СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(14–27.04)

2015 № 8

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(14–27.04)
№ 8

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

Відповідальний редактор
Л. Чуприна, канд. наук із соц. комунікацій

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ 4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 14
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 17
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 33
Інформаційно-психологічний вплив мережевого спілкування на особистість 33
Маніпулятивні технології 36
Зарубіжні спецслужби і технології «соціального контролю» 41
Проблема захисту даних. DDOS та вірусні атаки 50

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Исследовательская компания Gemius сравнила то, как развиваются в разных странах самые популярные социальные сети. Помимо Украины, аналитики смотрели также на Турцию, Россию, Данию, Румынию, Венгрию и Беларусь. Как оказалось, быстрее всего в нашей стране растет Twitter – по аудитории сервиса микроблогов Украина занимает третье место среди попавших в исследование стран. Количество пользователей Facebook также увеличивается. В то же время в России крупнейшая соцсеть мира растет медленнее всех, а в Беларуси динамика и вовсе отрицательная. Самой «социально активной» оказалась Турция, пишет AIN.UA (http://ain.ua/2015/04/16/575766).

Среди анализируемых стран Twitter пользуется наибольшей популярность в Турции, где ежемесячно его посещал каждый третий пользователь Интернета. В Украине доля Twitter-аудитории за год возросла на 56 %.

В 2015 г. Украина оказалась среди стран, меньше всего пользующихся Facebook – опережают нас в данном разрезе только Россия и Беларусь («ВКонтакте» все еще лидирует в СНГ). За анализируемый период Facebook в среднем посещали 3 из 10 пользователей уанета. И все-же доля Facebook в Украине растет динамичней, чем в соседних странах – с 2013 г. аудитория возросла на 9 %, а в феврале 2015 г. социальную сеть посетили 38 % украинской аудитории.

Instagram был в тренде в каждой из исследуемых стран. По сравнению с предыдущим периодом, в 2014 г. Instagram привлек примерно в два раза больше пользователей в Украине, России и Польше (9 % в 2014, 5 % в 2013 г.). По другим странам рост был менее значительным.

Исследование проводилось среди интернет-пользователей в возрасте от 18 до 69 лет и основано на среднемесячных данных 2013–2014 гг. ***(Как растет аудитория соцсетей в Украине, России, Турции и других странах // AIN.UA (http://ain.ua/2015/04/16/575766). – 2015. – 16.04).***

***

Сервис микроблогов Twitter получил обновленный дизайн главной страницы. Свежий интерфейс создан с одной-единственной целью – для привлечения новых пользователей.

Новая главная страница Twitter будет отображаться тем пользователям, которые еще не зарегистрировались в системе или еще не успели залогиниться, пишет портал CNET. На ней отображаются наиболее популярные темы твитов, для удобства разбитые по категориям. Этих категорий несколько, и при каждом обновлении страницы пользователь сможет узнать новое из мира политики, бизнеса, космоса, селебрити и т. д.

После выбора категории и клика по ней система сама соберет подборку самых свежих и актуальных твитов по теме и сгенерирует страницу с ними. Все это выполняется в реальном времени и за считанные мгновения. По мнению руководства Twitter, данное новшество позволит потенциальным пользователям не только ознакомиться с возможностями сервиса, но также узнать что-то новое по интересующей их теме и даже высказать свое мнение по тому или иному вопросу. Последнее действие потребует регистрации, и именно так и планируется расширять пользовательскую базу.

Но даже если желание создать аккаунт не появится, Twitter все равно останется в плюсе, ведь в сгенерированной твит-ленте будет демонстрироваться реклама. Это тоже солидный доход для компании, так как, согласно статистике, около 200 млн человек посещают сервис в месяц, не проходя процедуру аутентификации.

