СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(14–31.01)

2015 № 2

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(14–31.01)
№ 2

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

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

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Что ждет социальные сети в 2015 году

Весь 2014 г. был полон неожиданных событий. В первой его половине все крутилось вокруг М. Цукерберга с его невероятными покупками, и П. Дурова – с его скандалами вокруг расставания с акционерами «ВКонтакте». Осень 2014 г. запомнилась еще больше. Массовые утечки личных фотографий знаменитостей, атаки хакеров и беспрецедентный скандал вокруг Sony Pictures, который привлек внимание лично Б. Обамы. Forbes оставил скандалы в стороне и решил посмотреть, как события прошлого года повлияли на будущее развитие социальных сетей и интернет-сервисов.

Быстрорастущие фотосервисы

Количество активных пользователей Instagram в 2014 г. возросло до 300 млн. Именно столько людей как минимум раз в месяц включают приложение. Миллиарды лайков к миллионам свежих фотографий ставят пользователи сервиса каждый день. Благодаря столь высоким показателям Citigroup уже оценивает Instagram в сумму свыше 35 млрд дол., а покупка сервиса социальной сетью Facebook в 2012 г. за 750 млн дол. (первоначальная оценка в 1 млрд дол. была снижена) теперь не кажется столь безумным решением М. Цукерберга.

В настоящее время Instagram уже обогнал Twitter как по количеству пользователей (около 280 млн), так и по стоимости (около 23 млрд дол.). Впрочем, есть у обоих сервисов и общее: слабая монетизация. Citigroup дает оценку в 2 млрд дол. прибыли ежегодно, но пока сервис избегает агрессивной рекламы. В отличие от разработчиков, небольшой и средний бизнес уже активно использует Instagram в своих целях: реклама через людей с большим количеством подписчиков дает больше пользы, нежели кампания в Facebook или «ВКонтакте».

В будущем количество пользователей сервиса будет расти, что доказано опытом прошлых лет. В 2012 г. Instagram использовало лишь 30 млн человек. В начале 2013 г. их число возросло до 100 млн активных пользователей, а через 12 месяцев – до 200 млн. Если скорость роста сервиса сохранится, уже к концу этого года количество активных пользователей достигнет 400 млн человек.

Отлично себя показывает и сеть для размещения понравившихся картинок и фото – Pinterest. Только в США у сервиса свыше 40 млн активных пользователей, количество зарубежных юзеров еще выше. В настоящее время у компании есть несколько офисов по всему миру, любовь рекламодателей и лучшая аудитория в мире: около 80 % пользователей – женщины, которые, согласно исследованиям, более лояльно воспринимают рекламу. Pinterest, с его досками, является отличной площадкой для рекламных брендов.

Неполная анонимность

2014 г. отчетливо показал, что люди больше не желают былой публичности и всячески интересуются вопросами сохранности информации о себе. Это привело к тому, что Facebook официально начал уведомлять о настройках своей новостной ленты, где ранее появлялось огромное количество неясных новостей. Негативный имидж социальной сети дошел до того, что М. Цукерберг официально заявил: пользователей теперь будут называть «люди».

На фоне шумихи вокруг Facebook активный рост показывает Snapchat. Сервис позволяет обмениваться фото, которые через несколько секунд самоликвидируются. До конца года оценка сервиса возросла до 10 млрд дол., а Snapchat совместно со стартапом Square запустил сервис платежей Snapcash. Большая часть аудитории – молодые люди в возрасте до 22 лет, которые ранее покинули Facebook.

Небывалую популярность получило приложение Secret, позволяющее отправлять анонимные сообщения людям из списка своих контактов. Буквально за несколько недель создатели получили инвестиции в размере 2,5 млн дол. на развитие, а спустя месяц – судебный иск правительства Бразилии: оказывается, в этой стране можно говорить, что угодно, но без анонимности. Приложение удалили с App Store и Google Play. Secret быстро стал знаменитым и получил несколько клонов, среди которых самыми известными стали Whisper и Yik Yak.

Еще одним приложением с ограниченной подачей личной информации, взрыва которого ожидают в 2015 г., стал Tinder. Особенность приложения в том, что здесь нет анкет и списка достижений – только фото. Каждый пользователь одобряет или отклоняет фото других людей. Если позитивное мнение двух людей насчет друг друга совпадает, система открывает возможность для общения. Это снимает всю лишнюю неловкость и глупое начало разговора: два человека ведь уже одобрили друг друга. Американский Forbes оценил сервис в 2 млрд дол., и в будущем его популярность будет расти: Tinder займется выходом на международный рынок, так как сейчас ограничивается только территорией США.

Борьба за безопасность

Наиболее актуальной проблемой 2014 г. стала сохранность данных и безопасность пользователей в сети. Согласно информации компании Kaspersky, в 2015 г. каждый день будет осуществляться 4 млн атак на компьютеры пользователей и их смартфоны. В частности это касается Android-устройств. Впрочем, как показали события вокруг Apple осенью и Sony Pictures в декабре, хакеры выбирают себе самые разные цели. Атаковать взялись даже анонимную сеть Tor, которую в быту используют сами же хакеры.

В связи с этим пользователи мобильных устройств все больше внимания обращают на возможности защиты себя и своих данных. Сервис Apple Pay быстро обрел популярность в США, и через месяц после запуска

уже обрабатывал 1 % всех безналичных платежей, а сервис iCloud получил двойную верификацию. Мессенджер Telegram позиционирует себя как самый надежный способ для общения, что уже было доказано независимыми агентствами, а количество активных пользователей превысило 50 млн человек. Об усилении защиты и шифровке сообщений в конце года заявили и представители WhatsApp.

В будущем социальные сети и мессенджеры все больше внимания будут обращать на угрозу взлома: пользователи оставляют в них массу своих личных данных, утечка которых может поднять огромный скандал и станет началом конца для одного из сервисов.

Проблема монетизации

Несмотря на свой бурный рост, все западные сервисы пока не могут показать значительных достижений в плане монетизации. К примеру, Twitter уже седьмой год подряд остается убыточной компанией и пока не может похвастаться значительным ростом доходов. В конце 2014 г. было принято решение увеличить число рекламных блоков в ленте пользователей, а также взять курс на активное развитие сервиса вне США.

Та же ситуация и у Instagram. Несмотря на 300 млн активных пользователей, с помощью сервиса пока зарабатывают лишь отдельные игроки, тогда как сам Instagram остается практически ни с чем. Мессенджер WhatsApp за весь 2014 г. заработал 15 млн дол. и получил более 232 млн дол. убытков только за девять месяцев работы. Основатели WhatsApp собираются брать за использование сервиса по 1 дол. в год, но пока модель действует лишь в нескольких странах мира. Сам М. Цукерберг во время выступления в Индии заявил, что в настоящее время не знает, как правильно монетизировать мессенджер, который стоил ему свыше 22 млрд дол. (часть WhatsApp была оплачена акциями, которые во второй половине 2014 г. сильно возросли).

Убыточными также остаются Telegram и Viber, который пытается зарабатывать на продаже стикеров. Не лучше ситуация и у Snapchat и Secret, которые сегодня у всех на слуху. Tinder ввел монетизацию лишь в конце года, но на сегодняшний день компания не зарабатывает больших денег. Слабые доходы показывает и российская социальная сеть «ВКонтакте», в отличие от своих восточных коллег.

Сервисы Line и WeChat в Азии полностью себя окупают. Пользователи мессенджеров покупают стикеры, дополнительные возможности и огромное количество контента. За последние 12 месяцев общие доходы компаний превысили 500 млн дол.

Основатель WhatsApp Я. Кум, украинец по происхождению, открыто заявил, что мессенджеры – это длительный бизнес, ждать отдачи через год не стоит. Судя по всему, М. Цукербергу об этом сообщили слишком поздно.

Бурный рост мессенджеров

В отличие от социальных сетей с набором лишних функций, мессенджеры пользуются большой популярностью за счет простоты: есть

лишь контакты и возможность быстро и фактически бесплатно с ними общаться. За 2014 г. WhatsApp возрос еще на 150 млн пользователей, и их общее число в начале января достигло 700 млн человек. Viber набрал 100 млн активных пользователей: теперь сервисом пользуется свыше 200 млн человек. Серьезный рост показал Telegram П. Дурова, который благодаря сильному пиару на фоне WhatsApp быстро достиг показателей в 50 млн пользователей.

Не отстает и азиатский рынок. Там практически никто не использует Skype или WhatsApp, а их место заняли местные аналоги – Line и WeChat. На двоих у них свыше 650 млн пользователей, а охватывают они лишь Китай, Японию и Южную Корею.

Показательным стал пример Facebook, который за два месяца искусственно создал мессенджер на 500 млн пользователей. Желая разгрузить мобильное приложение социальной сети, М. Цукерберг принял решение создать сервис для общения Facebook Messenger на мобильных платформах. Выбирать особо не приходилось: в самом Facebook общение было закрыто. Сегодня Facebook Messenger является самым популярным мессенджером на планете после WhatsApp.

Прорыв мелких игроков

В 2014 г. нашлось место и для мелких игроков, которые сумели набрать популярность за счет слабых сторон крупных сервисов. К примеру, когда во время Евромайдана за всеми социальными сетями следили, активисты массово использовали закрытые каналы Zello. Спустя несколько недель сервис успешно показал себя во время восстаний в Венесуэле. При этом первоначально Zello создавался для использования на стройках и крупных производствах.

Во время декабрьских выступлений в Москве сторонники А. Навального использовали сервис FireChat. Спецслужбы глушили Интернет в районе Красной и Манежной площадей, что не давало возможности использовать Twitter и Facebook. Мессенджер FireChat работает с помощью Bluetooth и Wi-Fi, необходимости в сети нет, но круг работы ограничен 30 м. Впрочем, это не помешало приложению подняться в топ самых популярных в российском сегменте ***(Что ждет социальные сети в 2015 году // InternetUA (http://internetua.com/cto-jdet-socialnie-seti-v-2015-godu). – 2015. – 15.01).***

***

Facebook запустил в тестовом режиме новый сервис Facebook at Work, который предназначен для общения сотрудников внутри той или иной компании.

«Facebook at Work – это отдельное приложение, которое позволит сотрудникам компаний связываться между собой и эффективно выстраивать совместную работу, используя инструменты Facebook», – отмечают разработчики.

Слухи о создании Facebook-сервиса для внутрикорпоративного общения ходили на рынке с прошлого года. В настоящее время приложение Facebook at Work для iOS и Android уже доступно в магазинах приложений, однако воспользоваться им могут только компании-партнеры пилотного проекта.

Facebook отмечает, что новинка предназначена сугубо для использования внутри компаний. Разработчики обещают, что будут созданы условия для безопасного обмена информацией, который будет полностью отделен от личных Facebook-профилей. Данные, которыми коллеги будут обмениваться в рамках сервиса, будут доступны только сотрудникам конкретной компании.

В Facebook не уточнили список партнеров, которые тестируют сервис на пилотной стадии, а также, когда Facebook at Work появится в свободном доступе. На рынке корпоративных онлайн-сервисов этому приложению придется конкурировать с Google, Microsoft и LinkedIn.

Компании придется убедить корпорации в безопасности использования нового сервиса и, в частности, в том, что информация из чатов не попадет к конкурентам. Многие компании запрещают доступ к Facebook на рабочем месте, так как опасаются, что сотрудники будут тратить время на общение в соцсети ***(Facebook запустил сервис для внутрикорпоративного общения // InternetUA (http://internetua.com/Facebook-zapustil-servis-dlya-vnutrikorporativnogo-obsxeniya). – 2015. – 14.01).***

***

В сети появилось приложение Facebook Unliker, которое позволяет найти и легко убрать пользовательские отметки Like, поставленные на тех или иных страницах в социальной сети, пишет Блог Imena.UA (http://www.imena.ua/blog/facebook-unliker/).

Разработчики приложения отмечают, что Unliker рассчитан, в первую очередь, на снятие отметок Like со страниц актёров, музыкантов, шоу и других пристрастий, оставленных несколько лет назад.

Прежде чем начать убирать свои Like пользователю нужно авторизироваться на странице приложения через Facebook. Затем можно увидеть все поставленные различным страницам Like – причём, первыми отображаются более ранние отметки ***(В Сети появилось Facebook-приложение для снятия своих «Like» // Блог Imena.UA (http://www.imena.ua/blog/facebook-unliker/). – 2015. – 15.01).***

***

Сервис микроблогов Twitter вернул функцию Bing Translator в TweetDeck, предоставляя пользователям возможность оперативно читать переводы твитов с иностранных языков. Мгновенные переводы доступны по ссылке «Перевести Tweet», которая появляется в твитах на не родном пользователю языке.

Возвращение функции заметили пользователи. Пресс-секретарь Twitter подтвердил этот факт, но от дальнейших комментариев отказался. Возвращение перевода в TweetDeck может быть сигналом, что Twitter тестирует его перед повторным подключением на других платформах.

Twitter экспериментирует с переводами Bing с 2012 г. Последний раз функция переводов была отключена в августе 2014 г. ***(Twitter вернул переводчик Bing // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_vernul_perevodchik_bing). – 2015. – 16.01).***

***

Засновник і генеральний директор Facebook М. Цукерберг заявив, що мета його соцмережі – об'єднувати людей по всьому світу і давати їм можливість спілкуватися.

Про це пише techcrunch.com.

За словами очільника Facebook, те, що компанія продовжує працювати навіть у країнах з репресивними режимами, допомагає людям. За допомогою соцмережі люди можуть спілкуватися з коханими, навчатися чи шукати роботу, наводить приклад М. Цукерберг.

«Дехто каже, що ми робимо так лише тому, що це добре для бізнесу. Але є країни, де ми не працюємо і при цьому фінансово у нас все гаразд. Якщо нас заблокують у ще кількох країнах, це не буде надто болісно, – каже він. – Тут йдеться про нашу місію, а не якесь короткотривале бізнес-рішення».

М. Цукерберг також додав: вірить, що таким чином підтримує свободу слова. За словами бізнесмена, його компанія намагається боротися із запитами на блокування контенту і завжди ретельно вивчає подібні звернення, щоб перевірити його законність.

Нагадаємо, нещодавно гендиректора Facebook розкритикували за «пропаганду Китаю» ***(Цукерберг пояснив, чому його соцмережа діє у країнах, де є цензура // MediaSapiens (http://osvita.mediasapiens.ua/web/social/tsukerberg_poyasniv_chomu_yogo_sotsmerezha_die_u_krainakh_de_e_tsenzura/). – 2015. – 15.01).***

***

Группа по исследованиям в области искусственного интеллекта Facebook AI Research поделилась с сообществом собственными наработками в области глубокого обучения (deep learning) – алгоритмов машинного обучения, которые пытаются моделировать высокоуровневые абстракции в данных, используя архитектуры, состоящие из множества нелинейных трансформаций.

Под свободной лицензией опубликован исходный код модулей для Torch, популярного фреймворка на Lua, который широко используется в

научном сообществе для разработки и тестирования алгоритмов машинного обучения. Фреймворк использует скриптовый язык LuaJIT.

Оптимизированные модули от компании Facebook гораздо эффективнее, чем штатные модули Torch. С их помощью можно обучать нейросети большего размера за меньшее время, что позволяет существенно ускорить научно-исследовательские работы. Оптимизация включает в себя, среди прочего, эффективное использования GPU в свёрточных нейронных сетях (ConvNets), а также в сетях, которые часто применяются в приложениях по обработке информации на естественном языке (Natural Language Processing). Более подробно о модулях ConvNets рассказано в научной работе.

Кроме упомянутого модуля, в свободный доступ попали и другие модули, использующие архитектуру CUDA, в том числе контейнеры для параллелизации обучения нейросети на нескольких GPU, оптимизированные модули Lookup Table и Hierarchical SoftMax и др.

В последние годы deep learning стало одной из самых перспективных областей информатики. Технологии машинного обучения широко используются, в том числе, в различных веб-сервисах для распознавания образов, анализа логов, распознавания спама и т. д. Нейросети применяют такие компании как Google, Twitter, Nvidia, AMD, Intel, Facebook и многие другие, не считая бесчисленного количества стартапов, действующих в этой области ***(Facebook выложил в свободный доступ модули для машинного обучения // InternetUA (http://internetua.com/Facebook-vilojil-v-svobodnii-dostup-moduli-dlya-mashinnogo-obucseniya). – 2015. – 18.01).***

***

Google в четвертом квартале 2014 г. увеличил долю интернет-пользователей, которые осуществляют авторизованный вход на сторонние сайты через его аккаунты. Об этом свидетельствуют данные компании JanRain.

Во втором и третьем квартале 2014 г. доля Facebook сохранялась неизменной, а в четвертом упала на 3 процентных пункта – до 43 %. Это всего на 3 пункта выше, чем доля Google – 40 % (+6 процентных пунктов). Разница между долями Facebook и Google достигла минимума за последние три года.

Вице-президент JanRain по маркетингу Д. Бэклэнд считает, что достижение Google можно отнести к усилиям компании по унификации идентификации пользователя во всех продуктах, таких как Gmail, YouTube, Android и Google+.

В то же время Facebook в 2014 г. сталкивался с проблемами, связанными с конфиденциальностью данных. Это могло поспособствовать переходу некоторых пользователей в другой сервис из-за отсутствия понимания того, как будут использованы их данные. Однако обновления обеих компаний в прошлом году – способ безопасного использования

Facebook с помощью анонимной сети и отмена обязательного создания профиля в Google+ при регистрации в других сервисах Google – скорее всего, вернут предыдущие показатели, считает Д. Бэклэнд.

Результаты JanRain демонстрируют только мгновенный снимок рынка использования аккаунтов социальных сетей для регистрации на других сайтах. Компания получает данные от сотен клиентов, использующих платформу. Компания Gigya, также исследующая этот рынок, пока не представила свой отчет за четвертый квартал 2014 г. Результаты третьего квартала распределились так: Facebook – 58 %, Google – 24 %.

Компания LoginRadius в своем отчете также отмечает преимущество Facebook (65 %) перед Google (25 %). По данным этого отчета, исследующего использование аккаунтов в социальных сетях для 120 тыс. сайтов по всему миру, лидерство Facebook никогда не было значительнее с тех пор, как компания начала отслеживать этот показатель в январе 2013 г.

Все авторы исследований сходятся в том, что все прочие социальные сети сильно отстают от Facebook и Google.

Отчет JanRain показывает, что LinkedIn стал лучшим выбором в сфере B2B, увеличив свою долю на 6 процентных пунктов по сравнению с третьим кварталом – до 35 %. Доля Google и Facebook снизилась на 3 процентных пункта по сравнению с предыдущим кварталом – до 28 и 24 % соответственно.

Facebook сохраняет лидерство в таких отраслях, как медиа, ритейл, игры и развлечения, музыка и потребительские бренды ***(Google догоняет Facebook по числу регистраций на сайтах с помощью его аккаунтов // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/google_dogonyaet_facebook_po_chislu_registratsiy_na_saytah_s_pomoschyu_ego_akkauntov). – 2015. – 16.01).***

***

Российская социальная сеть «ВКонтакте» преодолела рубеж в 70 млн человек в сутки, сообщает IT Expert.

Об этом в своем Twitter написал пресс-секретарь «ВКонтакте» Г. Лобушкин.

Украинская аудитория сети превышает 12 млн пользователей, своеобразный рекорд посещаемости был поставлен 14 января ***(«ВКонтакте» ежедневно посещает 70 млн человек // IT Expert (http://itexpert.org.ua/rubrikator/item/40560-vkontakte-ezhednevno-poseshchaet-70-mln-chelovek.html). – 2015. – 16.01).***

***

В Facebook Messenger тестируется автоматическое распознавание голоса

Голосовая почта – один из самых неэффективных способов коммуникации, и тем не менее, во многих современных мессенджерах эта функция присутствует. Facebook добавила возможность отправки звуковых клипов в Facebook Messenger ещё в 2013 г., благодаря чему пользователи могут наговаривать и пересылать друзьям свои аудиомонологи.

Но хотя текст не может передать всех эмоциональных оттенков и нюансов голоса собеседника, порой пользователю было бы удобно быстро и без необходимости прослушивания получить представление, о чём говорит его собеседник. И Facebook начала тестирование такой функции, которая напоминает текстовые транскрипции в духе Google Voice.

Теперь, когда пользователь отправляет или получает голосовое сообщение, он видит текстовый анонс. Как отправитель, так и получатель могут видеть текст (если только функция не отключена). Тем не менее, большинство пользователей вряд ли в ближайшее время смогут воспользоваться преимуществами этих возможностей – Д. Маркус, отвечающий за развитие Messenger, подчеркнул, что речь идёт о весьма ограниченном тестировании.

«Мы в настоящее время собираемся тестировать функцию в крошечном масштабе, чтобы оценить, насколько она окажется полезной конечным пользователям», – написал он. Одной из вероятных причин такого решения может быть сложность и неточность автоматического распознавания голоса, с чем сталкивалось большинство пользователей подобных служб ***(В Facebook Messenger тестируется автоматическое распознавание голоса // InternetUA (http://internetua.com/v-Facebook-Messenger-testiruetsya-avtomaticseskoe-raspoznavanie-golosa). – 2015. – 19.01).***

***

Профессиональная социальная сеть LinkedIn обновила функции поиска, чтобы обеспечить пользователям более быстрое и удобное взаимодействие с функционалом.

Теперь поиск стал персонализированным. LinkedIn будет пытаться предлагать результаты, основанные на связях пользователя, а не только на списке пользователей и брендов. Это поможет пользователям сэкономить время и поможет тем, кто не четко представляет субъект поиска. Используя связи, поиск LinkedIn теперь показывает самые близкие совпадения для запроса. Это значит, что поиск по имени с ошибкой может обеспечить желаемый результат.

Новый поисковый опыт доступен всем пользователям. Теперь все пользователи будут видеть полные имена в результатах поиска (ранее такой результат был доступен только премиум-пользователям). Обновление также коснулось поиска по ключевым словам. Теперь рядом с фото пользователя будут отображаться его имя и фамилия, а не текст LinkedIn Member.

Результаты поиска LinkedIn могут быть отфильтрованы по следующим группам:

Все
Люди
Профессии
Компании
Группы
Университеты
Сообщения
Входящие

Результаты поиска по сообщениям могут быть отсортированы по релевантности или дате.

LinkedIn объявил о существенном обновлении архитектуры поиска летом 2014 г. Новая архитектура поиска получила название Galene ***(LinkedIn улучшил функцию поиска людей, работы и сообщений // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/linkedin_uluchshil_funktsiyu_poiska_lyudey_raboty_i_soobscheniy). – 2015. – 21.01).***

***

Facebook начал уведомлять пользователей о характере материалов, помеченных как графические.

Нововведение призвано обеспечить информированное согласие пользователей на их просмотр. Компания также планирует ограничить доступ к контенту такого рода для пользователей в возрасте 13–17 лет.

В течение последних двух лет Facebook демонстрировал разные подходы по отношению к графическим материалам на сайте. В 2013 г. социальная сеть подчинилась волне общественного возмущения, онлайн-петиций и жёсткой критики со стороны пользователей и приняла решение запретить графическое видео обезглавливания женщины, которое циркулировало на сайте.

Спустя несколько месяцев Facebook изменил своё отношение к этой проблеме. Компания отменила запрет на указанное видео и, таким образом, ввела новую политику, регулирующую контент такого рода.

В скорости после этого были внесены официальные изменения в Нормы сообщества Facebook. Ниже – выдержка из этого документа, относящаяся к графическому контенту:

«Facebook уже давно стал тем местом, где люди делятся опытом и обсуждают важные проблемы. Иногда эти обсуждения сопровождаются публикацией графических материалов, которые могут быть связаны с общественными интересам, например, нарушением прав человека или террористическими актами. В большинстве случаев пользователи размещают такие материалы, чтобы осудить подобные действия. Однако, сценам насилия, опубликованным с целью пропаганды садистской жестокости или насилия, не место на нашем сайте.

Мы рассчитываем, что пользователи будут ответственно относиться к публикации материалов. Это также подразумевает тщательный выбор

целевой аудитории для них. При публикации видео, в которых содержатся сцены насилия, необходимо уведомить аудиторию о характере видео, чтобы пользователи могли сделать осознанный выбор – смотреть или не смотреть его».

При этом есть один нюанс – ожидание того, что люди будут ответственно подходить к публикации контента, и надежда на то, что они предупредят других пользователей о том, что те могут увидеть убийство человека, по меньшей мере наивно. Тем не менее, вряд ли руководство Facebook так наивно в своих ожиданиях. Именно поэтому компания заложила фундамент для своего последнего шага в этом направлении ещё в 2013 г. «Во-первых, когда мы рассматриваем материалы, о которых нам сообщается как о нарушающих правила, мы стараемся рассмотреть их целостно, учитывая контекст данного видео или изображения. Мы однозначно удалим контент, прославляющий насилие и жестокость. Во-вторых, мы смотрим на то, были ли эти материалы опубликованы с ответственной позиции – т. е. сопровождаются ли они предупреждением пользователей об их содержании и делились ли ими с подходящей по возрасту аудиторией», – сказал представитель компании.

Facebook действительно экспериментировал с показом предупреждений о характере содержания графических материалов, но они не распространялись на весь контент такого рода.

Теперь ситуация изменилась. В настоящее время предупреждение появляется в верхней части видео о смерти полицейского А. Мерабета, убитого во время атаки на редакцию французского журнала Charlie Hebdo.

Один из пользователей социальной сети задал вопрос в Справочном центре Facebook: «Почему я вижу предупреждение перед тем, как я смогу просмотреть фото или видео?».

«Люди приходят в Facebook, чтобы поделиться своим опытом и повысить свою осведомлённость в вопросах, важных для них. Чтобы помочь людям делиться контентом ответственно, мы можем ограничить видимость фото или видео, содержащих графический контент. Такого рода материалы могут появляться в сопровождении предупреждения, позволяющего другим пользователям узнать о содержании материалов перед их просмотром. Кроме того, этот тип контента могут видеть только пользователи старше 18 лет», – сказал представитель Facebook.

Пресс-секретарь компании рассказал BBC, что её «инженеры всё ещё ищут способы дальнейшего усовершенствования этой схемы», что может включать «добавление предупреждений к релевантным видео YouTube».

Судя по всему, Facebook подвергся как внешнему, так и внутреннему – со стороны совета по наблюдению за безопасностью – давлению, вынуждающему его предпринять шаги по обеспечению защиты пользователей (в частности, детей) от графических материалов сомнительного содержания.

Видео процветает в Facebook. В социальной сети производится, в среднем, более 1 млрд просмотров видео каждый день – почти 1 просмотр на человека. В 2014 г. количество видео публикаций увеличилось на 75 % в мировом масштабе и на 94 % в США.

На прошлой неделе компания приобрела QuickFire Networks для улучшения доступности видеоконтента. Facebook пытается построить собственную видеоплатформу, поскольку она позволяет увеличить вовлечённость пользователей и потенциальный рекламный доход. В то же время компания поощряет создателей видеоконтента публиковать материалы на своей социальной платформе.

Эти изменения важны для рекламодателей. Что ещё важно для них? Чтобы их реклама не демонстрировалась перед или после видео, в котором обезглавливают человека.

Добавление предупреждений к графическому контенту – разумный шаг. Он позволяет Facebook оставить графический контент на сайте и обеспечить так называемую «свободу слова». Кроме того, этот шаг даёт возможность рекламодателям чувствовать себя спокойнее в отношении своей рекламы на сайте, а также перекладывает ответственность в этом вопросе на пользователей – теперь это их выбор, смотреть какие-либо видео и изображения, или нет ***(Facebook начал предупреждать пользователей о характере графических материалов на сайте // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_nachal_preduprezhdat_polzovateley_o_haraktere_graficheskih_materialov_na_sayte). – 2015. – 21.01).***

***

«Одноклассники» объявили об итогах 2014 г.

