google, Facebook и Twitter участниками инициативы уже являются такие крупные интернет-компании, как Microsoft и Yahoo ***(Google, Twitter и Facebook объединили усилия для борьбы с распространением детской порнографии // IGate (http://igate.com.ua/lenta/9404-google-twitter-i-facebook-***

obedinili-usiliya-dlya-borby-s-rasprostraneniem-detskoj-pornografii?ref=ukrnet). – 2015. – 12.08).

***

Глобальный PR-сервис Cision недавно провел исследование: как журналисты по всему миру пользуются соцсетями в 2015 г.

В исследовании приняли участие 3 тыс. журналистов из 11 стран. Вот результаты этого исследования, чтобы быть готовыми к новым тенденциям и подумать о том, как можно их использовать.

Еще недавно журналисты скептически относились к социальным медиа. Однако сегодня очевидна обратная тенденция: все больше репортеров обращают внимание на соцсети. Почему же произошла такая перемена?

Проведя это исследование, в Cision сделали следующие выводы о возможных причинах.

1. Чем больше ты пользуешься социальными сетями, тем больше ты знаешь.

Согласно исследованию, количество журналистов, использующих социальные сети каждый день, в 2015 г. составило 67 %. Это на 29 % больше, чем в 2012 г. Количество же журналистов, которые совсем не пользуются социальными сетями, за это время сократилось вдвое – с 12 до 6 %.

Изменилось и отношение журналистов к использованию соцсетей в профессиональных интересах: почти 50 % опрошенных журналистов признались, что не смогли бы сегодня работать без использования социальных сетей. Самыми активными в этом смысле оказались австралийские журналисты, 60 % которых признались, что не представляют свою профессиональную жизнь без социальных сетей.

2. Вы можете делиться своими новостями в социальных сетях.

Согласно исследованию Pew Research Center, половина пользователей Facebook и Twitter признались, что постоянно читают новости в своих лентах. Несмотря на то что 78 % пользователей не ищет целенаправленно новости в Facebook, почти каждый рано или поздно поделится в своей ленте какой-нибудь статьей, новостью, фотографией или видео.

Журналисты сознают, что могут быть полезными для пользователей социальных сетей, размещая свой контент в ленте. Популярность использования соцсетей для расшаривания своих новостей отличается в разных странах, но 75 % журналистов в США и Великобритании постят свои материалы в социальных сетях (особенно в Twitter) практически каждый день. Для всех англоговорящих журналистов возможность продвигать свой контент в Facebook является одной из главных причин использования этой социальной сети ***(Как журналисты пользуются соцсетями в 2015 году // Sostav.ua (http://sostav.ua/publication/kak-zhurnalisty-polzuyutsya-sotssetyami-v-2015-godu-68034.html). – 2015. – 20.08).***

Пользователи сети обратили внимание на появление рекламных блоков в видеоплеере социальной сети «ВКонтакте». Представители компании подтвердили изданию «Цукерберг Позвонит» (ЦП) тестирование нового формата объявлений, пишет siliconrus.com.

Новый рекламный формат – объявления, которые демонстрируются «поверх» видеороликов и которые пользователь может скрыть кликом мыши. Пресс-секретарь «ВКонтакте» Г. Лобушкин в беседе с ЦП подтвердил, что социальная сеть уже некоторое время тестирует этот формат, но отказался от дальнейших комментариев.

Когда функциональность будет представлена публично, кому она доступна в ходе тестирования, смогут ли авторы видеороликов как-то влиять на содержание рекламных объявлений, как будет настраиваться аудитория подобных объявлений и как часто пользователь будет их видеть, неизвестно.

Ранее подобные объявления пользователи социальной сети могли увидеть при просмотре видеороликов во встраиваемом видеоплеере YouTube. Теперь компания внедряет этот формат в собственном видеоплеере сети.

В июле 2014 г. газета «Известия» сообщила, что руководство «ВКонтакте» планирует полностью переработать видеоплатформу сервиса и дать создателям контента возможность зарабатывать на его размещении. В октябре 2014 г. «ВКонтакте» объявила о сотрудничестве с сервисом Pladform, который помогает управлять дистрибуцией и монетизацией видео в Интернете.

В рамках этого сотрудничества крупнейшая российская социальная сеть и ее партнеры занялись разработкой единого стандарта рекламной нагрузки для видеоплатформы «ВКонтакте». Речь в этом стандарте идет о рекламных роликах, которые встраиваются в видео на протяжении его показа ***(«ВКонтакте» тестирует показ рекламных объявлений поверх видеороликов // МедиаБизнес (http://www.mediabusiness.com.ua/?option=com_content&task=view&id=44264&Itemid). – 2015. – 10.08).***

***

Facebook открыл доступ к своим наиболее эффективным форматам рекламы, включая объявления в формате карусели и автопроигрываемые видео, для издателей мобильной рекламной сети Audience Network.

Теперь в число доступных нативных форматов рекламы входят динамические товарные объявления; межстраничные видеообъявления, запускаемые по клику; а также автопроигрываемые видео и объявления в формате карусели, упомянутые выше.

По словам продакт-менеджера Б. Вогеля, в настоящее время 80 % показов в Audience Network приходится на нативные объявления – на 20 % больше, чем в марте этого года (60 %).

Нововведение поможет как Facebook, так и рекламодателям. По данным социальной сети, эффективность нативной рекламы в приложениях в Audience Network в семь раз превышает показатели традиционных баннеров. Поддержка видео призвана увеличить эти цифры.

Facebook запустил свою платформу по размещению рекламы в мобильных приложениях Audience Network, анонсированную на конференции разработчиков F8 в апреле 2014 г.

Новая платформа позволила клиентам размещать встроенную рекламу в играх и сторонних мобильных приложениях с учетом таргетинга на пользователей Facebook. Что касается Facebook, запуск дал возможность существенно расширить охват аудитории и повысить прибыль компании от продажи мобильной рекламы.

В мае этого года Facebook обновил инструментарий нативной рекламы в Audience Network, добавив новые шаблоны, менеджер объявлений и возможность горизонтальной прокрутки.

Теперь через мобильную сеть доступно больше эффективных форматов рекламы ***(Facebook дал издателям Audience Network доступ к новым форматам рекламы, включая видео // Sostav.ua (http://sostav.ua/publication/facebook-dal-izdatelyam-audience-network-dostup-k-novym-formatam-reklamy-vklyuchaya-video-67913.html). – 2015. – 12.08).***

***

Facebook является основным социальным источником конверсии продаж для 64 % интернет-магазинов США и Великобритании. Об этом свидетельствуют данные нового опроса 200 компаний электронной коммерции из Великобритании и США, проведенного поставщиком программного обеспечения для электронной коммерции ChannelAdvisor.

При этом только 5 % опрошенных назвали главным источником конверсии продаж Pinterest, 19 % – Twitter, 9 % – Instagram.

Исполнительный председатель ChannelAdvisor С. Винго считает, что низкий рейтинг Pinterest по сравнению с Facebook можно объяснить разницей в размере аудитории: «Мы считаем, что это в значительной степени из-за достигнутого Facebook масштаба. Трафик Facebook и Pinterest конвертируется примерно одинаково». Кроме того, из 200 опрошенных онлайн-продавцов 89 % используют Facebook и только 41 % – Pinterest. Twitter используют 70 % продавцов, Instagram – 45 %.

Исследование также показало, что повышение узнаваемости бренда является главной бизнес-целью использования социальных медиа для трети респондентов, тогда ка 24 % опрошенных считают основной целью налаживание связей с новым поколением клиентов, а почти 20 % используют социальные медиа, в основном, для рекламы и акций ***(Владельцы интернет-магазинов считают Facebook главным социальным каналом продаж // IGate (http://igate.com.ua/lenta/9325-vladeltsy-internet-magazinov-schitayut-facebook-glavnym-sotsialnym-kanalom-prodazh?ref=ukrnet). – 2015. – 10.08).***

***

Продвижение компании в соцсетях: 9 ошибок CEO

Чем бы вы не занимались, что бы не продавали – бетон или апельсиновый конфітюр, вам пора задуматься о создании своей страницы, страницы вашей компании в Facebook и о том, что на них происходит. Не стоит думать, что пути ваших потенциальных клиентов в соцсетях неисповедимы. И не заблуждайтесь, что SMM – это чистая технология. Поверьте, «человеческий фактор», то есть включение в процесс лидера компании, подчас более важен, чем владение технологиями, пишет «Капитал» (http://www.capital.ua/ru/publication/51548-prodvizhenie-kompanii-v-sotssetyakh-9-oshibok-seo).

Вот наиболее грубые ошибки CEO, которые наблюдаются в социальных сетях:

1. Возлагать работу в соцсетях на маркетинговый отдел.

Социальные сети – это не еще один канал маркетинга. Это новый способ общения с потребителями для всех членов вашей компании. Не задумывались, почему малые компании обходят крупных конкурентов в соцсетях? Это происходит именно благодаря открытости лидеров компании и «доверительности» коммуникации ее сотрудников.

Ваш технологический отдел может нуждаться в информации от социального общения с потребителями. Ваша команда продаж должна использовать соцсети для контакта с реальными клиентами. И создавать контент должны все отделы. Например, в нашей компании наиболее читаемый контент часто пишет бэк-офис, так как это интересно бэк-офисам всех клиентов, вне зависимости от индустрии.

2. Использовать соцсети, чтобы проталкивать свой продукт.

Социальные сети существуют в мире уже 10 лет. У нас немного меньше. Но по-прежнему маркетологи не могут посчитать окупаемость инвестиций – ROI – в социальные сети. В данном случае лучше инвестировать именно в то, для чего, собственно, и предназначены социальные сети, а именно в «промежуточные показатели». Имеется в виду, что именно соцсети демонстрируют, насколько больше люди говорят о бренде, что они говорят о бренде, следят ли за вашим контентом, вовлекаются ли в диалоги. Высокий уровень вовлеченности говорит о повышении вашей экспертности, ято ведет к увеличению продаж оффлайн.

3. Инвестировать в SMM потому, что так делают все.

На самом деле, у вас должна быть собственная стратегия, которую следует проверять практикой. Вначале такая стратегия является не более чем гипотезой «а что, если». Но в соцсетях, где интерактивные акции с потребителем характеризуются высокой частотой и быстрой отдачей, позволяющей проводить мгновенный анализ эффективности, гипотеза приобретет облик стратегии достаточно быстро.

4. Ожидать немедленного результата.

Социальные медиа – это способ собирать своих реальных фанов, беседуя с каждым лично онлайн. Именно поэтому, кстати, считаю попытки посчитать ROI в присутствие в сетях, бессмысленными. Соцсети – это эффективное современное средство коммуникации. Вам же не приходит в голову считать ROI на использование e-mail вместо обычных почтовых писем? Но, кстати, объективный анализ происходящего в соцсетях может здорово сэкономить на маркетинговых исследованиях.

5. CEO не служит идеальной ролевой моделью.

А должен! Лидер компании должен стать неким примером поведения для своих сотрудников в использовании соцсетей для развития бизнеса и коммуникации с потребителями. Как и в любом другом новом канале коммуникации, ваши сотрудники скорее будут поддерживать компанию, если CEO сам подает прогрессивный пример.

6. Ответственные за работу в соцсетях занимаются исключительно репостами чужого контента.

По такому пути наименьшего сопротивления часто идут сотрудники, лишенные прямого контроля CEO компании. Необходимо же генерировать собственный контент. Но и здесь есть камни преткновения. Создавая свой контент, многие зачастую скатываются на путь самовосхваления своего бренда. На самом же деле компания должна заработать, заслужить свое место на «стенах» своих потребителей. Если вы не вовлекаете своих потребителей в некой полезной для них, потребителей, манере, объем денег, потраченных на дизайн и копирайтинг, становится неважным. Вас просто не станут читать. Почему? Потому что просто не увидят ваши посты на своих стенах...

7. CEO воспринимают соцсети как еще одно место для размещения пресс-релизов компании.

Социальные медиа срабатывают лучше всего, вам удается у людей, к которым обращены ваши послания, пробудить чувства. Эти эмоции также являются способом «гуманизировать», сделать более очеловеченной, персонифицированной вашу компанию. Соцсети – это не место для монолога компании, подобно, например, публикации в газете. А площадка, где потребители хотят услышать ваше мнение, как первого лица компании. Но еще важнее то, что они хотят, чтобы слышали их и отвечали им напрямую.

8. Компания в лице ее сотрудников укрывается за своим названием в соцсетях.

То есть реальные, конкретные сотрудники компании не снисходят до прямого общения с фанами странички. Но чем более ваши сотрудники будут считаться людьми, к которыми следует обращаться по определенным вопросам, тем более вероятно, что в будущем клиенты придут в вашу организацию за решением своих проблем.

9. CEO отвечают на любую критику.

Иногда наблюдаю мультимиллионеров, которые ввязываются в Facebook-драки с малоизвестными им людьми. Рекомендую отвечать CEO только на ту критику, которая искажает факты. Реагировать, чтобы корректировать ошибки

и неточности в отношении вашей компании, а не атаковать оппонента. Также не следует отвечать на нападки, когда оппонент обладает более слабым брендом, чем вы. Вне зависимости от результата спора, он получает бесплатное внимание к своей персоне за счет вашего бренда.

Корпоративная культура сегодня простирается гораздо дальше, чем когда-либо. И по сути, именно от CEO зависит создание корпоративной культуры, которая позволит компании быть лидером не только в оффлайне, но и в социальных сетях. Такая культура подразумевает развитие открытости и желания сотрудничать с клиентами каждого сотрудника. Что подкрепляется стимулированием «расшериванием» идей и информации каждым членом коллектива. В результате формируется некая «экосистема социальных электронных связей», которая неизбежно вознаградит ваш бизнес: за хорошее качество бетона (или конфитюра), отзывчивость к клиентам, честность и искренность ***(Саусь А. Продвижение компании в соцсетях: 9 ошибок CEO // Капитал (http://www.capital.ua/ru/publication/51548-prodvizhenie-kompanii-v-sotssetyakh-9-oshibok-seo). – 2015. – 18.08).***

***

Facebook поддерживают MasterCard и Visa

Facebook выкатывает сервис платежей, работающий по схеме от «человека к человеку» (P2P) и функционирующий через мессенджер для всех пользователей в США.