Для Twitter очень важно привлечение новых пользователей ввиду того проект существует с июля 2006 г., и на текущее время количество зарегистрированных в нем пользователей составляет около 500 млн. Из них активными являются порядка 140 млн. Добавим, что новая страница доступна пока лишь пользователям из США. Дата ее международного распространения не назначена ***(Twitter обновил дизайн главной страницы // InternetUA (http://internetua.com/Twitter-obnovil-dizain-glavnoi-stranici). – 2015. – 18.04).***

***

Пользователи Android-устройств получили долгожданную возможность искать посты в Facebook. Ранее поиск по постам был доступен пользователям десктопной версии, мобильного сайта и iOS-приложения Facebook.

По словам представителя соцсети, функция поиска уже запущена и будет постепенно распространяться в течение ближайших недель.

Напомним, искать посты в Facebook в настоящее время могут только пользователи, указавшие в настройках американский вариант английского языка ***(Facebook запустил поиск по постам для Android-устройств // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_zapustil_poisk_po_postam_dlya_android_ustroystv). – 2015. – 15.04).***

***

Facebook интегрирует WhatsApp в свою платформу

Несмотря на то что компания Facebook владеет контрольным пакетом акций мессенджера WhatsApp, он до последнего времени не был частью платформы социальной сети. Скоро при помощи кнопки «Отправить» (Send) пользователи смогут превращать статусы и новости Facebook в сообщения WhatsApp.

В последнее время новости из стана разработчиков мессенджеров, принадлежащих Facebook, приходят одна за одной. WhatsApp недавно добавила

долгожданную функцию телефонных звонков, а Messenger превратился в отдельную платформу.

Когда в 2014 г. социальная сеть приобрела популярное приложение, руководство интернет-гиганта пообещало, что разработчики WhatsApp останутся независимой компанией. Анонс новой функции – первый знак интеграции Facebook и самого массового в мире мессенджера. Среди экспертов ходят слухи, что следующим шагом станет включение WhatsApp в платформу Facebook Messenger.

Кнопка «Отправить» будет выглядеть как одноименная иконка в WhatsApp. Она будет располагаться внизу экрана рядом с кнопкой «Мне нравится».

Новая функция находится в стадии бета-тестирования. Когда она станет доступна широкому кругу пользователей, пока не сообщается ***(Facebook интегрирует WhatsApp в свою платформу // InternetUA (http://internetua.com/Facebook-integriruet-WhatsApp-v-svoua-platformu). – 2015. – 19.04).***

***

Гейм-дизайнер М. Кокс опубликовал в своём блоге небольшое исследование, посвящённое интересу пользователей Google к соцсети Foursquare с течением времени – по данным Google Trends, число поисковых запросов значительно снизилось после разделения Foursquare на два сервиса.

М. Кокс пишет, что был лояльным пользователем Foursquare – каждый день чекинился и публиковал развёрнутые отзывы о ресторанах, парках, отелях, театрах. При помощи приложения встречался с людьми и хорошо проводил время.

В мае 2014 г. Foursquare убрал чекины из основного приложения и преобразовал его в аналог Yelp – агрегатор отзывов о местах.

По словам М. Кокса, пользователи почувствовали себя «преданными» – сервис использовал их отзывы, но отнял у них то, за что они изначально его полюбили.

В апреле 2015 г. источники Techcrunch сообщили, что Yahoo и Foursquare ведут переговоры о продаже компании за 900 млн дол. ***(Пользователи полностью разочаровались в Foursquare после разделения сервиса // InternetUA (http://internetua.com/polzovateli-polnostua-razocsarovalis-v-Foursquare-posle-razdeleniya-servisa). – 2015. – 20.04).***

***

Twitter дал возможность принимать личные сообщения от любого пользователя сервиса. Активировать её можно будет в настройках, пишет Marketing Media Review (http://mmr.ua/news/id/twitter-dal-vozmozhnost-prinimat-lichnye-soobschenija-ot-ljubogo-polzovatelja-servisa-44047/).