За прошедшие 12 месяцев в соцсети произошли следующие изменения:

– было выпущено несколько важных обновлений для основных платформ (iOS, Android, Windows);

– аудитория мобильных приложений ОК.ru для Android и Windows за год возросла вдвое;

– были существенно доработаны Лента, а также сообщения, в которых появились вложения;

– запущена функция Push2Talk, позволяющая отправлять друзьям голосовые сообщения прямо в мобильном приложении;

– было запущено отдельное мобильное приложение Модератор ОК (для Android).

Изменения не обошли и видеораздел:

– были запущены пользовательские каналы;

– в веб-версии появился новый плеер просмотра видео;

– появился каталог каналов;

– добавлена возможность проигрывать видео качества UltraHD.

Нововведения позволили увеличить ежедневную аудиторию пользователей, просматривающих видео. Теперь их количество превышает 12 млн человек.

Интерфейс веб-версии «Одноклассников» также был значительно переработан:

– был обновлен тул бар;

– добавлены аудио- и видеовложения в сообщениях;

– были запущены геометки.

Команда «Одноклассников» уделяла большое внимание привлечению контента, как блогерского, так и профессионального. Помимо этого, в 2014 г. был осуществлен редизайн проекта и изменено название сайта (на сокращенную версию «ОК»).

Аудитория «Одноклассников» в 2014 г. превысила 47 млн человек, а мобильная аудитория составляет более 20 млн человек ежедневно ***(«Одноклассники» берут курс на мобильное направление // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/odnoklassniki_berut_kurs_na_mobilnoe_napravlenie). – 2015. – 20.01).***

***

Соцсеть Facebook начала борьбу с поддельными и вводящими в заблуждение пользователей новостями на своем сайте. Об этом сообщается в корпоративном блоге Facebook, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-nachala-borbu-s-lozhnymi-novostjami-v-socseti-42907/).

«Сегодняшнее обновление ленты новостей снизит активность распространения новостей, которые пользователи отметили как ложные, и начнет добавлять предупреждения к записям, которые получили много подобных отметок», – говорят в Facebook.

Под ложными записями Facebook понимает мошеннические записи (к примеру, «Нажмите сюда, чтобы выиграть запас кофе на всю жизнь») или новости-«утки» («Ученые подтвердили существование Санта-Клауса»).

«Люди часто делятся подобными записями, а позже удаляют их, поняв, что их обманули. Кроме того, такие записи часто привлекают много комментариев от друзей, которые предупреждают об обмане, и комментариев с ссылками на сайты, где разоблачается ложная новость», – отмечают разработчики.

Ранее Facebook добавила в ленту новостей функцию, которая позволяет отметить запись как ложную – аналогично тому, как пользователи могут сообщить о спаме. Соцсеть будет учитывать, насколько часто пользователи отмечают запись как ложную, а также сколько людей удаляют запись с одинаковым контентом – например, ссылку на новость или сайт.

Подобные записи будут менее активно демонстрироваться на Facebook. Перед некоторыми новостями также появится предупреждение: «Многие пользователи Facebook сообщили, что в этой записи содержится ложная

информация». Нововведение будет касаться обновлений статуса, а также записей со ссылками на сторонние сайты, фотографиями и видеороликами.

В то же время Facebook говорит, что не будет удалять с сайта записи, которые отмечены пользователями как ложные, и не будет самостоятельно анализировать контент на предмет его подлинности.

Кроме того, Facebook отмечает, что пользователи не склонны отмечать сатирические и юмористические статьи как ложные, поэтому специализированные ресурсы нововведение не затронет. Ранее Facebook начала тестировать кнопку для маркировки сатирических и пародийных статей, чтобы пользователи могли отличать их от реальных историй.

Facebook стала важным источником распространения новостей в мире – по данным исследования Pew Research Center, около 30 % американцев узнают новости именно из этой соцсети ***(Facebook начала борьбу с ложными новостями в соцсети // Marketing Media Review (http://mmr.ua/news/id/facebook-nachala-borbu-s-lozhnymi-novostjami-v-socseti-42907/). – 2015. – 21.01).***

***

LinkedIn работает над созданием нескольких новых инструментов, предназначенных для совместного использования сервиса руководителями и сотрудниками одной компании. Среди них значатся новое приложение и инструмент для шеринга контактной информации сотрудников, а также возможность делиться контентом с конкретной группой работников.

Первый продукт, который LinkedIn собирается запустить в пилотном режиме в ближайшие недели, даст пользователям возможность отправлять InMail-сообщения (приватные сообщения по типу e-mail в LinkedIn) коллегам, даже если они не подключены к сети. Новый функционал также будет поощрять пользователей загружать свою контактную информацию – адреса электронной почты, телефонные номера и т. п. – в базу данных компании, которую смогут видеть их коллеги в сервисе.

Это нововведение призвано дать пользователям LinbkedIn возможность лучше взаимодействовать с сотрудниками в рамках собственной компании. Тем не менее, оно не будет включать функционал по типу чата.

По словам пресс-секретаря LinkedIn, новые функции – часть более масштабной программы, направленной на создание бóльшего количества инструментов для использования внутри компаний. В настоящее время максимальная полезность социальной сети для профессионалов достигается тогда, когда пользователи соединяются с людьми за пределами компании, в которой они работают, – как с целью поиска новой работы, так и для создания сети специалистов в конкретной отрасли. Предстоящие изменения – способ сделать сервис более ценным для настоящей работы пользователей.

Новые продукты также согласованы с более ранними внедрениями LinkedIn, направленными на усовершенствование шеринга контента в рамках

платформы. По этой причине в декабре 2014 г. компания изменила дизайн главной страницы сервиса.

Другой продукт, который LinkedIn начнёт тестировать в конце первого квартала 2015 г., поможет компаниям делиться контентом с конкретными группами сотрудников.

LinkedIn надеется, что прямой и целевой шеринг приведёт к увеличению количества репостов контента в рамках её платформы. Например, если компания хочет нанять на работу новых инженеров по мобильным технологиям, она, например, может поделиться публикацией о философии инжиниринга в компании с уже работающими инженерами в надежде на то, что они передадут эту информацию дальше – своим знакомым и друзьям. Идея состоит в том, что эти работники будут иметь наиболее релевантную сеть контактов для этого конкретного сообщения.

Кроме того, разработчики LinkedIn работают над созданием отдельного мобильного приложения, которое работники смогут использовать для того, чтобы присоединиться к группам сотрудников внутри своей компании. Затем администратор компании сможет распространять контент, адаптированный под определённую группу работников. В LinkedIn уже есть возможность создания групп, но существующий функционал больше предназначен для нетворкинга. Новые группы будут создаваться специально для шеринга контента внутри компании.

В настоящее время разработчики LinkedIn также занимаются исследованием других способов добавления этого функционала к существующей платформе. С помощью нового инструмента работодатели смогут отслеживать статистику того, как часто сотрудники компании делились контентом и с каким количеством пользователей.

Напомним, что в ноябре 2014 г. LinkedIn упростила шеринг контента SlideShare. Теперь с помощью одного клика пользователи могут загрузить презентацию, инфографику или видео в свой профайл в LinkedIn. Социальная сеть будет спрашивать новых пользователей SlideShare, хотят ли они опубликовать свой контент в социальной сети. Тот же вопрос будет задаваться и существующим пользователям ***(LinkedIn планирует запуск инструментов, объединяющих работников одной компании // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/linkedin_planiruet_zapusk_instrumentov_obedinyayuschih_rabotnikov_odnoy_kompanii). – 2015. – 22.01).***

***

Никто не использует Google+. Мы в общем-то догадывались, но даже не могли представить масштабы. Руководитель проекта Д. Бесбрис в своем интервью для Re/Code отказался говорить о цифрах. Можно понять причину, если взглянуть на подсчеты Э. Морбиуса и К. Андерсона. Итак, Google+ есть в каждом нашем смартфоне и практически у каждого пользователя YouTube, Gmail и других сервисов, ибо навязали. Но сколько людей его использует?

В Google+ зарегистрировано 2,2 млрд учетных записей, и это показатель, которым можно гордиться. Однако, по подсчетам, лишь 9 % этих записей генерируют публикации. В свой записи в Ello Э. Морбиус написал, что лишь 4–6 млн пользователей Google+ активно взаимодействуют друг с другом. Это данные за январь 2015 г. Вот краткий перечень известных данных:

– около 2,2 млрд аккаунтов Google+

– 9 % из них публикует публичный контент

– из них 37 % комментируют видео на YouTube, и только 8 % имеют измененную фотографию пользователя

– 6 % активных профилей проявили активность в 2015 г.

– из них половина никак не относится к YouTube

– другими словами, 0,2–0,3 % всех профилей в Google+, что около 4–6 млн человек, проявили публичную активность в сети в 2015 г.

Как вы могли заметить, оценить пытаются именно количество пользователей социальной сети, отсеяв комментарии на YouTube. Видеосервис играет не последнюю роль в жизни Google+, 37 % ее активных пользователей – это пользователи YouTube, которые вынуждены иметь дело с Google+. Теперь понятно, почему в Google так торопились со слиянием. А вот по какой причине Google+ до сих пор тянут за собой, неясно. Данные исследуют лишь публичные сообщения на сервисе, но, кажется, этого достаточно для того, чтобы сделать выводы ***(Никто не использует Google+ // InternetUA (http://internetua.com/nikto-ne-ispolzuet-Google). – 2015. – 23.01).***

***

Согласно данным GlobalWebIndex, в 2014 г. активная аудитория Facebook снизилась на 9 %. Больше всего из Facebook ушло молодых пользователей: самое большое падение отмечено в возрастной группе 16–24 года (11 %) и 25–34 года (12 %).

Если посмотреть данные по регионам, то больше всего в Facebook разочаровались жители Азии: здесь сеть потеряла 12 % активных пользователей.

Куда же люди уходят из Facebook? Например, в Pinterest и Tumblr – они показали рост в 97 % и 95 % соответственно. Tumblr особенно популярен у молодёжи.

Многие люди всё чаще предпочитают социальным сетям мессенджеры и фотосервисы типа Instagram (который, по иронии, принадлежит Facebook). Популярнейший фотосервис в прошлом году смог увеличить свою аудиторию аж на 50 % и стал вторым по росту аудитории после Snapchat (57 %). Сильно возросла и аудитория мессенджера WhatsApp (который тоже принадлежит Facebook) – на 34 %.

Впрочем, пока эти тенденции не мешают Facebook оставаться крупнейшей социальной сетью мира. Если не учитывать Китай, ежемесячная аудитория проекта в прошлом году составляла 1,35 млрд человек.

В исследовании отмечаются, что по мере ухода молодёжи в более новые соцсети и мессенджеры среднестатистический пользователь Facebook стремительно «стареет». Сегодня Facebook по возрасту своей аудитории уступает только LinkedIn. Кроме того, аудитория Facebook относится к числу самых пассивных. 40 % опрошенных пользователей Facebook сказали, что не пишут сообщения и комментарии, а только читают чужой контент.

GlobalWebIndex опросила почти 42 тыс. пользователей в 30 странах ***(В прошлом году Facebook потеряла 9 % активных пользователей // InternetUA (http://internetua.com/v-proshlom-godu-Facebook-poteryala-9---aktivnih-polzovatelei). – 2015. – 25.01).***

***

Facebook тестує новий додаток для бюджетних Android-смартфонів

Соціальна мережа випустила окрему програму Facebook Lite. Вона розроблена спеціально для недорогих Android-пристроїв, які продаються в країнах, що розвиваються.

Як повідомляє techcrunch.com, додаток тихо, непублічно презентували в країнах Азії та Африки – Бангладеш, Непалі, Нігерії, ПАР, Судані, Шрі-Ланці, В'єтнамі та Зімбабве. Там програма тестується з перспективою подальшого поширення.

Водночас наміри Facebook достеменно невідомі. Як зазначає TechCrunch, компанія може спокійно згорнути проект, якщо не віритиме в його успіх.

Додаток був розроблений, щоб пристосувати соцмережу до недорогих Android-пристроїв, а також для користувачів із повільним Інтернетом або 2G.

Випуск Facebook Lite також можна пояснити тим, що на азійському ринку, зокрема в Індії, зростають продажі смартфонів. У багатьох країнах регіону мобільний телефон є (або, як очікується, стане) головною інтернет-платформою для мільйонів користувачів. Android при цьому є найбільш затребуваною операційною системою в країнах, що розвиваються. Пристрої на базі цієї системи коштують від 30 дол.

Наразі Facebook Lite встановило понад 10 тис. користувачів.

Нагадаємо, раніше М. Цукерберг запустив проект Internet.org, у рамках якого планується підключити до Інтернету 5 млрд користувачів.

Завдяки йому вдалося частково забезпечити вільним доступом до мобільного Інтернету Замбію ***(Facebook тестує новий додаток для бюджетних Android-смартфонів // MediaSapiens (http://osvita.mediasapiens.ua/web/social/facebook_testue_noviy_dodatok_dlya_byudzhetnikh_androidsmartfoniv/). – 2015. – 26.01).***

***

Социальная сеть Twitter представила сразу два обновления: возможность создания групповых чатов и встроенный видеоредактор. Новые версии клиентов с поддержкой этих функций уже доступны пользователям Android и iOS, версии для Windows и Mac OS X появятся позднее.

Личные сообщения в Twitter можно было отправлять и ранее, но до настоящего времени их можно было отправлять одному пользователю, и создание чатов было невозможным. Кроме того, в групповые чаты теперь можно отправлять отдельные твиты.

Видеоредактор позволяет снимать, редактировать и выкладывать видеоролики продолжительностью до 30 секунд. Это в 5 раз больше, чем в видеосервисе Vine, который также принадлежит Twitter ***(Twitter получил поддержку групповых чатов и встроенный видеоредактор // InternetUA (http://internetua.com/Twitter-polucsil-podderjku-gruppovih-csatov-i-vstroennii-videoredaktor). – 2015. – 27.01).***

***

Для тех, кто устал от постоянных споров и конфликтов в обычных социальных сетях, появились хорошие новости. Группа энтузиастов из Above Average представила идею создания альтернативной соцсети Jynx, которая сама позаботится о том, чтобы лента новостей пользователя была наполнена только приятными ему постами. На канале YouTube была размещена шутливая презентация. Об этом сообщает CNET.

Авторы видео представили социальную сеть, доведенную до абсурда. «Конечно, общаться на Facebook весело, однако бывает, что сильно устаешь от потока различных мнений в ленте новостей от своих друзей и семьи. Поэтому мы придумали Jynx», – рассказывается в ролике. По мнению создателей видео, новая социальная сеть – это прекрасная альтернатива обычным соцсетям. Здесь пользователи видят только публичные сообщения своих друзей, мнение которых они разделяют.

Разработчики уверяют, что благодаря их идее можно будет отдохнуть от всевозможных дискуссий о политике, спорах о футболе и различных острых проблем. Jynx создаст идиллию, в которой пользователи будут общаться только с теми, кто полностью согласен с ними, а провокаторы и тролли не смогут испортить приятную беседу.

«На Jynx вы не будете видеть посты от вашего дяди, который, быть может, немного не в себе! А если вы и сами такой же, то в вашей ленте будут посты только от вашего дяди. И нет никакой разницы, правы вы или нет», – объясняют авторы. Больше не придется удалять из списка агрессивно настроенных против селфи и котиков друзей, терпеть сообщения от фаната «вражеской» команды или постоянно пролистывать однотипные стихи какого-нибудь «романтика» с разбитым сердцем. Социальная сеть будет разработана таким образом, что сама избавит пользователей от всего этого,

«потому что вы и ваши друзья всегда правы». Правда, есть опасность увидеть в ленте новостей только свои посты, но с собой точно не поспоришь.

Пока Jynx остается лишь идеей. Неизвестно, будет ли проект на самом деле запущен. Однако многие пользователи встретили новость с воодушевлением. «Я сразу же принялась искать это в App Store…очень расстроилась», – сокрушается одна из пользовательниц. «Больше не придется искать аргументы против …тупости! Эта социальная сеть должна быть запущена», – считает подписчик Perceptions100 ***(«Альтернативный Facebook» спасет от троллей и провокаторов // InternetUA (http://internetua.com/alternativnii-Facebook--spaset-ot-trollei-i-provokatorov). – 2015. – 29.01).***

***

Twitter представил веб-версию SDK Digits для создания приложений, позволяющих осуществлять вход в аккаунты по номеру телефона без использования постоянного пароля. Digits SDK даёт возможность разработчикам привязывать свои приложения к партнёрским сайтам и обеспечивать функцию единого входа в систему. В случае, если у пользователя настроен синхронизированный вход в аккаунт из iOS и Android-приложений, он может с лёгкостью осуществить вход в собственный аккаунт на веб-сайте в случае необходимости.

Механизм входа в приложения и на веб-сайты, который обеспечивает Digits SDK, – абсолютно безопасен для пользователя и не позволяет осуществлять повторные несанкционированные заходы в аккаунт по номеру телефона без дополнительного подтверждения. При каждой последующей попытке входа в аккаунт пользователю будет необходимо вводить SMS-пароль.

«Разработчики восхищены возможностью заменить технологию использования паролей на какие-либо другие механизмы безопасного доступа к сайтам и приложениям», – комментирует М. Дакер директор по продукции Digits.

В октябре 2014 г. Twitter представил новую мобильную платформу для разработчиков приложений Fabric. Платформа состоит из трех модульных комплектов, которые призваны решить основные проблемы разработчиков: стабильность, дистрибуцию, доход и идентификацию. Fabric сочетает услуги Twitter, сервиса Crashlytics и сети для управления и обмена рекламой MoPub. Большинство функций требуют всего нескольких строк кода.

Тогда же Twitter анонсировал приложение под названием Digits, которое является частью Twitter Kit. Приложения, созданные с использованием технологии Digits уже доступны в 216 странах мира и на 28 языках ***(Twitter представил SDK Digits для веб-приложений // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_predstavil_sdk_digits_dlya_veb_prilozheniy). – 2015. – 28.01).***

***

Создатель компании Opera Software представил техническую версию своего нового браузера Vivaldi с элементами соцсети.

Программа, выпущенная Й. Стефенсоном фон Течнером для компьютеров под управлением Windows, OS X и Linux, расчитана на продвинутых пользователей. К примеру, команды можно отдавать не только мышью, но и через командную строку браузера.

По словам разработчика, Vivaldi предназначен для тех, кто хочет получить больше от браузера. Помимо функций веб-обозревателя, программа обладает встроенными элементами социальной сети и позволяет налаживать общение между пользователями.

Впрочем, принимая во внимание, что в настоящее время перед нами самая первая, техническая версия продукта, к финалу браузер может существенно преобразиться ***(Создатель Opera выпустил новый браузер с элементами соцсети // Блог Imena.UA (http://www.imena.ua/blog/opera-vivaldi-browser/). – 2015. – 28.01).***

***

Twitter объявил о запуске новой функции «Пока ты отсутствовал» (While you were away) в хронике пользователей iOS-устройств. Нововведение представляет собой показ твитов, пропущенных пользователем в связи с его отсутствием в сервисе в течение какого-то времени.

Для определения того, какие твиты были пропущены, компания использует данные о времени, в течение которого пользователь не использовал мобильное приложение Twitter, и количестве твитов, опубликованных с момента его последнего посещения сервиса. Эта комбинация различна для разных пользователей. Twitter планирует усовершенствовать этот алгоритм по мере более широкого запуска нового функционала.

Функция «Пока ты отсутствовал» будет отображать только твиты от тех аккаунтов, на которые пользователь подписан, и взаимодействует чаще всего, – не обязательно наиболее популярные твиты в сервисе. Другими словами, Twitter пытается предсказать, твиты каких аккаунтов интересны конкретному пользователю, независимо от их популярности в рамках социальной сети.

Движущей силой этого нововведения является желание Twitter усилить вовлечённость пользователей во взаимодействие с сервисом. Это – не первый эксперимент компании в этом направлении. Сервис микроблогов уже показывает в хронике пользователей твиты от тех аккаунтов, на которые они не подписаны.

Кроме того, в ноябре 2014 г. компания позволила пользователям делиться твитами в личных сообщениях, чтобы заставить их чаще общаться посредством мобильного приложения социальной сети.

В течение последних нескольких недель функция «Пока ты отсутствовал» тестировалась на ограниченной выборке пользователей. В настоящее время нововведение запущено только для пользователей iOS-устройств. В ближайшее время будет произведён запуск этого функционала для Android. В будущем он также будет внедрён в десктопной версии Twitter.

Своими планами по предстоящему запуску функции While you were awa» и другимиTwitter поделился в ноябре 2014 г. во время телефонной конференции для аналитиков Analyst's Day Conference ***(Twitter запустил функцию «Пока ты отсутствовал» для пользователей iOS-устройств // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_zapustil_funktsiyu_poka_ty_otsutstvoval_dlya_polzovateley_ios_ustroystv). – 2015. – 28.01).***

***

Крупнейшая в мире соцсеть Facebook начала тестировать функцию Place Tips, с помощью которой пользователи будут получать подсказки о местах, где они находятся. Об этом говорится в блоге Facebook.

Идея функции такова, что когда пользователь приближается к достопримечательности, магазину, ресторану или другому месту, которое потенциально может вызвать его интерес, Facebook отправит ему push-оповещение розового цвета.

Кликнув на сообщение, пользователь сможет увидеть фотографии места, его описание, подписаться на его Facebook-страницу, а также узнать, кто из его друзей тоже был здесь и даже фотографировался. Кроме того, он увидит запланированные в этом месте мероприятия и новости.

По сути, отмечает Business Insider, Facebook отображает официальную страницу того или иного места на мобильных в новом формате – в виде напоминания с геолокационной привязкой.

Функция будет подключена в мобильных приложениях по умолчанию, поэтому для ее отключения потребуется зайти в настройки устройства. Facebook подчеркнула, что открытие информационной карточки-подсказки не влечет за собой автоматический чекин или другую публикацию, позволяющую выяснить местонахождение пользователя.

Однако функция отслеживает перемещения пользователя с помощью GPS и Wi-Fi. Кроме того, Facebook также тестирует Bluetooth-биконы, чтобы рассылать оповещения, когда пользователь не подключен к Интернету.

Функция Place Tips конкурирует со специализированными сервисами Foursquare и Yelp. Однако Facebook поступила мудро, не выводя ее сразу в отдельное приложение и не бросая в прямую конкуренцию.

В настоящее время тестирование функции ведется в Нью-Йорке в районах, традиционно популярных среди туристов – в Центральном парке, на Таймс-сквер, Бруклинском мосту, около статуи Свободы и в аэропорту JFK ***(Facebook расскажет пользователю о местах вокруг него // InternetUA***

(http://internetua.com/Facebook-rasskajet-polzovatelua-o-mestah-vokrug-nego). – 2015. – 30.01).

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

У соціальній мережі мікроблогів Twitter стартував хештег, який має розповісти англомовній частині світу про трагедію, яка сталася в українському Маріуполі.

Хештег #WorldwakeupRussiainvadedUkraine на момент написання новини зайняв перше місце у всеукраїнських трендах Twitter, а до пятірки увійшли також #Mariupol і #Мариуполь.

Новий хештег активно просувається завдяки використанню прес-службою Президента України П. Порошенка ***(#WorldwakeupRussiaInvadedUkraine: як розповісти світу про трагедію в Україні // UkrainianWatcher (http://watcher.com.ua/2015/01/24/worldwakeuprussiainvadedukraine-yak-rozpovisty-svitu-pro-trahediyu-v-ukrayini/). – 2015. – 24.01).***

***

Українськими волонтерами, що допомагають солдатам у зоні АТО, була ініційована акція, згідно з якою за кожен репост запису на Facebook на рахунок благодійників буде перераховано 2 грн. За добу кількість поширень цього запису перевищила 50 тис.

Автором спонсорської допомоги, який надасть суму в понад 100 тис. грн, залишиться неназваний меценат. Отримані кошти будуть використані для допомоги бійцям 81-ї бригади, які воюють у зоні АТО поблизу Донецького аеропорту. Список потреб буде оприлюднено відомим волонтером Т. Ричковою, яка перебуває у зоні конфлікту і збирає списки необхідної амуніції, продуктів та речей.

На момент написання новини пост зібрав 52 879 поширень на Facebook.

Окрім того, будь-хто може допомогти власними коштами на краудфандинговій платформі Народного проекту, де збирають кошти на різноманітні волонтерські допомоги для воїнів у зону АТО ***(Українські волонтери виміняють 50 тисяч поширень на Facebook на 100 тис. гривень // UkrainianWatcher (http://watcher.com.ua/2015/01/23/ukrayinski-volontery-vyminyayut-50-tysyach-poshyren-na-facebook-na-100-tys-hryven/). – 2015. – 23.01).***

***

Команда волонтерського освітнього проекту «Мова – ДНК нації» запустила новий онлайн-ресурс для вдосконалення знань української мови. На сайті зібрані авторські ілюстрації, завдяки яким можна пригадати основні правила правопису, дізнатися нові фразеологізми й синоніми, навчитися правильно наголошувати слова й позбутися росіянізмів. Крім того, зареєстровані користувачі сайту мають можливість перевіряти знання й одночасно навчатися, виконуючи тематичні вправи.

Ініціатором проекту стала Н. Клименко, PR-фахівець, яка вирішила створити сторінку в соціальній мережі, щоб ділитися знаннями й популяризувати українську мову.

«Усе починалося зі сторінки “Мова – ДНК нації” у Facebook, створюючи яку, я розуміла, що в наш час люди не хочуть читати складні правила й довго розбиратися. Саме тому вирішила готувати дуже лаконічні тексти й гарно їх оформлювати. На щастя, мій чоловік захопився моєю ідеєю й придумав нашого героя – розумного Лепетуна. Я почала підбирати теми, писати тексти, а він – створювати до них ілюстрації. За дев’ять місяців на нашу сторінку підписалося майже 20 тис. людей. Ми переконалися, що багато українців прагнуть вивчати мову, але не мають сучасних ресурсів для цього», – розповіла Н. Клименко, засновниця проекту «Мова – ДНК нації».

За перші 10 днів на сайті зареєструвалося понад 4 тис. осіб з різних куточків України, найактивнішими користувачами є мешканці Києва, Львова, Харкова, Дніпропетровська, Одеси, Івано-Франківська, Запоріжжя, Тернополя й Черкас. Сайт відвідують і мешканці інших країн – Росії, Німеччини, США, Польщі, Великобританії, Туреччини, Канади, Італії тощо.

Наразі команда проекту працює над удосконаленням сайту, розробкою застосунку для iPhone, Android і Windows Phone. Крім того, у майбутньому вони планують зробити посібник з ілюстраціями й серію анімаційних фільмів з головним персонажем.

«У мене є мрія. Я хочу, щоб в Україні було модно говорити українською. Звичайно, можна нарікати на владу, вимагати від неї активніше підвищувати популярність національної мови, сприяти її всебічному вивченню. Але Майдан навчив мене, що потрібно не лише вимагати, а й віддавати – робити щось корисне для країни. Я намагаюся передати людям свою захопленість мовою. Вірю, що чим краще вони її знатимуть, тим більше пишатимуться нею», – прокоментувала Н. Клименко ***(Волонтери розробили ресурс для вдосконалення знань української мови // InternetUA (http://internetua.com/volonteri-rozrobili-resurs-dlya-vdoskonalennya-znan-ukra-nsko--movi). – 2015. – 24.01).***

***

Со времени революции в Украине новые власти часто демонстрируют открытость и готовность общаться с пользователями напрямую в социальных сетях. Но не обходится и без «злоупотреблений». На днях SMM-

специалисты, ведущие Twitter-аккаунт Президента П. Порошенко, провели массовый бан, причем под блокировку попадали даже лояльные к власти пользователи, осмелившиеся высказывать критические комментарии. Редакции пока не удалось связаться с пресс-службой Президента для комментариев, пишет AIN.UA (http://ain.ua/2015/01/20/559540).