После запуска Messenger любой пользователь может отправлять деньги друзьям и членам семьи прямо со своих банковских счетов, при этом у стороны, которая принимает платеж, даже могут быть неподвязаны банковские карты.

С помощью бывшего президента PayPal Д. Маркуса, Facebook первым делом выкатил свою платежную платформу уже в мае 2015 г. для пользователей в Нью-Йорке. Людям, которые хотят, воспользоваться услугой, будет предложено подвязать свою Visa или MasterCard дебетовую карту к аккаунту, прежде чем они смогут отправить деньги другому пользователю.

В Facebook отметили, что к приему будут допущены лишь карты дебетовые, кредитные карты, по мнению самой социальной сети, связаны с мошенничеством и высокими налогами, которые будут включены в стоимость услуги для пользователя.

Venmo, к примеру, сервис P2P платежей, подобный к сервису от социальной сети, позволяет принимать кредитные карточки, но взимает сбор в размере 3 % для каждой транзакции по кредитным картам.

Для отправки платежей, пользователю достаточно нажать на иконку доллара ниже беседы и ввести сумму, которую они хотели бы отправить. Они могут нажать на кнопку Pay на верхнем углу экрана, чтобы завершить сделку. Статусное сообщение будет отображаться ниже сделки, чтобы сообщить пользователю, если платеж был отправлен. Получатели должны принять оплату, когда они открывают мессенджер, и ждать, пока в течении трех дней

средства поступят на аккаунт ***(Facebook поддерживают MasterCard и Visa // Ультрамир.NET (http://ultramir.net/techno/21958-facebook-podderzhivayut-mastercard-i-visa.html). – 2015. – 18.08).***

***

Facebook дал администраторам публичных страниц новые инструменты, призванные улучшить клиентский сервис в рамках социальной сети.

Среди основных нововведений – возможность отвечать на жалобы и вопросы клиентов в приватном порядке. Эта опция будет запущена в ближайшие недели для всех публичных страниц.

Ранее администраторы могли ответить только тем же способом, которым было опубликовано сообщение клиента. Например, ответить на комментарий или публикацию на стене страницы. Такого рода взаимодействия были публичными, а возможность негласно перевести дискуссию в приватный режим отсутствовала.

Теперь у администраторов страниц будет в распоряжении новая опция, позволяющая ответить на обращения клиентов в приватном режиме, нажав на кнопку Message. Новая ветка обсуждения будет включать ссылку на оригинальный комментарий.

Кроме того, администраторы также получили возможность создать и сохранить шаблоны ответов на часто задаваемые вопросы. Эту опцию Facebook тестировал в течение последних нескольких месяцев.

Также был обновлен ящик для входящих сообщений у администраторов. Теперь он дает возможность пометить как прочитанные, непрочитанные или как спам, внести в архив или удалить несколько сообщений за раз.

В целом, эти нововведения со стороны Facebook – попытка расширить клиентский сервис за рамки традиционного телефонного общения и повысить эффективность новых каналов коммуникации компаний с клиентами. Эту же цель преследует и запуск нового сервиса Messenger for Businesses, анонсированного на конференции F8 весной.

Facebook также внедрил новый способ показать, что компания отзывчива к обращениям – бейдж на ее странице с текстом Very responsive to messages («Очень активно отвечает на сообщения»).

Компании получают этот бейдж в том случае, если они отвечают на 90 % сообщений и среднее время ответа составляет менее 5 мин. Статистика отзывчивости будет основана на данных за последнюю неделю. Администраторы смогут просматривать эту информацию в разделе «Статистика страницы».

Этот функционал тестировался на ограниченной группе страниц в июне.

Facebook также добавил новую CTA-кнопку «Отправить сообщение» в рекламный блок «Местные уведомляющие объявления». Кнопка дает возможность потенциальным клиентам отправить личное сообщение рекламодателю прямо из объявления.

Напомним, что, по данным Locowise, клиентский сервис компаний в Facebook – неудовлетворительный. Восемьдесят сем процентов обращений клиентов остаются вообще без ответа. При этом компании, отвечающие на вопросы клиентов на своей странице в социальной сети, делают это выборочно, откликаясь только на 37 % всех постов.

В то же время, согласно данным Northridge Group, компании не обеспечивают качественный сервис в социальных медиа в целом, а не только в Facebook. Потребители рассматривают этот канал в качестве последнего варианта для связи с компанией по поводу решения какой-либо проблемы ***(Facebook дал компаниям новые инструменты для общения с клиентами // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_dal_kompaniyam_novye_instrumenty_dlya_obscheniya_s_klientami). – 2015. – 14.08).***

***

Instagram объявил о внедрении рекламного API, который был анонсирован в июне этого года.

Партнерами по запуску выступили Ampush, Brand Networks, 4C, Kenshoo, Nanigans, Salesforce Marketing Cloud, SocialCode, Unified.

Новый API позволит брендам автоматизированным образом покупать рекламу в сервисе и управлять рекламными кампаниями, а также публиковать контент, отслеживать различные сегменты аудитории и делится доступом к аккаунтам с членами команды.

«Рекламный API поможет сделать рекламу более релевантной для пользователей, обслуживать различные бизнес-задачи и облегчить рекламодателям покупку рекламу в сервисе. Несколько недель назад мы начали сотрудничать с группой партнеров программы Marketing Partners Facebook, которые привнесли свой опыт и квалификацию в работу платформы. Мы продолжим расширять функционал рекламного API в ближайшие недели и месяцы», – прокомментировал запуск пресс-секретарь Instagram изданию VentureBeat.

В настоящее время новый функционал доступен лишь ограниченному числу компаний-партнеров. В ближайшие месяцы доступ к нему получат остальные бренды.

Напомним, что осенью этого года фотосервис откроет свою рекламную платформу для всех рекламодателей. Клиентам компании станут доступны все виды рекламы в сервисе, включая тестируемые новые форматы и опции таргетинга.

По прогнозам comScore, в 2017 г. Instagram обгонит Google и Twitter по доходу от мобильной рекламы в США ***(Instagram запустил рекламный API // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/instagram_zapustil_reklamnyy_api). – 2015. – 12.08).***

***

В Twitter появился редактор Ads Editor, задача которого помочь рекламодателям быстро вносить изменения в рекламные кампании. При этом можно создавать и редактировать несколько кампаний за один раз.

Ads Aditor позволяет выгружать данные кампаний в едином Excel-файле, вносить изменения и после экспортировать обновленный документ в редактор. Также в редакторе есть возможность корректировать суммы затрат на кампании и период их проведения.

Для создания кампании необходимо ввести данные в Excel-таблицу и экспортировать ее в редактор.

В настоящее время Ads Editor доступен ограниченному числу рекламодателей. Но в ближайшие несколько недель редактор будет запущен для всех. После активации Ads Editor в отдельном аккаунте владельцу будет отправлено оповещение об этом ***(Twitter запустил новый редактор Ads Editor // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_zapustil_novyy_redaktor_ads_editor). – 2015. – 11.08).***

***

Администрация Facebook изменила правила публикации рекламных объявлений в соцсети и разрешила размещать баннеры с рекламой в формате GIF. Об этом 21 августа сообщает TechCrunch.

Компании могут использовать GIF-рекламу на страницах собственных брендов (Pages). Например, внутри отдельных объявлений или в качестве прикрепленного изображения в так называемых продвигаемых записях (Boosted posts).

В других рекламных форматах применять «гифки» пока нельзя. По словам представителей Facebook, соцсеть сначала хочет «протестировать» реакцию пользователей на подобные изменения.

Опубликовать GIF-рекламу в настоящее время могут не все. Первыми брендами, кому Facebook разрешила это сделать, стали американская сеть закусочных Wendy’s и бразильская сеть Kuat, принадлежащая Coca-Cola.

В мае Facebook официально объявила о поддержке использования формата GIF обычными пользователями. Ранее руководство социальной сети заявляло, что не хочет массового внедрения популярного формата из-за опасений, что это сделает новостную ленту сайта «слишком хаотичной» ***(Facebook впервые разрешила брендам размещать GIF-рекламу // Sostav.ua (http://sostav.ua/publication/facebook-vpervye-razreshila-brendam-razmeshchat-gif-reklamu-68043.html). – 2015. – 21.08).***

***

Як управляти брендом у соціальних мережах. Десять цінних порад CEO

З появою кіно театр не зник. Так само не варто відкидати традиційні медіа та їхній вплив через неактуальність. Але об'єктивність розростання павутини соціальних мереж невблаганна: за кожною угодою B2B завжди стоїть «С». Угоди корпоративного рівня укладають живі люди. Прихід соціальних медіа підтвердив, що бізнес робиться на рівні спілкування, через дрібну міжособистісну взаємодію, яка показує всім, хто ми є, чого варті й у що віримо, пише Forbes (http://forbes.net.ua/ua/opinions/1399072-yak-upravlyati-brendom-u-socialnih-merezhah).

Шляхи соцмереж не звідані: випадковий відвідувач вашої сторінки може стати клієнтом, а клієнтадвокатом, тобто гарячим прихильником і пропагандистом. Дедалі частіше знаходяться підтвердження тому, що CEO компанії й сама компанія – це, по суті, один бренд. І обидва акаунти− CEO і компанії − багато в чому тотожні й служать одним цілям. Тому я й називаю обидва акаунти − бренд. І розвивати їх потрібно за одним алгоритмом.

Пропоную деякі свої ефективні знахідки, що стосуються побудови бренду компанії та її керівника в соціальних медіа.

1. Будьте послідовними. Ви не зможете розвинути групу прихильників у Facebook, якщо люди не знають, коли випаде нагода прочитати ваш контент наступного разу. Газети виходять за чітко визначеним графіком. І ви не будуєте бізнес по натхненню. Тому намагайтеся зробити прогнозованим для читачів графік виходу свого контенту.

2. Коментарі онлайн. Необхідно відповіді на коментарі зробити такими ж регулярними й приділяти їм стільки ж часу, як і постам. Ефективні соціальні медіа − це не монолог, а діалог. Наприклад, при спілкуванні з клієнтами в режимі реального часу ви зможете тут же врегулювати будь-який огріх в обслуговуванні. Пам'ятайте, що незнайомці можуть стати вашими адвокатами в мережі. Поступово онлайн перетворюється на ефективний майданчик для нетворкінгу.

3. Забудьте про перфекціонізм − ви не зможете це собі дозволити. Навіть якщо ви не впевнені в пості на 100 % − все одно розмістіть його. Присутність у соцмережах − це рутина, як чищення зубів. І тут послідовність важливіша за ідеал. Якщо сумніваєтеся− натискайте на «відправити». Якщо пост не вдався, можна його видалити через добу.

4. Диктуйте тексти постів. На диктофон чи секретарю. Соціальні медіа − гра довгострокова. Часу ж ніколи не вистачає. Іноді тому ви й не починаєте свою подорож у соціальні медіа. Адже, почавши, доведеться продовжувати, або є загроза програшу.

5. Пишіть пости «авансом» на тиждень. Це істотно економить час. Крім того, що вам не потрібно буде змушувати себе «креативити» кожного дня, тексти «відлежаться». Можливо, через тиждень щось вам розподобається і ви не захочете цей пост публікувати. Щось же ж, навпаки, виявиться «в тему».

6. Усвідомте: створювати свіжий контент щодня – не реально. Використовуйте ваш контент з інших каналів. Наприклад, одна стаття може

стати 5−6 окремими постами. Залучайте контент своїх коллег, не забуваючи на них посилатися.

7. Не вторгатися на «чужу територію». Соціальні медіа– принципово інша платформа, тут просто так не зіштовхнеш того, хто почав раніше за вас. Перестаньте «ревнувати».

8. Єдиний спосіб боротися із сумнівною чи негативною інформацією про ваш бренд у соціальних медіа– це витісняти її масою позитивного контенту, регулярно розміщеного протягом тривалого проміжку часу. Перед тим як почати цю роботу, поставте собі питання «Завдяки чому я хочу бути відомим?»

9. Ви прийшли в соціальні медіа для того, щоб стати відомим тим, у чому сильні саме ви, а не в чому слабкий ваш конкурент. Чітко сформулюйте свою біографію та цілі в одній фразі. Після цього пропагуйте цей імідж роками.

10. Найкращий спосіб продавати ваш товар чи послугу через соціальні медіа це... не продавати їх зовсім. Принаймні досить тривалий час. Для створення товариства шанувальників вашої компанії щедро діліться своїми лідерськими напрацюваннями. Ваші співробітники-професіонали в свою чергу мають безкоштовно консультувати клієнтів для створення такої спільноти. Коли хтось із вдячності прямо запитує вас про ваш продукт чи сервіс – ось це і є реальний шанс продати.

Весь контент компанії і мій власний я і мої колеги генеруємо самостійно. Так, можна найняти райтерів, але надто заманливо мати можливість впливати на читачів самостійно. Усе вищеперелічене займе мінімум один рік копіткої та системної праці – поки ви прийдете до результату, описаного в п. 10.

Не вірте консультантам, які пропонують новітні трюки для розкрутки. У соціальних медіа, як у спорті: є кілька простих секретів і багато важкої щоденної роботи. Принципи роботи описані вище. Головний же секрет полягає ось у чому: потрібно бути висококваліфікованими професіоналами й одночасно хорошими людьми, яким не шкода праці та часу для розмови з клієнтом безпосередньо ***(Саусь О. Як управляти брендом у соціальних мережах // Forbes (http://forbes.net.ua/ua/opinions/1399072-yak-upravlyati-brendom-u-socialnih-merezhah). – 2015. – 24.08).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Соцсети заставляют молодых людей чувствовать себя неудачниками

Исследователи из компании Future Foundation опросили 5 тыс. британцев. Оказалось, более трети респондентов считали, что не полностью реализовывали

свой потенциал. Среди пользователей социальных сетей людей с таким мнением было еще больше (56 %).

Каждый третий мужчина в возрасте от 25 до 34 лет мечтал о том, чтобы стать похожим на того человека, за которого он себя выдавал в соцсетях. Многим не нравилась собственная внешность, а остальных беспокоила карьера и то, что они недостаточно счастливы или почти ничем не занимаются, информирует news.eizvestia.com.

По словам ученых, социальные сети заставляют людей сравнивать себя с другими. Вероятно, эта проблема в ближайшее время не исчезнет. Ведь те любители соцсетей, которые полагают, будто они чем-то хуже своих сверстников, начинают проводить много времени, хвастаясь своими достижениями и вводя в заблуждение других пользователей. В результате возникает порочный круг.