Пользователи также получат возможность ответить любому другому пользователю, который отправил им личное сообщение, даже если он не

является их подписчиком. Ранее, для обмена личными сообщениями они должны были подписаться на обновления друг друга.

«Личные сообщения – лучший способ перевести своё публичное общение в Twitter в приватный режим», – пояснил инженер по программному обеспечению Twitter Н. Вонг. «Мы изменили механизм работы личных сообщений, чтобы вам было ещё проще общаться с другим человеком один на один или же с выбранной группой людей в любой точке мира».

Напомним, что групповые сообщения были запущены в Twitter в январе.

Кроме того, Twitter также внедрил новую кнопку для отправки личных сообщений на странице профиля пользователя в приложениях для iOS и Android.

По мнению представителей компании, новые возможности отправки и получения личных сообщений могут заинтересовать многие бизнесы. Эти изменения помогут тем компаниям, которые хотят предоставить своим клиентам ещё одну возможность взаимодействия с ними или же просто связи. Кроме того, в Twitter люди также обсуждают бренды, но не все готовы высказать свою точку зрения публично. Личные сообщения могут стать для этих пользователей возможностью более открыто поделиться своим мнением с другими людьми и компаниями ***(Twitter дал возможность принимать личные сообщения от любого пользователя сервиса // Marketing Media Review (http://mmr.ua/news/id/twitter-dal-vozmozhnost-prinimat-lichnye-soobschenija-ot-ljubogo-polzovatelja-servisa-44047/). – 2015. – 21.04).***

***

Основатель «ВКонтакте» и главный разработчик мессенджера Telegram П. Дуров дал интервью сообществу Live Plus. В нём он, в частности, рассказал о том, почему его соцсети не удалось выйти на международный рынок.

«После многих попыток международной экспансии стало понятно, что для успеха на зарубежных рынках “ВКонтакте” необходимо изменить три вещи – концепцию, название и акционерный состав, – рассказал П. Дуров. – Замена этих трёх компонентов на более актуальные для глобального рынка в итоге привела к появлению Telegram».

Говоря о будущем соцсети, он сделал благоприятный прогноз. «Технологических, интерфейсных и идеологических решений, заложенных в эту социальную сеть, хватит на много лет вперед, – считает П. Дуров. – Текущая команда имеет все шансы эти идеи и решения сохранить и развить». Однако он отметил, что «ценности и подходы “ВКонтакте”» должны распространяться на Mail.Ru Group, а не наоборот.

Кроме того, П. Дуров заявил, что не жалеет о продаже своих 12 % акций «ВКонтакте» генеральному директору «Мегафона» и совладельцу холдинга ЮТВ И. Таврину примерно за 3–4 млрд дол. После этого, уточнил он, «IT-рынок обвалился примерно в три раза». Однако вырученные деньги «позволили избавить Telegram от необходимости привлекать инвесторов». «В результате удалось не допустить той ошибки, которая в конечном счёте привела к

поглощению “ВКонтакте” холдингом Mail.Ru Group», – добавил он ***(Павел Дуров объяснил причины неудачи «ВКонтакте» в других странах // InternetUA (http://internetua.com/pavel-durov-ob-yasnil-pricsini-neudacsi--vkontakte--v-drugih-stranah). – 2015. – 22.04).***

***

Как «ВКонтакте» прожил год без П. Дурова

Год назад, 21 апреля, основатель соцсети «ВКонтакте» П. Дуров узнал о своём увольнении с поста гендиректора. Это стало результатом долгой корпоративной войны, которую он вёл с Mail.Ru Group и фондом UCP. «Таким образом, сегодня “ВКонтакте” переходит под полный контроль И. Сечина и А. Усманова. Наверное, в российских условиях нечто подобное было неизбежно, но я рад, что мы продержались семь с половиной лет», – написал он тогда. Через неделю предприниматель стал гражданином карибского государства Сент-Китс и Невис и сосредоточился на развитии своего нового проекта, мессенджера Telegram. Дела у П. Дурова идут вполне успешно, в прошлом году его включили в международный список перспективных молодых предпринимателей, его мессенджер стал популярен по всему миру, известные издания, вроде Wired или Dazed, берут у него интервью. The Village вспомнил, что произошло за это время с крупнейшей российской социальной сетью «ВКонтакте».