Такое поведение вызвало бурную реакцию в украинском Twitter-сообществе, был запущен даже тег #ПорохЗвільниПридурківЗПресслужби. Собственно, по этому тегу можно наблюдать всю картину пользовательского негодования.

Кто-то из пользователей искренне возмущается, кто-то привычно троллит.

Но, вместо того, чтобы как-то объясниться перед аудиторией, SMM-щики решили и дальше придерживаться «жесткого курса». Они напомнили три причины, через которые пользователи могут получить бан: оскорбление, нецензурная лексика, неуважение к суверенитету.

Такой очевидный прокол в SMM-политике нужно было признать, возможно – отшутиться, ведь это Интернет, а не пресс-конференция, и здесь свои законы общения с пользователями. «То что SMM-щики П. Порошенко начали банить за любую критику без разбора в том числе лояльную к нему аудиторию – большая ошибка, но ошибки бывают, стоило просто признать и отшутиться, но они решили пойти дальше. Такое впечетление, что люди, которые ведут аккаунт, совсем не чувствуют блогосферу», – считает популярный киевский блогер А. Барабошко (Крус Крус).

Справедливости ради некоторые пострадавшие уже отчитались о том, что аккаунт Президента их разбанил ***(Президентский банхаммер: в Twitter-аккаунте Петра Порошенко массово банят за критику // AIN.UA (http://ain.ua/2015/01/20/559540). – 2015. – 20.01).***

***

Десятки тисяч користувачів соцмереж долучилися до акції підтримки Н. Савченко. Хештег #FreeSavchenko 27 січня одним з найпопулярніших в українському сегменті цього сервісу.

Лише за 24 години хештег #FreeSavchenko використало близько 60 тис. користувачів у Twitter. Повідомлення з’являються зі швидкістю 100–200 штук на хвилину.

Активно поширюється хештег у «ВКонтакті» та Facebook. Там з’являються фото з акцій на підтримку Надії з різних країн світу, фотожаби та плакати.

27 січня Н. Савченко написала листа до колег по ПАРЄ з приводу свого утримання. Вона наголосила, що її утримують за злочини, яких вона не скоювала, незважаючи на відповідні докази, надані захистом.

«Я винна тільки у тому, що захищала свою Батьківщину, свій український народ, якому давала присягу, свободу і благополуччя моєї землі», – написала вона ***(#FreeSavchenko: користувачі соцмереж***

вимагають звільнення української Надії // UkrainianWatcher (http://watcher.com.ua/2015/01/26/freesavchenko-korystuvachi-sotsmerezh-vymahayut-zvilnennya-ukrayinskoyi-nadiyi/). – 2015. – 27.01).

***

Отныне профессиональные разъяснения и комментарии от руководителей Главного управления ГФС в Запорожской области к новациям налогового законодательства, которые вступили в действие с 2015 г., доступны широкой общественности пользователей сети Интернет.

Об этом сообщает пресс-служба регионального управления фискальной службы, пишет Readandtrust.info (http://readandtrust.info/component/k2/item/6224-zaporozhskie-fiskaly-osvaivayut-sotsseti/).

Соответствующие видеообращения размещены на канале YouTube и на странице ГУ ДФС области в Facebook.

Так, разъяснение отдельных положений налоговой реформы, в частности, об особенностях взимания налога на имущество рассказывает первый заместитель начальника ГУ ГФС в Запорожской области Е. Фоменко. А о новых положениях налогового законодательства по акцизному налогу говорит заместитель начальника ГУ ГФС в Запорожской области Р. Афонов.

Посмотреть видеокомментарии руководства ГУ ГФС в Запорожской области можно по адресам:

https://www.youtube.com/channel/UCM9GDhiRJWMQZ-FcjLqsH8

и https://www.facebook.com/pages/Головне-управління-ДФС-у-Запорізькій-області/288573044665105?fref=ts

Кроме того, на страницах ГФС Запорожье в YouTube и Facebook можно узнать последние новости в работе фискальной службы ***(Запорожские фискалы осваивают соцсети // Readandtrust.info (http://readandtrust.info/component/k2/item/6224-zaporozhskie-fiskaly-osvaivayut-sotsseti/). – 2015. – 30.01).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Рекламодателям «ВКонтакте» и администраторам сообществ доступен новый специальный формат для продвижения сообществ в новостной ленте соцсети. Новый формат позволяет рекомендовать страницы и группы в разделе «Мои новости» – между обновлениями от друзей и сообществ, на которые подписан пользователь.

Формат поддерживает более 20 видов таргетинга, что позволяет охватывать только нужную аудиторию. Также поддерживается поведенческий таргетинг и ретаргетинг «ВКонтакте».

«Новый формат идеально подходит для организаций, которые стремятся быть в контакте со своими потребителями. По нашим оценкам, использование этого формата сильно облегчает привлечение подписчиков в сообщество бренда или контент-проекта», – отметил А. Усманов, евангелист соцсети.

Н. Истомина, community-менеджер Likeni.ru и SEOnews.ru:

«Это отличная новость. Такой формат рекламы должен стать очень эффективным, так как является ненавязчивым, так как органично встраивается в новостную ленту пользователей. Большое преимущество он имеет и перед форматом таргетированной рекламы, позволяя избежать отравляющего жизнь многих интернет-маркетологов эффекта “баннерной слепоты”, который заключается в том, что пользователи просто не обращают внимания на мелькающие на периферии зрения небольшие текстово-графические блоки.

Новый формат продвижения должен успешно работать на привлечение подписчиков, но меня, конечно, беспокоит вопрос ценообразования» ***(Новый формат рекламы сообществ во «ВКонтакте» // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/novyy_format_reklamy_soobschestv_vo_vkontakte). – 2015. – 23.01).***

***

WSJ сообщает, что социальная сеть Facebook приобрела компанию Quickfire Networks, которая специализируется на технологиях обработки и сжатия видеозаписей.

Издание отмечает, что приобретение Quickfire может означать концентрацию Facebook на видеоконтенте. По утверждению представителей Quickfire, технология компании позволяет быстро конвертировать между собой различные видеоформаты и передавать их по каналам связи с низкой пропускной способностью без потерь в качестве.

Facebook стремится стимулировать своих пользователей загружать видео напрямую на сайт, а не использовать сторонние платформы – например, YouTube. Таким образом, компания может продлить время нахождения пользователей на сайте и более гибко контролировать размещение рекламы.

В 2014 г. Facebook позволил видеороликам в новостной ленте пользователя запускаться автоматически. К настоящему времени видео на Facebook в совокупности набирает в среднем более миллиарда просмотров ежедневно. В августе 2014 г. среди пользователей настольных компьютеров видео на Facebook обогнало ролики на YouTube по просмотрам, однако соцсеть до сих пор отстаёт по числу просмотров на мобильных устройствах.

Ранее в прошлом году Facebook приобрела компанию LiveRail, специализирующуюся на видеорекламе. Ранее о сделке с Facebook объявил и стартап Wit.ai, который занимается технологиями распознавания речи ***(Компания Facebook приобрела видеоплатформу Quickfire Networks // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/kompaniya_facebook_priobrela_videoplatformu_quickfire_networks). – 2015. – 15.01).***

***

Доля кликов рекламных объявлений в социальной сети Facebook существенно сдвинулась в сторону мобайла, чего нельзя сказать о конверсии в покупки, – сообщает AdWeek со ссылкой на исследование компании Marin Software, пишет Marketing Media Review (http://mmr.ua/news/id/bolshaja-dolja-reklamnyh-klikov-na-facebook-ushla-v-mobajl-a-konversija-ostalas-na-desktopah-42844/).

Несмотря на то, что в четвертом квартале 2014 г. 63 % кликов на рекламные посты в Facebook были сделаны с мобильных устройств, только 34 % реальных действий – будь то покупка, загрузка продукта или заполнение анкеты – совершались с планшетов и смартфонов.

Эти результаты, полученные в ходе ежеквартального исследования Global Online Advertising Index, означают, что более двух третей конверсии с рекламных объявлений, размещенных в социальной сети, приходится на стационарные компьютеры. И это в то время, когда взаимодействие с платформой сместилось преимущественно в сторону мобайла ***(Большая доля рекламных кликов на Facebook ушла в мобайл, а конверсия осталась на десктопах // Marketing Media Review (http://mmr.ua/news/id/bolshaja-dolja-reklamnyh-klikov-na-facebook-ushla-v-mobajl-a-konversija-ostalas-na-desktopah-42844/). – 2015. – 15.01).***

***

ТОП-10 фатальных ошибок, которые могут навредить странице бренда в Facebook

Какие ошибки совершают бренды в Facebook и как избежать их в будущем? Ниже описаны 10 распространенных ошибок в Facebook, которые могут нанести вред вашей странице, пишет Marketing Media Review (http://mmr.ua/news/id/top-10-fatalnyh-oshibok-kotorye-mogut-navredit-vashej-stranice-v-facebook-42892/).

1. Отсутствие отличия от других страниц.

Вы четко говорите о том, что отличает вашу компанию от конкурентов? Если нет, вы идете по опасному пути.

Часто используется тактика не уникального маркетинга, когда компании смотрят на конкурентов, что у них работает в Facebook, и воспроизводят это на своей странице. К сожалению, в такой тактике есть ряд недостатков. Выделиться в онлайн среде довольно трудно. Если ваш

маркетинг шаблонный, вы сводите свои шансы к тому, чтобы выделиться на фоне остальных, к нулю.

Используйте цвета бренда, шрифт и общий стиль на каналах в социальных сетях, включая и Facebook. Это позволяет создать последовательный потребительский опыт.

2. Нет специально созданной обложки.

Ваша обложка на Facebook – это первое, что видят пользователи, когда заходят на вашу страницу. Привлекательная обложка с хорошим дизайном поможет вам привлечь их внимание и поощрит их к действию.

Подумайте о вашей обложке как об онлайн билборде!

Предпочтете ли вы ничем не примечательное фото, представляющее вашу страницу, или обложку, которая сразу же расскажет о том, кто вы и что вы?

Используйте обложку, чтобы поделиться своим продуктом, сервисом или историей, важно чтобы вы поделились тем, что делает вас уникальными.

3. Нет брендированной графики.

Кроме обложки важно использовать фото, созвучное вашему бренду, в постах.

4. Отсутствие рекламных постов Facebook.

Рекламные объявления Facebook могут быть умным дополнением к вашему существующему рекламному бюджету. Реклама Facebook позволяет вашей странице расти без внушительных расходов. Использовали ли вы Power Editor? Если нет, вы теряете возможность быть более точными с рекламным таргетингом.

Вы не только можете нацеливать свою кампанию на определенный рынок благодаря возрастным группам, полу, городам, или странам, но и проводить несколько кампаний.

Если вы продвигаете рекламную кампанию без определенных целей – это рецепт неудачи.

Спросите себя, чего вы хотите достичь благодаря рекламе Facebook, прежде чем вы создадите рекламное сообщение, потратите деньги и не увидите впечатляющие результаты.

5. Страница в Facebook не соответствует маркетинговой стратегии.

Вы размещаете посты без плана?

У вас некачественный контент и нет специально созданных изображений?

Если это про вас, вам необходима Facebook стратегия, которая соответствует вашим общим маркетинговым целям. Имея стратегию, вы размещаете посты целенаправленно, а не бессистемно.

6. Отсутствие взаимодействия с сообществом в Facebook.

Одна из грубейших ошибок, которые многие компании продолжают совершать, это следовании стратегии «размести и убеги». Это видно по тому, как размещаются посты на странице, и никто не возвращается, чтобы взаимодействовать с фанатами. Ключ к взаимодействию прост.

Создайте стратегию – как и когда вы будете размещать посты, и систему для последующего обращения.

Три способа взаимодействовать с фанатами:

Приложите особые усилия, чтобы ваши фанаты почувствовали себя особенными. Задайте вопросы, которые углубляют ваши отношения и отвечайте глубоко и вовремя.

Обращайте внимание на то, что говорят ваши фанаты. Какие их потребности и как вы можете решить их проблемы? Умение слушать это искусство, которое оправдает себя в последующих годах.

Оставайтесь вовлеченными в разговор и всегда предоставляйте релевантный и насыщенный контент. Максимизируйте видимость, размещая посты часто и систематически.

7. Мало информации о компании.

Ваш раздел в Facebook «о компании» рисует образ о вашей компании. Поэтому это важный шаг при оформлении и оптимизации вашей страницы.

Советы, как правильно заполнить раздел «о компании»

Добавьте детали об основании. Как и когда была основана ваша компания. Какова ее миссия и что двигает вашей компанией ежедневно?

Пользователи быстро пробегут глазами ваш контент. Добавьте самую важную информацию в первом параграфе.

Добавьте ключевые слова, термины и фразы, которые использовали бы все, кто искал бы вашу компанию, продукты или услуги. Ключевые слова важны в социальных медиа так же, как и для вашего веб-сайта или блога.

Ответьте на вопросы, которые важны для вашего сообщества, чтобы они могли принять обоснованное решение. Этот раздел поможет вам выделиться на фоне остальных компаний.

Дайте короткий обзор ваших продуктов или услуг. Как они решают проблемы ваших клиентов и что они могут ожидать?

Поделитесь успешными историями и предоставьте отзывы ваших клиентов, которым вы помогли.

Не используйте отраслевой жаргон в этом разделе. Ваш потребитель не работает в вашей отрасли, поэтому не говорите с ними так, как будто они там работают. Ваш язык должен быть простым для чтения.

8. Вы не делитесь последовательным контентом.

Делиться последовательным контентом на странице в Facebook может быть сложно. Посмотрите на контент, который вы создавали в прошлом, или на существующий контент, который вы используете на других платформах. Теперь подумайте, как вы можете использовать его для новой аудитории.

9. Вы не используете настраиваемые вкладки.

У вашей страницы есть стандартные и настраиваемые вкладки. Вы можете использовать настраиваемые вкладки для того, чтобы разместить релевантные детали относительно вашей компании. Например, вы недавно написали е-книгу, и хотите, чтобы она стала доступной. Создание такой вкладки позволит вам направить фанатов прямо на специальный контент в

рамках вашей страницы, позволив любому пользователи получить доступ к материалу и скачать его.

Вы можете создать удивительные вкладки с Shortstack, Heyo и другими.

10. Отсутствует четкий призыв к действию.

Никогда не думайте, что ваши фанаты знают, какой шаг по вашему мнению они должны предпринять. Не предоставляйте действие фанатов воле случая.

Например, вы делитесь постом из блога. Вместо того, чтобы просто разместить ссылку с заголовком вашего поста, дайте фанатам тизер вашего контента.

Если заголовок вашего поста: «Визуальные маркетинговые стратегии, которые увеличат посещение страницы Facebook», призыв к действию может быть следующим:

Вы используете визуальный маркетинг для создания притягивающих взгляд изображений, которые привлекают внимание фанатов? Зайдите по ссылке и посмотрите, затем оставьте свой комментарий. Я хочу узнать, что вы думаете об этом!

Другие четкие призыва к действию могут включать:

Подпишитесь сейчас

Зарегистрируйтесь здесь

Начните сегодня

Узнайте больше

Нажмите здесь, чтобы загрузить

Свяжитесь с нами

Удостоверьтесь, что вы ясно представляете, как вы хотите, чтобы фанаты взаимодействовали с вашей страницей, и каким должен быть следующий шаг.

И напоследок:

Не все ошибки в Facebook будут фатальными – но большинство могут стать причиной огромной потери момента или возможности.

Прежде чем разместить следующий пост, посмотрите на вашу страницу.

Какие ошибки вы видите?

Приложите усилия сегодня, чтобы преодолеть эти ошибки.

Продолжайте с позитивным и продуктивным настроем!

Р. Рэдис, CEO Rebekah Radice LLC, диджитал маркетингового агентства, реализующего интегрированные онлайн-стратегии ***(ТОП-10 фатальных ошибок, которые могут навредить странице бренда в Facebook // Marketing Media Review (http://mmr.ua/news/id/top-10-fatalnyh-oshibok-kotorye-mogut-navredit-vashej-stranice-v-facebook-42892/). – 2015. – 20.01).***

***

Видеореклама в Facebook против YouTube. Как соцсеть может стать главным победителем в Super Bowl

В декабре агентство Shareability выпустило видео для компании Freshpet. В рекламе были показаны собаки, копирующие поведение людей во время праздничного ужина. Ролик быстро стал вирусным, что неудивительно. Откровение случилось, когда стал заметен разрыв между количеством просмотров в YouTube и количеством просмотров в Facebook, пишет Marketing Media Review (http://mmr.ua/news/id/videoreklama-v-facebook-protiv-youtube-kak-socset-mozhet-stat-glavnym-pobeditelem-v-super-bowl-42898/).

На YouTube видео заработало порядка 7,5 млн просмотров. На Facebook – около 20 млн, пишет Mashable.com. Благодаря подобной статистике может оказаться так, что впервые в истории Суперкубка реклама на Facebook затмит рекламу на YouTube.

Так что неудивительно, что многие рекламодатели, участвующие в Super Bowl (в американском футболе название финальной игры за звание чемпиона Национальной футбольной лиги (НФЛ) США. – Прим. ред.), заинтересованы в нативной рекламе в Facebook. Wix, новичок в списке рекламодателей Суперкубка, разместил свои тизеры в социальной сети в нативном формате Facebook вместо того, чтобы повесить ссылку на YouTube.

«Думаю, у YouTube нет никакой коммуникационной сети, а Facebook с легкостью ее вам предоставляет», – говорит Э. Мейсон из Wix.

Также нативный видеоформат для своих тизеров в Facebook будет использовать GoDaddy , Anheuser-Busch и Carnival Cruise Lines.

Почему рекламодатели уходят в Facebook?

Facebook последние два года безжалостно расправлялась с органическими постами от брендов в новостных лентах пользователей, снижая органический охват. Но видео оставляет компаниям небольшую лазейку. Поскольку этот формат очень популярен, ролики показываются чаще остальных постов. Рекламодатели говорят, что видео, размещенное с помощью нативного плеера Facebook, получает в шесть раз больше взаимодействия, чем ссылка на видео, размещенное в YouTube. Facebook не смогла подтвердить эти данные и не предложила для сравнения собственную статистику.

Почему? Видео в Facebook определенно выглядит гораздо лучше. А еще нативное видео в Facebook проигрывается автоматически – в отличие от ссылки на ролик в YouTube. «Facebook целенаправленно сокращает появление брендов на YouTube», – говорит аналитик eMarketer Д. Уильямсон.

По словам менеджера по рекламным продуктам Facebook Ф. Симо, дело не в том, что появление в YouTube неэффективно, а в том, что пройти по ссылке для многих пользователей становится проблематичным и неудобным.

Соблазн видео

Привлекательность видеороликов в Facebook понять легко. За прошлый год количество видеопостов на душу пользователей возросло на 75 % в мире и на 94 % в США. Согласно статистике, 50 % пользователей ежедневно заглядывают в Facebook, чтобы посмотреть как минимум один ролик. В итоге видео набирает зрителей в четыре раза больше, чем вся аудитория Суперкубка.

Это большая удача для соцсети, так как видео приносит больше дохода, чем баннерная реклама. По данным eMarketer, средняя CPM (оплата за 1000 показов) для видеорекламы составляет 25 дол. США, тогда как для баннерной рекламы – всего 11 дол. США. Для таргетинговых кампаний цены еще выше.

Помимо того, что видеопосты помогают в продажах рекламы, они еще и удерживают людей от перехода на другие сайты, что увеличивает общие показатели социальной сети.

Критика

Однако в видеорекламе есть и свои проблемы. Не все рекламодатели покупаются на впечатляющие цифры по просмотрам видео в Facebook. Проблема в том, что Facebook измеряет количество просмотров лишь по первым трем секундам автоматического проигрывания. Это гораздо меньше, чем показатели, которыми пользуется YouTube (данные о системе измерений не разглашаются). Однако представитель Facebook говорит, что трех секунд вполне достаточно: «В редком случаете вы остановите интересный рассказ через три секунды после его начала».

Также сотрудник сети утверждает, что рекламодатели могут увидеть, как много людей продолжили или прекратили смотреть видео – вплоть до одной секунды.

Еще одно критическое замечание в адрес Facebook заключается в том, что ролики, появившиеся в социальной сети, перестают быть популярными с той же скоростью, с какой однажды стали вирусными, замечает Mashable.com. Ф. Симо признает тот факт, что хиты на Facebook – не долгоиграющая история. К примеру, 12 января Marvel выпустила на Facebook свой трейлер к фильму «Мстители: Эра Альтрона». Поначалу показатели просмотров на YouTube и Facebook были примерно одинаковыми, но потом количество просмотров на YouTube достигло отметки в 18 млн, а в Facebook остановилось на 6,7 млн. То есть кампания была не столь удачной, как для FreshPet.

У британской розничной сети John Lewis были похожие показатели в случае с рождественской рекламной кампанией 2014 г. В начале ноября, почти сразу после запуска, реклама, загруженная с помощью нативного плеера Facebook, получила 4 млн просмотров. В настоящее время она насчитывает 6 млн, а вот на YouTube – 22 млн. Так что опытные рекламодатели скорее будут использовать Facebook как способ подкрепить свою телевизионную рекламу, а YouTube – как поисковый канал.

Что Facebook собирается делать дальше

Самой большой жертвой перемен в Facebook является YouTube. Хотя сайт не обязательно будет страдать сильно, ведь популярность видеоформата растет повсеместно. Информированные источники утверждают, что лишь небольшая часть трафика YouTube приходится на долю социальных сетей. Однако YouTube как минимум потерял часть рекламодателей, и нативный плеер Facebook скорее всего будет препятствовать дальнейшему развитию платформы.

Суперкубок станет для Facebook главным призом и, возможно, укрепит мнение маркетологов о том, что социальная сеть играет важную роль для вторых экранов и просмотров в реальном времени – сегментах где ранее господствовал Twitter, который, кстати, также планирует запустить свой видеоплеер.

Правда, Facebook может не только давать, но и отнимать. Маркетологи, потратившие немало времени и денег на создание брендированных страниц в Facebook, заговорили о недобросовестности социальной сети, когда она слегка подправила свой алгоритм, сделав органические посты менее заметными. Посыл был следующим: хотите, чтобы посты были более заметными – платите за рекламу. Такая же история может повториться и с видеопостами.

Все возможно, хотя представитель Facebook утверждает, что никто не планирует строить козни. «Мы не можем гарантировать, что алгоритм не изменится. Но мы всегда призывали маркетологов оценить ROI, которые они получают», – говорит она ***(Видеореклама в Facebook против YouTube. Как соцсеть может стать главным победителем в Super Bowl // Marketing Media Review (http://mmr.ua/news/id/videoreklama-v-facebook-protiv-youtube-kak-socset-mozhet-stat-glavnym-pobeditelem-v-super-bowl-42898/). – 2015. – 20.01).***

***

Мировая экономика получила от Facebook около 227 млрд дол.

Всего за несколько лет Facebook смогла превратиться из университетского стартапа в крупнейшую в мире социальную сеть, которая оказывает ощутимое влияние на мировую экономику. О какой степени воздействия идет речь, выяснили в консалтинговой компании Deloitte & Touche, которая провела исследование по заказу Facebook.

По оценкам аналитиков, в 2014 г. вклад Facebook в глобальную экономику измерялся денежным показателем в размере 227 млрд дол. и 4,5 млн созданных рабочих мест. В указанную сумму вошла экономическая отдача от корпоративных учетных записей в Facebook, использования приложений и игр в социальной сети и стимулируемого соцсетью спроса на мобильные устройства и онлайн-сервисы.

По словам операционного директора Facebook Ш. Сэндберг, социальная сеть помогает в создании новых компаний, представляющих

самые различные сферы – от моды до спорта ***(Мировая экономика получила от Facebook около 227 млрд долларов // InternetUA (http://internetua.com/mirovaya-ekonomika-polucsila-ot-Facebook-okolo-227-mlrd-dollarov). – 2015. – 21.01).***

***

Англоязычные пользователи заметили, что Google начал показывать социальные профили брендов на панели выдачи сети знаний (Knowledge Graph). Например, при поиске по запросу [Wendy] в этом блоке отображаются ссылки на страницы бренда в Facebook, Twitter, YouTube, LinkedIn и Google+.

Аналогичные результаты появляются при поиске, связанном с такими торговыми марками, как Chase, Nike, Starbucks и любыми другими брендами в США.

Нововведение облегчает потребителям поиск информации о брендах. Теперь им не нужно пересматривать многочисленные поисковые результаты в поисках нужных данных.

С другой стороны, это также полезно для компаний, учитывая тот факт, что нововведение не ограничивается только крупными брендами, упомянутыми выше.

Google предлагает бизнесам новую микроразметку, которая даёт возможность поисковой системе отобразить социальные профили их брендов на панели выдачи Сети знаний. Представитель Google З. Бахаджи сообщила об этом в Google+.

Теперь поисковик отображает на панели сети знаний профили брендов в Facebook, Twitter, Google+, Instagram, YouTube, LinkedIn и Myspace. Кроме того, лидер поиска предлагает компаниям разметить данные о дополнительных социальных профилях, если они есть, но в настоящее время они не появляются в выдаче сети знаний.

Согласно информации Google, алгоритмы поисковой системы обрабатывают профили, которые указаны компаниями с помощью микроразметки, и отображают наиболее релевантные из них, основываясь на запросах отдельных пользователей. Таким образом, разные люди могут видеть разные результаты. Кроме того, Google показывает только проверенные профили брендов на тех сайтах, где функционирует процесс подтверждения данных.

В русскоязычной выдаче сети знаний Google это нововведение пока не запущено.

Напомним, что в сентябре 2014 г. поисковик начал убирать информацию Google+ из панели выдачи сети знаний.

В ноябре на панель выдачи сети знаний были добавлены ссылки на профили в социальных сетях для запросов, связанных с персоналиями знаменитостей и общественных деятелей ***(Google добавил социальные профили брендов на панель англоязычной выдачи сети знаний //***

ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/internet_dlya_chaynikov/novosti/google_dobavil_sotsialnye_profili_brendov_na_panel_angloyazychnoy_vydachi_seti_znaniy). – 2015. – 22.01).

***

Pinterest неинтересна рекламодателям

В то время как рекламная стратегия социальной сети Pinterest только обретает форму, эксперты рынка считают, что маркетинговый потенциал ресурса на сегодняшний день незначителен, – сообщает MediaPost со ссылкой на данные аналитического центра Forrester.

«Многие маркетологи просто не видят перспектив для успеха своих кампаний в Pinterest, – пишет аналитик Forrester Н. Эллиотт в своем новом отчете. – Менее половины крупных имен представлены на брендированных бордах в этой соцсети, и даже они не понимают, какой контент им постить, так как имеют немногочисленных фоловеров и незначительное взаимодействие с аудиторией».

К примеру, у Coca Cola всего около 5 тыс. фоловеров в Pinterest, и последние 50 пинов компании получили в среднем лишь по 11 репинов каждый.

После восьми месяцев бета-тестирования социальная сеть наконец объявила запуске в начале этого года формата рекламы для брендов Promoted Pins.