Молодые люди, выросшие с социальными сетями, страдают из-за данной проблемы сильнее тех пользователей, которые старше. Более зрелые пользователи обычно скептически относятся к соцсетям. Опрос показал, что почти 63 % участников в возрасте от 17 до 33 лет чувствовали себя неудачниками по сравнению с 37 % респондентов в возрасте от 55 до 70 лет ***(Соцсети заставляют молодых людей чувствовать себя неудачниками // Экономические известия (http://news.eizvestia.com/news_technology/full/221-socseti-zastavlyayut-molodyh-lyudej-chuvstvovat-sebya-neudachnikami). – 2015. – 12.08).***

***

Дослідження бізнес-школи Технологічного університету Сіднея показало, що жінки менш чесні, ніж чоловіки, коли справа стосується соціальних мереж. Щоб з’ясувати це, дослідники навчилися розпізнавати брехню в соцмережах і розповіли, як вони це робили.

Учені використовували спеціально розроблений алгоритм для виявлення брехні в постах соціальних мереж. Аналізу піддалися тисячі загальнодоступних постів у Facebook, Twitter, TripAdvisor та Instagram. Виявилося, що майже вдвічі більше жінок, порівняно із чоловіками, публікували поліпшену інформацію у Twitter та Instagram. Жінки брехали більше в цілому, але чоловіки з Аделаїди та Сіднея зайняли перше й друге місця серед брехунів в Instagram.

За даними вчених, слова, використовувані в повідомленнях у соцмережах, видають брехню. Наприклад, якщо в записі використовуються займенники «я» або «мені», то, швидше за все, людина говорить правду. Справа в тому, що ми, не усвідомлюючи цього, намагаємося дистанціюватися від брехні, що виливається в певний лексичний вибір. Люди спотворюють реальність у соцмережах, намагаючись створити привабливий образ або потішити своє самолюбство. Брехня допомагає людям відчути свою значущість або навіть отримати щось від компаній, якщо йдеться про неправдивий відгук про товар або послугу ***(Як відрізнити в соцмережах правду від брехні // InternetUA***

(http://internetua.com/yak-v-dr-zniti-v-socmerejah-pravdu-v-d-brehn). – 2015. – 11.08).

***

Социальные сети вредны для детской психики

В ходе нового иследования ученые анализировали анкеты 750 студентов 7–12 классов, проживающих в Оттаве, Канаде. Чуть более четверти из них признались, что сидят в социальных сетях более двух часов в день, а пятая часть почти не делали этого. Пятьдесят четыре процента опрошенных ответили, что посещают социальные сети, но не более двух часов в день.

Две трети детей оценили свое психическое здоровье как «отличное» или «очень хорошее», пятая часть – как «хорошее», 17 % – как «плохое». Кроме того, четверть детей отметили, что им необходима психическая поддержка, в то время как остальным такая помощь оказывалась. Тринадцать процентов опрошенных задумывались о суициде.

Результаты анализа показали, что тинэйджеры, которые проводили много времени в социальных сетях, чаще других оказывались среди тех, чье психическое здоровье оставляло желать лучшего и кто нуждался в поддержке, но не получал ее. Также привязанность к социальным сетям была связана с повышенным риском психической нестабильности и склонностью к суициду.

Одной из причин, по которым социальные сети плохо воздействуют на психическое здоровье детей, может быть их анонимность, повышающая вероятность издевательств онлайн. Кроме того, подростки начинают сравнивать себя с другими участниками сетей, далеко не всегда с положительными выводами.

По мнению ученых, детям не стоит полностью перекрывать доступ к социальным сетям: все дело – в умеренности ***(Социальные сети вредны для детской психики // Николаевская областная интернет-газета «Новости N» (http://novosti-n.org/ukraine/read/100192.html). – 2015. – 11.08).***

***

Украинские психологи бьют в набат. У все большего количества людей, по их словам, увлечение селфи перерастает в патологическую зависимость, пишут «Вести» (http://vesti-ukr.com/strana/110940-selfi-v-ukraine-pererastaet-v-v-patologicheskuju-zavisimost).

По словам психолога Е. Яковенко, теперь она постоянно сталкивается с клиентами, которые не могут прожить дня без того, чтобы не выложить четыре-шесть фотографий самого себя в социальные сети. «Когда я задаю вопрос: неужели ради кадра ты готов чуть не в пасть к тигру лезть, то многие отвечают утвердительно. У них возникает зависимость от лайков в Facebook, одобрения их снимков виртуальными друзьями, а потому для поддержания славы готовы на все. В основном этим грешат женщины. Я бы сказала, что это даже угроза национальной безопасности», – говорит Е. Яковенко.

Американские ученые официально признали зависимость от селфи психическим заболеванием, которое, кстати говоря, пока не совсем понятно как лечить. В Украине только в этом году уже зафиксировано два несчастных случая от селфи. В мае в с. Смильно Львовской области 13-летняя школьница залезла на крышу поезда и попросила подружек сфотографировать ее на камеру. Вместо красивых снимков, девочка получила мощнейший удар током. У ребенка ожоги I–II степени 70 % тела.

Примерно тогда же пострадал еще один подросток в Киевской области. Двенадцатилетний мальчик залез на крышу вагона ради кадров. Получив разряд током в 27 тыс. вольт, ребенок умер в больнице.

Что модно

После подобных случаев в России правоохранители даже составили памятку, где нельзя делать селфи. Например, за рулем, на железнодорожных путях, на крыше... В Украине же о памятке пока не задумывались, зато движение любителей селфи набирает обороты.

По словам координатора группы любителей селфи «ВКонтакте» М. Зиньковской, селфи разнятся по социальным сетям. «ВКонтакте» до сих пор преобладают лифтолук и селфи в зеркале, причем очень часто из туалетных комнат, а вот в Facebook и Instagram популярны тренды здорового образа жизни: селфи с пробежек, из тренажерного зала, со штангой, во время групповых занятий аэробикой или йогой. Люди любят демонстрировать свои спортивные достижения, им хочется показывать накачанное тело, над которым они много работали», – говорит администратор группы.

Также популярность набирает и селфи с активного отдыха – с велопрогулок, вейкборда, катания на лодке, походов в горах, также некоторые «умельцы» фотографируют себя во время прыжка с парашютом, специальными камерами делают и подводное селфи.

Для ценителей селфи даже проходят специальные фестивали. Там обустраивают концептуальные площадки с разнообразными фонами, декорациями, стелят «селфи-ковры», «сновалы», «лошадь для селфи».

«Анализ лент соцсетей показал, что украинцы любят селфи со знаменитостями, а также в нелепых ситуациях (из разряда “спящий бомж и я”), а также в путешествиях. Но это все лента Facebook и Instagram, лента “ВКонтакте” продолжает кишеть надутыми губами, селфи в туалете клубов и с маленькими собачками», – говорит «Вестям» организатор I Киевского фестиваля селфи М. Куликова ***(Литвинова Н. Селфи в Украине перерастает в патологическую зависимость // Вести (http://vesti-ukr.com/strana/110940-selfi-v-ukraine-pererastaet-v-v-patologicheskuju-zavisimost). – 2015. – 14.08).***

***

Ведущие эксперты из университета Суррея совместно с коллегами из Лундского университета реализовали интересный комплекс наблюдений, сообщает «Сегодня.ua» со ссылкой на «Ортодокс»

(http://www.segodnya.ua/science/polzovateli-instagram-riskuyut-sobstvennym-zdorovem-i-semeynym-blagopoluchiem-639172.html).

По словам исследователей, им удалось обнаружить уникальную закономерность. Оказалось, что люди, которые часто путешествуют на длительные расстояния, имеют повышенную вероятность развития летального исхода. Кроме того, любители Instagram чаще остальных мужчин и женщин болеют десинхронозом. Как сообщили инициаторы испытаний, этот вид недуга является признаком нестабильности биологических ритмов.

Также, представители слабого и сильного пола, выкладывающие в подобную социальную сеть множество новых снимков, жалуются на повышенную усталость, одиночество, тромбоз вен и полную изоляцию от любимых и друзей ***(Пользователи Instagram рискуют собственным здоровьем и семейным благополучием // Сегодня.ua (http://www.segodnya.ua/science/polzovateli-instagram-riskuyut-sobstvennym-zdorovem-i-semeynym-blagopoluchiem-639172.html). – 2015. – 10.08).***

***

Ученые обнаружили, что положительные и отрицательные комментарии к новостям в социальных сетях оказывают на пользователей разное по силе влияние: негативные высказывания снижают доверие к статье, в то же время положительные комментарии и большое число «лайков» существенного эффекта тоже не оказывают, передает «Корреспондент».

Во время работы исследователи показывали испытуемым новостные посты в социальной сети Facebook и просили людей оценить их убедительность. Показывая одни и те же новости, публикуемые авторитетными СМИ, исследователи изменяли число «лайков», а также положительные и отрицательные комментарии к посту.

Оказалось, что негативные комментарии снижали уровень доверия к новостной заметке и заставляли быстрее ее забывать.

Что касается большого количества «лайков» и позитивных комментариев, то они, к удивлению исследователей, не повышали, но и не снижали убедительность статей ***(Ученые выяснили, как комментарии в соцсетях влияют на мнение пользователей // МОСТ ДНЕПР – новости Днепропетровска и Украины (http://most-dnepr.info/news/society/uchenye_vyjasnili_kak_kommentarii_v_socsetjah_vlijajut_na_mnenie_polzovatelej.htm). – 2015. – 19.08).***

***

Исследователи из Великобритании обнаружили, что экстраверты и невротики склонны загружать значительное число фотографий на свои страницы Facebook. Однако, экстраверты, как правило, размещают фото в свой профайл сверху, в то время как невротики загружают несколько фотографий в одном альбоме.

Исследователи с кафедры психологии в Университете Вулверхэмптон наблюдали более 100 человек в возрасте от 17 до 55 лет. Более 70 % добровольцев были женщины. Все участники заполнили анкеты и ответили на вопросы об их личности и демографии. Затем исследователи изучили, как они размещали фотографии и взаимодействовали со своими друзьями на Facebook.

Связь между экстраверсией и склонностью размещать много фотографий не может показаться удивительной. Но вот как же эта тенденция объясняется у невротиков, которых исследователи описывают, как людей «склонных к стрессу и тревоге»? «Невротики сильно желают одобрения, но они не могут быть хорошими коммуникаторами и им не хватает социальных навыков, так что они видят в Facebook безопасное место для самовыражения и пытаются компенсировать свои недостатки оффлайн», – отвечают авторы работы.

Исследователи также обнаружили, что добросовестные люди загружают больше видео и создают больше фотоальбомов, чем люди, которые безалаберны в реальной жизни. «Дело в том, что добросовестные индивиды склонны к самодисциплине и ориентированы на цель и, таким образом, они проявляют тенденцию к документации», – объясняют исследователи.

Исследователи отмечают, что результаты исследования указывают на сходство между тем, как человек взаимодействует на Facebook и в реальной жизни. Например, люди в исследовании, которые были более «приятны» в реальной жизни, как правило, дружелюбны к другим в социальной сети. «Facebook-отношения, как правило, отражают реальную жизнь», – резюмировали авторы работы ***(Facebook выдаст все ваши слабости с головой // ZdravoE (http://zdravoe.com/101/p16615/index.html). – 2015. – 18.08).***

***

Психологи из Американского института поведенческих исследований и технологий (American Institute for Behavioral Research and Technology) обнаружили, что манипуляции с порядком выдачи сайтов о кандидатах на те или иные должности во время выборов способны склонить от 12 до 80 % неопределившихся избирателей на сторону какого-либо кандидата. При этом, даже если люди понимают, что их мнением манипулируют, они не только не меняют своего решения, но еще больше укрепляются в нем.

Работа опубликована в журнале Proceedings of the National Academy of Sciences.

Ученые провели три серии экспериментов – два лабораторных и один в условиях реальных выборов. Для этого они создали собственную поисковую систему Kadoodle и использовали настоящие предвыборные сайты и материалы о кандидатах.

В первой серии экспериментов психологи отобрали 102 имеющих право голоса испытуемых среди населения города Сан-Диего (Калифорния). Их разбили на две экспериментальных и одну контрольную группу и попросили представить, что им необходимо участвовать в выборах премьер-министра Австралии от 2010 г. (на самом деле премьер-министр является выдвиженцем

партии, имеющей большинство в Палате представителей Австралийского парламента). Подавляющее большинство испытуемых ничего не знало о главных кандидатах на эту должность – Т. Эбботе и Д. Гиллард. Свое мнение они должны были составить, основываясь на изучении сайтов и публикаций о кандидатах.

Контрольной группе предоставили выдачу из 30 сайтов об обоих кандидатах, сортированную в совершенно случайном порядке. В выдаче первой экспериментальной группы верхние пятнадцать позиций занимали сайты о Т. Эбботе, а во второй – Д. Гиллард. В подавляющем большинстве случаев испытуемые провели значительно больше времени за чтением сайтов из топа выдачи, чем из хвоста.

При опросе о предпочтительном кандидате члены контрольной группы не выразили значимых преференций тому или иному кандидату. В то же время в обеих экспериментальных группах сдвиг в пользу кандидата, чьи сайты были в топе выдачи, составил около 48 %. Но самым удивительным было то, что хотя некоторые испытуемые заметили искажение в выдаче и озвучили его, тем не менее, это еще более укрепило их в желании проголосовать за кандидата из топа выдачи. Они мотивировали это примерно так: «Да, я вижу искажение, но раз поисковик выдает сайты об этом кандидате на первой странице, значит это не просто так, это отражает его популярность».

При повторе этого же эксперимента на более крупной выборке из 2100 человек, сдвиг составил уже до 80 %. При этом было установлено, что наиболее подвержены влиянию при помощи манипуляций с поисковой выдачей избиратели, поддерживающие республиканскую партию, разведенные и совсем неосведомленные о кандидатах люди.

В третьей серии экспериментов во время реальных выборов в Индии в 2014 г. выборка составила 2150 неопределившихся в своих предпочтениях избирателей. Австралийские кандидаты были заменены на трех действующих индийских политиков, борющихся на выборах. В реальных условиях сдвиг предпочтений оказался слабее, чем при предыдущих экспериментах, но и здесь составил значительную долю – 12 %. Также подтвердился и эффект «осведомленности о манипуляции» – люди, которые понимали, что их пытаются склонить к выбору определенного кандидата, все равно поддерживали именно его.