Полное поглощение

В сентябре прошлого года завершилась долгая история продажи «ВКонтакте». Медиахолдинг Mail.Ru Group, принадлежащий А. Усманову, полностью поглотил компанию. Он выкупил 48 % акций у второго акционера соцсети – фонда UCP И. Щербовича. Сумму сделки тогда оценивали в 1,47 млрд дол.

После этого холдинг договорился о прекращении судебных разбирательств между П. Дуровым и И. Щербовичем. А 10 октября А. Усманов даже поздравил П. Дурова с 30-летним юбилеем со страниц своей газеты «Коммерсантъ».

Родственник ВГТРК

После ухода П. Дурова исполняющим обязанности директора стал Б. Добродеев, сын гендиректора ВГТРК О. Добродеева. С 2013 г. он входил в совет директоров Mail.Ru Group и работал во «ВКонтакте» замдиректора по связям с инвесторами. После того как Mail.Ru стала единоличным владельцем соцсети, Б. Добродеев стал главой компании. Чуть позже он стал и директором по стратегии и развитию Mail.Ru Group.

Недавно он выступил в Госдуме и попросил у депутатов налоговые льготы. «Наша компания активно конкурирует с Google, крупными китайскими игроками интернет-рынка. Многие из них имеют в своих странах значительные налоговые льготы, и нам бы казалось логичным предоставить российским интернет-компаниям схожие льготы», – сказал он.

Контакт с телевизором

В прошлом году соцсеть отключила возможность встраивать видео с неё на другие сайты. Параллельно она начала сотрудничать с Первым каналом: он стал размещать во «ВКонтакте» свои передачи «Вечерний Ургант», «Пусть говорят», «Здоровье», «Пока все дома», «Точь-в-точь», «Ледниковый период», «Познер», «Что? Где? Когда?», «Человек и закон». Видео монетизируются за счёт встроенной рекламы, доходами от которой соцсеть делится с телеканалом. Пиратские видео тех же программ удаляются модераторами.

Кроме того, «ВКонтакте» стал направлять желающих посмотреть популярные зарубежные сериалы в онлайн-кинотеатр «Амедиатека», получая комиссию за каждого перешедшего на сайт. Так из самого большого онлайн-склада пиратского контента соцсеть превращается в рекламную площадку для производителей кино и телепередач. К примеру, поиск видео новых серий «Игры престолов» результатов не даёт.

Больше рекламы

После падения рынка медийной рекламы Mail.Ru Group решила сосредоточиться на новых источниках доходов. В частности, она собирается размещать больше мобильной и видеорекламы. Это не в последнюю очередь относится к «ВКонтакте», ведь её конкурент Facebook уже сделала ставку на видеоконтент.

Соцсеть хочет размещать больше рекламы и старается стать более комфортной для компаний. Недавно она запустила метрику постов в сообществах, численность которых превышает 10 тыс. пользователей. Их администраторы могут узнать, сколько людей увидело пост, перешло по ссылке и поделилось информацией. Предполагается, что эта опция поможет брендам и рекламным агентствам точнее оценить эффективность рекламы во «ВКонтакте».

Технические сложности

Количество сбоев «ВКонтакте» в последний год заметно увеличилось. Причины были разные. Летом соцсеть упала из-за жары. В сентябре пользователи некоторых стран не могли зайти на сайт из-за обрыва кабеля в Финляндии. 24 января возникли проблемы с сетевым оборудованием.