Однако, согласно оценке Forrester, новый проект пока не способен предоставить рекламодателям достаточно репрезентативных данных по таргетингу.

«Маркетинговая ценность Pinterest, если и существует, то только в будущем, но не в настоящем», – утверждают эксперты Forrester ***(Pinterest неинтересна рекламодателям // Marketing Media Review (MMR) (http://mmr.ua/news/id/pinterest-neinteresna-reklamodateljam-42896/). – 2015. – 20.01).***

***

Компания ChangeTip, приложение которой позволяет совершать микроплатежи в виртуальной валюте Bitcoin в социальных сетях, добавила Facebook в список поддерживаемых платформ, пишет Блог Imena.UA (http://www.imena.ua/blog/changetip-now-allows-facebook/).

Теперь чтобы отправить перевод в виртуальной валюте в Facebook пользователю достаточно подключить свою учётную запись к панели настроек ChangeTip.

После этого опция проведения микроплатежей в Bitcoin через ChangeTip появится рядом с полем «Отправить». Отметим, что приложение ChangeTip уже работает с Twitter и Reddit.

Разработчики назвали интеграцию с крупнейшей в мире социальной сетью заметным шагом вперёд. Благодаря сотрудничеству с Facebook компания ChangeTip планирует привлечь ещё больше Bitcoin-юзеров со всего мира.

А пользователи платных сервисов Microsoft, начиная с 11 декабря 2014 г., могут пополнять свой счёт с помощью цифровой валюты Bitcoin. Функция пока что доступна только для американских учётных записей.

Тем временем, компания Coinkite предоставила бесплатный сервис для пользователей Bitcoin – кошельки с функцией мультиподписи. Любые операции с деньгами, лежащими на кошельке, защищённом мультиподписью, будут подписываться минимум двумя из трёх секретных ключей ***(Facebook присоединилась к сервису онлайн-платежей в Bitcoin // Блог Imena.UA (http://www.imena.ua/blog/changetip-now-allows-facebook/). – 2015. – 21.01).***

***

Вот пять причин, чтобы представить ваше предприятие в Instagram, Pinterest, Vine, YouTube и других визуальных социальных сетях.

1. Не нужно недооценивать силу визуализации.

Наш мозг обрабатывает визуальные сигналы в 60 тыс. раз быстрее, чем текстовые. Обычно пользователю требуется всего 3 секунды, чтобы решить, останется ли он на вашем сайте и будет ли следить за вашей работой в социальных сетях. Если вы хотите по максимуму использовать эти три секунды, изображения и видео станут для вас лучшим подспорьем. Они вместе с грамотно составленными подписями помогут вам создать историю, которая привлечет внимание пользователей. Выложите качественные фотографии, сделайте хорошие аннотации и приспособьтесь к правилам каждой соцсети, если хотите оставить след в умах.

2. Вы должны быть там же, где и ваши клиенты.

Визуальные соцсети сейчас в моде. В одном только Instagram насчитывается 300 млн активных пользователей в месяц, оставляющих 8 тыс. «лайков» в секунду. Вам обязательно нужно заявить о себе в этой сети, если вы нацелены на подростковую аудиторию: 23 % из них считают ее своей любимой соцсетью. Пользуется среди них большой популярностью и Vine. На женщин приходится 80 % из 70 млн пользователей Pinterest, и 47 % из них совершают реальные покупки с помощью этой сети. YouTube в свою очередь куда универсальнее и позволит вам обратиться к самой разнообразной аудитории. Перед тем как начать работу в той или иной соцсети, спросите себя, кто ваши клиенты и где их проще найти.

3. Отличный способ привлечь внимание к вашей работе.

Не важно, сантехник вы или парикмахер, у вашей работы непременно есть эстетическая сторона, которую вы можете обставить так, чтобы привлечь к ней внимание. В Instagram вы можете продемонстрировать ваши достижения и даже донести их до аудитории за пределами ваших

подписчиков с помощью подходящих хэштегов. Pinterest и Tumblr – идеально средство, чтобы поделиться вашей работой, а также стать источником вдохновения, вызвать у потенциальных клиентов творческий порыв и желание с вами связаться.

4. Эффективное средство обмена опытом.

У вас наверняка есть маленькие хитрости, которыми вы обычно делитесь с клиентами. Вы не берете за них денег, однако они обладают большой добавочной стоимостью. Поэтому вы можете легко сделать из них короткие видеоуроки продолжительностью в 2–3 минуты и разместить их на YouTube или Vimeo, если ваша работа связана с искусством или модой. Эти уроки помогут тем, кто пытается найти решение для, казалось бы, сложнейшей задачи и в результате откроет для себя ваше предприятием и ваш опыт. А потом свяжется с вами, если ему потребуется нечто большее.

5. Так проще следить за конкурентами.

Вам, безусловно, интересно, чем занимаются ваши конкуренты. В визуальных соцсетях вы легко можете подписаться на публикации ваших конкурентов или следить за последними тенденциями в вашей области. Кроме того, вы сможете взаимодействовать с теми, кто проявляет интерес к вашей работе, чтобы привлечь больше внимания к себе ***(Пять причин, чтобы представить ваше предприятие в визуальных соцсетях // InternetUA (http://internetua.com/pyat-pricsin--cstobi-predstavit-vashe-predpriyatie-v-vizualnih-socsetyah). – 2015. – 22.01).***

***

Как создать SMM-кампанию, которую будут обсуждать

Социальные медиа – это не только и не столько лайки, репосты и ретвиты, сколько создание значимых и длительных отношений с аудиторией, пишет Marketing Media Review (http://mmr.ua/news/id/kak-sozdat-smm-kampaniju-kotoruju-budut-obsuzhdat-42976/).

Несколько лет назад на конференции SXSW было высказано предположение, что все человеческие отношения могут быть разделены на три основные категории:

Управление (Authority relationships): Отношения, в которых один человек имеет власть над другим, дает ему указания. Например, работодатель – работник.

Обмен (Exchange relationships): Отношения, где обе стороны идут на уступки. Такая связь носит устойчивый характер, пока обе стороны предлагают стимулы для продолжения контакта. Награждение пользователя за лайк на Facebook – классический пример таких отношений.

Общность (Communal relationships): Отношения, где между сторонами установлено взаимное доверие, которое не зависит от поощрений и льгот. Это что-то вроде близкой дружбы.

К сожалению, многие маркетологи выбирают отношения обмена и пытаются подкупить пользователей. Исследования показывают, что 67 %

пользователей лайкают страницу бренда на Facebook, чтобы получить что-то взамен.

Но эта модель жизнеспособна только до определенного момента. Она эффективна при привлечении подписчиков, но вы можете серьезно просчитаться и получить «некачественных» пользователей, заинтересованных только в получении халявы.

Целью рекламной компании в социальных сетях должно быть создание с подписчиками общности, типа отношений, который обеспечит постоянные возвращения посетителей без всяких «взяток».

Предлагаем вам пять психологических тактик, которые позволят наладить долгосрочный контакт со своими подписчиками и обеспечить правильный тип взаимоотношений.

1. Дайте своему бренду человеческое лицо.

Вспомните бренды с яркой индивидуальностью – Old Spice (мужской, авантюрный, резкий), Nike (спортивный, готовый к любым вызовам), UGG (удобный, модный, веселый) – каждый из них создает в голове яркую картину.

Когда позиционирование бренда проходит действительно успешно, потребители идентифицируют его с личностью. Вот тогда-то и появляется обсуждение.

Это показывает, что в соцсетях дружить с человеком легче, чем с безликой маркетинговой машиной.

Психология в действии

Исследования показывают, что чем лучше бренд отражает конкретные черты человеческой личности, тем легче пользователям идентифицировать себя с ним. И, как говорит Р. Чалдини в «Шести принципах убеждения», люди скорее купят что-то у тех, кто им нравится.

Как применить это в вашей SMM-кампании

Привнесите личность бренда в свой аккаунт в социальных сетях. Пусть ваш профиль, сообщения и голос будут созвучны вашим фанатам.

Сеть ресторанов Chipotle очень здорово делает это в своем Twitter-аккаунте: они указывают имя сотрудника, который оставил конкретный твит.

Чтобы добавить индивидуальности своей SMM-кампании:

Используйте возможности социальных медиа, например, фотографию в профиле или обложке, чтобы создать личность бренда. Вы можете также включать фото SMM-команды или закулисной жизни в свою маркетинговую стратегию.

Пусть ваши сотрудники общаются с пользователями один на один, со своими реальными именами и характерами. Помимо того, что так они представляют ваш бренд, они еще и получают большее чувство причастности к делу компании и, следовательно, больше мотивации.

2. Используйте убедительные истории для вдохновения подписчиков на действия.

Не просите пользователей просто поставить лайк в обмен на купон или скидку. Дайте им стоящую причину сделать это.

Отличный способ мотивировать людей сделать что-то – говорить убедительно. Позвольте пользователям взглянуть на то малое, с чего началась история бренда, во что он превратился сегодня, и поделитесь историей о том, чем вы занимаетесь сегодня.

Психология в действии

Люди чувствуют доверие и важность, когда вы открыты для них. По данным исследований, потребность принадлежать к какой-то группе и идентифицировать себя с ней – сильный эмоциональный мотиватор.

Рассказывая об истории бренда или его достижениях, вы обращаете на себя больше внимания, чем просто впаривая свои товары. Ваша открытость вызывает у пользователей желание в ответ делиться своей историей с вами.

Как применить это в вашей SMM-кампании

Американский ретейлер Target провел весьма успешную SMM-кампанию в 2013 г., просто рассказав о голоде и людях, которым повезло меньше, чем нам с вами. В ходе кампании пользователи могли стать частью истории, облегчив чей-то голод.

При партнерстве с FEED Projects Target создали благотворительную коллекцию одежды и аксессуаров. Прибыль с каждой покупки шла на пищу 35–40 голодающим.

Эта кампания принесла Target огромное количество просмотров и серьезную вовлеченность в соцмедиа, а еще помогла сделать действительно доброе дело.

Если вы хотите использовать повествование в SMM для привлечения подписчиков:

Поделитесь историей (о вашем бренде или деле, в которое вы вкладываете всю душу), которая несет эмоциональную окраску.

Попросите поклонников поделиться своей историей, чтобы процесс был интересным для обеих сторон.

3. Будьте веселыми и поощряйте участие в активностях.

Большинство маркетологов настолько погружены в свои бренды и увеличение охвата в социальных медиа, что они забывают: главное правило взаимодействия в социальных медиа – это должно быть весело!

Вспомните: чем чаще делятся ваши друзья и родственники в социальных сетях? Новостями финансового отдела какой-то компании? Или все-таки веселыми анекдотами, мемами и цитатами? Спорим, выиграет второй вариант?

Психология в действии

Если у вас есть аккаунт в какой-либо соцсети, то в своей ленте вы, скорее всего, видите много забавных вещей. Исследование Ipsos, посвященное мотивам расшариваний в социальных медиа, показало, что по распространенности «смешные» посты уступают разве что «интересным» (43 % против 61 %).

Кстати, современные психологи считают, что развлечения и смех помогают объединить людей.

Как применить это в вашей SMM-кампании

Конечно, вы можете возразить, что ваш бренд ориентирован на серьезную аудитории, а не на легкомысленную молодежь.

Но вряд ли ваш бренд серьезнее, чем боковой амиотрофических склероз (ALS). Этим летом многие знаменитости, начиная с Б. Гейтса и заканчивая О. Уинфри, выливали на себя ведра ледяной воды в рамках акции в поддержку исследований ALS.

Кто сказал, что социальные медиа не могут приносить конверсии? С момента запуска акции Ice Bucket Challenge 29 июля 2014 г. Американская ассоциация по борьбе с боковым амиотрофическим склерозом смогла собрать более 100 млн дол. Эта и без того немалая сумма впечатляет еще больше, если вспомнить, что в аналогичном периоде прошлого года было собрано всего 2,5 млн дол.

Так что расслабьтесь и немного пошутите. Сделайте что-то такое, что заставит ваших подписчиков смеяться. А еще лучше – бросьте им вызов и предложите сделать что-нибудь эдакое самим.

4. Используйте чувство ностальгии, чтобы вызвать приятные чувства.

Как правило, люди чаще всего смотрят на прошлое через розовые очки. И обращение к воспоминаниям ваших пользователей – один из способов построения личных, семейных взаимоотношений.

Психология в действии

Ностальгия – сильный психологический триггер, создающий расшаривания, вовлеченность и социальную связанность.

И это может помочь в увеличении конверсии. Доктор наук Р. Брехт утверждает:

Когда потребители испытывают ностальгию в процессе потребления, вероятность покупки рекламируемой продукции увеличивается.

Когда Pepsi запустили кампанию Pepsi Throwback, стилизованную под 70-е годы, поклонники с немедленно смели все с полок супермаркетов. Pepsi Throwback принесла компании 41 млн дол. всего за год.

Как применить это в вашей SMM-кампании

BMW пробуждает ностальгию своих подписчиков с помощью хештега #ThrowbackThursday в Twitter:

Каждую неделю они размещают фото винтажного автомобиля, чтобы поддерживать отношения со старыми клиентами и вызвать у них теплые воспоминания.

В одной из статей блога HootSuite содержится много идей, которые могут пригодиться и вам:

Размещайте фотографии своего первого офиса и сотрудников или покажите, как ваш продукт развивался с течением времени.

Включите в свою контент-стратегию посты, благодаря которым подписчики будут думать о «старых добрых временах».

Создавайте викторины, которые будут вызывать ностальгию и способствовать расшариваниям.

5. Переместите фокус мышления с продаж на обмен.

Никто не любит общаться с людьми, которые не могут прекратить говорить о себе. То же самое касается брендов в соцмедиа. У вас может быть цель – продать побольше товаров, но зацикливаться только на этой теме, значит обрекать себя на провал.

Психология в действии

Люди ненавидят продажи. И это не новость. Вот что люди действительно делают с удовольствием, так это делятся идеями, опытом, информацией – а именно это составляет основу социальных медиа.

Исследование, проведенное New York Times Customer Insight Group, показало, как именно «обмен» в социальных медиа помогает пользователям принимать решение о покупке. Один из респондентов утверждает:

Обмен информацией помогает мне работать лучше. Я запоминаю продукты и информационные источники лучше, когда поделюсь ими, и с большей вероятностью использую их при случае.

Конечно, информация о собственных товарах и услугах может казаться вам суперинтересной, но ваши подписчики хотят читать о том, что близко им. Признание и удовлетворение потребностей ваших пользователей – отличный способ повысить вовлеченность, интерес и – в конечном счете – конверсии.

Как применить это в вашей SMM-кампании

Вместо того чтобы говорить о себе в соцсетях, обратитесь к интересам ваших подписчиков.

Вы работаете в сфере здравоохранения? Расскажите о пациентах, которые преодолели тяжелую болезнь. Вы fashion-ретейлер? Поделитесь модными тенденциями со своими подписчиками.

В заключение

Общайтесь со своими подписчиками как с обычными людьми, как с друзьями. Помните, ваша цель в социальных медиа должна заключаться в переходе от «валютных отношений» со своими подписчиками к доверию и дружбе ***(Как создать SMM-кампанию, которую будут обсуждать // Marketing Media Review (http://mmr.ua/news/id/kak-sozdat-smm-kampaniju-kotoruju-budut-obsuzhdat-42976/). – 2015. – 26.01).***

***

Facebook намеревается предложить брендам новый способ расчета конверсии, сделав продажи, а не клики, лучшим показателем эффективности кампании на этой платформе. Об этом пишет adindex.ru.

Этот шаг станет ответом на стоны рекламодателей о том, что им хочется каким-то образом выйти за рамки подсчета кликов. И бренды смогут оценить, какая часть их бюджетов, выделяемых на работу в Facebook, влияет на продажи в магазинах и Интернете, пишет The Drum.

Подсчеты будут проводиться с помощью инструмента, названного Lift и показывающего скорость конверсии. После создания рекламной кампании, социальная сеть сформирует тестовую группу, куда войдут те, кто видит рекламу, и контрольную группу с теми, кто не видит рекламу. Рекламодатели будут загружать в зашифрованном виде информацию о конверсии, а Facebook рассчитает вклад кампании на основе сравнения двух групп. Все результаты анализа будут доступны в менеджере рекламы.

Социальная сеть надеется, что этот показатель станет стандартным способом измерения эффективности кампаний, поскольку он вынуждает рекламодателей платить за рекламу, а не полагаться на органический, нетаргетированный контент.

Как и Google, Facebook пытается убедить бренды меньше зависеть от кликов и показов и выпускает инструменты, рассчитывающие более реальные вещи – в частности, продажи.

Многие из наиболее часто используемых измерительных систем переоценивают значение последнего клика. Об этом говорил и М. Цукерберг, подчеркнувший, что, по данным недавних исследований, 90 % людей, обеспечивших продажи обычным магазинам, пришли туда потому, что просмотрели их рекламу и при этом не кликали на нее.

Испытания похожего инструмента уже проводились в прошлом году, когда рекламодатели получили возможность использовать пользовательскую аудиторию для измерения своих оффлайн-продаж. Теперь же возможности опции будут расширены.

Facebook обладает уникальными возможностями для того, чтобы выяснить, как сильно просмотренная реклама влияет на покупки, ведь социальная сеть владеет активной пользовательской базой в 1,3 млрд человек, которые пользуются одним аккаунтом на всех устройствах. Также бренды могут связать пользователей Facebook с продажами с помощью собственных баз данных, сообщающихся с базой Facebook анонимно через такие программы, как Custom Audiences ***(Facebook предложила рекламодателям измерять продажи, а не клики // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42238/118/lang,ru/). – 2015. – 29.01).***

***

С 1 января Facebook понизил видимость коммерческих сообщений в новостной ленте пользователей. Это станет проблемой для малого и среднего бизнеса, активно использовавшего крупнейшую социальную сеть мира для генерации лидов. Как сохранить видимость ваших сообщений, не увеличивая бюджет на платное продвижение? Ниже описание 30 тактик от texterra.ru, которые помогут доносить сообщения до аудитории, несмотря на обновления алгоритмов Facebook, пишет Marketing Media Review (http://mmr.ua/news/id/kak-prodvigat-malyj-biznes-posle-obnovlenija-novostnoj-lenty-facebook-30-taktik-43022/).

В конце прошлого года Facebook сообщил об обновлении алгоритма ранжирования постов в новостной ленте. Чтобы пользователи получали актуальную их потребностям информацию, крупнейшая социальная сеть мира уменьшила видимость публикуемых на страницах компаний постов рекламного характера. В частности, речь идет о публикациях со следующими характеристиками:

Посты, содержащие предложение что-либо купить или установить программу.

Заметки, которые рекламируют продукт, предлагают участие в акциях и розыгрышах.

Публикации, в которых используется одинаковый с платными объявлениями контент.

Такие посты будут реже попадать в вашу новостную ленту

Facebook не хочет, чтобы в новостной ленте пользователи видели исключительно промо-контент. Можно догадаться, что есть еще один мотив этого обновления: социальная сеть желает, чтобы владельцы бизнеса платили за рекламу.

Крупные корпорации легко решат проблему видимости сообщений, увеличив бюджеты на платное продвижение в Facebook. Малому и среднему бизнесу придется изменить стратегию и тактику работы с аудиторией в самой популярной социальной сети мира.

Во-первых, небольшим компаниям стоит отказаться от публикации на страницах постов явно рекламного характера. Во-вторых, им следует увеличить число публикаций, обеспечивающих вовлеченность пользователей: анонсов полезного контента, советов, ответов на часто задаваемые вопросы и т. п. В-третьих, для поддержки естественных публикаций малому бизнесу будет полезно использовать рекламу. Небольшим компаниям необходимо уделить внимание таргетированию объявлений, которое повышает их эффективность.

Платные публикации частично решат проблему, с которой столкнуться компании при изменении стратегии и тактики продвижения в Facebook. Она заключается в следующем: контент нерекламного характера имеет более низкий потенциал лидогенерации по сравнению с промо-постами. Однако малому и среднему бизнесу следует диверсифицировать тактики лидогенерации, чтобы не зависеть от алгоритмов Facebook и уменьшить негативное влияние последних нововведений. Описанные ниже 30 шагов помогут вам решить эту задачу.

Создайте базу подписчиков

Люди, которые подписались на вашу электронную рассылку, готовы читать ваши сообщения всех типов. На их решение не влияют алгоритмы социальных сетей и поисковых систем. Начните продвигать проект с помощью Email-маркетинга:

1. Создайте форму подписки на рассылку и опубликуйте ее на сайте. Позаботьтесь о ее видимости.

2. Используйте HelloBar, чтобы перенаправлять трафик на лендинг, стимулирующий подписки.

3. Используйте объявления в сайдбаре или внутри текста на сайте, чтобы стимулировать подписки.

4. Отправляйте электронные письма клиентам с личных адресов сотрудников, а не с корпоративного адреса для рассылок. Включите в подпись ссылку на страницу с формой подписки.

5. Создайте отдельный электронный адрес для вопросов пользователей о вашем продукте. Это поможет вовлечь клиентов во взаимодействие и получить новые адреса.

6. Включите ссылку на страницу с формой подписки в письма, которые вы отправляете клиентам после покупки вашего продукта.

7. Используйте плагин для сбора электронных адресов Sumome. Он бесплатен и подходит для любых CMS.

8. Рекламируйте электронный адрес вашей компании в офлайне: на полиграфической продукции, сувенирах, кассовых чеках и т. п.

9. Стимулируйте подписчиков. Например, пообещайте каждому подписавшемуся бесплатную электронную книгу.

Ведите блог

Вообще-то, вам надо было создать блог немного раньше, например, в 2010 г. У вашей компании должен быть автономный блог или корпоративный сайт с блогом. В нем необходимо регулярно публиковать полезную для аудитории информацию. Если вы еще не делаете этого, начните прямо сейчас. А следующие рекомендации сделают ваш блог более эффективным:

10. Создайте в блоге рубрику «ЧаВо». Собирайте вопросы пользователей и подробно отвечайте на них. Так вы решите проблему с дефицитом контент-идей.

11. Публикуйте образовательный контент. Например, покажите клиентам, как правильно использовать ваш продукт.

12. Дайте слово клиентам. Позвольте им написать отзыв, опубликовать фото- или видеоотчет об использовании вашего продукта. Принимайте даже негативные отзывы и отвечайте на них.

13. Сошлитесь на блог в своих профилях в социальных сетях. Попросите об этом коллег.

14. Анонсируйте публикации в блоге в электронных письмах, а также в социальных сетях.

15. Убедитесь, что ваш блог можно читать с помощью RSS-агрегаторов, например, Feedly.

16. Добавьте кнопки шеринга и социальные плагины на страницы блога.

17. Попросите авторитетных в вашей отрасли экспертов и ключевых фолловеров прокомментировать ваши материалы или сделать репост.

18. Подружитесь с другими блоггерами, работающими с вашей тематикой. Помогайте друг другу распространять контент и привлекать аудиторию.

Активно используйте «ВКонтакте»

Аудитории русскоязычного сегмента Facebook и «ВКонтакте» отличаются. Однако бизнес активно пытается превратить vk.com из ресурса для общения и развлечений в деловую площадку. Присоединяйтесь к этим попыткам и пробуйте играть на противоречиях между Facebook и «ВКонтакте».

19. Создайте публичную страницу бренда или тематическую группу.

20. Попробуйте найти «ВКонтакте» самых активных подписчиков вашей страницы в Facebook.

21. Участвуйте в тематических дискуссиях в популярных деловых группах «ВКонтакте».

22. Анонсируйте на публичной странице «ВКонтакте» контент, который публикуете в корпоративном блоге.

23. Предлагайте аудитории «ВКонтакте» визуальный контент: видео, изображения, презентации.

Уделите внимание YouTube

Как известно, визуальный контент – король. А видео можно назвать императором визуального контента. Лучшим хостингом для публикации маркетингового видео остается YouTube. Поэтому начните вести канал на этой площадке.

24. Публикуйте видеогайды. Например, вы можете рассказать аудитории о фишках вашего продукта. Снимать видео можно даже с помощью старенького смартфона.

25. Снимайте промо-видео, посвященные вашему продукту. Искренность и остроумие компенсируют вам отсутствие профессиональной аппаратуры и актеров.

26. Станьте Познером в своей нише. Берите интервью у отраслевых экспертов, рассказывайте о конференциях и семинарах.

27. Покажите своих коллег и подчиненных. Попросите их рассказать о своей работе, увлечениях, досуге.

28. Покажите ваших клиентов. Возьмите у них интервью, попросите рассказать о сотрудничестве с вашим бизнесом.

29. Публикуйте развлекательные видео. Например, попросите ваших сотрудников и клиентов рассказать любимые анекдоты.

Публикуйте контент в Pinterest и Instagram

Эти социальные сети могут дать фору Facebook по популярности среди некоторых возрастных категорий пользователей.

30. Решите, какая из платформ вам больше подходит. Возможно, вам будет удобно работать одновременно с двумя ресурсами.

31. Создайте базу подписчиков. Расскажите о своих аккаунтах в Pinterest и Instagram в блоге и в других социальных сетях.

32. Публикуйте фото ваших продуктов. Используйте подходящие хэштеги.

Facebook будет менять алгоритмы ранжирования постов снова и снова

Поэтому вам нужно использовать альтернативные инструменты продвижения бизнеса и лидогенерации. Сделайте свой блог интересным для аудитории, работайте с «ВКонтакте», YouTube и другими соцсетями, используйте email-маркетинг. Используйте таргетированную рекламу в Facebook, чтобы периодически предлагать сформировавшейся аудитории промо-контент. В этом случае изменения алгоритмов Facebook не повредят вашему бизнесу ***(Как продвигать малый бизнес после обновления новостной ленты Facebook: 30+ тактик // Marketing Media Review (http://mmr.ua/news/id/kak-prodvigat-malyj-biznes-posle-obnovlenija-novostnoj-lenty-facebook-30-taktik-43022/). – 2015. – 29.01).***

***

Pinterest приобрёл стартап Kosei, который владеет алгоритмом машинного обучения, способным устанавливать взаимосвязь между различными сущностями. Покупка призвана улучшить рекомендации, поиск по сервису, кроме того, технологии будут использованы для повышения точности рекламных сообщений.

«У команды сформировано прекрасное понимание того, как должен работать алгоритм машинного обучения с точки зрения анализа данных, разработан рекомендательный движок. Продукты компании эффективны с коммерческой точки зрения: они позволяют создавать персонализированные рекомендательные предложения. Одним из главных достижений Kosei стало создание специального графа, способного распознавать до 400 млн различных взаимосвязей между 30 млн сущностями», – комментирует сделку представитель пресс-службы Pinterest.

Пока точно не известно, в каких конкретно направлениях развития социального сервиса будут использованы технологии Kosei. Однако с наибольшей вероятностью они могут быть использованы в рекламе и для улучшения внутреннего поиска по сервису. «В течение нескольких лет мы работали над построением системы, которая бы позволила людям находить пины, максимально соответствующие их интересам. Команда Kosei преуспела в создании таких технологии, их продукт станет отличным дополнением к нашим разработкам. Покупка Kosei позволит нам предоставлять пользователям максимально релевантные рекомендации, улучшить таргетинг рекламных объявлений и обеспечить максимально точную аналитику клиентам, использующим “Продвигаемые пины” (Promoted Pins)», – добавляет представитель Pinterest.

Kosei стала шестой покупкой Pinterest. Социальный сервис уже приобрёл такие проекты, как: Punchfork, Livestar, Hackermeter, Icebergs, технологию визуального поиска Visual Graph.