Как объясняют авторы исследования, этот процент может показаться небольшим, но нередко реальные выборы выигрываются с преимуществом лишь в 1 % голосов. В современных демократических государствах процент пользователей Интернета среди населения, как правило, достаточно высок. Таким образом, манипуляция с результатами поисковой выдачи может дать решающий процент для победы одному из кандидатов ***(Поисковики могут оказать влияние на результаты выборов // InternetUA (http://internetua.com/poiskoviki-mogut-okazat-vliyanie-na-rezultati-viborov). – 2015. – 11.08).***

***

Британские психологи из Манчестерского университета пришли к выводу, что апатия и плохое настроение могут передаваться от одного человека к другому как при непосредственном контакте, так и через социальные сети.

Подтвердить этот факт смогли эксперименты с участием более чем 2000 добровольцев, информирует «Экономические известия» (http://news.eizvestia.com/zdorove/full/213-plohim-nastroenie-mozhno-zarazitsya-cherez-socseti-uchenye).

Оказалось, что плохое настроение даже быстрее передается не при личном общении, а через соцсети. Общение с депрессивно настроенными людьми практически наверняка приведет к схожему состоянию у тех, кто ведет с ними переписку ***(Плохим настроением можно заразиться через соцсети, – ученые // Экономические известия (http://news.eizvestia.com/zdorove/full/213-plohim-nastroenie-mozhno-zarazitsya-cherez-socseti-uchenye). – 2015. – 20.08).***

***

Люди, які проводять час у соціальних мережах, почувають себе менш самотніми. Особливо добре цей ефект помітний на людях похилого віку, чиї діти живуть в іншому місті.

Дворічне дослідження, проведене в Університеті Ексетера, стосувалося 76-ти людей у віці 60–95 років. Частина з них навчилася користуватися соціальними мережами, частина – ні. Виявилося, що люди похилого віку, які стали користуватися електронною поштою, Skype і Facebook, відчули себе на зв’язку зі світом, а тому стали рідше страждати від депресій і відчуття, що «все скінчено».

Причин тут декілька. По-перше, причетність до нових технологій змушує людей похилого віку відчути почуття власної компетентності. По-друге, соцмережі дають змогу їм залишатися на зв’язку з близькими людьми молодшого покоління.

Експерти дійшли висновку, що результати цього дослідження допоможуть людям впоратися з маразмом. Для цього необхідно лише, щоб вони не лякалися Інтернету і активно ним користувалися. Доктор Т. Мортон з університету Ексетера говорить, що в цих відкриттях немає нічого дивного. Просто люди – це соціальні істоти, і вони відчувають себе краще, коли в них є можливість спілкуватися з іншими людьми, причому бажано «не зі свого кола».

Є також докази того, що Facebook дає можливість літнім людям відстрочити настання маразму. Тобто якщо ваші батьки будуть сидіти в Інтернеті, то збережуть контакт з реальністю якомога довше. Тому, може досить лаяти М. Цукерберга за те, що нібито «заважає спілкуватися» вживу? Для вашої мами Facebook може бути єдиною можливістю відчути, що вона поруч з вами ***(Чим корисний Facebook для літніх людей? // Бізнес область (http://biznesoblast.com/society/49744/). – 2015. – 24.08).***

Маніпулятивні технології

Украинцев все чаще разводят в соцсетях. Многие попадаются на удочку о легком заработке: мол, кликните и выиграете приз. Таким образом мошенники выманивают небольшие суммы денег или подсаживают ваш компьютер на вирус.

«Самсунг» из-за океана

В социальной сети «ВКонтакте» все чаще стали появляться группы, в которых за лайк или перепост можно выиграть подарок – смартфон, дорогие брендовые духи, путевки на море или модную вещь. Пользователи соцсети активно ставят лайки. «Вести» также провели эксперимент и стали участниками конкурса. Прошло всего несколько дней, как нам сообщили, что мы стали счастливыми обладателями смартфона «Самсунг». Правда, потом предупредили, что за подарок нужно перечислить деньги. Мол, это за доставку, почему-то корейский телефон прилетит из США. «Всего 550 рублей на qiwi-кошелек», – написали организаторы. Это примерно 8,5 дол. или 180 грн. Хотя некоторые пользователи уверяют, что в таких группах им удавалось выигрывать набор сыра и даже билет в аквапарк.

В сети также можно попасться на малоизвестные интернет-магазины техники, где вам будут предлагать покупку товара на очень выгодных условиях, но с полной предоплатой. Часто люди ведутся на это, в результате – ни денег, ни товара не получают.

Встреча старых друзей

Это не единственный способ развода в сети. Также в Интернете на малоизвестных сайтах вам могут предложить «кликнуть и заработать». Кликать нужно на фото с животными или на ценник, где написано «Заработай 10 тыс.», либо на надпись «Заработать легко». Попавшись на удочку, человек кликает, и его компьютер получает вирус. Далее ваш ПК могут использовать в DOS-атаках или же вам будет приходить вал рекламы.

SMS или сообщение на электронную почту с текстом, что ваш номер выиграл приз от национального оператора, также должно заставить вас насторожиться. Вам предложат позвонить на номера, начинающиеся на «070» или «090», в итоге такой звонок может снять с вашего телефонного счета все деньги. Случается, что мошенники регистрируются в сетях под видом бывших одноклассников или сотрудников других пользователей, предлагают организовать встречу «старых друзей», собирают деньги на ресторан, на тот же qiwi-кошелек, после чего пропадают. «У меня такое случилось в июне. Вдруг в соцсети появился старинный одноклассник, которого тут давно не было. Он начал со всеми общаться и предложил встретиться. Мол, организовывает встречу в заведении друга, все будет дешевле, выпивка за ним, а вот на еду по 150 грн киньте на этот счет. Человек десять согласились, после этого он как в воду канул, и страничка пропала», – рассказала жительница Одессы О. Крамаренко. Женщина говорит, что в милицию обращаться не стали, но осадок остался.

Обращайтесь в милицию

В милиции говорят, что к ним очень редко обращаются с подобными жалобами на разводы в сетях. По словам адвоката «Кравец и партнеры» Р. Кравца, все, что предлагается бесплатно, должно сразу насторожить. И советует пострадавшим обращаться в правоохранительные органы. «Правоохранители могут сделать запрос для блокировки qiwi-кошельков, на которые происходит перечисление средства», – говорит адвокат. Также можно в судебном порядке вернуть свои деньги. «Поскольку суммы небольшие, большинство людей этим не занимаются, на что мошенники и рассчитывают», – добавил Р. Кравец. Адвокат подчеркнул, что за интернет-мошенничество предусмотрена уголовная ответственность ***(Как мошенники разводят украинцев в соцсетях // Domik.ua (http://domik.ua/novosti/kak-moshenniki-razvodyat-ukraincev-v-socsetyax-n240654.html). – 2015. – 11.08).***

***

Google «спалив» російські ферми тролів

Сервіс Google Trends дає змогу дивитися статистику пошукових запитів. Важливо, що тут можна дивитись статистику по окремих населених пунктах, де конкретні слова гуглять найчастіше. При цьому до уваги береться не кількість пошукових запитів, а інтенсивність пошукових запитів у країні/регіоні/місті.

І от що цікавого відкопали блогери. Якщо подивитись такі пошукові запити, як «Майдан», «Боїнг», «Референдум», «Порошенко», «Правий сектор», «Донбас», то статистика виглядає дуже цікаво.

На перші місця в таких запитах виходять маленькі селища Ольгино, Яблоновский, Перекатний та Зелений Город.

Нагадаємо: у м. Ольгино розташовано ТОВ «Агентство інтернет-досліджень», яке займається інтернет-пропагандою. Сотні співробітників днями безперервно пишуть коментарі, розміщують картинки, обливають брудом Україну, Америку і Європу та гноблять незгодних росіян, створюючи таким чином видимість громадської думки.

Завдяки сервісу, вдалося встановити, що вищезгадані центри активно почали працювати ще в кінці 2013 р. Наприклад, подивившись статистику по слову «НАТО» легко помітити – до середини 2013 р. найбільше ця тема цікавила жителів Ульяновської області, що не дивно – в цей час по ЗМІ якраз прокотилася інформація про відкриття в Ульяновську перевалочної бази НАТО для літаків, що воювали в Афганістані. Уже через півроку ситуація кардинально змінилася і в топ вирвалася вже знайома трійка. Той же феномен спостерігається майже у всіх пошукових запитах. Так само вищевказані агентства, швидше за все, намагаються впливати на думку росіян щодо внутрішньополітичної ситуації. Про це говорить статистика за запитами «Гречка», «Санкції» тощо ***(Google спалив російські ферми тролів // Watcher (http://watcher.com.ua/2015/08/19/google-spalyv-rosiyski-fermy-troliv). – 2015. – 19.08).***

Зарубіжні спецслужби і технології «соціального контролю»

В первом полугодии Россия направила в сервис микроблогов Twitter 43 запроса о предоставлении персональной информации о пользователях. Ни один из них не был удовлетворен, сообщается в опубликованном компанией докладе Transparency Report за первую половину 2015 г.

Также не был удовлетворен ни один запрос Турции. Эта страна оказалась на третьем месте по количеству запросов – 412. Больше всего запросов поступило из США – 2436. Восемьдесят процентов информации по американским запросам частично раскрыто. Затем следует Япония – 425 запросов, 42 % удовлетворено. Россия в этой категории оказалась на 10 месте.

Зато Россия оказалась на втором месте по числу запросов на ограничение доступа к публикациям – 68. Удовлетворено было 63 % обращений. Россию значительно опередила Турция – 718 запросов, 34 % удовлетворено. При этом Twitter отклонил все запросы на ограничение доступа идущих на третьем и четвертом местах Южной Кореи (40) и Индии (33).

В компании отмечают рост с предыдущим периодом числа запросов на предоставление информации о пользователях на 52 %, а на ограничение доступа – на 26 %.

В отчете за вторую половину 2014 г. Россия также заняла второе место по запросам на блокировку. По запросам о пользовательских данных у страны было пятое место

В первом полугодии 2014 г. Россия стала третьей по числу запросов об удалении информации в Twitter. Роскомнадзор за этот период направил 32 запроса. В 59 % случаев Twitter их удовлетворил. Это была самая высокая доля «успешных» для страны обращений.

Претензии Роскомнадзора были связаны с нарушением федеральных законов «О защите детей от информации, причиняющей вред их здоровью и развитию» и «Об информации, информационных технологиях и о защите информации» ***(Twitter отклонил все запросы России о раскрытии персональной информации // Главное™ (http://glavnoe.ua/news/n237682). – 2015. – 13.08).***

***

Как обеспечить конфиденциальность переписки в Viber

Депутаты отказываются от мессенджера Viber из-за его небезопасности. Тенденцию озвучил М. Найем из БПП: «Сотрудники нескольких ведомств мне рассказали, что найден способ взламывать систему безопасности и извлекать данные. Получить содержание Viber-переписки с телефона непросто и требует времени. А в качестве превентивной меры посоветовали время от времени переустанавливать программу», – рассказал нардеп. Кстати, по его словам,

высокопоставленные чиновники уже жаловались, что видели распечатки собственных переписок.

«Взломать можно, что угодно»

Ввиду предстоящих выборов технология вбросов информации и дезинформации посредством взлома переписки будет набирать обороты. «Тем более, что гарантий безопасности не дает ни один из существующих коммуникаторов, мессенджеров, – утверждает экс-замглавы ГПУ Н. Голомша. – При желании и бюджете можно контролировать все, от смартфона до электроники – взломать почту вообще элементарно».

Специалисты из столичного детективного агентства «Кассандра» пояснили схему взлома: в Viber используется аутентификация посредством OTP-пароля (SMS с комбинацией из четырех цифр при привязке аккаунта к Sim-карте).

«С появлением версии для компьютеров возможно повторно запросить OTP-пароль, и SMS придет на телефон жертвы. Если есть физический доступ к аппарату, пароль можно ввести на ПК или планшет, а сообщение с телефона удалить. Доступ получен, – рассказали детективы. – Если доступа к телефону нет, нужно перехватить текст SMS, что является уже достаточно сложной процедурой».

Обезопасить себя можно, если следовать нескольким правилам: часто менять пароли, не привязывать номер телефона, связанный с Viber, к своим имени и фамилии (не заключать контракт). Плюс периодически чистить переписку – через какое-то время она удалится и на сервере приложения. По словам Н. Голомши, при разговоре по смартфону нужно отключать системы геолокации, блютус.

П. Порошенко «ходит» в «Телеграм»

Актуален вопрос безопасности партийных чатов. Дело в том, что большинство политсил пользуются в обсуждении идей и проблем Viber-конференциями. Чат Блока Порошенко именуется лаконично, БПП, а лидеры Оппозиционного блока пару месяцев назад прокололись, назвав чат «политсоветом» (над чем долго потешались парламентские фотографы).

«Фракции по старинке пользуются Viber, причем активно. То же – министры. Хоть можно перейти и на новые сервисы, – утверждает политолог А. Золотарев. – К Telegram есть вопросы (его создали на средства П. Дурова, разработчика “ВКонтакте”. – Прим. авт.), а вот европейцы пользуются WhatsApp».

В Блоке Порошенко дилемму решили переходом на Telegram: там обретается большая часть фракции. «У нас два чата – в Viber и Telegram, причем и там, и там неполным составом, – пояснил львовский мажоритарщик Т. Батенко. – Несколько месяцев назад к Telegram подключился П. Порошенко – там теперь происходит основное общение. Про Viber мы, конечно, слышали. Среди депутатов и в бизнес-группах ходят слухи, что он легко ломается, считывается разными спецслужбами, в т. ч. украинскими».

Во фракции «Самопомощи» From-UA также подтвердили использование Viber-чата. По данным «Вестей», им же пользуется и «Народный фронт».

«Меня в этот чат не приглашали, и я вообще не слышал о его существовании, – открестился нардеп-комбат Е. Дейдей. – Я звоню по Viber друзьям в Канаду и США – это бесплатно».

СБУ рекомендует криптошифр

Вопрос, существуют ли по-настоящему надежные программы для общения, открыт. Специалисты-детективы осторожно предполагают: еще на этапе создания мессенджеров их разработчики имеют договоренности со спецслужбами (либо спецслужбы есть среди самих авторов).