В апреле социальная сеть падала несколько дней подряд. Операционный директор компании А. Рогозов объяснял технические неполадки конкурсом в одном из популярных сообществ, который привлёк чересчур большое внимание пользователей ***(Как «ВКонтакте» прожил год без Дурова // InternetUA (http://internetua.com/kak--vkontakte--projil-god-bez-durova). – 2015. – 22.04).***

***

«ВКонтакте» закрыла возможность загружать mp3-файлы в раздел документов. Об этом сообщило сообщество LIVE Express, обозревающее новости соцсети.

Как рассказал TJ пресс-секретарь «ВКонтакте» Г. Лобушкин, ограничение связано с претензиями правообладателей. Какие компании

потребовали таких изменений, он не уточнил, однако заявил, что эта мера не связана с так называемым «списком 301».

Загрузка в документы музыкальных файлов других форматов (например, m4a, использующийся для песен в магазине iTunes Store) по-прежнему доступна без ограничений. Песни в формате mp3 можно добавлять в раздел аудиозаписей, однако в нём работает фильтрация: если запись была изъята по требованию правообладателей, повторно загрузить её нельзя.

В феврале «ВКонтакте» обновила свои приложения для операционной системы iOS, убрав раздел с музыкой из меню, однако пользователи обнаружили, что он оказался доступным через поиск по короткой ссылке vk.com/audio. В начале марта стало известно, что власти США проигнорировали просьбу «ВКонтакте» исключить соцсеть из «списка 301», в котором перечислены пиратские сайты.

Возможность передачи файлов в виде документов появилась во «ВКонтакте» 25 мая 2011 г., а позднее превратилась в неструктурированный каталог. В 2014 г. функция передачи документов появилась в мессенджере П. Дурова Telegram: его представители предлагали пересылать через mp3-файлы аудиосообщения. Позднее для звуковых сообщений появилась отдельная функция, но загрузка mp3-файлов осталась ***(«ВКонтакте» запретила передавать mp3-файлы через документы // InternetUA (http://internetua.com/vkontakte--zapretila-peredavat-mp3-faili-cserez-dokumenti). – 2015. – 22.04).***

***

«ВКонтакте» отключила «Яндекс.Музыку»

Социальная сеть «ВКонтакте» отключила приложение стримингового сервиса «Яндекс.Музыка» от своего API. Об этом сообщает Roem со ссылкой на заявление «Яндекса».

Отключение произошло около двух месяцев назад. Приблизительно в те же сроки, в феврале 2015 г., «ВКонтакте» убрала музыку из собственного iOS-приложения. Речь шла о прослушивании записей с серверов соцсети.

«“ВКонтакте” попросила прекратить использовать API, – заявили представители «Яндекса». «Это связано с настоятельной просьбой “ВКонтакте”», – отметили в компании.

В соцсети подтвердили разрыв соединения с Яндекс.Музыкой. «Да, отключили. По своим внутренним соображениям», – рассказал пресс-секретарь «ВКонтакте» Г. Лобушкин. Он отметил, что компания «оставляет за собой право ограничивать доступ к API в случаях использования данных в приложениях-конкурентах».

Сервис от «Яндекса» использовал данные «ВКонтакте» для импорта аудиозаписей пользователей соцсети в плейлист «Яндекс.Музыки». По данным источника, с конца июня 2013 г. импортом треков из «ВКонтакте» воспользовались около 548 тыс. раз.

В июне 2014 г. стало известно, что «ВКонтакте» планирует создать «отдельное мобильное приложение, с помощью которого можно прослушивать музыку из сети, подключившись к Интернету или сохранив записи, чтобы прослушать их позже без доступа к сети». В феврале 2015 г. соцсеть выпустила новое приложение для iPad и обновила версию для iPhone, исключив из программ для iOS музыкальный раздел ***(«ВКонтакте» отключила «Яндекс.Музыку» // InternetUA (http://internetua.com/vkontakte--otkluacsila--yandeks-muziku). – 2015. – 27.04).***

***

Социальная платформа «ВКонтакте» в течение ближайших нескольких дней запустит новый видеораздел, представляющий собой отдельную вкладку в «Моем видео». Информация поступила от А. Круглова во время его выступления на РИФ+КИБ 2015, пишет Marketing Media Review (http://mmr.ua/news/id/vkontakte-zapustit-konkurenta-youtube-44107/).