Бета-версия рекламных пинов Promoted Pins была запущена в мае 2014 г. Функционал был доступен лишь ограниченному числу брендов в США. По информации компании, во время тестового периода продвигаемые пины работали так же эффективно, а иногда даже лучше, чем органические. С 1 января 2015 г. программа «Продвигаемые пины» расширена на рекламодателей во всём мире ***(Pinterest намерен улучшить поиск и повысить эффективность таргетинга с помощью Kosei // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/pinterest_nameren_uluchshit_poisk_i_povysit_effektivnost_targetinga_s_pomoschyu_kosei). – 2015. – 30.01).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Учені Кембриджського і Стенфордського університетів з'ясували, що профіль користувача у Facebook, складений на основі «лайків» і відміток «подобається», описує його особистість краще, ніж навіть найближчі люди, включаючи батьків і партнера.

Дослідники вивчали особистості людей на основі опитувальника, який заповнили 86 700 користувачів соцмережі. Після цього вони сформували модель їх особистості і запропонували родичам опитаних також оцінити своїх близьких. Результати виявилися страшними навіть для вчених.

Після порівняння результатів виявилося, що комп'ютер описує особистість людини краще, ніж його колеги по роботі після аналізу 10 «лайків», ніж друг – після 70 «лайків», ніж родич – після 150 «лайків», і ніж чоловік/дружина – після 300 «лайків».

У середньому опитані користувачі ставили по 227 відміток «подобається». Як критерії для оцінки особистості людини виступали такі риси характеру як екстраверсія, доброзичливість, сумлінність, невротизм і відкритість досвіду.

Робота була опублікована в журналі досліджень Національної академії наук. Вона заснована на дослідженні 2013 р., яке доводить, що на основі «лайків» користувачів у Facebook можна досить точно передбачити їх IQ, політичні погляди і сексуальну орієнтацію ***(Facebook знає про вінничан більше, ніж родичі // ВІННИЦЯ.info (http://www.vinnitsa.info/news/facebook-znaye-pro-vinnichan-bilshe-nizh-rodichi.html). – 2015. – 14.01).***

***

От картинок в профилях Facebook и Twitter до фото на сайтах онлайн-знакомств и игровых аватаров, мы сталкиваемся с постоянно растущим числом решений о том, как представлять себя в Интернете. И согласно новому исследованию, то, как мы показываем себя онлайн, выдает ценную, порой удивительную информацию о наших личностях в реальном мире.

Исследователи из Йоркского университета провели эксперимент, чтобы проверить, отражают ли онлайн-аватары людей реальные черты личности. Они попросили группу студентов высших учебных заведений заполнить анкету, оценивующую так называемую Большую пятёрку личностных качеств – экстраверсию, доброжелательность (приятность в общении), добросовестность, невротизм (эмоциональную стабильность) и открытость опыту.

Затем студентам было предложено создать аватар для себя, используя сервис weeworld.com. Затем, отдельной группе студентов было показано подмножество из 15–16 аватаров, созданных в первой группе студентов. Вторую группу попросили оценить личность создателя аватара, а также определить, захотят ли они дружить с этим человеком.

Хотя аватары, конечно, не предложили полной картины личности их создателей, они содержат некоторые важные подсказки об индивидуальности человека. Исследователи обнаружили, что только лишь из аватаров, вторая группа студентов смогла вывести информацию об уровнях экстраверсии, доброжелательности и эмоциональной стабильности их создателя. Тем не менее, аватары ничего не говорят об открытости и добросовестности личности.

Студенты, оценивавшие аватары, в подавляющем большинстве заявили, что хотели бы дружить с обладателями аватаров, которые показали открытые глаза, улыбки, каштановые волосы и свитера. Аватары с короткими волосами, нейтральными выражениями лиц, черными волосами, головными уборами и солнцезащитными очками, с меньшей вероятностью вызывают желание подружиться с человеком.

Исследователи предупреждают, что аватары, используемые в исследовании, были очень простыми, так что вполне возможно, что результаты не будут распространяться на более сложные аватары. Тем не менее, есть некоторые другие данные, свидетельствующие, что люди склонны использовать аватары, чтобы передать информацию о своей личности. Канадское исследование 2010 г. показало, что у людей есть естественное желание в своих аватарах отразить, кто они, и, как правило, люди выбирают аватары, похожие на самих себя ***(Как личность пользователя отражается в его аватаре // InternetUA (http://internetua.com/kak-licsnost-polzovatelya-otrajaetsya-v-ego-avatare). – 2015. – 17.01).***

***

Центр аналитики PewResearch исследовал аудиторию социальных сетей на предмет подвержения стрессу, депрессии или тревоги.

По результатам проведенных тестов и опросов выяснилось, что активные пользователи социальных сетей подвергаются стрессу, депрессии и тревоге с такой же периодичностью, что и обычные люди, не пользующиеся так много Интернетом.

Забота обходится дорого

Авторы исследования замечают, что технологии всегда связывали со стрессом. Паровозы нарушали пасторальную жизнь отдаленных селений. Телефонные звонки бесцеремонно врывались в дома. Радио и телевидение вываливали на людей рекламу. Что уж говорить о новых цифровых технологиях.

В последнее время было принято считать, что Интернет в целом и соцсети в частности ответственны за высокий уровень стресса. Аналитики полагали, что завсегдатаи Facebook и Twitter определенно находятся в группе риска. Ученые поставили задачу выяснить, так ли это на самом деле.

Оказалось, что нет. Данные показали, что активные пользователи Интернета страдают от стресса не больше обычных людей. А пользователи-женщины даже меньше. Однако иногда социальные сети действительно «повинны» в стрессе. Дело в том, что негативные эмоции заразительны и знание о неприятных ситуациях в жизни других людей провоцирует возникновение собственных отрицательных эмоций.

Исследователи назвали этот феномен «цена заботы». Иначе говоря, частота использования соцмедиа и количество друзей со стрессом не связаны. Имеет значение только то, насколько часто люди узнают о негативных событиях и насколько им сопереживают.

Типичный пользователь Facebook, по словам авторов, вообще во многом счастливее остальных. У него больше друзей, ему больше доверяют, он чувствует поддержку.

Ранее было принято считать, что он испытывает разнообразное давление и вынужден противостоять страху исчезновения. На практике – ничего подобного: уровень стресса у них одинаков с теми, кто подобного давления не испытывает.

«Выходит, что страх исчезновения и зависть к богатеньким дружкам, рапортующих о прекрасных каникулах и счастливых детях, – это неправда», – так Л. Рейни, один из авторов исследования, прокомментировал его результаты New York Times.

Обратная сторона монеты: новые технологии позволяют постоянно быть в курсе жизни близких людей. И если люди постоянно общаются с ними через Интернет (например, в соцсетях или мессенджерах), то больше знают о неприятностях. Одним словом, страдают от частого использования Интернета только самые внимательные и заботливые люди.

Twitter и Instagram полезны для женщин

Авторы отмечают, что гендерные различия серьезно влияют на уровень стресса. Более того, мужчины и женщины по-разному используют цифровые технологии, поэтому и воздействуют они на них по-разному.

В целом, исследование показало, что женщины испытывают больше стресса, чем мужчины. Однако на женщин Интернет оказывает «целебное» действие.

Между мужчинами, которые активно пользуются Интернетом, и мужчинами, которые не признают новые технологии, в уровне стресса никаких различий нет. У женщин ситуация другая. Те из них, кто «дружит» со смартфонами, общается по электронной почте, «твитит» и делится своими снимками, более стрессоустойчивы по сравнению с женщинами, которые этого не делают.

Что касается осведомленности о неприятностях в жизни близких, то здесь мужчины оказались менее уязвимы. Перечень нежелательных событий, которые провоцируют стресс, у женщин обширнее, чем у мужчин. Однако у женщин есть механизм самозащиты – они по-настоящему расстраиваются в основном из-за того, что происходит в жизни близких.

К. Хемптон, один из исследователей, заявил, что негативные происшествия в жизни малознакомых людей не повышают, а понижают уровень стресса женщин, помогая им правильно расставить собственные приоритеты. Ученый назвал это «радостью исчезновения» – разновидностью благодарности за то, что это случилось не с ними и не с их семьей.

Соцсети приносят плохие вести

Исследователи выбрали 12 негативных событий и сравнили осведомленность о них у тех, кто пользуется соцсетями и тех, кто ими не пользуется. Выяснилось, что каждая социальная сеть неизбежно повышает уровень осведомленности о неприятностях. Интересно, что самый высокий уровень знания о плохих событиях в жизни других людей оказался у пользователей Pinterest.

Самым универсальным проводником негативных новостей оказался Facebook. Он сообщает о неприятностях как в жизни близких, так и в жизни малознакомых людей. Другие соцсети более специфичны: одни рассказывают о происшествиях, приключившихся у друзей и родственников, другие повествуют о злоключениях шапочных знакомых.

При этом женщины и мужчины узнают о неприятностях в разных сервисах. Женщины умудряются получать плохие новости через Instagram и Pinterest. Мужчины, скорее, узнают о них через мессенджеры и электронную почту ***(PewResearch: Пользователи соцсетей подвержены стрессу не чаще других // iLenta.com (http://ilenta.com/news/internet/news_5498.html). – 2015. – 17.01).***

***

В Великобритании социальную сеть Facebook цитируют в трети всех дел о разводе, сообщает The Daily Mirror со ссылкой на данные юридических

фирм. В ходе нового исследования выяснилось, что информация, полученная из соцсети, все чаще используется для доказательства неподобающего поведения супругов.

Facebook «непреднамеренно» предоставляет информацию о неверности партнеров и об их новых отношениях, помогает проследить за передвижениями пользователей и выявить их расходы буквально на все – от машин до отпуска, говорится в статье.

Как рассказали в юридической фирме Lake Legal из Лидса, «расшаривание» постов и фотографий, нередко с указанием геотега, позволяет получить данные, которые могут быть использован в суде. Не исключено, что если партнер ссылается на грядущий бонус, на новое предложение о работе или на отпускные планы, то он не говорит всей правды о своем финансовом положении, отмечают юристы.

Фотографии и комментарии могут использоваться для доказательства наличия отношений или ведения образа жизни, которые противоречат другим попыткам людей описать себя, сообщили, в свою очередь, в Stowe Family Law ***(В Великобритании Facebook цитируют в трети всех дел о розводе // InternetUA (http://internetua.com/v-velikobritanii-Facebook-citiruuat-v-treti-vseh-del-o-razvode). – 2015. – 22.01).***

***

Исследователи из нескольких американских университетов обнаружили прямую связь между нестабильностью в отношениях и открытостью в социальной сети, пишет Блог Imena.UA (http://www.imena.ua/blog/facebook-relationships/).

В ходе экспериментов группа психологов предложила 108 парам вести дневник, в котором они делали бы записи о своих ощущениях ежедневно. По истечении срока эксперимента дневники были соотнесены с публикациями подопытных на Facebook.

Как оказалось, в наиболее неудачные для отношений дни участники эксперимента выкладывали тематические записи на свою страницу, демонстрируя прямую связь между открытостью в социальных сетях и проблемами в личной жизни.

Следовательно, любители слишком подробного описания личной жизни в социальных сетях, как правило, больше всего неуверенны в своих отношениях или находятся как раз в стадии кризиса личной жизни ***(Статусы в Facebook об отношениях свидетельствуют о проблемах в личной жизни // Блог Imena.UA (http://www.imena.ua/blog/facebook-relationships/). – 2015. – 27.01).***

***

Исследователи Университета Айовы, США, опросив более 1,6 тыс. студентов, выяснили, что общение в социальной сети Facebook помогает им в учёбе.

При помощи Facebook студенты не только поддерживают связь с друзьями, но и повышают собственный уровень успеваемости. Возможность обменяться ссылками, а также, переписка друг с другом очень связаны с хорошими отметками – таковы результаты исследования.

Специалисты опровергли мнение о том, что если студент будет тратить меньше времени на социальную сеть, его успеваемость автоматически повысится.

Вместо этого, учёные предлагают рассказывать студентам о правильном, полезном и целесообразном использовании Facebook, и о необходимости самодисциплины в учебном процессе ***(Facebook способствует успехам в учёбе // InternetUA (http://internetua.com/Facebook-sposobstvuet-uspeham-v-ucs-be). – 2015. – 29.01).***

Маніпулятивні технології

Поліція безпеки (ПБ) Латвії почала перевірку за фактом популяризації у соціальних мережах ідеї так званої «Латгальської народної республіки», пише ZAXID.NET (http://zaxid.net/news/showNews.do?u_sotsmerezhah_v_latviyi_zyavilisya_zakliki_do_stvorennya_latgalskoyi_narodnoyi_respubliki&objectId=1338685).

Зазначається, що в соцмережі Facebook опубліковано зображення прапора з написом «Латгальська народна республіка», а також зображення карти Латвії з відокремленою Латгалією, передає латвійське видання Focus.

У відділі зв'язків із громадськістю Поліції безпеки Латвії підкреслили, що поширення в публічному просторі ідей, спрямованих на оскарження закріпленого в Сатверсмі принципу територіальної цілісності країни, відповідає геополітичним інтересам Росії.

Як відомо, у листопаді 2014 р. неподалік від російсько-латвійської кордону в регіоні Латгалія з'явилися активісти, які агітували за його від'єднання від Латвії та приєднання до Росії.

Між тим, національні збройні сили підкреслюють, що російські військові кораблі і літаки регулярно ідентифікуються в небезпечній близькості від кордонів Латвії.

Раніше, на 69-й сесії Генеральної асамблеї ООН, 26 вересня, президент Латвії А. Берзіньш заявив, що дії Кремля загрожують безпеці всього світу, а політика Росії проти України демонструє ігнорування Кремлем основних принципів ООН, що руйнує основи всієї міжнародної системи ***(Ганкевич Р. У соцмережах в Латвії з'явилися заклики до створення «Латгальської народної республіки» // ZAXID.NET (http://zaxid.net/news/showNews.do?u_sotsmerezhah_v_latviyi_zyavilisya_zaklik i_do_stvorennya_latgalskoyi_narodnoyi_respubliki&objectId=1338685). – 2015. – 29.01).***

***

В социальных сетях херсонские антинационалисты активно обсуждают варианты уничтожения офиса местной организации «Правого сектора».

Скриншоты таких обсуждений активисты ПС публикуют в своих пабликах.

Напомним, офис организации «Правого сектора» по адресу ул. Горбкого,13 уже пытались поджечь. Виновных в поджоге милиция до сих пор не нашла. Не исключено, что при следующей попытке уничтожить офис организации, в круг подозреваемых попадут и те, кто обсуждает эту идею в соцсетях. Ведь всего несколько дней назад СБУ Херсонщины обьявила об усилении контроля за тем, что происходит в Интернете ***(Херсонские антинационалисты обсуждают в сетях уничтожение «Правого сектора» // ХЕРСОН Онлайн (http://khersonline.net/novosti/politika/34599-hersonskie-antinacionalisty-obsuzhdayut-v-setyah-unichtozhenie-pravogo-sektora.html). – 2015. – 25.01).***

***

Российские пропагандисты в соцсетях приноровились легко одурачивать интернет-пользователей, «закосив» под украинцев, ставив украинские аватарки и используя специфические для украинцев слова. Но «троллей» можно легко разоблачить, просто зайдя на их аккаунт в соцсетях, пишет «Обозреватель» (http://obozrevatel.com/crime/58724-v-seti-razoblachili-ocherednogo-rossijskogo-trollya-provokatora.htm).

Такая же история произошла с фейковой «новостью» о том, что якобы парень патриотичной украинской писательницы А. Дмитрук уехал в Россию, чтобы откосить от армии, которую опубликовал российский провокатор в Twitter.

Очередной «суперхит» российских интернет-провокаторов набрал около 1000 ретвитов.

При этом позже сама А. Дмитрук в Facebook опровергла «новость»: «Мой парень со мной, в нашей родной Украине!! У нас тут еще некошеное поле работы, у каждого свой фронт! А “ватным активистам” могу повторить снова и снова: Никогда мы НЕ будем братьями!» – написала девушка дублируя название своего знаменитого стихотворения.

Как сообщал «Обозреватель», в России с апреля действует организованная группа интернет-пользователей, в задачи которых входит комментирование публикаций популярных американских информационных сайтов. В бюджете на апрель прописаны 25 сотрудников и расходы на общую сумму свыше 75 тыс. дол. По данным российских СМИ, проект организовали власти РФ.

Украинская группа хакеров организовала «охоту на троллей»: блокирование аккаунтов, страниц и групп сепаратистов и троллей в соцсетях» ***(В сети разоблачили очередного российского «тролля» –***

провокатора // Обозреватель (http://obozrevatel.com/crime/58724-v-seti-razoblachili-ocherednogo-rossijskogo-trollya-provokatora.htm). – 2015. – 29.01).

***

Новый вид мошенничества появился в соцсетях. Хакеры создают клоны страничек друзей и выманивают у них деньги: кто-то просит пополнить мобилку, а кто-то срочно перекинуть деньги на карточку.

«Мошенники заходят на страничку, скачивают ваши фотографии и сообщения и создают точную копию странички с данными, а потом заходят к вашим друзьям и просят выручить до завтра – кинуть какую-то сумму на карточку или телефон... Особенно эта информация актуальна для тех, у кого много друзей и подписчиков! Выбирают именно таких, кто-то беспечный среди них все равно найдется», – предупреждает в Facebook Марина.

Пользовательница «ВКонтакте» Анастасия Б. рассказала «Вестям» о похожем виде мошенничества: «Написала мне в личку давнишняя подруга, мол, срочно пополни счет мобильного – проблема. Отдать деньги пообещала при встрече, тогда же и все объяснить. Я сразу бросилась помогать, а потом остановилась. Подруга ведь моя переехала в Питер, и счет ей, соответственно, надо пополнять российского оператора. Она ведь должна знать, что в Киеве вряд ли можно найти такие пополняшки. Я и проигнорировала просьбу. Спустя несколько дней страничка подруги была удалена, а еще через два дня она мне написала, что кто-то взломал аккаунт и стал с ее страницы выманивать у друзей деньги».

В пресс-службе столичной милиции говорят, что такие разводы в соцсетях – не редкость: «Создаются поддельные странички или взламываются существующие, иногда даже создаются копии популярных интернет-магазинов. Первым делом людям следует не реагировать на такие сообщения, а тут же обращаться в милицию. Злоумышленникам в таком случае грозит до трех лет тюрьмы. Заподозрить мошенничество можно в первую очередь по манере написания текста. Он чаще имеет вид рассылки, нежели авторской переписки. Если человек получил сообщение от знакомого с просьбой помочь, стоит позвонить другу, который просит о помощи, и проверить достоверность информации» ***(На киевлянах начали испытывать новый вид мошенничества в соцсетях // Вести (http://vesti-ukr.com/kiev/86907-na-kievljanah-nachali-ispytyvat-novyj-vid-moshennichestva-v-socsetjah). – 2015. – 30.01).***

***

Еще с конца августа прошлого года в украинском сегменте Facebook участились блокировки политических активистов и волонтеров. Тогда родилась идея написать письмо М. Цукербергу с жалобой на несправедливое отношение администрации сети. Подобные случаи нередки и сейчас. Недавно активисты З. Антипоп и Д. Иванов даже провели пресс-

конференцию, где описали проблему, которая за полгода никуда не исчезла, пишет AIN.UA (http://ain.ua/2015/01/29/561255).

Механизм блокировки постов и пользователей в Facebook напрямую связан с количеством жалоб пользователей. Но иногда понять причину блокировки сложно. К примеру, из ленты З. Антипопа удалили картинку с отрывком из Шевченко («кохайтеся, чорнобриві, та не з москалями…»). «Случай с картинкой довольно курьезный, но это симптом намного большей проблемы. Начиная с прошлой весны, администрация Facebook блокировала аккаунты украинских блогеров, которые писали на политические темы», – рассказал он.

На днях на произвол администрации жаловался известный гонщик и волонтер А. Мочанов. По его словам, на видео были доказательства зверского обращения сепаратистов с пленными. «Шутки-шутками, но доказательное видео совсем пропало. Не только у меня, а вообще – из соцсетей и Интернета. Это как суслик и российские артиллеристы. Ты их видишь? А их – нет», – жалуется А. Мочанов.

Ранее в Facebook уже давали разъяснения на тему того, почему украинских политических активистов так часто (и по странным причинам) банят в сети. Но это были не очень убедительные разъяснения.

В компании тогда заявили, что Facebook не имеет представителей ни в России, ни в Украине, поддержку пользователям из Украины предоставляют сотрудники из разных стран, работающие в штаб-квартире в Дублине. Иногда случается, что из-за большого количества пользователей сети в разных странах мира полученное обращение рассматривается ненадлежащим образом, говорилось в сообщении компании ***(Карпенко О. Украинские блогеры обвиняют Facebook в пророссийских банах и блокировках // AIN.UA (http://ain.ua/2015/01/29/561255). – 2015. – 29.01).***

***

После обстрела в субботу, 24 января, террористами Мариуполя немедленно активизировалась армия кремлевских ботов, изображающих в сети Интернет местных жителей, сообщает портал Новое Время.

Mykola Malukha выложил в своем Facebook доказательство идентичности сообщений «жителей Мариуполя», которые якобы ждут «освободителей» из так называемого ополчения.

О том, что атаку Мариуполя произвели именно боевики доказывают также посты пророссийски настроенных пользователей о том, что «началось освобождение Мариуполя вооруженными силами ДНР».

В то же время проукраинские активисты цитируют сообщение одного из главарей ДНР П. Губарева, в котором он также написал о наступлении на Мариуполь.

Напомним, утром 24 января боевики террористической организации ДНР обстреляли Мариуполь из реактивных систем залпового огня Град.

Стоит отметить, что после атаки на Мариуполь со стороны боевиков жители города вышли на протест против «русского мира» ***(После атаки на Мариуполь в сети активизировались кремлевские боты // Marketing Media Review (http://mmr.ua/news/id/posle-ataki-na-mariupol-v-seti-aktivizirovalis-kremlevskie-boty-42953/). – 2015. – 24.01).***

***

Twitter начал использоваться как канал сообщений о возможных терактах

В США за последние четыре дня сообщения в Twitter с информацией о возможных терактах нарушили нормальное выполнение рейсов как минимум 16 раз. Об этом сообщает USA Today.

Рейс 1192 авиакомпании American Airlines из Лос-Анджелеса успешно приземлился в Чикаго, несмотря на сообщение о заложенной на борту бомбе в Twitter-аккаунте, предположительно, связанном с «Исламским государством» (ИГ).

Кроме того, ранее другой пользователь @RansomTheThug заявил, что бомба заложена на борту самолета United Airlines, следующего из Ньюарка в Майами. В авиакомпании заявили, что рейс был отменен из-за погодных условий. В то же время работа этого Twitter-аккаунта приостановлена.

Как минимум 10 таких угроз американские авиакомпании получили в 26 января, некоторые публикуются в аккаунтах, похожих на хакерские. Из-за одной из них рейс JetBlue из Бостона в Палм-Бич был отменен – салон самолета и багаж пассажиров еще раз обыскали, но ничего опасного не нашли. Ряд угроз привели к эвакуации пассажиров, перенаправлению самолетов в другие аэропорты и даже к вызову сопровождения в виде военных истребителей.

Подобные инциденты стали учащаться, причем они наглядно демонстрируют, как один человек в соцсети может нарушить работу и планы множества других. Причем это касается как реального кибертерроризма, так и малолетних шутников.

Так, в прошлом апреле 14-летняя датчанка была арестована после того, как опубликовала в Twitter сообщение следующего содержания в адрес American Airlines: «@AmericanAir привет, меня зовут Ибрагим и я из Афганистана. Я участник Аль-каиды, и 1 июня я планирую сделать кое-что очень большое».

Специалисты отмечают, что найти таких шутников несложно, даже если у них скрыт IP-адрес. По их словам, почти все пользователи оставляют за собой «след» в сети, а интернет-провайдеры чаще всего сотрудничают со следствием ***(Twitter начал использоваться как канал сообщений о возможных терактах // InternetUA (http://internetua.com/Twitter-nacsal-ispolzovatsya-kak-kanal-soobsxenii-o-vozmojnih-teraktah). – 2015. – 29.01).***

***

Как организована работа кремле-троллей

Петербург прославился на всю Россию как колыбель информационных войн и «интернет-троллей», обосновавшихся в элитном жилом комплексе в Ольгино, позже переехавших ближе к центру города. Бывшая сотрудница этой организации на условиях анонимности рассказала нам, как устроена гигантская машина пропаганды и почему долго на такой работе не продержаться.

«Вакансии в это великолепное место раскиданы по всем хэдхантерским ресурсам. Компании, которые ищут “копирайтеров” или “контент-менеджеров”, фигурируют в них самые разные. Конспирация не срабатывает по двум причинам: везде указывается заработная плата 40–45 тыс. р. и адрес “м. Старая Деревня / м. Черная речка”. В вакансии дается минимум информации о том, кто, куда и зачем нужен – весь расчет на то, что столь высокая зарплата отобьет желание узнавать, куда ты намереваешься устроиться. Как выясняется позже, это работает: многие попали сюда после долгих и мучительных поисков работы, почти отчаявшись. Лично я, не так давно приехав из крупного областного центра и имея журналистское образование, в конце августа просто послала резюме по одному из десятков объявлений, размещенных на сайте поиска работы. Звонок с приглашением прийти на собеседование в медиахолдинг “Интернет-исследования” раздался через пару дней. Собеседование я проходила в новом красивом офисном здании, что на улице Савушкина, 55, которое занимает четыре этажа. Попасть туда просто так с улицы невозможно: суровая охрана, турникетная система. Если у тебя нет пропускной карточки, то пишешь объяснительную, в которой указываешь свои паспортные данные.

Собеседование начинается с того, что тебе протягивают анкету. В ней указываешь свои данные, вплоть до места прописки, места фактического проживания, полную информацию о бывших местах работы, сведения о местах работы родителей и т. д. После чего тебе задают пару вопросов и просят “переписать” любую актуальную новость. Такое ощущение, что на работу берут всех, кто сможет доказать, что умеет писать и говорить на русском языке. При этом никакой информации о том, куда ты попала, не раскрывается: “медиахолдинг, несколько сайтов, нужно нарабатывать трафик, зарплата выше средней”. Если ты до этого несколько месяцев не мог найти работу, то соглашаешься сразу же после слов “сорок пять тысяч рублей”. Это базовая зарплата всех рядовых сотрудников – будь то “блогеры” (пишущие в LiveJornal и соцсетях), “контент-менеджеры”, “СЕО-специалисты” или создатели патриотических “демотиваторов”, которые именуются “иллюстраторами”. Те, кто дослуживаются до более высоких должностей, получают больше – 55 тыс., 60 тыс. и т. д. Про личные политические убеждения при приеме на работу практически не спрашивают.

Первый рабочий день. С 9.00 до 17.30. “Ты должна сделать 20 новостей, уникальность – около 75 %, новости должны быть актуальные,

держи логин и пароль от сайта, за работу". Все напоминает школу – офисы очень похожи на компьютерные классы, опаздывать даже на 2 мин. нельзя (за это штрафуют), уходить с работы нужно сразу после ее окончания и ни минутой позже. Всего, как я поняла, в холдинге 12 сайтов разных тематик, но все так или иначе затрагивают политику и Украину. Хоть "визиткой" считается "Федеральное агентство новостей" (звоня по телефону с работы, большинство сотрудников разных отделов представляются именно как сотрудники "ФАН"), большую часть трафика получает так называемое "новостное агентство Харькова" (иронично названное nahnews.com.ua). Сайт будто бы украинский, но все публикации делаются на Савушкина 55. Таких "украинских сайтов" в медиахолдинге несколько, в том числе и знаменитый сайт "Антимайдан". Прямых провокационных фейков такие фальш-сайты не делают, но переписывают новости в определенном ключе: например, сепаратисты переименовываются в "ополченцев". Работает "медиахолдинг" с июля 2014 г.