«И даже если взять проект с чисто бизнес-идеей продажи услуг, с ростом популярности и количества пользователей он неминуемо заинтересует специальные структуры. А те пользователи, которые ценят конфиденциальность переговоров, со временем будут искать новые способы общения», – отметили в «Кассандре».

Сами спецслужбы имеют несколько разработок для защищенного общения. Кроме всего прочего, это «шифрованные» каналы связи. «В бытность губернатором Черновицкой области мне выдали телефон с криптозащитой. Обычный с виду мобильный, но, если позвонить на некодированный телефон, будет слышно не голос, а бульканье, – рассказал «Вестям» экс-глава облгосадминистрации М. Папиев. – Принимать сигнал может только аппарат с дешифратором. Правда, я ни единого разу им не воспользовался, больше любил защищенные линии со спецкоммутатором».

Методы

Существует и чисто механический способ съема информации с телефона. Источники уверяют, что просьба при входе в госорганы сдавать мобильник «дабы не мешать беседе» неслучайна.

«Если человек важен, то когда он уходит в кабинет, капитан СБ передает аппарат техникам. Они снимают данные, а особо важным посетителям вшивают небольшую плату, которая позволяет контролировать телефон, считывать беседы по Skype, Viber, и обычные звонки, конечно». Впрочем, собеседники «Вестей» в спецслужбах не подтвердили такие методы ***(Как обеспечить конфиденциальность переписки в Viber // From-UA (http://www.from-ua.com/obzor-pressi/354834-kak-obespechit-konfidencialnost-perepiski-v-viber.html). – 2015. – 13.08).***

***

Все большая опасность для цивилизованного мира исход со стороны Исламского Государства. ФБР считает, что отличным источником информации на эту тему есть Twitter, поэтому фокусирует свои действия на этом популярном сайте социальной сети.

По словам директора агентства Д. Камея, Twitter доказал свою пригодность в обеспечении доказательств по отношению к людям, поддерживающим терроризм. Агенты отслеживают много аккаунтов, которые содержат записи, опубликованные ISIS или ISIL, так как такие действия могут быть сигналом, указывающим на преступную деятельность их владельцев.

Правда посты о Исламском Государстве еще не является поводом для ареста, по крайней мере, не в каждом случае, однако этого достаточно, чтобы ФБР заинтересовал такой человек и началась тщательная проверка личности, отвечающего за запись.

Посты в Twitter в нескольких случаях уже были основанием для предъявления обвинения, примером чего является, в частности, 17-летний А. Амин, который использовал Twitter, чтобы поощрять людей к финансовой поддержке ISIS или ISIL с помощью Биткойнов. Приговор также получил Б. Абуд, который публично заявлял свою преданность А. аль-Багдади, лидеру Исламского Государства Ирака и Леванта ***(Канопка И. ФБР ищет террористов в Twitter // IT Business.com.ua (http://itbusiness.com.ua/social-networks/2917-fbr-ishhet-terroristov-v-twitter.html). – 2015. – 10.08).***

***

Снимки из Flickr помогли предсказать будущее местоположение пользователя

Исследователи Университетского колледжа в Англии разработали алгоритм, предсказывающее, где будут находиться люди в тот или иной момент времени. Для этого использовалась информация со снимков, загруженных на фотохостинг Flickr. Исследование было опубликовано в журнале Royal Society Open Science, его результаты кратко приводит Phys.org.

Большинство современных камер автоматически привязывают к снимку статистику о кадре, например GPS-координаты, а также время и дату, когда сделана фотография. Существование таких информационных карточек можно заметить при загрузке фотографий на файлообменник. Но иногда пользователь может не подозревать о том, что данные сохранены.

В созданную базу были собраны данные с 8 млн снимков, сделанных 16 тыс. людей в Великобритании. Отмечается, что эти фотографии хранились в свободном доступе на Flickr. Затем созданный компьютерный алгоритм анализировал кадры, снятые одной и той же камерой, запоминая все места, где они были сделаны. Подобная операция проводилась со всеми снимками, запечатленными конкретным фотоаппаратом.

Основываясь на полученных данных, алгоритм научился определять, где окажутся целые группы людей в следующий раз: робот отталкивался от предыдущих передвижений, затегированных в фото. Чтобы проверить свои результаты, ученые обратились к исследованию британского правительства, которое касалось поведения путешествующих внутри страны, их маршрутов. Предположения компьютера оказались верными примерно в 92 % случаев.

Исследователи подчеркнули, что они также могут проанализировать данные камеры одного человека и предсказать, где тот будет в определенный момент.

Результаты исследования будут полезны государству: например, отслеживание передвижения граждан поможет в строительстве дорог или проектировании прочих транспортных проектов. В то же время выводы ученых

поднимают вопрос о конфиденциальности личных данных, которые можно получить с помощью выложенных в Интернет фотографий ***(Снимки из Flickr помогли предсказать будущее местоположение пользователя // InternetUA (http://internetua.com/snimki-iz-Flickr-pomogli-predskazat-budusxee-mestopolojenie-polzovatelya). – 2015. – 14.08).***

***

У Facebook появилось новое малоизвестное программное обеспечение, отслеживающее вашу переписку в чате в целях предотвращения преступной деятельности. Программа предупреждает работника компании, за которым остаётся принятие решения, стоит ли уведомлять правоохранительные органы или нет. Об этом сообщают theantimedia.org

Согласно заявлению заместителя генерального директора по безопасности Facebook Д. Салливана, программа будет наблюдать за отдельными людьми, имеющими «свободные» отношения в социальных сетях.

Новая программа Facebook фокусируется на переписке между участниками, которые имеют свободные отношения в социальной сети. Например, если два пользователя не являются друзьями, только недавно стали друзьями, не имеют общих друзей, очень мало общаются друг с другом, имеют большую разницу в возрасте и/или проживают далеко друг от друга, то им уделяется особое внимание.

Сканирующая программа ищет определенные фразы, ранее взятые из переписки преступников, в том числе сексуальных маньяков. Материалы и результаты анализа передаются сотруднику Facebook, который, изучив связи, принимает окончательное решение, следует ли сообщить властям.

«Мы никогда не хотели допустить такой ситуации, в которой нашим сотрудникам пришлось бы читать личные сообщения, поэтому очень важно, что мы используем технологию, имеющую очень низкий показатель ошибочных выявлений», – сказал Д. Салливан.

Программа помогает собирать информацию о возможных подозреваемых в убийстве. Только по последнему судебному запросу сотрудниками Facebook были собраны и переданы местным властям 62 страницы фотографий, переписки и сообщений.

Facebook, скорее всего, хочет сохранить в тайне применение этого программного обеспечения, пока большинство людей не задумываются, что кто-то просматривает их личные сообщения и фотографии в поисках признаков преступной деятельности. К тому же, как далеко готовы зайти разработчики этой системы, и будут ли они скоро преследовать мелкие преступления или даже всего лишь преступные мысли? ***(Facebook будет сообщать властям о преступных намерениях пользователей // Хвиля (http://hvylya.net/news/digest/facebook-budet-soobshhat-vlastyam-o-prestupnyih-namereniyah-polzovateley.html). – 2015. – 10.08).***

***

Блогер із Севастополя І. Горелікова змушена була з'явитися на допит у ФСБ після того, як на своїй сторінці в Facebook поділилася матеріалом з прес-конференції уповноваженого Президента України у справах кримськотатарського народу М. Джемілєва. Про це повідомляє Центр журналістських розслідувань.

«У Севастополі блогера І. Горелікову відвезли на допит у ФСБ після того, як на своїй сторінці в Facebook вона поділилася посиланням на новину з прес-конференції уповноваженого Президента України у справах кримськотатарського народу, народного депутата України М. Джемілєва», – ідеться в повідомленні. За її словами, співробітник ФСБ цікавився цілями її «активного протистояння в мережах» і питав, чи не закликає вона таким чином до бунту.

Крім того, у ФСБ були «стурбовані цілісністю такої держави, як Росія» і цікавилися навіщо блогер постила статтю про М. Джемілєва. «Відповіла, що це моя думка і дуже поважаю М. Джемілєва, довіряю йому», – написала І. Горелікова.

Вона також повідомила, що співробітники ФСБ запропонували їй переїхати із Севастополя на материкову частину України, на що блогер заявила, що їхати нікуди зі свого будинку не планує. «Я їм запропонувала фізичну ліквідацію, бо їхати навіть не думаю», – цитує І. Горелікову Центр журналістських розслідувань ***(ФСБ у Севастополі забрала блогера за новину про Мустафу Джемілєва // InternetUA (http://internetua.com/fsb-u-sevastopol--zabrala-blogera-za-novinu-pro-mustafu-djem-l-va). – 2015. – 16.08).***

***

Война России с социальными сетями – страх и немощь перед неизведанным

Намедни Роскомнадзор внес в реестр запрещенных сайтов одну из наиболее популярных в мире социальных сетей с ежемесячной аудиторией более 55 млн человек – Reddit. С 10 августа провайдеры РФ обязаны заблокировать доступ к Reddit на территории России. Причиной такого решения стала публикация в социальной сети статьи о выращивании марихуаны и прочей растительности, оказывающей галлюциногенный эффект.

Откровенно говоря, подавляющее большинство пользователей России даже не слышало о существовании этой социальной сети. И это верно, поскольку основная аудитория Reddit (68 % пользователей) это граждане США. Вот и, казалось бы, с какой такой стати эта социальная сеть стала столь неугодна для Роскомнадзора? Ведь тот же Facebook и Twitter содержат куда большую российскую аудиторию.

Дабы понять мотивацию российской госструктуры, следует иметь представление, что такое Reddit, и чем отличается от всех имеющихся ныне аналогов.

Эта социальная сеть представляет собой ссылочную ленту новостей, которые публикуют пользователи, и чья ссылка на новость окажется более популярной та и попадет в ТОП. Благодаря такой рейтинговой системе в тематический ТОП могут попадать темы, неудобные для российских контролирующих органов, не имеющих своей бот-армии в этой социальной сети, как в том же Twitter, «Одноклассники» или «ВКонтакте».

Reddit, по сути, это одна из тех темных лошадок для пропаганды Кремля, на мало-мальский контроль которой попросту не хватает ресурсов. Если в Facebook имеется влияние через акции и долю, благодаря чему на нем не концентрируются так называемые кремле-боты, а выполняется блокировка неугодных аккаунтов на уровне администрирования, а Twitter попросту наводнен ордой фейковых спам-ботов, которые разносят необходимую информацию и выводят в ТОП хэштэгов необходимые посылы численным вещанием, то с Reddit ни один из этих номеров не прошел.

Фактически, мы стали свидетелями того как Россия будет в дальнейшем бороться с социальными сетями, которые не способна контролировать, либо влиять в их среде. А потому, фанаты Facebook и Twitter, «ВКонтакте» и «Одноклассники» (тем более), LiveJournal и Google+, могут спать спокойно – ваши виртуальные обители останутся нетронутыми.

Дело в том, что когда Россия стала формировать свою Концепцию Информационной Безопасности, то она, в отличие от Украины, которая до последнего времени и не задумывалась даже о подобной стратегии, уделила достаточное внимание развитию российского сегмента в киберпространстве посредством создания и контроля социальных ресурсов. На сегодняшний день Россия не только имеет в распоряжении свои собственные ресурсы «ВКонтакте», «Одноклассники», Surfingbird и прочие, но и старается увеличить присутствие в иностранном социальном продукте.

Когда началась волна массовых блокировок украинских пользователей в Facebook, созрела необходимость наличия команды блогеров в сторонних социальных сетях, не столь популярных в Украине и России, но имеющих отличные рейтинги на Западе и являющимися конкурентами тому же Facebook. К примеру, LinkedIn, Pinterest, MySpace. Причем блогеры не нулевые, а с развитыми и популярными аккаунтами, обширной аудиторией и репутацией.

Да, это не одного дня работа, это год, а то и больше тематического постинга и создания сети влияния, но это принесло бы свои плоды в тот критический момент, когда критика М. Цукерберга в конкурирующих социальных сетях и черный пиар против него сыграли бы куда большую роль, чем обращения Президента Украины.

В Украине нет своей социальной сети и нет вышеупомянутой команды. А как мы видим, этого направления информационного противостояния в киберпространстве спецслужбы Кремля боятся в не меньшей мере, чем профессиональных контрпропагандистских групп в подконтрольных себе ресурсах ***(Война России с социальными сетями – страх и немощь перед неизведанным // «Информационное сопротивление – ЮГ»***

(http://sprotyv.info/ru/news/yug/voyna-rossii-s-socialnymi-setyami-strah-i-nemoshch-pered-neizvedannym). – 2015. – 14.08).

***

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) сможет проводить внезапные проверки интернет-компаний, зарегистрированных как организаторы распространения информации, сообщает газета «Известия».

Ведомство сможет проверять информацию в почтовых сервисах, социальных сетях, мессенджерах. О новых правах Роскомнадзора говорится в проекте административного регламента исполнения Роскомнадзором функции по контролю над деятельностью организаторов распространения информации в Интернете, пишет издание.

Роскомнадзор должен будет сообщить о готовящейся проверке за 24 часа, однако в некоторых случаях надзорный орган будет проводить ее без предупреждения. Оговоренный срок проверки – не более 30 дней, однако в случае необходимости она может быть продлена еще на 20 суток, говорится в статье.

В специальный реестр организаторов распространения информации, внесены такие компании, как «ВКонтакте», сервисы «Яндекса», Mail.Ru Group. Американским интернет-сервисам Facebook, Gmail и Twitter Роскомнадзор «направлял уведомления о необходимости зарегистрироваться в России в качестве организаторов распространения информации. Но эти компании так и не зарегистрировались», пишет издание со ссылкой на заместителя Роскомнадора М. Ксензова ***(В России разрешат внезапно проверять почту и соцсети // Главное™ (http://glavnoe.ua/news/n238151). – 2015. – 17.08).***

***

Китайские власти после взрыва в Тяньцзине заблокировали или приостановили работу более 360 аккаунтов в различных социальных сетях из-за слухов, публикуемых их владельцами. Об этом сообщают местные СМИ со ссылкой на администрацию киберпространства КНР, пишет Сегодня.ua (http://www.segodnya.ua/world/v-kitae-blokiruyut-socseti-iz-za-rasprostraneniya-paniki-posle-vzryva-640984.html).