«Мы очень много чего знаем о пользователе; знаем, какие видео смотрит он, какие видео смотрят и загружают его друзья. Мы знаем, чем в принципе он интересуется», – комментирует А. Круглов.

На основе этих знаний и будет запущена платформа, демонстрирующая собранный по рекомендательной модели видеоконтент.

Представитель соцсети не исключил возможность продвижения видео с альтернативных площадок при условии его популярности. Для увеличения шансов добавления ролика в «рекомендуемые» производителям видеоконтента рекомендуется загружать видео в нативный плеер ***(ВКонтакте запустит конкурента YouTube // Marketing Media Review (http://mmr.ua/news/id/vkontakte-zapustit-konkurenta-youtube-44107/). – 2015. – 24.04).***

***

Facebook изменил алгоритм формирования новостной ленты

Измененный алгоритм серьезно повлияет на реферальный трафик издателей, сообщает Marketing Media Review со ссылкой на businessinsider.com (http://mmr.ua/news/id/facebook-izmenil-algoritm-formirovnija-novostnoj-lenty-44067/).

Топ-3 обновления:

Пользователи Facebook смогут увидеть более одного поста в новостной ленте от одного источника подряд. Ранее алгоритм Facebook не допускал этого. Поэтому пользователи смогут теперь увидеть больше контента в своей ленте.

Facebook начнет отдавать предпочтение контенту, размещенному друзьями. Пользователи теперь не пропустят контент, размещенный напрямую друзьями, который включает фото, видео, обновленный статусы и ссылки. Пользователь сможет также увидеть контент, размещенный издателями и контент страниц Facebook.

Facebook начнет прятать посты, которые получили лайки и комментарии от друзей. Такие истории появятся внизу новостной ленты или вообще не появятся. Это обновление может серьезно уменьшить охват пользователей издателями.

Обновления войдут в силу в течение нескольких недель ***(Facebook изменил алгоритм формирования новостной ленты // Marketing Media Review (http://mmr.ua/news/id/facebook-izmenil-algoritm-formirovnija-novostnoj-lenty-44067/). – 2015. – 22.04).***

***

Facebook в настоящее время обслуживает более 4 млрд просмотров видео в день. Об этом заявил генеральный директор компании М. Цукерберг. В январе 2015 г. этот показатель составлял 1 млрд, пишет Marketing Media Review (http://mmr.ua/news/id/polzovateli-facebook-ezhednevno-smotrjat-4-mlrd-video-44106/).

Facebook становится сильнее в сфере видео. Видео также связывает мобильную и рекламную стратегии. Более 75 % просмотров видео в Facebook происходят с мобильных устройств, и это означает, что люди готовы смотреть видео-рекламу.

Более 1 млн предприятий малого и среднего бизнеса выложили видео и разместили небольшое объявление рядом с ним.

М. Цукерберг также отметил, что 80 тыс. видео Facebook были встроены на сторонних сайтах в первый месяц после запуска функции, и анонсировал запуск сферического видео в лентах новостей в этом году.

Представители социальной сети также огласили следующую статистику:

Люди ежедневно осуществляют более 1 млрд поисков на мобильных устройствах в Facebook.

Сервис Instagram ежедневно используют 200 млн человек. Пользователи Instagram ежедневно тратят 21 мин. в сети.

В США более чем одна из каждых пяти минут, проведенных с мобильным телефоном, приходится на Facebook или Instagram.