Первые дни ты просто не понимаешь, где находишься, зачем переписываешь эти новости, наполняешь ими сайты. Создается ощущение, что это какой-то социальный эксперимент или реалити-шоу: тем более, что в каждом оупенспейсе, где сидят примерно по 20–30 сотрудников, установлены камеры наблюдения.

Идеологической промывки мозгов или регулярного инструктажа не было, все очень просто и понятно практически всем, устроившимся на работу: про Путина плохо нельзя, ополченцы не террористы, "ну ты ведь понимаешь…". Такое ощущение, что все вновь пришедшие сами понимают, куда попали и как нужно писать, идеологический инструктаж если и проводится, то на уровне шеф-редакторов. Никаких планерок или общих собраний нет. Кстати о рядовых сотрудниках: чаще всего это приезжие из других городов, все люди с высшим образованием, весьма неглупые. Много совсем молодых людей неформального вида, с пирсингом или дредами. Условно сотрудники делятся на три категории: 1) "Мне платят и пофиг, кто это, я даже не в курсе": у многих из таких семьи, кредиты и т. д., 2) "Да, я знаю, что это прокремлевская фабрика троллей, но к черту душевные терзания – платят и ладно", 3) "Я веду информационную войну против фашисткой хунты!". Последние в подавляющем меньшинстве. Пожалуй, свою работу искренне любят только они. В нашем отделе таких было, кажется, всего двое.

Сам "медиахолдинг" занимает лишь один этаж здания. На остальных сидят другие работники пропагандистского фронта: в том числе и те самые "тролли", которые прославились на весь Питер, собственно наемные острословы, забивающие всякий тред в соцсетях и блогах агрессивными комментариями. Работники "медиахолдинга" относятся к ним с ироний, граничащей все-таки с некоторой опаской. Лично мне не довелось близко пообщаться с "троллями", только видела их в курилке. Непрофессионализм руководства "холдинга" чувствуется уже после недели работы. Главная цель

– количество просмотров, посетителей. По плану их количество (на всех сайтах холдинга в целом) должно повышаться на 3 тыс. человек каждый день. При этом не учитываются выходные, праздники и т. д. – просто “пятилетку за месяц”. СЕО-отдел, который должен продвигать контент этих сайтов, занимается банальным спамом (из-за чего ссылки многих сайтов блокируются в Google и “ВКонтакте”). Учитывая, каким образом набирается персонал, это неудивительно.

Тем временем руководство трясет шефов сайтов, те требуют от своих работников “актуальных новостей”, сотрудники пытаются первыми “переписать” новости ключевых информагентств России. Для повышения трафика берутся новости про убийства, изнасилования и прочий криминал в регионах России, сенсации шоубиза, про Пугачеву, Мадонну и т. д. Очень популярны новости про геев: понятно, что в негативном по отношению к ЛГБТ духе. Если упоминают феминизм, то обязательно с привязкой к украинским акционисткам Femen, не иначе. Но, тем не менее, главные новости каждого сайта – Путин, Крым, “Новороссия”. При этом постоянно ведутся разговоры “мы на стартапе, нужно накручивать посещаемость, чтобы выйти на самоокупаемость за счет рекламы, это только пока мы живем на деньги инвесторов”, но все это воспринимается с улыбкой. Потому что кто на самом деле эти “инвесторы”, понятно даже самым наивным.

Решение уйти из “заповедника троллей” созревало достаточно долго. С одной стороны, я понимала, что такую, в принципе, непыльную работу с приличной для Петербурга зарплатой, будет сложно найти в условиях кризиса: не было ни одного дня на Савушкина, когда бы я столкнулась с непреодолимыми трудностями именно технического характера. Вопрос был в психологической тяжести этой работы. К декабрю от нервного напряжения у меня начал дергаться глаз, а по ночам я видела сны, в которых я все переписываю и переписываю новости про Путина и Украину. К тому же убеждений я придерживаюсь либеральных, среди моих знакомых есть немало оппозиционно настроенных людей, и в какой-то момент я поняла, что мне просто стыдно рассказывать, чем я занимаюсь. Все эти факторы перевесили соображения комфорта, и я с облегчением уволилась» ***(Как организована работа кремле-троллей // InternetUA (http://internetua.com/kak-organizovana-rabota-kremle-trollei). – 2015. – 31.01).***

Зарубіжні спецслужби і технології «соціального контролю»

Премьер-министр Великобритании готовит запрет защищённых мессенджеров, непроницаемых для анализа спецслужб, пишет Блог Imena.UA (http://www.imena.ua/blog/new-snoopers-charter/).

В случае победы на следующих выборах, которые состоятся уже весной 2015 г., действующий премьер-министр Великобритании Д. Кэмерон собирается усилить контроль за средствами интернет-коммуникации.

По мнению премьер-министра, существующее британское законодательство нуждается в обновлении. Д. Кэмерон отмечает, что государство должно обеспечивать защиту граждан от терроризма и прочих угроз, для чего спецслужбам необходимо иметь доступ к информации.

Поэтому ни одна форма коммуникации не должна быть полностью закрыта от правоохранительных органов.

В случае принятия соответствующих нормативных актов, в Великобритании могут быть полностью запрещены средства интернет-коммуникации, обеспечивающие шифрование передаваемых данных, в первую очередь, WhatsApp, iMessage и Snapchat.

Ранее специалисты организации Electronic Frontier Foundation провели аудит нескольких десятков приложений для обмена сообщениями и установили, что лишь малая их часть соответствует хотя бы минимальным требованиям обеспечения безопасности ***(В Великобритании готовят запрет защищённых мессенджеров // Блог Imena.UA (http://www.imena.ua/blog/new-snoopers-charter/). – 2015. – 14.01).***

***

Лидер оппозиционной партии Бахрейна «Аль-Вифак» Д. Кадим приговорён к шести месяцам тюремного заключения и штрафу в 500 бахрейнских динаров –1350 дол. – за запись в своём микроблоге Twitter, пишет Блог Imena.UA (http://www.imena.ua/blog/bahrain-wefaq/).

Во время избирательной кампании Д. Кадим написал в своём микроблоге об использовании на выборах «политических денег» для покупки голосов избирателей. По мнению суда, замечание, которое разместил в Twitter Д. Кадим, «очерняет процесс проведения выборов в парламент».

После объявления приговора оппозиционер в беседе с журналистами назвал его «политическим», связанным с общим наступлением властей на «Аль-Вифак».

Партийные юристы отмечают, что нет никаких правовых оснований для вынесения такого приговора в отношении руководителя партии, поскольку в своей записи в Twitter он просто выразил своё мнение ***(Лидера оппозиции Бахрейна посадили за Twitter // Блог Imena.UA (http://www.imena.ua/blog/bahrain-wefaq/). – 2015. – 14.01).***

***

Служба безопасности Украины призывает граждан воздержаться от передачи важной информации, используя сервис мобильной рации Zello, в связи с тем, что спецслужбы России осуществляют его мониторинг, написал на своей странице в социальной сети Facebook советник главы СБУ М. Лубкивский, сообщают «Украинские новости».

По его словам, об опасности использования российских соцсетей неоднократно отмечала СБУ, однако до последнего времени приложение-рация Zello считалось украинцами достаточно безопасным сервисом.

Вместе с этим СБУ получила от одного из боевиков, жителя Донецкого региона, который перешел на украинскую сторону, неопровержимые доказательства того, что сепаратисты могут идентифицировать пользователей интернет-сервиса Zello.

«Поэтому избегайте передачи каналами Zello важной информации и принимайте меры, которые бы сделали невозможным вашу идентификацию. Помните, Zello мониторится врагом, который делает все возможное для поиска и борьбы с украинскими патриотами», – написал он. М. Лубкивский отметил, что российские спецслужбы, которые действуют в Донецке, обладают значительными объемами актуальной технической информации о пользователях упомянутого сервиса (имя, данные из профилей, другие псевдонимы, которые авторизовались с одного телефонного терминала; IMEI мобильных терминалов и их IP-адреса и т. д.) ***(В СБУ уверены, что российские спецслужбы прослушивают мобильное приложение Zello // Наш Век (http://wek.com.ua/article/82695/). – 2015. – 16.01).***

***

Співробітники Служби безпеки України викрили протиправну діяльність мешканця Черкаської області, який поширював матеріали із закликами до змін меж території та державного кордону України.

Встановлено, що 36-річний безробітний у соціальній мережі Інтернету «ВКонтакті» розміщував матеріали антиукраїнського змісту, зокрема агітував за приєднання території Сходу України до Російської Федерації.

17 січня 2015 р. слідчими управління було розпочато кримінальне провадження за ч. 1 ст. 110 (посягання на територіальну цілісність і недоторканність України) Кримінального кодексу України.

Триває досудове розслідування. Санкції статті передбачають покарання до трьох років позбавлення волі ***(СБУ викрило черкащанина, який вів антиукраїнську агітацію у соцмережі // InternetUA (http://internetua.com/sbu-vikrilo-cserkasxanina--yakii-v-v-antiukra-nsku-ag-tac-ua-u-socmerej). – 2015. – 22.01).***

***

Турецкий суд потребовал от соцсети Facebook ограничить доступ к ряду аккаунтов, где размещены материалы, оскорбляющие пророка Мухаммеда. Об этом сообщает lenta.ru.

В случае невыполнения предписаний суда соцсети грозит полная блокировка на территории Турции. Соответствующее решение было принято в воскресенье, 25 января. Оно уже было передано в Управление по телекоммуникациям и Союз провайдеров страны.

Кроме того, 14 января суд Турции запретил всем новостным сайтам публиковать обложку последнего номера сатирического журнала Charlie Hebdo, который вышел 14 января. На ней изображен плачущий пророк Мухаммед с плакатом «Я – Шарли».

9 января гендиректор Facebook М. Цукерберг сообщил на своей странице, что компания не будет цензурировать контент, который публикуют пользователи в связи с атаками на Charlie Hebdo. По его словам, социальная сеть «никогда не позволит какой-либо стране или группе людей диктовать, чем люди должны делиться с миром».

Согласно статистике Facebook, за первое полугодие 2014 г. соцсеть удалила в Турции 1893 материалов по просьбе различных органов страны. По этому показателю страна находится на втором месте, опережает ее лишь Индия ***(В Турции потребовали от Facebook заблокировать страницы с оскорблениями Мухаммеда // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42194/118/lang,ru/). – 2015. – 26.01).***

***

В Украине планируют создать координационный центр блогеров, который мог бы распространять правдивую информацию о ситуации на Востоке страны или опровергать ложные новости. Об этом сообщает министр информационной политики Украины Ю. Стець, передает новость «Пресса Украины».

По его словам, он пока не знает, сколько именно надо блогеров для эффективности проекта.

«Донести правдивую информацию тем, кто общается в Интернете, для этого не нужны боты или тролли. Тот, кто пользуется соцсетями не первый день, видит это и понимает. Для этого надо объединить авторитетных людей в соцсетях и они расскажут правду всем, кто их читает», – подчеркнул Ю. Стець.

Он также добавил, что чем больше будет блогеров – тем лучше.

«Прежде всего, все осознанные в Интернете станут интернет-армией Украины», – отметил Ю. Стець.

Напомним, что Ю. Стець выделил три направления работы вновь созданного Министерства информполитики: создание концепции стратегии информационной политики государства, борьба с геополитическими угрозами в информационных войнах и налаживания коммуникаций между органами власти ***(В Украине могут создать интернет-войска – министр информполитики // Час Пик (http://vchaspik.ua/ukraina/300471v-ukraine-mogut-sozdat-internet-voyska-ministr-informpolitiki). – 2015. – 28.01).***

***

Міноборони РФ спостерігатиме за соцмережами через спецсистему

«Об'єднана приладобудівна корпорація» (ОПК) створює для Національного центру управління обороною (НЦУО) РФ системи моніторингу та аналізу військово-політичної обстановки в країні і світі, які здатні автоматично моделювати прогнози розвитку ключових світових подій для керівництва Міноборони РФ.

НЦУО почав штатну роботу 1 грудня 2014 р., пишуть РИА Новости.

За словами міністра оборони РФ С. Шойгу, центр «дає змогу не тільки відслідковувати обстановку, але і в реальному масштабі часу забезпечити управління всією військовою організацією держави».

Фахівці холдингу «Системи управління» (входить в ОПК) розробляють програмно-апаратний комплекс аналізу військово-політичної обстановки (ПАК ВПО) та аналізу суспільно-політичної та соціально-економічної ситуації в країні (ПАК ОПВ).

Наразі завершується виготовлення дослідного зразка та підготовка до попередніх випробувань. Закінчення робіт заплановано на середину 2016 р.

Комплекси призначені для оперативного спостереження через відкриті джерела – ЗМІ та соціальні мережі.

За словами генерального директора холдингу «Системи управління» А. Різника, ПАК ВПО і ПАК ОПС повністю забезпечать керівництво військового відомства інформацією про найбільш значущі події в країні і за кордоном, а також сценарії розвитку обстановки.

«Ми також впроваджуємо крос-мовну підтримку: системи здатні відбирати в потоці інформації світових ЗМІ ті повідомлення, які відносяться до заданого запиту, перекладати іншомовний текст, аналізувати його і включати дані в статистику і підсумковий матеріал. На початкових етапах роботи комплекси будуть працювати з 5–6 мовами, надалі їхня кількість може бути збільшена на вимогу замовника», – сказав А. Різник.

Крім того, ПАК ВПО і ПАК ОПВ, на відміну від аналогічних систем моніторингу, здатні аналізувати не тільки друкований текст, а й ефірне мовлення, працюючи з матеріалами прямого ефіру.

У них також впроваджена функція графічного відбору: системи розпізнають зображення і здатні ідентифікувати людей та об'єкти, зчитують біжучий рядок і обробляють радіосюжети ***(Міноборони РФ спостерігатиме за соцмережами через спецсистему // INSIDER (http://www.theinsider.ua/politics/54c8afbb367b8/). – 2015. – 28.01).***

***

Доступ к видеохостингу YouTube в России ограничен по решению Мосгорсуда. Это следует из данных, размещенных на универсальном сервисе Роскомнадзора для проверки ограничения доступа к сайтам. Об этом пишет rbc.ru.

Основанием для ограничения доступа называется статья 15.2 Закона «Об информации, информационных технологиях и о защите информации».

Она предусматривает обеспечительные меры в виде ограничения доступа в отношении информационного ресурса, распространяющего информацию с нарушением прав правообладателя.

Согласно описанному в статье механизму, правообладатель обращается в Мосгорсуд с заявлением. Тот на основании заявления в срок, не превышающий 15 дней, ограничивает доступ к ресурсу, распространившему информацию с нарушением авторских прав. Впоследствии правообладатель может подать иск в тот же суд в отношении владельца информационного ресурса или провайдера хостинга с требованием прекратить нарушение его исключительных прав. На протяжении судебного процесса обеспечительные меры не прекращают свое действие, отмечается в Законе.

«Некоторые ссылки на материалы, размещенные на YouTube, действительно есть в реестрах Роскомнадзора, но формат взаимодействия с этим ресурсом не предполагает в этом случае блокировку на территории всей России», – сказал РБК представитель Роскомнадзора В. Ампелонский. Он добавил, что в Роскомнадзоре разбираются в ситуации.

В. Ампелонский упомянул в разговоре с РБК, что ограничение связано и с роликом на YouTube, который попал в реестр сайтов, заблокированных по ФЗ-398, то есть за «призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка».

Представитель Google (владеет YouTube) С. Анурова попросила у РБК ссылки на информацию пользователей о недоступности YouTube, сказав, что до этого ничего не слышала о блокировках. Позже С. Анурова не отвечала на звонки РБК ***(В рамках борьбы с пиратством в России ограничили доступ к YouTube // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42241/118/lang,ru/). – 2015. – 29.01).***

***

Во Франции могут принять закон, из-за которого Google и Facebook будут считаться пособниками террористов.

Правительство разрабатывает законопроект, по которому интернет-сервисы станут сообщниками разжигателей ненависти, если пользователи будут размещать на их площадках экстремистские материалы. Об этом заявил президент Франции Ф. Олланд. Законопроект будет представлен в феврале. Министр внутренних дел Франции Б. Казнев планирует отправиться в США, чтобы обсудить это предложение с руководителями Google, Microsoft, Facebook и Twitter, пишет RevolverLab (http://revolverlab.com/news/2015/01/29/frantsiya-zakruchivaet-gayki-google-i-facebook/).

«Большие интернет-сервисы уже не смогут закрывать глаза на то, что происходит, если они будут считаться причастными к высказываниям, которые размещают у себя, – сказал Ф. Олланд. – Мы должны действовать на

европейском и международном уровне для определения нормативно-правовой базы, чтобы интернет-платформы могли считаться ответственными, и чтобы к ним могли быть предприняты санкции».

Непонятно только, на основании каких критериев «экстремизма» будут оцениваться материалы, а также в какой степени буду задействованы веб-компании ***(Франция «закручивает гайки» Google и Facebook // RevolverLab (http://revolverlab.com/news/2015/01/29/frantsiya-zakruchivaet-gayki-google-i-facebook/). – 2015. – 29.01).***

***

В Китае разблокировали крупнейший фотосервис Instagram. Об этом рассказали Tech In Asia, ссылаясь на свои источники среди китайских властей, пишет RevolverLab (http://revolverlab.com/news/2015/01/28/posle-4-mesyachnoy-blokadyi-instagram-vernulsya-v-kitay/).

С сентября 2014 г. пользователей Китая лишили доступа к Instagram. Кстати, ранее он считался одним из немногих сервисов, которому позволялось работать на территории Китая. «Блокада» совпала с началом жесткого разгона демонстрантов в Гонконге.

Протестные акции окончательно «рассосались» в середине декабря 2014 г. Тогда же были разобраны все баррикады в центре. Многие из этих событий активно освещались в Instagram местными активистами, что не могло нравиться правительству ***(После 4-месячной блокады Instagram вернулся в Китай // RevolverLab (http://revolverlab.com/news/2015/01/28/posle-4-mesyachnoy-blokadyi-instagram-vernulsya-v-kitay/). – 2015. – 28.01).***

Проблема захисту даних. DDOS та вірусні атаки

Эксперты в области безопасности SCADA-систем столкнулись с неожиданным поворотом в используемой злоумышленниками тактике осуществления атак на автоматизированные системы управления (АСУ). Как сообщает издание DarkReading со ссылкой на исследователя Trend Micro К. Уилхойта, вместо разработанного по заказу государства мощного вредоносного ПО наподобие Stuxnet для атак на АСУ хакеры стали использовать банковские трояны.

Недавно К. Уилхойт обнаружил 13 различных типов мошеннического ПО, маскирующегося под человеко-машинный интерфейс Siemens Simatic WinCC и GE Cimplicity, а также под драйверы устройств Advantech и другие файлы. Похоже, что за атаками на SCADA-системы с использованием подобных вредоносов стоят обычные преступники, которые не применяют инструменты для промышленного шпионажа.

Предприятия, использующие АСУ, хорошо осведомлены о возможных атаках с помощью Stuxnet и недавно обнаруженных Havex и BlackEnergy, которые осуществляются с целью шпионажа или выведения оборудования из строя. Однако сделанное К. Уилхойтом открытие демонстрирует, что преступники также начали интересоваться атаками на SCADA-системы. При этом злоумышленников интересуют не корпоративные секреты, а данные, которые помогут похитить денежные средства с банковских счетов.

По словам К. Уилхойта, преступники обратили свое внимание на АСУ, поскольку эти системы имеют слабую защиту и являются очень легкой целью. Несмотря на то что Havex и BlackEnergy по-прежнему несут большую опасность, банковские трояны, используемые для атак на SCADA-системы, также представляют серьезную угрозу безопасности ***(Преступники используют банковские трояны для атак на SCADA-системы // InternetUA (http://internetua.com/prestupniki-ispolzuuat-bankovskie-troyani-dlya-atak-na-SCADA-sistemi). – 2015. – 14.01).***

***

Независимые исследователи безопасности провели анализ официального веб-сайта северокорейского новостного агентства Korean Central News Agency и выяснили, что ресурс содержит исполняемый вредоносный код, замаскированный под обновление для Flash. Об этом сообщает Ars Technica.

Как сообщается, часть кода JavaScript, вызываемого с главной страницы веб-сайта, скачивает на систему пользователя архив с названием «FlashPlayer10.zip». Внутри него находится два исполняемых файла Windows, один из которых является обновлением для давно устаревшего Flash Player 10, а второй – расширением для веб-обозревателя. Наличие в архиве вредоносного кода удалось подтвердить при помощи сервиса VirusTotal.

В результате предварительного анализа экспертов стало явно, что вирус находится на веб-сайте как минимум с декабря 2012 г. Кроме того, работа ресурса настроена таким образом, что скачивание FlashPlayer10.zip может быть инициировано администрацией портала по собственному желанию (например, для пользователей определенных браузеров тех или иных версий).

В Korean Central News Agency в настоящее время никак не комментируют ситуацию ***(Сайт северокорейского новостного агентства распространял вредоносное ПО // InternetUA (http://internetua.com/sait-severokoreiskogo-novostnogo-agentstva-rasprostranyal-vredonosnoe-po). – 2015. – 15.01).***

***

Эксперт компании Core Security обнаружил уязвимость нулевого дня в программных продуктах Corel Software. Эксплуатация бреши позволяет

выполнить подмену DLL-файлов (DLL hijacking) при открытии медиа-файлов, ассоциированных с уязвимыми продуктами Corel.

Поддельная динамическая библиотека содержит исполняемый код, который позволяет атакующему установить на компьютер жертвы вредносное ПО. Подмена происходит в случае, если открываемый медиа-файл находится в той же директории, что и подлинная библиотека.

В настоящее время брешь выявлена в восьми приложениях Corel: CorelDRAW X7, Corel Photo-Paint X7, Corel PaintShop Pro X7, CorelCAD 2014, Corel Painter 2015, Corel PDF Fusion, Corel VideoStudio PRO X7 и Corel FastFlick, а потенциальными жертвами злоумышленников являются более 100 млн пользователей.

Информацию об уязвимости предал огласке исследователь М. Аккоссатто после того, как разработчики Corel Softwear не отреагировали на несколько его уведомлений, сделанных в частном порядке.

Компания Corel Softwear пока что не предложила исправления безопасности для перечисленного программного обеспечения ***(В программных продуктах Corel Software обнаружена уязвимость нулевого дня // InternetUA (http://internetua.com/v-programmnih-produktah-Corel-Software-obnarujena-uyazvimost-nulevogo-dnya). – 2015. – 15.01).***

***

После того как Google сообщила о серьезной уязвимости в Windows, не менее существенный баг нашли и в старых версиях Android. Эта уязвимость подвергает угрозе взлома 60 % пользователей мобильной операционной системы от Google.

Конфликты между IT-гигантами стали уже привычным явлением, причем проигравшей стороной в противостоянии технологических корпораций нередко становятся сами пользователи.

Пользователи Windows попали под риск стать жертвами хакеров после того, как в блоге Google Project Zero, посвященном информационной безопасности, появилась информация о незакрытой уязвимости в операционной системе от Microsoft. В ответ на это глава Microsoft по безопасности К. Бец заявил, что решение Google публиковать свою находку до того, как для устранения уязвимости в Windows 8.1 выйдет патч, говорит не столько о принципах компании, сколько о желании напакостить конкурентам.

До выпуска патча в момент публикации Project Zero оставалось всего два дня.

По словам старшего антивирусного аналитика «Лаборатории Касперского» А. Иванова, уязвимость для Windows 8.1 достаточно серьезная, так как она позволяет обойти UAC (User Account Control). Обход этого защитного механизма Windows увеличивает шансы у вредоносного софта остаться незамеченным в системе.

Молчать о «дырах» в ПО до тех пор, пока они не будут устранены, было хорошей идеей, добавил К. Бец. Если сообщать о них заранее, то это может принести пользователям только вред, подвергнув их риску взломов. Кроме того, это только подгоняет компании к выпуску обновлений, хотя процесс подготовки хорошо работающих патчей – достаточно длительный.

Project Zero публично не сообщали об обнаруженной уязвимости 90 дней (ее нашли еще 13 октября), поэтому представители компании вполне могли оставить свою находку в тайне и чуть дольше.

«Мы попросили Google сотрудничать с нами для защиты пользователей и задержать публикацию этих данных до вторника 13 января, когда мы планируем выпустить патч», – подчеркнул К. Бец.

На следующий же день после публикации сообщения об уязвимости Windows аналитик исследовательской компании Rapid7 Т. Бирдсли заявил о серьезном баге в компоненте WebView операционной системы Android 4.3 и более ранних ее версий. WebView – это часть ПО, которое позволяет просматривать веб-страницы, не запуская для этого отдельное приложение.

Уязвимости в браузере Android представляют достаточно серьезную угрозу для пользователей, отмечает антивирусный эксперт «Лаборатории Касперского» В. Чебышев. Последствиями атаки на браузер могут стать кража персональной информации (например, данных банковских карт), установка вредоносных приложений, которые будут шпионить за устройством и совершать другие вредоносные операции. На сегодняшний день «Лаборатория Касперского» не зафиксировала ни одного массового случая атак подобного рода, так как авторы вирусов в основном пользуются методами социальной инженерии для распространения мобильного вредоносного ПО, но в будущем ситуация может измениться.

Android 4.3 – не новая версия операционной системы, она вышла еще в 2013 г., но 60 % пользователей Android (а это почти миллиард человек) до сих пор используют ее или более старые версии ОС. Уязвимость WebView может дать хакерам доступ к данным всех этих людей.

При этом Google не сможет просто решить эту проблему: как сообщили в компании, Google не разрабатывает самостоятельно патчи для версий Android старше 4.4, они смогут лишь одобрить поступивший к ним патч для устранения этой уязвимости и сообщить о ней производителям устройств.

«Текущая модель распространения ОС Android среди производителей мобильных устройств не предполагает единой точки хранения патчей для операционной системы. Более того, сама система построена таким образом, что пользователь не может “накатить” патч самостоятельно», – пояснил В. Чебышев «Газете.Ru».

Пользователи вынуждены ждать обновления всей прошивки от изготовителя устройства, а они не торопятся выпускать такие прошивки, так как выгоднее для них просто выпустить новое устройство. Ситуация, при которой изготовитель выпустит свежий Android 5 для устройства, которое появилось несколько лет назад, маловероятна ***(Google и Microsoft меряются***

багами // InternetUA (http://internetua.com/Google-i-Microsoft-meryauatsya-bagami). – 2015. – 15.01).

***

Ранее сообщалось о не совсем корректном поведении компании Google, которая опубликовала в открытом виде информацию об уязвимости в операционной системе Windows 8.1. Microsoft просила задержать размещение данных на несколько дней до выхода патча, однако поисковая корпорация продолжила следовать собственным правилам.

Google не стала останавливаться на достигнутом и накануне вновь поступила аналогичным образом: опубликовала информацию о нескольких уязвимостях, сопроводив их описанием алгоритма для эксплуатации. На этот раз баг касается пользователей не только Windows 8.1, но и Windows 7. От Microsoft также последовала просьба задержать распространение данных, так как релиз «заплатки» задерживался из-за технических сложностей, однако Google осталась непреклонна.