Как отмечается, после катастрофы некоторые пользователи, в том числе популярные в стране блогеры, стали размещать ложные сообщения о разграбленных магазинах, а также о том, что никто в радиусе километра от взрыва не выжил и другую не соответствующую действительности информацию.

Кроме того, некоторые пользователи под видом родственников жертв трагедии пытались заработать за счет фиктивных благотворительных фондов.

Напомним, взрывы и последующий пожар произошли вечером 12 августа в портовом городе Тяньцзинь, расположенном в 120 км к юго-востоку от Пекина ***(В Китае блокируют соцсети из-за распространения паники после взрыва //***

Сегодня.ua (http://www.segodnya.ua/world/v-kitae-blokiruyut-socseti-iz-za-rasprostraneniya-paniki-posle-vzryva-640984.html). – 2015. – 15.08).

***

Служба безпеки України затримала мешканця Дніпропетровська, який вів активну антиукраїнську пропаганду в соціальних мережах за гроші кураторів з Російської Федерації. Про це повідомляє Еспресо.TV з посиланням на прес-центр СБУ.

«37-річний адміністратор декількох груп "ВКонтакте" поширював матеріали, спрямовані на зрив мобілізації, дискредитацію діючої влади, відкрито закликав до підтримки злочинних дій терористів так званих ДНР і ЛНР та створення подібних "республік" в інших областях України», – ідеться у повідомленні.

Під час обшуку співробітники управління СБ України в Дніпропетровській області вилучили у зловмисника комп'ютерну техніку з матеріалами, що підтверджують його протиправну діяльність.

У рамках кримінального провадження за ч. 2 ст. 110 (посягання на територіальну цілісність і недоторканість України) Кримінального кодексу України тривають слідчі дії ***(СБУ затримала адміністратора антиукраїнських груп у «ВКонтакте» // Еспресо.TV (http://espreso.tv/news/2015/08/18/sbu_zatrymala_administratora_antyukrayinskykh_grup_u_socmerezhakh). – 2015. – 18.08).***

***

Крымчанина подозревают в пропаганде нацизма, – сообщает российская прокуратура Крыма, которая совместно с органами внутренних дел провела проверку неких сообщений жителя Бахчисарайского района в социальной сети «ВКонтакте», пишут «Крым. Реалии» (http://ru.krymr.com/content/news/27196064.html).

Как сообщает пресс-служба ведомства, житель Бахчисарайского района «разместил на своей странице в социальной сети "ВКонтакте" текстовые, аудио- и видеозаписи, которые содержат признаки пропаганды и оправдания нацизма, одобрения преступлений нацистов и их русских пособников».

В этих действиях силовики усмотрели признаки преступления, предусмотренного ч. 2 ст. 354.1 УК России (отрицание фактов, установленных приговором Международного военного трибунала для суда и наказания главных военных преступников европейских стран оси, одобрение преступлений, установленных указанным приговором, совершенные с использованием средств массовой информации).

Как сообщается, материалы проверки направлены в следственный комитет для организации в отношении пользователя сети уголовного преследования.

Это не первый случай, когда силовики обвиняют крымчан в пропаганде нацизма на основании их записей в социальных сетях ***(Жителя Бахчисарайского района Крыма обвинили в пропаганде нацизма из-за записи***

в соцсети // Крым. Реалии (http://ru.krymr.com/content/news/27196064.html). – 2015. – 18.08).

***

Windows 10 продолжает шпионить за пользователем, даже если ей запретить

Новейшая ОС Windows 10 стала доступна для загрузки совсем недавно, а потому появляется все больше и больше информации о системе, причем как позитивной, так и негативной, а порой даже забавной. Одним из неприятных моментов стали настройки сбора данных о владельце компьютера по умолчанию. Теперь раскрыта еще одна тайна ОС – даже выключив все возможные варианты сбора данных, новейший продукт Microsoft продолжает собирать данные и отправляет их софтверному гиганту.

Как стало известно ArsTechnica во время эксперимента, даже в случае отключения всех параметров в настройках приватности Windows 10 продолжает заботливо собирать и отправлять наши данные на сервера Microsoft. Есть в передаваемой информации совсем безобидные материалы (например, при подключении к сети отправляет пакет для проверки доступа к Интернету). Тут, утверждают эксперты, не содержится никаких идентификаторов пользователя. Есть и менее приятные, но некритичные данные: MSN обновляет информацию для «живой» плитки, даже если соответствующее меню отсутствует в «Пуске».

А вот что вызывает больше вопросов, так это поведение Windows 10 с отключенными персонализированными сервисами – она периодически отправляет данные в Microsoft на сервер ssw.live.com. Специалисты считают, что он используется для работы OneDrive и других сервисов Microsoft. Windows 10 передает данные даже когда OneDrive отключен и входит на сервер под локальным аккаунтом, который подключен к учетной записи Microsoft. Точно вычислить, что именно передается таким образом из личных данных, не удалось, но сам факт передачи сведений выглядит странно – если служба отключена, зачем вообще что-либо отправлять на сервер?

Эксперты выяснили, что часть информаци передается по незашифрованному каналу, потенциально открывая пользовательский трафик для перехвата хакерами. Однако есть и отдельные зашифрованные данные (что и помешало отследить содержание пакетов, передаваемых на ssw.live.com). И хотя соглашение об использовании служб Microsoft предопределяет право компании проверять ПО на легальность и отключать «пиратский» софт, не совсем ясно, почему что-то вообще должно передаваться в неиспользуемых программах и сервисах.

Кроме того, на запрос в Microsoft ответили, что передаваемые данные не затрагивают личные сведения, а необходимы для поддержания всех предлагаемых функций в актуальном состоянии, апеллируя к новой концепции «Windows 10 как сервис». Впрочем, часть разобранных экспертами данных содержит в себе идентификатор компьютера (уникальный номер для каждого

устройства), который, если уж Microsoft до конца честна, для предоставления новых функций не нужен.

Возможно, Microsoft не обманывает и делает это исключительно из благих намерений. Но непонятно, почему даже если пользователь отключил ту или иную службу и запретил ей отсылать информацию, она все равно продолжает это делать, пусть и не в том объеме, как это было ранее.

Hi-Tech Mail.Ru получил официальный комментарий Microsoft, в котором компания опровергает обвинения экспертов:

«Windows не собирает личную информацию без Вашего согласия. Чтобы обеспечить эффективность работы Windows как сервиса, Microsoft собирает некоторые данные об использовании, диагностике и производительности Windows, которые помогают поддерживать бесперебойную и правильную работу ОС и приложений. Microsoft использует эту информацию, чтобы выявить проблемы и найти их решения» ***(Windows 10 продолжает шпионить за пользователем, даже если ей запретить // InternetUA (http://internetua.com/Windows-10-prodoljaet-shpionit-za-polzovatelem--daje-esli-ei-zapretit). – 2015. – 17.08).***

***

Через мариупольский сегмент соцсети «ВКонтакте» продолжают фиксироваться попытки сбора развединформации о дислокации и перемещении украинских войск, местах попадания артиллерии террористов и т. д., сбор которых входит в круг функциональных задач войсковой разведки военизированных формирований ДНР. В силовых структурах напоминают: криминальная ответственность за подобную деятельность – от 8 до 15 лет тюрьмы. Об этом сообщает сайт города Мариуполя.

Наиболее активные из указанной категории ресурсов – администраторы антиукраинских групп в соцсети «ВКонтакте»:

– група «Шторм Мариуполя», администратор и организатор сбора информации – аккаунт С. Абриковос, в периоды активизации военных действий сбор информации производится через «перекличку», которая выставляется на заглавной странице группы.

– група «МИД НОВОРОССИИ Мариуполь», администратор и организатор сбора информации – аккаунт М. Калашников.

Владельцы обоих аккаунтов работают с оккупированных территорий в интересах террористической организации ДНР.

Через открытые форумы выявляются люди, которые обладают и готовы предоставить информацию, после чего переписка с ними переносится в «личку».

Как прокомментировали в пресс-службе СБУ, предоставление такой информации представителям террористических организаций ЛНР/ДНР содержит признаки преступления, предусмотренного ст. 258-3 (организационное или иное содействие деятельности террористической организации) и наказывается лишением свободы на срок от 8 до 15 лет.

Кроме того, из неофициальных источников известно, что представители отдельных проукраинских патриотических организаций контролируют часть мариупольских антиукраинских групп Мариуполя (через права администрирования). Они выявляют лиц, содействующих террористическим организациям, а потом данные на них передают в правоохранительные органы для привлечения этих лиц к уголовной ответственности ***(В Мариуполе боевики собирают развединформацию о ВСУ через соцсети // «Информационное Сопротивление» (http://sprotyv.info/ru/news/kiev/v-mariupole-boeviki-sobirayut-razvedinformaciyu-o-vsu-cherez-socseti). – 2015. – 20.08).***

Проблема захисту даних. DDOS та вірусні атаки

Функцию Facebook можно использовать для получения доступа к данным

Используя настройку приватности, установленную в социальной сети Facebook по умолчанию, ИБ-исследователь Р. Моайандин смог привязать тысячи номеров телефонов к учетным записям в Facebook. Злоумышленники могут повторить эту схему и скомпрометировать данные еще большего количества людей для того, чтобы в дальнейшем продать их на нелегальном рынке. Об этом сообщило издание The Guardian.

По данным издания, речь идет о настройке «Кто может меня найти?», в которой по умолчанию выбрана опция «Все» во всех профилях Facebook. Это означает, что любой пользователь, вводящий номер телефона интересующего человека, может найти его, так как последний имеет учетную запись в Facebook, в которой указан его номер телефона.

Р. Моайандин использовал алгоритм для генерации тысяч номеров телефонов и затем с помощью интерфейса прикладного программирования Facebook получил доступ к данным учетных записей.

Пользователи могут сделать две вещи для того, чтобы избежать атаки. Прежде всего, следует выбрать опцию, не разрешающую привязывать телефонный номер к учетной записи Facebook. Второй вариант – изменить настройку указанной выше функции и выбрать опцию «только друзья».

По словам Р. Моайандина, он дважды связывался с представителями Facebook после обнаружения такой возможности. Тем не менее, исследователь получил ответ, что компания контролирует ситуацию ***(Функцию Facebook можно использовать для получения доступа к данным // InternetUA (http://internetua.com/funkciua-Facebook-mojno-ispolzovat-dlya-polucseniya-dostupa-k-dannim). – 2015. – 11.08).***

***

Как защитить свой аккаунт в Facebook от взлома

Социальная сеть Facebook, несмотря на огромную популярность, обладает на редкость трудной для освоения системой настроек. Разобраться во множестве опций формирования ленты, отображения личных данных и

безопасности сможет далеко не каждый пользователь. В компании, очевидно, тоже понимают эту проблему, и поэтому представили на днях новый инструмент, с помощью которого вы сможете наконец-то понять, как защитить свой аккаунт от взлома.

Новый инструмент под названием «Проверка безопасности» появился в Facebook 30 июля и проходит пока предварительное тестирование. Он предназначен для быстрой проверки текущих настроек безопасности и устранения проблем в случае их обнаружения. В течение нескольких следующих недель вы сможете увидеть на своей странице приглашение пройти проверку или, если хотите, можете запустить её самостоятельно.

«Проверка безопасности» оформлена в виде пошагового мастера, который за три простых шага поможет вам обезопасить свою учётную запись. Первым делом нам предлагается закрыть сессии из программ, которые мы давно не использовали.

Следующий шаг заключается в активации уведомлений о том, что кто-то пытается войти в ваш аккаунт с нового устройства или браузера. Можно получать оповещения непосредственно в Facebook или в виде писем на указанный адрес электронной почты. Таким образом, вы моментально узнаете о том, что злоумышленники хотят взломать вашу учётную запись.

И наконец, на третьем шаге можно сменить свой пароль на более надёжный. Здесь нас знакомят с рекомендациями по выбору надёжного пароля, после чего его прямо здесь же предлагается применить. Теперь вы точно будете уверены, что доступ к вашему Facebook-аккаунту находится в безопасности и под полным вашим контролем.

Разумеется, описанные выше функции не являются чем-то новым, но ранее они были погребены где-то в глубинах системы настроек и вряд ли попадались на глаза широкому кругу пользователей. Теперь же добраться до них стало гораздо легче, так что можно надеяться, что максимальное количество людей сможет обезопасить свой аккаунт в Facebook от взлома ***(Как защитить свой аккаунт в Facebook от взлома // InternetUA (http://internetua.com/kak-zasxitit-svoi-akkaunt-v-Facebook-ot-vzloma). – 2015. – 10.08).***

***

Хакерам удалось найти еще одну опаснейшую брешь в операционной системе от Google. Под угрозой взлома оказались миллионы смартфонов под управлением Android.

О новой уязвимости рассказали эксперты из компании Check Point. По их словам, Certify-gate (так программисты назвали угрозу) позволяет вирусам получить полный контроль над смартфоном: хакеры могут извлечь любую персональную информацию о владельце гаджета. Кроме того, у мошенников есть возможность даже записывать телефонные разговоры обладателя смартфона.

По информации программистов, с помощью Certify-gate хакер может представиться в системе зараженного устройства как официальный поставщик

услуги дистанционного обслуживания, а затем без проблем получить всю необходимую информацию о владельце ***(В миллионах смартфонов нашли «дыру» для записи разговоров // InternetUA (http://internetua.com/v-millionah-smartfonov-nashli--diru--dlya-zapisi-razgovorov). – 2015. – 11.08).***

***

Исследователи обнаружили в пиринговых протоколах уязвимость, позволяющую злоумышленникам проводить распределенные атаки типа «отказ в обслуживании» (Distributed Denial of Service – DDoS), используя компьютеры пользователей торрентов с запущенным торрент-клиентом. Аналогичная уязвимость также была обнаружена в клиенте BitTorrent Sync.

Речь, в частности, идет о протоколах Micro Transport Protocol (uTP), Distributed Hash Table (DHT) и Message Stream Encryption (MSE). Все они упомянуты в работе, опубликованной британскими и германскими исследователями на сайте организации USENIX.

Суть уязвимости заключается в том, что упомянутые пиринговые протоколы не содержат механизмов защиты от IP-спуфинга – вида хакерских атак, когда IP-адрес атакующего заменяется на IP-адрес жертвы. Это позволяет злоумышленникам использовать миллионы ПК пользователей популярных торрент-клиентов в качестве усилителей DDoS-атаки.

Используя уязвимость, злоумышленник отправляет в торрент-клиент на ПК пользователей запрос на инициализацию пирингового соединения. Однако в сообщении IP-адрес инициализатора заменен на IP-адрес компьютера, на который необходимо совершить атаку.

Торрент-клиенты, получая запрос, пытаются установить соединение, но уже с компьютером жертвы, так как именно его IP-адрес был указан в сообщении как источник. Клиенты устроены таким образом, что они отправляют большее количество данных в ответном сообщении.

Когда торрент-клиент не дожидается ответа с целевого IP-адреса, он еще несколько раз отправляет запрос перед тем, как полностью прекратить попытку соединения. Все это позволяет хакеру увеличить поступающий на атакуемый узел объем трафика, хотя сам он такой же объем трафика не отправляет, а отсылает лишь один начальный пакет для инициализации всего процесса. Более того, такая атака дает возможность злоумышленнику эффективно скрывать свое местоположение, так как DDoS-трафик исходит от усилителей или так называемых «отражателей».

Исследователи провели эксперимент с различными торрент-клиентами, чтобы увидеть их эффективность. В результате они показали разный Bandwidth Amplification Factor (BAF) – коэффициент увеличения трафика. Наибольший продемонстрировало приложение BitTorrent Sync – оно увеличило трафик в 129 раз.

На втором месте – торрент-клиент Vuze, продемонстрировавший BAF в размере 54,3. Далее следуют официальные клиенты BitTorrent и uTorrent – 39,6. Наименее эффективными для злоумышленников оказались программы

Transmission и LibTorrent (BAF равен 4 и 5,2 соответственно) ***(Миллионы компьютеров готовы стать «зомби» из-за торрентов // InternetUA (http://internetua.com/millioni-kompuaterov-gotovi-stat--zombi--iz-za-torrentov). – 2015. – 17.08).***

***

С 2010 г. китайские хакеры имели доступ к личной электронной почте высокопоставленных чиновников из администрации президента США Б. Обамы. Об этом сообщает NBC News со ссылкой на секретные документы.

Согласно отчету Агентства национальной безопасности 2014 г., который оказался в распоряжении телеканала, работа шпионской программы под кодовым названием Dancing Panda («Танцующая панда», позже – Legion Amethyst, «Легион Аметист») началась как минимум в апреле 2010 г. Отмечается, что слежка продолжается и по сей день.

Целью шпионов была переписка, которую вели с нерабочих электронных ящиков высокопоставленные чиновники из силовых и торговых ведомств США. Должности и имена пострадавших от действий взломщиков не называются. При этом хакеры не тронули рабочие почтовые аккаунты, так как они более защищены.

Отчет о Dancing Panda датируется 2014 г. Выяснилось, что этот проект являлся одной из 30 программ Китая по шпионажу за США, обнаруженных АНБ. Согласно документам, в рамках проекта китайские хакеры смогли провести 600 успешных кибератак.

Ранее в 2013 г. NBC News сообщил, что во время президентской гонки 2008 г. целью кибершпионов были переписки соперников Б. Обамы и Д. Маккейна. Как сообщалось, злоумышленникам удалось получить доступ к некоторым электронным письмам, в том числе они смогли прочитать корреспонденцию сенатора Д. Маккейна.

Ранее АНБ неоднократно было уличено в кибершпионаже. Госсекретарь США Д. Керри назвал всеобщей практикой слежку за другими странами, комментируя данные о шпионаже за представителями Германии, Китая, Ирака и стран Евросоюза ***(Китайские хакеры читали личную переписку американских чиновников с 2010 года // Центр Інформаційної Безпеки (http://www.bezpeka.com/ru/news/2015/08/11/chinaspies.html). – 2015. – 11.08).***

***

Ведущие мировые государства договорились использовать кибертехнологии только в мирных целях. Об этом сообщает газета «Коммерсант» со ссылкой на доклад группы правительственных экспертов ООН по международной информационной безопасности. Согласились на ограничение «гонки вооружений» в киберпространстве 20 стран: Россия, США, Китай, Великобритания, Франция, Бразилия, Япония, Южная Корея, Израиль и др.

Доклад был представлен генеральному секретарю ООН Пан Ги Муну. В нем представители государств договорились об отказе от использования хакерских атак на критически важную инфраструктуру: банки, атомные станции, транспортные системы и т. д. Принято решение не устанавливать в технологическое оборудование «закладок» для отслеживания и сбора данных. Договоренность носит добровольный характер и не предполагает наказания за нарушение.

Также подписавшимся под договоренностью странам рекомендовано не обвинять друг друга в кибератаках без основательных доказательств ***(Россия, США и Китай договорились не использовать хакеров против друг друга // InternetUA (http://internetua.com/rossiya--ssha-i-kitai-dogovorilis-ne-ispolzovat-hakerov-protiv-drug-druga). – 2015. – 18.08).***

***

Компания «Доктор Веб» предупреждает о том, что злоумышленники распространяют по электронной почте вредоносную программу W97M.DownLoader.507, замаскированную под документ в формате Word.

Зловред, представляющий собой трояна-загрузчика, рассылается в письмах с вложением. Так, в одном из случаев злоумышленники маскировали программу под факсимильное сообщение, однако в процессе формирования письма киберпреступники ошиблись с указанной в параметрах датой его создания.

Сам документ якобы зашифрован с использованием алгоритма RSA, и для ознакомления с его содержимым пользователям предлагается включить в редакторе Word использование макросов. Любопытно, что документ содержит якобы пустую страницу, на которой, тем не менее, находится полная версия письма, набранная шрифтом белого цвета.

После включения макросов жертве демонстрируется полный текст документа, а в это время троян загружает с удалённого сервера несколько фрагментов кода, формирует из них файлы сценариев в форматах .bat, .vbs или .ps1 в зависимости от установленной на компьютере версии Windows, сохраняет их на диск компьютера и запускает на исполнение.

Сценарии, в свою очередь, скачивают с принадлежащего злоумышленникам сервера и запускают исполняемый файл – в качестве такового с помощью зловреда на атакуемый компьютер проникает опасный банковский троян Trojan.Dyre.553. В результате пользователи рискуют потерять деньги со своих счетов ***(Банковский троян распространяется в документах Microsoft Word // InternetUA (http://internetua.com/bankovskii-troyan-rasprostranyaetsya-v-dokumentah-Microsoft-Word). – 2015. – 16.08).***

***

«Лаборатория Касперского» (ЛК) вводила в заблуждение антивирусные программы конкурентов, заставляя их считать вирусами безопасные файлы на компьютерах и тем самым нарушать их работу. Об этом агентству Reuters

рассказали на условиях анонимности два бывших сотрудника российской компании, находящихся в курсе этой практики.

По их словам, эта деятельность ЛК была нацелена на продукты Microsoft, AVG Technologies, Avast Software и других конкурентов, имела место более 10 лет назад и длилась неделями и месяцами.

Операция возмездия

Заказчиком некоторых из атак был лично один из основателей компании Е. Касперский, утверждают источники. По их словам, Е. Касперский был недоволен тем, что небольшие разработчики копируют технологии, применяемые ЛК в своих продуктах, вместо того чтобы создавать нечто собственное. Поэтому обман конкурирующих программ он называл возмездием.

Обратный инжиниринг

Перед проведением атаки на конкретное приложение, специалисты «Лаборатории Касперского» выясняли, как работает программа и как ее можно обмануть, с помощью обратного инжиниринга – процесса, за использование которого независимых экспертов недавно раскритиковала глава Oracle по безопасности М. Девидсон.

По словам одного из бывших сотрудников ЛК, которые приводит Reuters, аналитики компании внедряли в файлы операционной системы дополнительный код таким образом, чтобы антивирусы конкурентов считали, что этот файл заражен. Затем образцы анонимно отправлялисо в онлайн-агрегатор VirusTotal. Какие именно файлы подвергались внедрению дополнительного кода, источники Reuters не сообщают.

Широкие возможности

Сервис VirusTotal служит для обмена экземплярами вредоносных файлов между производителями антивирусов. В 2010 г. «Лаборатория Касперского» провела эксперимент, в рамках которого создала 10 файлов и отправила из в VirusTotal, сообщив, что считает их вредоносными. Примерно через полторы недели все 10 файлов расценивались вредоносными 14 независимыми антивирусными компаниями.

Комментарии игроков рынка

Представители Microsoft, AVG и Avast ранее сообщали Reuters, что в последние годы заметили попытки неизвестной стороны увеличить количество ложных срабатываний. Однако на просьбу прокомментировать новый материал, они ответили, что не имеют подозрений и претензий конкретно к «Лаборатории Касперского».

Один из примеров ложного срабатывания агентству Reuters привел вирусный аналитик Microsoft Д. Бачелдера. Он рассказал, что в марте 2013 г. к ним обратилась масса клиентов с жалобой на то, что антивирусы Microsoft посчитали вирусом и поместили в карантин драйвер принтера.

Комментарий ЛК

В ответ на просьбу Reuters прокомментировать информацию в «Лаборатории Касперского» опровергли обвинения. «Наша компания никогда

не проводила подобных секретных операций и не вводила в заблуждение продукты конкурентов с целью снижения их рыночной доли, – заявил Reuters Е. Касперский. – Я считаю подобные действия неэтичными, нечестными и вызывающими вопросы в своей законности».

Кроме того, в ноябре 2012 г. ЛК сама столкнулась с такой атакой на себя, добавил Е. Касперский. По его словам, «неизвестная третья сторона» заставила антивирусы компании считать вредоносными безопасные файлы Tencent, Mail.ru и Steam (игровой облачный сервис Valve).

Ложные срабатывания

В 2007 г. неправильная работа антивирусов ЛК привела к серьезным проблемам на компьютерах с операционной системой Microsoft Windows – после очередного обновления сигнатур у пользователей пропали «Рабочий стол», меню «Пуск» и «Панели задач». В компании тогда объяснили это допущенными ошибками технического плана и принесли извинения перед клиентами ***(«Касперский» «портил» файлы ОС, чтобы нарушить работу антивирусов-конкурентов // InternetUA (http://internetua.com/kasperskii---portil--faili-os--cstobi-narushit-rabotu-antivirusov-konkurentov). – 2015. – 15.08).***

***

Встроенные в ноутбуки и планшеты LTE/3G модемы могут стать мишенью для хакеров, которые ищут лазейки, позволяющие им установить вредоносное ПО на целевую систему и получить к ней постоянный доступ.

Во время конференции DEF CON, проходившей в Лас-Вегасе, исследователи Intel М. Шкатов и Д. Майкл продемонстрировали, как злоумышленник при помощи установленного на компьютере вредоносного ПО может переписать прошивку модуля популярного LTE-модема Huawei, установленного в значительном количестве устройств.

Модуль работает под управлением ОС на базе Linux, полностью независимой от основной операционной системы компьютера, пишет интернет-портал NetworkWorld. Система модуля подключена к компьютеру через внутренний USB-интерфейс, позволяющий эмулировать клавиатуру, мышь, драйвер CD-ROM, сетевую карту или другой USB-девайс.

Главная проблема, по словам специалистов, заключается в том, что в процессе получения обновлений для прошивки отсутствует механизм проверки криптографической подписи. Это позволило исследователям создать вредоносный образ прошивки, который мог быть записан на утилиту обновлений для ОС Windows, установленную производителем.

В случае успешной атаки злоумышленник сможет повторно инфицировать главную ОС, даже если она была переустановлена. Более того, преступник может модифицировать прошивку таким образом, что все последующие запросы на обновления будут проигнорированы. Таким образом, у пользователя не будет иного способа избавиться от проблемы, кроме как разобрать ноутбук или планшет и заменить инфицированный модуль.

По словам экспертов, компания Huawei осведомлена о проблеме и уже исправила ее, реализовав в своих модулях механизм безопасной загрузки ***(Встроенные LTE/3G модемы могут использоваться хакерами для повторного заражения ОС // InternetUA (http://internetua.com/vstroennie-LTE-3G-modemi-mogut-ispolzovatsya-hakerami-dlya-povtornogo-zarajeniya-os). – 2015. – 11.08).***

***

Microsoft предупредила пользователей о том, что злоумышленники с помощью USB-устройств эксплуатируют уязвимость в продукте компании, позволяющую выполнить вредоносный код. Брешь затрагивает все поддерживаемые версии ОС Windows.

Уязвимость существует из-за того, что компонент Mount Manager некорректно обрабатывает символические ссылки. Локальный злоумышленник может повысить свои привилегии и выполнить код. Для того чтобы проэксплуатировать уязвимость, атакующему необходимо подключить вредоносное USB-устройство к целевой системе.

Эта брешь CVE-2015-1769 очень напоминает уязвимость .LNK, которую в прошлом эксплуатировали создатели Stuxnet, отмечает ИБ-исследователь П. Паганини. Единственное различие между брешами заключается в том, что эксплуатировать первую можно только локально с помощью вредоносных USB-устройств, а вторую – удаленно.

Компания Microsoft полагает, что такая брешь эксплуатируется злоумышленниками в кибератаках на пользователей продуктов компании. Устранить уязвимость можно, установив обновления с сайта производителя ***(Злоумышленники эксплуатируют уязвимость в Windows с помощью USB // InternetUA (http://internetua.com/zloumishlenniki-ekspluatiruuat-uyazvimost-v-Windows-s-pomosxua-USB). – 2015. – 16.08).***

***

Не прошло и недели с тех пор, как ИБ-эксперт обнаружил критическую уязвимость в мобильной операционной системе Android, которая затрагивает 55 % устройств пользователей, как исследователями была выявлена новая брешь. Специалисты из Trend Micro сообщили об уязвимости в Android-компоненте mediaserver, которая позволяет злоумышленникам с помощью специально созданного мультимедийного сообщения установить на целевом устройстве вредоносное ПО.

Бреши CVE-2015-3842 подвержены практически все устройства на базе Android – от Android 2.3 Gingerbread до Android 5.1.1 Lollipop. Уязвимость содержится в компоненте mediaserver, известном как AudioEffect. Согласно данным исследователей, брешь можно проэксплуатировать с помощью различных вредоносных приложений. Все, что нужно злоумышленникам, это убедить жертву установить на устройстве приложение, которое не требует особых разрешений, тем самым, не вызывая у пользователя подозрений.