В Microsoft отметили, что уязвимость не носит критического характера, однако потенциально открывает доступ к некоторой пользовательской информации. В то же время, утверждают в корпорации, отсутствуют доказательства того, что данная уязвимость когда-либо использовалась. Кроме того, чтобы эксплуатировать ее, предварительно потребуется использовать другую уязвимость ***(Google снова подставила пользователей Windows // InternetUA (http://internetua.com/Google-snova-podstavila-polzovatelei-Windows). – 2015. – 17.01).***

***

Фишеры подделывают письма от LinkedIn для хищения учетных данных жертв

В последнее время увеличилась активность мошенников, отправляющих фишинговые письма якобы от имени поддержки LinkedIn. Как сообщают специалисты Symantec в блоге компании, в теле фишингового сообщения указывается, что в связи с подозрительной активностью на учетной записи пользователя было применено «принудительное обновление безопасности».

Для того чтобы восстановить свою учетную запись, пользователь якобы должен загрузить прикрепленный HTML-документ и следовать указанным в нем инструкциям. Документ внешне копирует форму входа в учетную запись LinkedIn, но введенные логин с паролем передаются на сторонний сайт.

Мошенники используют достаточно простую технику обхода спам-фильтров, прописывая Linkedin вместо LinkedIn в теме сообщения. Обычно жертва не успевает заметить ошибку в написании названия веб-сайта и поддается на уловки преступников. Более того, использование

прикрепленного HTML-документа позволяет обойти черные списки браузеров с нежелательными сайтами.

Для того чтобы защитить учетную запись от взлома, достаточно не переходить по ссылкам в подозрительных письмах и не передавать свои логин и пароль сторонним личностям. Также рекомендуется подключить двухфакторную аутентификацию ***(Фишеры подделывают письма от LinkedIn для хищения учетных данных жертв // InternetUA (http://internetua.com/fisheri-poddelivauat-pisma-ot-LinkedIn-dlya-hisxeniya-ucsetnih-dannih-jertv). – 2015. – 16.01).***

***

В социальной сети Instagram появилась своеобразная брешь, позволяющая любому желающему получить доступ к конфиденциальным изображениям произвольного пользователя сервиса через уменьшенные копии (превью) снимков.

Недостаток был выявлен исследователями из Quartz и, как сообщается, затрагивает лишь те фото, которые ранее находились в открытом доступе, а позже были помечены, как личные. Более того, брешь затрагивает только владельцы общедоступных учетных записей.

Важно также отметить, что потенциальный злоумышленник может воспользоваться недостатком при помощи сторонних служб, интегрированных с Instagram, поскольку они раскрывают URL-адрес изображений.

Администрация социальной сети уверяет, что вместе со следующими обновлениями ошибка будет устранена, а процесс управления частными фото пользователя станет более простым ***(Instagram подвергает риску компрометации личные данные пользователей // InternetUA (http://internetua.com/Instagram-podvergaet-risku-komprometacii-licsnie-dannie-polzovatelei). – 2015. – 15.01).***

***

По информации управления кибербезопасности генштаба французской армии, после терактов в Париже Францию накрыла беспрецедентная волна хакерских атак. За прошедшие четыре дня зарегистрированы около 19 тыс. кибератак на французские сайты, сообщил в четверг, 15 января, глава управления, контр-адмирал А. Кустийер.

Франция впервые стала объектом столь масштабной кибератаки, указал он далее. «Подобного еще никогда не происходило», – цитирует его слова агентство AP. А. Кустийер указал, что на взломанных сайтах появляются флаги или исламистские лозунги. Атакам подверглись сайты самого разного содержания – от госучреждений до частных фирм, включая мелкие предприятия, такие как пиццерии ***(Францию накрыла беспрецедентная волна кибератак // МедиаБизнес***

(http://www.mediabusiness.com.ua/content/view/42075/118/lang,ru/). – 2015. – 16.01).

***

Исследователи отдела Counter Threat Unit (CTU) компании Dell обнаружили новый тип вируса, который обходит защиту пароля при авторизации в Active Directory.

Об этом пишут Новости ИТ со ссылкой на 3D-News.

Новая вредоносная программа получила название Skeleton Key.

Вирус позволяет злоумышленнику подключиться к Active Directory, если система использует пароль как единственный фактор идентификации. При этом для входа используется любая комбинация, которая принимается как правильный пароль.

Вредоносная программа впервые была обнаружена в клиентской сети, которая использует пароли для подключения к электронной почте и VPN-сервисам.

«Skeleton Key вводится как внутренний патч памяти на контроллере доменов AD жертвы и позволяет владельцу авторизоваться в качестве любого пользователя, в то время как реальный владелец учётной записи продолжает подключаться без изменений», – говорится в уведомлении. Исследователи также добавили, что с помощью данной программы можно подключиться от имени администратора Active Directory.

Главным преимуществом Skeleton Key является то, что вирус практически невозможно обнаружить, так как при аккуратном использовании он никак себя не проявляет. Active Directory – это очень популярный продукт в корпоративной среде, поэтому подобный вирус открывает широкие возможности для, например, корпоративного шпионажа.

Получив физический или VPN-доступ к сети, можно авторизоваться и просмотреть данные финансовой отчётности, HR-отдела или отдела перспективных разработок.

Вооружённого Skeleton Key взломщика от любой информации в крупной компании отделяет всего лишь один подкупленный или обманутый сотрудник.

У программы обнаружены и определённые слабости – после перезагрузки контроллера доменов вирус приходится устанавливать заново. Также изученная версия вируса совместима только с 64-битной Windows, что также накладывает определённые ограничения.

Наиболее надёжной защитой от Skeleton Key в Dell считают использование многофакторной идентификации в контроллере доменов – это делает вирус абсолютно безвредным ***(Вирус Skeleton Key взламывает любой пароль в Active Directory // Новости ИТ (http://www.novostiit.net/virus-skeleton-key-vzlamyivaet-lyuboy-parol-v-active-directory-00014250). – 2015. – 16.01).***

***

Компания ESET предупреждает о появлении новой разновидности трояна-шифратора с уникальным механизмом заражения файлов. Вредоносная программа носит название Win32/Virlock.

Как и другие известные шифраторы, Virlock блокирует рабочий стол инфицированного компьютера, кодирует файлы и выводит на экран требование выкупа. Зловред работает с широким перечнем типов файлов: среди них – .exe, .doc, .xls, .zip, .rar, .pdf, .ppt, .mdb, .mp3, .mpg, .png, .gif, .bmp, .p12, .cer, .psd, .crt, .pem, .pfx, .p12, .p7b, .wma, .jpg и .jpeg. При этом Virlock способен заражать файлы на сетевых дисках и съёмных носителях.

В дополнение к «традиционным» функциям вредоносная программа может инфицировать файлы как полиморфный вирус, встраивая в них свой код. Для этого применяется специальная схема. Вместо обычного для данного типа вредоносного ПО побайтного шифрования, зловред преобразует файл в исполняемый. Для этого Virlock создаёт новый файл с зашифрованным содержимым документа и своим кодом, удаляет оригинальный файл и перезаписывает новый с тем же именем, но с расширением .exe.

Запуск инфицированного файла сопровождается созданием двух новых, осуществляющих дальнейшее заражение системы. Полиморфизм гарантирует уникальность тела вредоносной программы в каждом «обработанном» файле.

Часть кода вымогателя ответственна за отображение пользователю экрана блокировки, при этом применяются уже ставшие типичными методы самозащиты, в том числе завершение процессов проводника и диспетчера задач. Сообщение в окне блокировки содержит текст предупреждения и предложение оплатить сумму выкупа в биткоинах в эквиваленте 250 дол. США.

Любопытно, что Virlock способен выполнять некоторую локализацию интерфейса окна блокировки. Для этого используется соединение с веб-сайтом google.com и дальнейший анализ домена, на который осуществляется перенаправление, например, google.com.au, google.ca, google.co.uk или google.co.nz. Также используется функция GetUserGeoID. Для стран, соответствующих вышеперечисленным доменам, отображается свой флаг, стоимость биткоинов и текущий курс национальной валюты.

Обнаружено уже несколько модификаций вредоносной программы. Кроме того, отмечается, что некоторые жертвы уже заплатили выкуп злоумышленникам ***(Обнаружен первый «саморазмножающийся» шифратор // InternetUA (http://internetua.com/obnarujen-pervii--samorazmnojauasxiisya--shifrator). – 2015. – 18.01).***

***

Эксперты предупреждают, что в социальной сети Facebook распространяется новая схема спамеров, получившая название «10 самых горячих Snapchat'ов».

Как сообщается в блоге компании BitDefender, за последние несколько недель эксперты заблокировали десятки сайтов, обещающих показать пользователям утекшие из Snapchat интимные фотографии и прочие данные. В Facebook вредоносная кампания проходит под тегами #TrendingUSA, #ViralTruck, #ViralDips и #FunChoke – один из сайтов уже набрал более 75 тыс. отметок «Мне нравится» и 4771 подписчиков в Twitter.

На прошлой неделе спам-кампания заняла второе место по популярности в Facebook, уступая лишь классической обманной схеме «узнай посетителей своей страницы». Специалисты BitDefender утверждают, что мошенники нацелены на хищение личных данных, взлом страниц пользователей и рассылку спама от их имени, а также использование финансовых данных в нелегальных целях.

Сценарий, задействованный спамерами, не вызывает удивления – обычные пользователи социальных сетей почти всегда следуют по ссылкам на сайты, обещающие показать интимный контент ***(Мошенники используют Facebook для проведения новой спам-кампании // InternetUA (http://internetua.com/moshenniki-ispolzuuat-Facebook-dlya-provedeniya-novoi-spam-kampanii). – 2015. – 18.01).***

***

ИБ-эксперт Э. Новелла обнаружил уязвимости в широкополосных маршрутизаторах ADB Pirelli, используемых операторами связи Movistar (Испания) и ISP (Аргентина). По словам исследователя, одна из брешей позволяет удаленно получить контроль над устройствами по всему Интернету, а также проникать в домашние сети и управлять ими.

Э. Новелла отметил, что в данном случае ни аутентификация, ни другие способы защиты не способны предотвратить похищение конфиденциальной информации. Проблема заключается в том, что внутренний веб-сервер маршрутизатора, используемый для настройки его конфигурации через браузер, доступен для интернет-пользователей без аутентификации.

Это позволяет злоумышленнику получить пароль владельца домашней сети Wi-Fi, используя простой запрос HTTP в виде открытого текста, например, curl -s http://x.x.x.x/wlsecurity.html | grep -i «var wpapskkey», где x.x.x.x – это IP-адрес маршрутизатора (его можно узнать с помощью сканеров сети, таких как Shodan). Этот способ также позволяет получить ключ сессии и как следствие, контроль над устройством. В результате, злоумышленник сможет осуществлять перезагрузку маршрутизатора, открывать порты компьютерам в локальной сети, менять настройки DNS и т. д.

Вторая уязвимость позволяет провести реверс-инжиниринг алгоритма генерации ключей WPA, и таким образом вычислить ключи шифрования по умолчанию, используемые в сети Wi-Fi ***(Уязвимости в маршрутизаторах ADB Pirelli позволяют получить контроль над устройствами // InternetUA (http://internetua.com/uyazvimosti-v-marshrutizatorah-ADB-Pirelli-pozvolyauat-polucsit-kontrol-nad-ustroistvami). – 2015. – 16.01).***

***

Twitter-акаунти газети The New York Post та інформаційної агенції United Press International (UPI) стали об'єктами хакерських атак, повідомила BBC.

Зловмисники опублікували на них фейкові твіти новин на військові та економічні теми.

Один з постів у Twitter UPI містив вигадане посилання на заяву Папи Римського про те, що «почалася третя світова війна».

Натомість на акаунті NYP було запущено качку про «початок військових дій між США і Китаєм». Ішлося про те, що американський авіаносець «Джордж Вашингтон» (USS George Washington) «бере участь в активній битві» з китайськими військовими кораблями у Південно-Китайському морі.

Офіційний представник Пентагону заявив, що твіт про військові дії з Китаєм «не відповідає дійсності». UPI підтвердила, що атаки зазнав її аккаунт та новинний сайт.

На Twitter-акаунті було розміщено шість фейкових заголовків. Крім того, до вигаданої історії про Федеральну резервну систему на домашній сторінці було додано баннер гарячих новин.

Нині всі згадувані фейкові твіти стерті. NYP повідомила, що вона розслідує кібератаку.

Протягом останніх двох років кібератак зазнав ряд західних медій, серед них Agence France-Presse та BBC, нагадує британська інформаційна агенція.

Хакерську атаку на NYP і UPI, зазначає BBC, було здійснено через чотири дні після вчиненої на акаунти регіонального Центрального командування (Centcom) Міністерства оборони США ***(Хакери здійснили атаки на сторінки у Twitter американських медійних сайтів // Телекритика (http://www.telekritika.ua/kontekst/2015-01-17/102622). – 2015. – 17.01).***

***

Прошло совсем немного времени после появления обновленного вируса-вымогателя CryptoWall, а Microsoft уже обнаружила очередную версию этого вредоносного ПО. Сценарий распространения CryptoWall 3.0 (или Win32/Crowti) практически повторяет предыдущую кампанию, с той

лишь разницей, что файлы, содержащие вирус, получили наименование HELP_DECRYPT.

12 января нынешнего года Microsoft выявила 288 устройств, инфицированных новейшей версией вредоносного ПО. Пострадавшие пользователи должны в недельный срок заплатить 500 дол. в биткоиновом эквиваленте, если хотят восстановить утраченные файлы. По истечении этого срока сумма выкупа увеличивается до 1000 дол.

Исследователь безопасности, известный под псевдонимом Kafeine, также проанализировал CryptoWall 3.0 и сообщает, что коммуникация вредоноса с C&C-серверами закодирована с помощью потокового шифра RC4 и осуществляется посредством сети I2P.

Ранее эксперты компании Cisco после тщательного изучения CryptoWall 2.0 установили, что вредоносное приложение способно самостоятельно переключаться между 64-битной и и 32-битной архитектурой ***(Обнаружена очередная версия вируса-вымогателя CryptoWall // InternetUA (http://internetua.com/obnarujena-ocserednaya-versiya-virusa-vimogatelya-CryptoWall). – 2015. – 16.01).***

***

Украинские IT-специалисты совместно с американскими экспертами обнаружили ряд компьютерных вирусов, осуществляющих кибератаки на государственные органы Украины, заявил экс-глава «Майкрософт Украина», а ныне заместитель главы администрации Президента по вопросам проведения административных, социальных и экономических реформ Д. Шимкив, пишет «Зеркало недели. Украина» (http://zn.ua/TECHNOLOGIES/u-poroshenko-soobschili-o-rossiyskih-virusah-atakuyuschih-gossayty-164420_.html).

«Обнаружили ряд вирусов, созданных российскими спецслужбами специально для атак на украинские госсайты. По крайней мере, так считают американские специалисты. Вирусы очень умные, грамотно построенные с инженерной точки зрения», – рассказал изданию AIN Д. Шимкив.

По его словам, украинская сторона активно работает с производителями антивирусов.

«Хотя эти вирусы хитрые, постоянно меняют сигнатуру. Но мы тоже хитрые. Есть очень неплохие ребята в Госспецсвязи, которые осуществляют защиту периметров», – говорит представитель АП.

В частности, он отметил, что особенно серьезные атаки происходят во время эскалации событий на востоке, а также когда Президент П. Порошенко достигает позитивных результатов в тех или иных переговорах.

«Видим связь. Атаки направлены на госсайты, на погашение каналов связи и ограничение доступа к ресурсам. Вирусы направлены на снятие и пересылку данных», – уточнил Д. Шимкив ***(У Порошенко сообщили о российских вирусах, атакующих госсайты // Зеркало недели. Украина***

(http://zn.ua/TECHNOLOGIES/u-poroshenko-soobschili-o-rossiyskih-virusah-atakuyuschih-gossayty-164420_.html). – 2015. – 19.01).

***

Эксперты утверждают, что в Украине участились атаки мошенников на банкоматы. При этом преступники придумывают более изощренные способы хищения средств.

Как сообщают «Вести», ограбления зачастую совершаются на следующий день после загрузки банкомата деньгами и в тех местах, где они не подключены к сигнализации. Об этом поведал начальник службы информационной безопасности УкрСиббанка BNP Paribas Group А. Моршнев.

В отличие от обычных скиммеров, которые воруют деньги со счетов клиентов с помощью спецнакладок на банкоматы, схема, по которой действуют злоумышленники, помогает опустошать сейф терминала с помощью специального вируса.

Чтобы обойти систему защиты, мошенники проделывали отверстие в корпусе банкомата, получали доступ к разъему USB и устанавливали вредоносную программу, благодаря которой выясняли, сколько в банкомате наличных, и могли запросить купюры необходимого номинала. После загрузки денег отверстие закрывали, скрывая следы преступления, чтобы можно было воровать деньги из одного банкомата по несколько раз.

Часто для мошеннических операций используются и «трояны». Программа считывает данные магнитной ленты пластиковой карты и посылает ложную команду на выдачу банкнот ***(Мошенники воруют деньги из банкоматов, запуская «троянов» // InternetUA (http://internetua.com/moshenniki-voruuat-dengi-iz-bankomatov--zapuskaya--troyanov). – 2015. – 18.01).***

***

Хакеры могут скомпрометировать популярные мобильные приложения для знакомств с целью получения информации о пользователях. Об этом предупреждают исследователи Synack в интервью изданию Ars Technica. По их словам, подобного рода взломы могут поспособствовать вторжению в личную жизнь жертв.

Исследователям К. Муру и П. Уордлу удалось отслеживать перемещения пользователей популярного приложения для знакомств Grindr, отправляя спуфинговые запросы к серверам, обслуживающим приложение. По их словам, уязвимость существует из-за специальной функции в Grindr, позволяющей пользователям увидеть, как далеко от них находятся другие люди, желающие завести знакомство через мобильное приложение.

Для того чтобы проэксплуатировать уязвимость, исследователи отправили несколько запросов на серверы, обслуживающие Grindr, в которых указывались разные данные о местоположении экспертов. Grindr передавал

исследователям расстояние к определенным пользователям, желающим познакомиться через приложение, и путем триангуляции К. Муру и П. Уордлу удалось установить точное местоположение жертвы.

Результаты исследования были представлены на конференции Shmoocon. Эксперты установили местоположение пользователей Grindr в области залива Сан-Франциско. По их словам, сопоставление этих данных с информацией, доступной в социальных сетях, позволит полностью деанонимизировать жертв. Исследователи призвали разработчиков Grindr исправить эту уязвимость, но в компании решили не вносить никаких изменений, поскольку считают данную функцию ключевым элементом приложения, а не брешью ***(Приложения для знакомств передают информацию о местоположении пользователей // InternetUA (http://internetua.com/prilojeniya-dlya-znakomstv-peredauat-informaciua-o-mestopolojenii-polzovatelei). – 2015. – 20.01).***

***

Министерство иностранных дел Украины обращает внимание на существование фальшивого блока информационных ресурсов, функционирующих якобы от имени министерства, сообщает корреспондент proIT.

Как информирует пресс-служба министерства, в последнее время блог mfa-gov-ukraine.blogspot.com распространяет сообщения якобы от имени МИД. Кроме того, сообщения этого ресурса рассылаются с электронных адресов mfa.gov.ukraine@gmail.com и mfa.gov.ukraine@hotmail.com.

МИД сообщает, что не имеет никакого отношения к блогу mfa-gov-ukraine.blogspot.com и просит не использовать его материалы в качестве официального источника информации министерства.

Пресс-служба МИД напомнили, что их ведомство направляет информационные сообщения исключительно из адресов press@mfa.gov.ua, dip@mfa.gov.ua и mfa.ukraine@gmail.com.

Кроме этого, Министерство иностранных дел еще раз напоминает об адресах своих официальных аккаунтов в соцсетях:

https://www.facebook.com/UkraineMFA

https://twitter.com/MFA_Ukraine

http://instagram.com/mfa_ukraine

http://www.youtube.com/user/UkraineMFA

http://vk.com/mfa_ukraine ***(МИД предупреждает о поддельных ресурсах рассылающих информацию от его шимени // ProIT (http://proit.com.ua/news/internet/2015/01/19/175628.html). – 2015. – 19.01).***

***

Выявлена критическая уязвимость в работающей с сертификатами библиотеке PolarSSL. Брешь позволяет удаленному пользователю выполнить произвольный вредоносный код на системе жертвы.

Как сообщают представители компании ARM, осуществляющей разработку и поддержку свободной крипографической библиотеки PolarSSL, в ней была устранена критическая уязвимость, позволяющая удаленно скомпрометировать атакуемую систему.

Брешь, получившая идентификатор CVE-2015-1182, существует из-за неправильной обработки определенных последовательностей ASN.1, содержащихся в сертификатах X.509. При этом опасность угрозы одинаково высока, как для серверных, так и для клиентских приложений.

Напомним, что поддержка PolarSSL среди прочего реализована в таких распространенных продуктах, как OpenVPN, FreeRDP и PowerDNS. В настоящее время разработчики уже выпустили исправление безопасности для всех затрагиваемых версий библиотеки ***(Выявлена критическая уязвимость в работающей с сертификатами библиотеке PolarSSL // InternetUA (http://internetua.com/viyavlena-kriticseskaya-uyazvimost-v-rabotauasxei-s-sertifikatami-biblioteke-PolarSSL). – 2015. – 21.01).***

***

Исследователь безопасности В. Хатас опубликовал подробности о двух уязвимостях в некоторых версиях популярного медиа-плеера VLC. Бреши позволяют злоумышленнику вызвать повреждение памяти и выполнить произвольный код. Одна из уязвимостей связана с нарушением доступа функции предотвращения выполнения данных (DEP), а другая – с доступом к записи данных.

Первая уязвимость, обнаруженная 24 ноября прошлого года, возникает, когда вводимые пользователем данные должным образом не проверяются при обработке специально созданного файла FLV. Подобно первой, вторая брешь возникает, когда вводимые пользователем данные не проверяются корректно при обработке специально созданного файла M2V. Как сообщил В. Хатас, обе уязвимости могут быть проэксплуатированы «контекстно-зависимым злоумышленником для того, чтобы вызвать повреждение памяти и потенциально выполнить произвольный код».

Бреши, классифицированные как опасные, присутствуют в версиях медиа-плеера VLC 2.1.5 и были протестированы в Windows XP SP3. Поскольку эта платформа больше не поддерживается, а значит, не получит обновлений безопасности, миллионы пользователей по всему миру потенциально подвергаются риску.

Разработчики медиа-плеера VideoLAN получили уведомление о брешах 26 декабря 2014 г., однако исправления до сих пор не выпущены ***(В медиа-плеере VLC обнаружены серьезные уязвимости // InternetUA (http://internetua.com/v-media-pleere-VLC-obnarujeni-sereznie-uyazvimosti). – 2015. – 21.01).***

***

Хакеры разрабатывают USB-кабель для осуществления атак «человек посередине». Устройство также позволит осуществлять шпионскую деятельность.

На конференции ShmooCon 2015 исследователь безопасности и основатель компании Great Scott Gadgets М. Оссман продемонстрировал проект TURNIPSCHOOL – USB-кабель, позволяющий совершать атаки «человек посередине» и осуществлять шпионскую деятельность, сообщает портал Arstechnica.

В ходе выступления М. Оссман и двое его коллег по проекту Д. Спилл и Д. Бун рассказали о разработке TURNIPSCHOOL и двух других проектах, целевым назначением которых является проведение мониторинга (и последующий перехват) данных, проходящих по USB-соединениям. По словам М. Оссмана, разработка шпионских инструментов не так сложна, как это кажется на первый взгляд.

Большинство подобных проектов основаны на готовом открытом аппаратном обеспечении, таком как BeagleBone Black. Например, USBProxy, разработанный Д. Спиллом на основе BeagleBone Black, позволяет осуществлять мониторинг траффика, проходящего через соединения USB 2.0 и реплицирует некоторые возможности более дорогостоящего USB-эммулятора FaceDancer.

В то время как большинство подобных проектов соответствуют и даже превышают возможности технологий, используемых АНБ, их разработка занимает довольно много времени и требует немалых денежных средств. В отличие от них, TURNIPSCHOOL использует недорогое аппаратное обеспечение, доступное даже любителю. По словам М. Оссмана, следующим шагом в разработке проекта, станет использование USB-кабеля для осуществления атаки на хост-компьютер ***(Хакеры разрабатывают USB-кабель для осуществления атак «человек посередине» // InternetUA (http://internetua.com/hakeri-razrabativauat-USB-kabel-dlya-osusxestvleniya-atak--cselovek-poseredine). – 2015. – 22.01).***

***

Во второй половине 2014 г. увеличилось количество злоумышленников, эксплуатирующих уязвимости в Microsoft Silverlight. Об этом сообщается в ежегодном отчете по безопасности компании Cisco. Тем не менее, Flash и Java до сих пор считаются лидерами по количеству существующих эксплоитов.

В 2014 г. наблюдалось снижение количества эксплоитов для Java. В основном это вызвано отсутствием в Java новых уязвимостей нулевого дня, введением функции автообновления в Java Runtime Environment и блокировкой устаревших версий JRE в браузерах.

Также отмечается, что киберпреступники стали гораздо реже использовать Flash для рассылки эксплоитов. В то же время наблюдается

значительное увеличение популярности атак с применением инфицированных PDF-документов, а также инфицированием ПК через Microsoft Silverlight.

Исследователи также обнаружили вредоносное ПО на основе Flash, взаимодействующее с JavaScript. По их словам, эксплоит разбит на два отдельных Flash- и JS-файла, что усложняет обнаружение и блокировку вредоносного ПО антивирусными продуктами. Это также помогает киберпреступникам повысить эффективность своих атак ***(Злоумышленники стали чаще эксплуатировать уязвимости в Silverlight // InternetUA (http://internetua.com/zloumishlenniki-stali-csasxe-ekspluatirovat-uyazvimosti-v-Silverlight). – 2015. – 22.01).***

***

Как следует из сообщения экспертов Symantec, 22 января, неподтвержденная уязвимость нулевого дня в Adobe Flash Player была обнаружена исследователем безопасности под псевдонимом Kafeine. По данным последнего, брешь затрагивает все актуальные версии Adobe Flash Player и уже эксплуатируется злоумышленниками при помощи наборе эксплоитов Angler.

«Symantec расценивает данную уязвимость как критическую, поскольку Adobe Flash Player широко распространен среди пользователей», – подчеркивают в антивирусной компании.

Представители Adobe на сегодняшний день не подтвердили наличие уязвимости. Какое-либо исправление безопасности также отсутствует, однако, согласно результатам предварительного анализа, в ходе атаки злоумышленники используют специально сформированные SWF-файлы.

В настоящее время специалисты Symantec Security Response продолжают изучение бреши и обещают опубликовать более подробную информацию, как только она появится ***(Неподтвержденная уязвимость нулевого дня обнаружена в Adobe Flash Player // InternetUA (http://internetua.com/nepodtverjdennaya-uyazvimost-nulevogo-dnya-obnarujena-v-Adobe-Flash-Player). – 2015. – 22.01).***

***

В «облачном» хранилище данных Google Drive обнаружена опасная уязвимость, позволяющая деанонимизировать пользователей, пишет Блог Imena.UA (http://www.imena.ua/blog/google-drive-bug-for-personality/).

Уязвимость позволяет раскрывать и отображать полные имена пользователей учётных записей, «привязанных» к почтовым сервисам Gmail, Yahoo!, Hotmail и другим. В сети уже опубликован исходный код эксплоита для этой бреши.

Пользователи требуют от Google немедленно исправить уязвимость, прежде чем все, кто хранит свои данные в «облачном» сервисе, не начали раскрывать данные друг друга.

Кроме того, уязвимостью могут воспользоваться спамеры, чтобы собирать имена и электронные адреса для последующих таргетированных кампаний ***(Уязвимость в Google Drive позволяет раскрыть личность пользователя // Блог Imena.UA (http://www.imena.ua/blog/google-drive-bug-for-personality/). – 2015. – 22.01).***

***

Компания «Доктор Веб» предупреждает пользователей о массовой почтовой рассылке, с использованием которой злоумышленники распространяют опасную вредоносную программу-загрузчик.

Основное предназначение этого приложения – скачивание и запуск на инфицированном компьютере троянца-шифровальщика Trojan.Encoder.686, представляющего для пользователей серьезную угрозу, поскольку пострадавшие от его действия файлы в настоящее время не поддаются расшифровке.

Троянец-загрузчик, добавленный в вирусную базу Dr.Web под наименованием Trojan.DownLoad3.35539, распространяется злоумышленниками при помощи массовой спам-рассылки в виде вложенного в сообщения электронной почты ZIP-архива. Специалисты «Доктор Веб» зафиксировали случаи распространения сообщений, содержащих опасное вложение, на разных языках, в том числе английском, немецком и даже грузинском.

Архив содержит .SCR-файл – к данному типу файлов по умолчанию относятся скринсейверы (заставки) Windows. Подобные файлы являются исполняемыми. При попытке запуска файла из архива Trojan.DownLoad3.35539 извлекает из своего тела, сохраняет на диск и открывает на экране атакуемого компьютера текстовый RTF-документ.

Одновременно с этим Trojan.DownLoad3.35539 устанавливает соединение с одним из принадлежащих злоумышленникам удаленных серверов, загружает оттуда архив, содержащий троянца-шифровальщика Trojan.Encoder.686, который также известен под названием CTB-Locker, после чего распаковывает и запускает его. Успешно инициализировавшись на зараженном компьютере, Trojan.Encoder.686 выполняет шифрование пользовательских файлов, после чего демонстрирует на экране заранее сформированное злоумышленниками сообщение.

Примечательно, что вирусописатели отводят своим жертвам лишь 96 часов на оплату расшифровки файлов, угрожая при этом, что в случае отказа от сотрудничества все зашифрованные файлы будут потеряны навсегда. При этом за подробной информацией об условиях и сумме выкупа киберпреступники предлагают пострадавшим пользователям обратиться на сайт, расположенный в анонимной сети TOR.

Троянец-шифровальщик Trojan.Encoder.686 собран с использованием библиотек TOR и OpenSSL, криптографию которых активно использует. В процессе шифрования пользовательских файлов энкодер активно

эксплуатирует возможности CryptoAPI с целью получения случайных данных и эллиптическую криптографию, в связи с чем расшифровка пострадавших от его действия файлов в настоящий момент не представляется возможной.

Компания «Доктор Веб» предупреждает пользователей о необходимости проявлять бдительность и не запускать присланные по e-mail исполняемые файлы, не открывать вложения в сообщениях электронной почты, полученных из сомнительных источников, а также напоминает о целесообразности своевременного резервного копирования всех представляющих ценность данных.

Также напоминаем, что в составе Dr.Web Security Space версии 9 и 10 имеется несколько компонентов, позволяющих настроить своевременное автоматическое резервное копирование наиболее ценной информации и обезопасить компьютер от действия троянцев-энкодеров, а также других вредоносных программ ***(Опасный троянец-шифровальщик распространяется в почтовой рассылке // ITnews (http://itnews.com.ua/news/75750-opasnyj-troyanets-shifrovalshhik-rasprostranyaetsya-v-pochtovoj-rassylke). – 2015. – 22.01).***

***

Хакеры и прочие злоумышленники проявляют всё больше интереса к личной информации пользователей на мобильных устройствах, которые хранят её там всё чаще. Последнее время наблюдается непрерывный рост вредоносного программного обеспечения для мобильных устройств, в основном на Android.

Компания Lookout провела исследование с участием свыше 60 млн пользователей по всему миру и выяснила, что только в США в 2014 г. распространённость вредоносного ПО для Android увеличилась на 75 % по сравнению с предыдущим годом. Исследователи оговариваются, что мобильные вирусы и прочие угрозы по-прежнему довольно редки, однако такой сильный рост не может не вызывать беспокойства.

Один из самых распространённых видов угроз – вирусы-вымогатели, или ransomware. Такие программы блокируют устройство и требуют денег для разблокировки. Вымогатели ScareMeNot и ScarePakage вошли в пятёрку самых опасных мобильных угроз в ряде развитых стран, таких как США, Великобритания и Германия.

Мобильные угрозы по-разному выражены в разных географических регионах. Так, в Западной Европе очень активны фиктивные услуги, снимающие деньги с телефонного счёта (chargeware), тогда как в США этот механизм часто запрещён операторами и редко встречается.

Есть и хорошие новости: в 2014 г. резко сократилось число заражений рекламными вирусами (adware), с 25 % до 10 %. В основном это произошло благодаря Google, которая предприняла радикальные меры по их искоренению в своём поиске и магазине Play ***(В 2014 году проникновение***

Android-вирусов в США выросло на 75 % // InternetUA (http://internetua.com/v-2014-godu-proniknovenie-Android-virusov-v-ssha-viroslo-na-75). – 2015. – 25.01).

***

Порядка 11 % из всех доступных Android-приложений для осуществления платежей содержат вирусы. Так, согласно данным компании RiskIQ, 40 тыс. программ из проверенных 350 тыс. имели опасные уязвимости, а еще 40 тыс. – требовали «опасные разрешения».

По утверждениям гендиректора компании Э. Манусоса, приложения мобильного банкинга предоставляют злоумышленникам уникальную возможность перехвата важных банковских данных. Последние они могут использовать для дальнейшего осуществления мошенничества, заявил он журналистам Forbes.

В каждой стране имеется по крайней мере одно Android-приложение online-банкинга, которое является непроверенным и способно нанести вред устройству. При этом Э. Манусос подчеркивает, что у девайсов Apple подобных проблем не возникает, поскольку она задействует весьма закрытую экосистему и проверяет каждое приложение перед его публикацией на сайтах online-магазинов программ.

Согласно информации RiskIQ, зачастую злоумышленники создают приложения, похожие на подлинные. Они встраивают в продукты вредоносный код, либо же запрашивают у пользователей практически неограниченный доступ к данным мобильного устройства.

Для того чтобы обезопасить себя от перехвата банковских и других данных через вредоносные приложения, стоит внимательно изучать разрешения, которые они затребуют. «Лучше избегать скачивания приложений через рекламы или электронную почту», – подчеркивает также Э. Манусос ***(11 % Android-приложений для осуществления платежей содержат вирусы // InternetUA (http://internetua.com/11--Android-prilojenii-dlya-osusxestvleniya-platejei-soderjat-virusi). – 2015. – 25.01).***

***

Исследователи из Fujitsu Limited и Fujitsu Laboratories разработали «первую в мире» технологию автоматической идентификации пользователей, потенциально уязвимых для кибератаки. Идентификация происходит с помощью наблюдения, как юзеры используют электронную почту и как ведут себя в Интернете во время веб-сёрфинга. Предполагается, что автоматический анализ значительно улучшит защищённость корпоративных сетей с большим количеством сотрудников, где никак нельзя уследить за всеми в ручном режиме.

Не секрет, что в большинстве компьютерных атак используется человеческий фактор – то самое уязвимое звено между экраном и креслом. Например, людям рассылают фишинговые письма с поддельным обратным

адресом, чтобы они щёлкнули по вредоносной ссылке или открыли файл с дроппером. Поскольку такие атаки проводятся на индивидуальной основе, отделу безопасности трудно выработать стандартизированные методы защиты.

Fujitsu Limited и Fujitsu Laboratories разработали онлайновый опросник, по результатам которого составляется профиль пользователя и вычисляется степень его уязвимости перед тремя видами атак:

1. Вирусные инфекции.
2. Мошенничество.
3. Утечка конфиденциальной информации.

В то же время система проводит анализ логов активности на персональном компьютере для уточнения оценки.

Разработанная методология представлена на 32-м симпозиуме по криптографии и информационной безопасности, который открылся 20 января 2015 г. в городе Китакюсю (Япония). Исследование сделано по заказу Министерства внутренних дел и коммуникаций Японии ***(Автоматическая идентификация потенциальных жертв взлома // InternetUA (http://internetua.com/avtomaticseskaya-identifikaciya-potencialnih-jertv-vzloma). – 2015. – 24.01).***

***

Неизвестные взломали российский сервис знакомств Topface и похитили данные 20 млн пользователей. Об этом сообщает Bloomberg со ссылкой на компанию Easy Solutions, занимающуюся вопросами безопасности в Интернете.

О взломе эксперты узнали благодаря сообщению на форуме для кибермошенников. Сообщается, что в руки преступников попали данные учетных записей 20 млн человек. Половина из них являются гражданами России. Уже известно, что хакеры смогли похитить логины и адреса электронной почты. Получили ли взломщики доступ к паролям, пока неизвестно.

В Easy Solutions не исключают, что украденные сведения могут использоваться для доступа к кредитным картам, банковским счетам, учётным записям о состоянии здоровья и другим личным данным. Подобная информация обычно быстро продаётся интернет-мошенникам, которые взламывают аккаунты пользователей на других сайтах при помощи автоматизированных программ, используя те же имена и пароли, которые вводились во время регистрации на сайте знакомств.

В отчете говорится, что около 50 % взломанных аккаунтов принадлежит россиянам. Ещё 40 % приходятся на жителей стран Евросоюза. При этом 7 млн пострадавших пользуются почтой на Hotmail, ещё 2,5 млн – на Yahoo!, а 2,3 – на Gmail.

Согласно информации с сайта Topface, сервис является «самым быстрорастущим сайтом знакомств в мире». Компания оценивает

посещаемость сайта в 1,6 млн посетителей. Головной офис компании находится в Санкт-Петербурге. Гендиректором Topface является Д. Филатов ***(Хакеры похитили данные 20 миллионов пользователей российского сервиса Topface // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/khakery-pokhitili-dannye-20-millionov-pol.html). – 2015. – 26.01).***

***

В конце декабря специалисты по безопасности из Google Security Team обнаружили ряд критических уязвимостей в реализации протокола NTP, который используется во многих промышленных системах управления для синхронизации времени на серверах.

Уязвимости, которым подвержены все NTP-сервера до версии 4.2.8, включают несколько вариантов переполнения буфера и позволяют атакующему удалённо выполнять произвольный код на сервере. Как отмечают исследователи, эксплоиты для данных уязвимостей уже существуют в публичном доступе.

По данным Positive Technologies, использование открытых источников позволяет легко выявить более 30 тыс. серверов в Интернет, до сих пор подверженных данной уязвимости. Причём 4300 из них расположены в российском сегменте сети Интернет.

Рекомендации по устранению уязвимостей можно найти в уведомлении ICS-CERT, а также на сайте поддержки NTP. Основной совет – обновить NTP до версии 4.2.8 с официального сайта ntp.org. В случае невозможности обновления предлагается два способа блокировать атаки через настройки конфигурации.

Запретить Autokey Authentication путем удаления или комментирования всех тех строк файла ntp.conf, которые начинаются с директивы crypto.

Для всех недоверенных клиентов указать в файле /etc/ntp.conf директиву restrict … noquery, что не позволит недоверенным клиентам запрашивать информацию о статусе NTP-сервера.

Можно поступить и проще: отключить службу NTP на серверах и сетевых устройствах или отфильтровать ее на межсетевом экране, если внешний доступ к ней не требуется. Но если служба всё же используется внешними клиентами, можно ограничить доступ к порту 123 списком доверенных IP-адресов.

Судя по опыту прошлых багов NTP, можно прогнозировать, что блокирование новых уязвимостей вряд ли будет происходить быстро, считают специалисты Positive Technologies.

К примеру, в начале прошлого года по Интернету прокатилась мощная волна DDoS-атак с усилением через NTP. Во время такой атаки злоумышленники отправляют на NTP-сервер специальный запрос, а в качестве отправителя подставляют IP-адрес жертвы; NTP-сервер посылает на этот адрес вполне легитимный ответ, который может быть в несколько сот

раз длиннее запроса – таким образом, сервер точного времени становится невольным усилителем атаки. Рекомендации CERT по защите от таких атак были опубликованы в январе прошлого года. Однако даже спустя полгода, в июне, насчитывалось ещё 17 тыс. уязвимых NTP-севеpов, причём многие из них продолжали участвовать в DDoS-атаках, усиливая мусорный трафик в сотни раз ***(Хуже, чем DDoS. Новые уязвимости в NTP-серверах // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/khuzhe-chem-ddos-novye-uyazvimosti-v-ntp-servera.html). – 2015. – 23.01).***

***

Киберпреступники разработали новые виды вредоносов с усовершенствованным функционалом.

Разработчики вредоносного ПО используют исходный код RAT-трояна Njw0rm для создания новых вредоносов, способных предоставить взломщику полный доступ к ПК жертв. Об этом сообщили исследователи Trend Micro в блоге компании.

Njw0rm представляет собой модифицированную версию RAT-трояна njRAT. В июле 2014 г. специалисты Microsoft проводили операцию, нацеленную на обезвреживание обеих версий вредоносов. Еще тогда они сказали, что киберпреступники могут свободно создать собственную версию данного вредоносного ПО, поскольку необходимая информация и исходный код трояна находились в открытом доступе.

По данным Trend Micro, исходный код Njw0rm был опубликован на хакерских форумах в мае 2013 г. Вскоре после этого киберпреступники начали создавать новые версии вредоносного ПО.

Одними из новых троянов, созданными на основе Njw0rm, стали Kjw0rm и Sir Do0om. Специалисты Trend Micro обнаружили их в январе и декабре 2014 г. соответственно. Вредоносы оснащенны улучшенной панелью управления и могут собирать больше информации. К примеру, Kjw0rm может обнаруживать установленные антивирусы и определять версию установленного пакета .NET Framework, в то время как Sir Do0om может передавать злоумышленнику информацию о характеристиках ПК жертвы, установленном антивирусном ПО и межсетевых экранах.

Njw0rm может исполнять произвольные команды и запускать файлы, похищать логины и пароли, а также автоматически обновляться. Его улучшенная версия Kjw0rm может выключать или перезагружать компьютер, загружать и открывать произвольные файлы. Еще более интересным выглядит Sir Do0om – троян может майнить биткоины, запускать DDoS-атаки, контролировать ПК по таймеру, завершать процессы антивирусных программ и открывать веб-сайт, на котором отображается текст Корана.

Трояны распространяются через переносные устройства. Они скрывают папки на флешках и создают ярлыки с их именами, которые на самом деле открывают вредонос ***(Исходный код RAT-трояна Njw0rm***

используется для создания нового вредоносного ПО // InternetUA (http://internetua.com/ishodnii-kod-RAT-troyana-Njw0rm-ispolzuetsya-dlya-sozdaniya-novogo-vredonosnogo-po). – 2015. – 26.01).

***

Эксперты раскрыли самые уязвимые места Windows

Самой уязвимой частью Windows в 2014 г. стал браузер Internet Explorer – к такому выводу пришли специалисты международной антивирусной компании ESET по итогам изучения кибератак на программное обеспечение.

Как сообщили в пресс-службе ESET, количество уязвимостей браузера версий 6–11 в сравнении с 2013 г. возросло почти в два раза и составило 243. По мнению экспертов, укрепить безопасность браузера можно за счет «использования режима Enhanced Protected Mode в IE, особенно в связке с 64-битной версией Windows 8.1».

Уязвимыми для киберугроз местами ОС Microsoft, хотя и значительно меньше браузера, также оказались драйвер win32k.sys, общие драйверы режима ядра Windows, .NET Framework, пользовательские компоненты Windows и продукт Office.

Самой популярной киберугрозой оказалось «удаленное исполнение кода», при которой злоумышленники устанавливали вредоносное ПО на компьютеры пользователей. Кроме того, по словам экспертов, операционная система оказалась уязвимой для state-sponsored атак, в частности трояна BlackEnergy, который использовался для кражи данных корпоративных пользователей, и Privilege Escalation (LPE) атаки, позволяющие повысить права атакующих в системе ***(Эксперты раскрыли самые уязвимые места Windows // InternetUA (http://internetua.com/eksperti-raskrili-samie-uyazvimie-mesta-Windows). – 2015. – 27.01).***

***

25 тыс. европейских пользователей Facebook подписались под коллективным иском к руководству социальной сети с требованием выплатить до 14 млн дол. компенсации за несанкционированное использование персональных данных. Первые слушания по делу назначены на 9 апреля.

Согласно информации на сайте инициаторов судебного процесса, заявители требуют от компании компенсации за несанкционированное использование персональных данных пользователей – до 500 евро каждому истцу. В частности, речь идет о данных для системы PRISM, и информации, используемой в служебных целях соцсети. Помимо компенсации от Facebook требуют прекратить использование информации пользователей в целях соцсети.

Инициатором иска выступил австрийский студент-юрист М. Шремс. Все международные операции Facebook проводит через свой ирландский

офис. Иск опирается на европейский закон о защите данных – европейцы строже относятся к вопросам защиты персональных данных, чем американцы.

Калифорнийская компания считает, что иск является недопустимым, так как подобные требования не могут выдвигаться со стороны пользователей. Первые слушания по делу пройдут 9 апреля в Вене.

Facebook регулярно оказывается в центре скандалов, связанных с нарушением политики приватности данных. В 2012 г. британские власти расследовали эксперимент над ничего не подозревающими пользователями, в ходе которого социальная сеть пыталась повлиять на их эмоциональное состояние, чтобы выяснить, как изменится тональность записей ***(Facebook ответит в суде перед 25 тысячами европейских пользователей // InternetUA (http://internetua.com/Facebook-otvetit-v-sude-pered-25-tisyacsami-evropeiskih-polzovatelei). – 2015. – 27.01).***

***

Українські кібервійська захопили сервер сепаратистів у Криму. Про це у Facebook повідомив провідний український хакер Є. Докукін.

Дані із сервера Є. Докукін передав СБУ.

Всього отримали 925,8 МБ даних. Для початку хакер виклав 21,6 МБ даних (17,7 МБ в архіві) до мережі. Потім він обіцяє викласти і нові дані з цього сервера ***(Українські кібервійська захопили сервер сепаратистів у Криму // InternetUA (http://internetua.com/ukra-nsk--k-berv-iska-zahopili-server-separatist-v-u-krimu). – 2015. – 27.01).***

***

Сайты так называемых пресс-центров террористических организаций «ДНР» и «ЛНР» прекратили свое существование, пишет «Обозреватель» (http://obozrevatel.com/politics/15847-sajtyi-press-sluzhb-lnr-i-dnr-prekratili-svoe-suschestvovanie.htm).

При попытке войти на сайты браузер сообщает, что сервер с таким доменным именем не найден.

Называющая себя и. о. «министра информации» «ДНР» М. Бережнева связала проблемы с «попыткой похищения домена», сообщает сайт террористов «Донецкое агентство новостей».

Киевский хакер Е. Докукин от имени команды «Украинских кибервойск» заявлял о блокировке 61 сайта террористов ***(Сайты пресс-служб «ЛНР» и «ДНР» прекратили свое существование // Обозреватель (http://obozrevatel.com/politics/15847-sajtyi-press-sluzhb-lnr-i-dnr-prekratili-svoe-suschestvovanie.htm). – 2015. – 29.01).***

***

Украинские хакеры заблокировали счета сторонников «ДНР» и «ЛНР» в системах QIWI, Яндекс.Деньги и WebMoney, написал в Facebook

Е. Докукин, сообщает «Обозреватель» (http://tech.obozrevatel.com/news/15872-hakeryi-zablokirovali-scheta-posobnikov-dnr-i-lnr.htm).

«После блокировки предыдущих счетов террористов http://on.fb.me/1JsLsNk, недавно я заблокировал новые счета. Это счета сторонников “ДНР” и “ЛНР” в системах QIWI, Яндекс.Деньги и WebMoney, которые указаны на сайте http://bne.su/tseli.html», – написал он.

Кроме того счета в трех системах уже заблокированы – в прошлом году в QIWI и Яндекс, а в январе в WM. В системе WebMoney кошельки привязаны к счету WMID 129610448782, принадлежащий ТАРМАН из Одинцово, Россия.

Также Е. Докукин отметил, что за июнь – ноябрь Украинские кибервойска заблокировали 2 млн дол. на 144 счетах террористов ***(Хакеры заблокировали счета пособников «ДНР» и «ЛНР» // Обозреватель (http://tech.obozrevatel.com/news/15872-hakeryi-zablokirovali-scheta-posobnikov-dnr-i-lnr.htm). – 2015. – 29.01).***

***

29 января пользователи социальной сети Facebook начали массово получать спам-рассылку, пишет «Обозреватель» (http://tech.obozrevatel.com/news/71842-facebook-porazil-virus-spam-ataki.htm).

Так пользователям приходило уведомление, что их и еще 19 человек отметили на видео. Но прежде чем начать просмотр видео просят установить видеоплеер.

«Обозреватель» советует вам ни в коем случае не открывать такие сообщения от друзей и устанавливать видеоплеер. Но если все-таки открыли – немедленно сменить пароль и проверить ваше устройство на вирусы.

Напомним, что ранее Facebook уже поражал похожий вирус, который начинал рассылать такие же сообщения от зараженного аккаунта ***(Facebook поразил вирус спам-атаки // Обозреватель (http://tech.obozrevatel.com/news/71842-facebook-porazil-virus-spam-ataki.htm). – 2015. – 29.01).***

***

В сети началась эпидемия вируса-блокировщика сайтов

В Интернете началась эпидемия нового вируса-блокировщика. Однако вместо пользовательских компьютеров он блокирует сайты.

Специалисты по безопасности из компании High-Tech Bridge отмечают, что троянская программа, как правило, устанавливается на серверы намеченного для блокировки сайта задолго до самого факта атаки.

Злоумышленники модифицируют несколько серверных скриптов таким образом, чтобы шифровать информацию перед занесением в базу данных, и расшифровывать её «на лету» при получении запроса к базе. Ключ шифрования хранится на удалённом сервере.

Таким образом, работа вредоноса оставалась незамеченной для пользователей и администрации, пока в «день Д» злоумышленники не пошли в атаку и не удалили ключ шифрования. После блокировки злоумышленники связываются с владельцами сайтов и требуют определённую сумму за расшифровку. Сначала специалисты High-Tech Bridge посчитали это уникальным случаем нацеленной атаки.

Однако несколько дней спустя с аналогичным вымогательством столкнулся ещё один клиент, у которого злоумышленники зашифровали базу с учётными данными пользователей.

При этом на сегодняшний день ни один антивирус не определяет инсталляторы данной вредоносной программы ***(В сети началась эпидемия вируса-блокировщика сайтов // InternetUA (http://internetua.com/v-seti-nacsalas-epidemiya-virusa-blokirovsxika-saitov). – 2015. – 31.01).***

***

RansomWeb: Новая угроза, затмевающая DDoS-атаки и кражу конфиденциальных данных

С помощью новой техники злоумышленники взламывают веб-сайты, шифруют базу данных и требуют выкуп за ее расшифрование.

Специалисты ИБ-компании High-Tech Bridge обнаружили новую угрозу безопасности, которая может затмить DDoS-атаки, похищение конфиденциальных данных и нанесение ущерба интернет-ресурсам. Речь идет о новой хакерской технике под названием RansomWeb, с помощью которой злоумышленники взламывают веб-сайты, шифруют базу данных и требуют выкуп за ее расшифрование.

В декабре прошлого года специалисты компании зафиксировали интересный случай компрометации веб-сайта одного из финансовых предприятий. Ресурс перестал функционировать, сообщая об ошибке базы данных, а его владелец получил письмо от злоумышленников с требованием выкупа за ее расшифрование.

В ходе анализа выяснилось, что несколько модифицированных скриптов осуществляли шифрование информации перед вводом в базу данных и ее расшифрование после извлечения из базы. Стоит отметить, что зашифрованными были только самые критические поля таблиц базы данных. При этом ключ расшифрования содержался на удаленном веб-сервере, доступ к которому можно было получить исключительно через HTTPS-соединение. В течение шести месяцев преступники наблюдали за веб-сайтом. В назначенный день хакеры удалили ключ с сервера, в результате чего использовать базу данных стало невозможно. Затем злоумышленники потребовали выкуп за ее расшифровку.

Как отмечают специалисты, подобные атаки могут быть использованы не только для получения выкупа, но и для нанесения ущерба веб-сайту на протяжении длительного времени. В случае успешно проведенной атаки восстановить базу данных возможно только после уплаты выкупа. При этом

создавать резервные копии практически не имеет смысла, поскольку база данных будет копироваться в зашифрованном виде. Однако подобную атаку достаточно легко обнаружить при помощи проведения постоянного мониторинга целостности файлов ***(RansomWeb: Новая угроза, затмевающая DDoS-атаки и кражу конфиденциальных данных // InternetUA (http://internetua.com/RansomWeb--novaya-ugroza--zatmevauasxaya-DDoS-ataki-i-kraju-konfidencialnih-dannih). – 2015. – 29.01).***

***

Как следует из сообщения хакера Р. Саси, ему удалось обнаружить и проэксплуатировать уязвимость в прошивке дронов Parrot AR Drones, в результате чего исследователь смог дистанционно осуществить угон летательного аппарата.

Первый в своем роде вирус получил название Maldrone. При этом, по словам Р. Саси, выявленный им бэкдор позволяет перехватить контроль над устройством на том же расстоянии, которое необходимо для осуществления беспроводного управления. «После того как мой вредонос атакует контроллеры, двигатели останавливаются, и беспилотник начинает падать кирпичом вниз, – поясняет исследователь. – Однако бэкдор мгновенно перехватывает управление, и если высота действительно большая, есть достаточное количество времени, чтобы избежать падения» ***(Создан инфицирующий дроны вирус // InternetUA (http://internetua.com/sozdan-inficiruuasxii-droni-virus). – 2015. – 29.01).***

***

Украина входит в десятку стран как по количеству жертв кибератак, так и по количеству их источников. Такой статистикой с ЛІГАБізнесІнформ поделился В. Илибман, менеджер по продуктам безопасности Cisco в Украине, Грузии и странах СНГ, во время презентации ежегодного отчета Cisco о киберугрозах.

По мнению В. Илибмана, в мире наблюдается восприятие постсоветского пространства как источника киберугроз наравне с Китаем, и Украина – не исключение. По мнению эксперта Cisco, существует взаимосвязь между количеством исходящих кибератак в стране и степенью развития сетевой инфраструктуры. Украина располагает одними из самых быстрых в Европе наземных волоконно-оптических сетей передачи трафика. Некоторые операторы достигли в своих сетях скорости передачи в 100 гигабит в секунду.

Более того, специалист Cisco считает, что количество кибератак в стране может возрасти после появления национального покрытия связи третьего и четвертого поколений (3G/4G). Это пример «обратной стороны» технологий – помимо стимулирования бизнеса и создания новых бизнес-моделей, сети 3G открывают хакерам доступ к огромной базе уязвимых

смартфонов с высокоскоростным подключением, которые могут быть «зомбированы» для DDoS-атак и рассылки спама.

Также в качестве факторов, способствовавших попаданию Украины в антирейтинг, эксперт Cisco называет несовершенство законодательной базы, из-за чего даже задержанным хакерам бывает тяжело инкриминировать преступление. Кроме этого, против имиджа Украины играет большое количество незанятых высококвалифицированных IT-специалистов, которые ищут альтернативные способы заработка ***(Украина входит в Топ-10 стран по количеству кібератак // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2015/01/30/ua-cyberattacks.html). – 2015. – 30.01).***