В настоящее время нет никаких свидетельств, что уязвимость, позволяющая получить контроль над целевым устройством, эксплуатируется хакерами. Разработчики Google сообщили, что уязвимость уже устранена. Однако недавняя новость о том, что выпущенное компанией обновление слишком простое и поэтому не устраняет уязвимость Stagefright, затрагивающую 950 млн Android-устройств, заставляет пользователей нервничать ***(Очередная брешь в Android позволяет хакерам получить полный контроль над устройством // InternetUA (http://internetua.com/ocserednaya-bresh-v-Android-pozvolyaet-hakeram-polucsit-polnii-kontrol-nad-ustroistvom). – 2015. – 19.08).***

***

Всё больше организаций признают серьёзность хакерских атак и приходят к пониманию важности защиты корпоративной IT-инфраструктуры от цифровых угроз. Об этом свидетельствует проведённое CyberEdge Group исследование, в котором приняли участие более 800 руководителей отделов IT-безопасности и практикующих специалистов – представителей 19 различных отраслей бизнеса.

Согласно представленному компанией отчёту Cyberthreat Defense Report, более половины (52 %) респондентов предполагают, что их предприятия станут жертвами успешных кибератак в 2015 г. В прошлом году на их долю пришлось 39 % участников опроса.

Как ключевые киберугрозы, которые беспокоят специалистов в области информационной безопасности, респонденты называют атаки на веб-приложения. Веб-сервисы широко распространены в современных компаниях и зачастую находятся в центре внимания злоумышленников. Причин для этого очень много, не последней из которых является возможность прямого доступа к конфиденциальным данным. Кроме того, особую озабоченность у экспертов вызывает безопасность мобильных устройств.

Более 2/3 организаций, принявших участие в опросе, планируют заменить или модернизировать уже имеющиеся у них инструменты защиты конечных устройств. Респонденты также отметили, что применение подхода использования собственных устройств в рабочих целях (BYOD) увеличится практически в два раза – от 30 до 59 % в течение этого года. Это указывает на необходимость дополнительного инвестирования в мобильную безопасность.

Положительное влияние на защиту от кибератак, по мнению участников опроса, может оказать технология SDN – 63 % респондентов разделяют эту точку зрения.

Подводя итоги исследования и задавая вопрос относительно перспектив на будущее, 62 % респондентов указали о том, что в 2015 г. бюджет на IT-защиту должен быть увеличен. Особое внимание при распределении средств эксперты советуют обращать на аспекты, касающиеся защиты следующего поколения для конечных и мобильных устройств, быстро развивающихся сервисов разведки в отношении киберугроз и программно-определяемых решений для

защиты ***(Бизнес опасается кибератак на корпоративные веб-сервисы // InternetUA (http://internetua.com/biznes-opasaetsya-kiberatak-na-korporativnie-veb-servisi). – 2015. – 13.08).***

***

Команда исследователей из университета Калифорнии смогла дистанционно управлять системами Chevrolet Corvette с помощью СМС. Об этом сообщает Wired.

Занимающиеся тестированием систем безопасности в благих целях хакеры обнаружили уязвимость, которая может позволить злоумышленникам управлять любой легковой машиной или грузовиком, если в них используются ключи-заглушки, вставляемые в диагностический порт бортового компьютера. Такие устройства обычно устанавливают страховщики и компании, занимающиеся грузовыми автоперевозками, чтобы иметь возможность измерить эффективность расходования горючего и пройденное расстояние.

«Мы раздобыли несколько таких устройств, разобрали программы на составляющие их коды и обнаружили немало дефектов в системе безопасности», – прокомментировал эксперимент возглавляющий команду исследователей профессор С. Севедж, преподающий компьютерные науки в университете Калифорнии.

Отправив СМС, содержащие фрагменты специально написанного кода, исследователям удалось заставить автомобиль включать дворники на лобовом стекле, тормозить и, наоборот, полностью отключать систему торможения, когда он двигался на небольшой скорости. По словам участвовавшего в эксперименте добровольца, после того как борткомпьютер получал сигнал, педаль тормоза переставала реагировать на любое давление ***(«Белые хакеры» научились управлять Chevrolet Corvette по СМС // InternetUA (http://internetua.com/belie-hakeri--naucsilis-upravlyat-Chevrolet-Corvette-po-sms). – 2015. – 13.08).***

***

ИБ-компания Symantec опубликовала доклад, проливающий свет на деятельность профессиональной хакерской группировки, получившей название Butterfly («Бабочка»), основной специализацией которой является корпоративный шпионаж.

Как указывается в документе, Butterfly – группа высококвалифицированных хакеров, занимающихся корпоративным шпионажем. Команда представляет значительную угрозу для компаний, обладающих большими объемами проприетарной интеллектуальной собственности.

По словам специалистов Symantec, впервые о деятельности Butterfly стало известно в 2013 г. Тогда группировка осуществила кибератаки на ряд крупных технологических компаний, в числе которых Twitter, Facebook, Apple и Microsoft. В ходе кампаний злоумышленники использовали эксплоит для

уязвимости нулевого дня в Java с целью инфицирования целевых компьютерных систем.

В конце 2013 г. атаки внезапно прекратились, но уже в конце 2014 г. Butterfly вновь проявила себя. По состоянию на июль 2015 г., жертвами группировки стали 49 организаций в 20 странах мира.

По данным экспертов, злоумышленники владеют внушительным арсеналом кастомного вредоносного ПО, которое используют наряду с хорошо известными бэкдорами для Mac OS X и Windows.

После проникновения в сеть атакующие компрометируют серверы электронной почты и системы управления содержимым/контентом, что дает им возможность перехватывать электронную переписку и получать доступ к различной документации, описаниям продуктов, а также финансовым записям. Представляющая ценность информация пересылается на принадлежащие Butterfly серверы, после чего злоумышленники выставляют ее на продажу.

Для того чтобы скрыть свою деятельность, группировка применяет ряд техник, в том числе модифицирует журнал событий, использует фиктивные имена и электронные адреса при регистрации доменов C&C-серверов (при этом ни разу не повторяясь), а также рассчитывается за хостинг-услуги только в биткоинах ***(Раскрыты подробности деятельности шпионской группы Butterfly // InternetUA (http://internetua.com/raskriti-podrobnosti-deyatelnosti-shpionskoi-gruppi-Butterfly). – 2015. – 13.08).***

***

Автозаправки многих стран сегодня оснащаются по последнему слову техники, имеют подключение к сети и, неизбежно, становятся объектами хакерских атак. В феврале текущего года уже был прецедент со взломом заправки, после чего сотрудники компании Trend Micro К. Уилхойт и С. Хилт решили провести эксперимент. Исследователи создали приманку, в виде полной имитации настоящей системы мониторинга заправочной станции, открыли свое детище сети и стали ждать.

Для хакеров приманка выглядела как обычная система заправочной станции, где для контроля за уровнем топлива, температурой и т. д. используются системы Guardian AST. Оказалось, автозаправки весьма популярны у хакеров. За полгода наблюдений исследователи Trend Micro зафиксировали целый ряд атак на свою фальшивку.

Учитывая, что Guardian AST используется только для мониторинга и никак не может повлиять на уровень топлива, большинство атак были безобидными. С другой стороны, даже безобидные атаки, по словам исследователей, могут привести к нарушениям поставок топлива. Если хакеры массово станут взламывать заправки и фальсифицировать данные, к примеру, сообщая операторам, что баки полны, когда, на самом деле, они пусты, теоретически, это может привести к хаосу. Также хакеры вполне могут выдать полную цистерну за пустую. Это приведет к разливу топлива, во время пополнения резервуара, что поставит жизни людей под угрозу.

Однако были и другие атаки. Так заправку пытались положить DDoS-атакой, длившейся два дня. IP-адреса атакующих вели в Сирию, и ранее были замечены в операциях Сирийской электронной армии (Syrian Electronic Army). Имя заправки пытались сменить с GasPot на SEAcannngo, что тоже указывает на сирийцев, однако они отрицают свою причастность к данным случаям.

В другом случае заправку переименовали в H4CK3D by IDC-TEAM, что уже указывает на группу хактивистов Iranian Dark Coders Team.

Подводя итог эксперименту, К. Уилхойт пояснил: «Хакеры выбирают подобные системы в качестве мишеней, потому что это просто. Сканирование сайтов, вроде Shodan, обнажает такие системы, которые вообще не должны быть подключены к Интернету. Нужно начинать работать с безопасностью. Потому что сейчас все эти устройства, подключенные к сети, это просто смешно» ***(Хакеры постоянно атакуют автозаправки // InternetUA (http://internetua.com/hakeri-postoyanno-atakuuat-avtozapravki). – 2015. – 13.08).***

***

В процессорах Intel на архитектуре x86 обнаружена существующая 18 лет уязвимость, позволяющая хакерам устанавливать на компьютеры «вечные» вирусы, а также нарушать работу ПК, перепрошивая «биос».

Архитектурный дефект

Дефект в архитектуре Intel x86 позволяет злоумышленникам помещать руткит в прошивку персональных компьютеров и получать к системе практически неограниченный доступ, сообщил на конференции Black Hat аналитик компании Battelle Memorial Institute К. Домас.

Примечательно, что уязвимость в архитектуре x86 появилась еще в 1997 г., но обнаружена она была только сейчас, спустя 18 лет.

Обновление «биоса»

Она позволяет злоумышленнику получить доступ к режиму работы процессора System Management Mode (SMM), реализованному в чипах Intel. Режим SMM предоставляет программе наивысший из возможных доступов в системе (выше любого уровня доступа в ОС, так как режим SMM находится на более низком системном уровне). В режиме SMM хакер может обнулить «биос», нарушив работу ПК, или внедрить в прошивку персонального компьютера вредоносный код.

Установка «вечных» вирусов

Этот код затем может быть использован, например, для восстановления удаленного вируса. Таким образом, вредоносная программа может поселиться на компьютере навечно – и пользователь не сможет понять, откуда «зараза» берется.

К. Домас протестировал на наличие уязвимости только чипы Intel, но отметил, что в процессорах AMD она тоже может присутствовать, так как они базируются на этой же архитектуре.

Патч от Intel

По словам К. Домаса, он уведомил о проблеме корпорацию Intel, и та уже исправила ошибку в процессорах последнего поколения. Кроме того, компания выпустила патч для чипов предыдущих поколений. Однако он позволяет «вылечить» далеко не все процессоры.

Для того чтобы провести атаку, хакер сначала должен получить в системе права администратора. То есть сама по себе уязвимость не позволяет получить доступ к компьютеру изначально, а лишь помогает замаскировать уже помещенный в нее вирус.

Работы других исследователей

Ранее безопасность базовых компонентов вычислительных систем неоднократно оказывалась под вопросом. Так, в марте 2015 г. исследователи К. Кова и К. Каленберг на конференции CanSecWest в Ванкувере, Канада, продемонстрировали способность дистанционно перепрошивать «биосы» персональных компьютеров, помещая в его программное обеспечение вредоносный код.

На днях К. Кова вместе с коллегой Т. Хадсоном объявили о разработке компьютерного червя под названием Thunderstrike 2, способного проникать в недосягаемую для антивирусов прошивку компьютеров Apple Mac, минуя все барьеры системы безопасности ***(Архитектурный дефект в процессорах Intel дает хакерам полный доступ к системе // InternetUA (http://internetua.com/arhitekturnii-defekt-v-processorah-Intel-daet-hakeram-polnii-dostup-k-sisteme). – 2015. – 10.08).***

***

ИБ-компания Tripwire опубликовала результаты опроса, проведенного среди 215 участников конференции Black Hat USA 2015, недавно проходившей в Лас-Вегасе. Как оказалось, почти две трети (64 %) респондентов считают, что их организации являются потенциальными мишенями для кибератак, осуществляемых из других стран. При этом, 86 % опрошенных признались, что за прошедший год число нападений на их корпоративные сети возросло в несколько раз.

Примечательно, что из этого количества только 47 % представителей выразили уверенность в способности своих компаний обнаруживать и противостоять угрозам. Также выяснилось, что более 53 % организаций не обладают достаточными возможностями для отслеживания всех угроз, нацеленных на их корпоративные сети. В то же время 41 % опрошенных отметил значительный рост количества успешных кибератак, совершенных за последние 12 месяцев.

По словам руководителя отдела информационной безопасности и стратегии риска Tripwire Т. Эрлина, организациям известно, что на них активно осуществляются кибератаки, и их текущих возможностей недостаточно для эффективной защиты от нападений. В то время как на рынке появляется все больше новых решений, компании испытывают затруднения с эффективным применением таких технологий, отметил Т. Эрлин ***(64 % организаций***

являются потенциальными целями кибератак // InternetUA (http://internetua.com/64--organizacii-yavlyauatsya-potencialnimi-celyami-kiberatak). – 2015. – 20.08).

***

Мошеннические атаки в секторе электронной коммерции возросли за II квартал текущего года на 20 % и составили 36 млн. Такие данные предоставлены в отчете ИБ-компании ThreatMetrix.

Результаты ежемесячного мониторинга одного миллиарда транзакций по всему миру показали, что за указанный период было заблокировано 75 млн операций высокой степени риска во всех секторах. Больше всего пострадал сектор электронной коммерции. Компания ThreatMetrix оценила, что потери интернет-трейдеров могли составить 3 млрд дол., если бы 36 млн транзакций не удалось заблокировать.

Наибольшее число атак было зафиксировано с территории США и Великобритании, вместе с которыми в список попали Германия, Индия и Доминиканская Республика. По словам экспертов ThreatMetrix, значительное число атак было направлено на жертв, находящихся в той же стране, что и злоумышленники.

Представитель руководства ThreatMetrix С. Муди пояснил, что множество атак совершается вследствие компрометации личных данных, ставших доступными киберпреступникам. «Первое, что делают преступники после компрометации данных – проверяют и используют информацию о кредитной карте. Часто эти проверки направлены на online-медиакомпании и связаны с созданием новых учетных записей». Последующие факты утечки данных позволят мошенникам получить полную информацию о своих жертвах, благодаря которой они смогут открыть банковский счет от имени пострадавшего ***(Количество атак в секторе электронной коммерции выросло на 20 % // InternetUA (http://internetua.com/kolicsestvo-atak-v-sektore-elektronnoi-kommercii-viroslo-na-20). – 2015. – 24.08).***