Более 45 млрд сообщений ежедневно отправляются в Facebook, Messenger и WhatsApp ***(Пользователи Facebook ежедневно смотрят 4 млрд видео // Marketing Media Review (http://mmr.ua/news/id/polzovateli-facebook-ezhednevno-smotrjat-4-mlrd-video-44106/). – 2015. – 24.04).***

***

Компания Facebook продолжает расширять ассортимент фирменных приложений и представляет альтернативный номеронабиратель Hello для платформы Android. Как несложно догадаться, в основу здесь положена экосистема социальной сети. В числе прочих приятных особенностей – возможность совершения бесплатных звонков через Wi-Fi.

Как отмечает сама компания, у новинки есть три ключевых достоинства:

– использование данных социальной сети Facebook для идентификации звонящего даже в том случае, если человека нет в контакт-листе смартфона;

– продвинутая система поиска, которая позволит быстрее найти номер нужного абонента или организации;

– расширенные возможности использования черного списка, причем вызов не блокируется, звонящий просто перенаправляется в голосовую почту.

Не лишним будет отметить и голосовые вызовы по протоколу VoIP. Данная возможность уже давно стала частью Facebook Messenger, но теперь появилась и в новом приложении. Если же абонент не смог дозвониться до требуемого человека, ему будет предложено написать сообщение через Messenger ***(acebook Hello заменит стандартный набиратель номера Android // InternetUA (http://internetua.com/Facebook-Hello-zamenit-standartnii-nabiratel-nomera-Android). – 2015. – 25.04).***

***

Twitter запускает новую функцию Highlights, которая два раза в день будет составлять для пользователя персональный дайджест самых интересных твитов, избавляя от необходимости просматривать бесконечное количество постов, сообщает Bloomderg.

Мобильное приложение Twitter для Android будет помещать дайджест прямо в список уведомлений от приложений. По нажатии на уведомление пользователь попадет не в стандартную ленту, а в выжимку самого важного, по мнению социальной сети. Дата внедрения функции в iOS версию пока неизвестна.

Таким образом Twitter пытается справиться с последствиями попыток ускорить рост аудитории и глубину контакта с лентой, которые превратили ее в бесконечную очередь твитов. «Мы хотим вызвать у пользователя ощущение, что он закончил с лентой на сегодня», – говорит Тодд Джексон, разработчик Highlights ***(Twitter избавит пользователей от бесконечной ленты // InternetUA (http://internetua.com/Twitter-izbavit-polzovatelei-ot-beskonecsnoi-lenti). – 2015. – 25.04).***

***

Профессиональная социальная сеть LinkedIn с 350 млн пользователей запускает платное приложение, которое позволит компаниям предлагать контент своим же сотрудникам, чтобы они делились им в LinkedIn и Twitter.

В течение последнего года LinkedIn делала большие ставки на контент, и новый продукт, компании – Elevate – только подчеркивает экспансию в этом направлении.

Рекомендательный инструмент разработан для работодателей, которые смогут эффективно управлять контентом и «подталкивать» сотрудников к взаимодействию с ним. Идея заключается в том, что информация, транслируемая работниками, носит аутентичный характер и воспринимается более естественно, чем сообщения непосредственно от компаний.

Приложение также предлагает аналитику для обеих сторон: пользователи смогут посмотреть количество лайков, перепостов и комментариев к публикациям, а также просмотров вакансий и фоловеров страницы компании.

В настоящее время Elevate запустился в платной закрытой пилотной версии, в широкий доступ LinkedIn планирует вывести приложение в III квартале 2015 г. В компании рассказали, что уже в начале года начали тестировать инструмент совместно с несколькими крупными брендами, среди которых Unilever, Adobe и Quintiles ***(Вершняк Н. LinkedIn запускает инструмент для аутентичного распространения контента компаний // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/linkedin_zapuskaet_instrument_dlya_autentichnogo_rasprostraneniya_kontenta_kompaniy). – 2015. – 24.04).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

В Днепре городские проблемы решают через Facebook

В начале апреля исполнилось три года с начала работы горячей линии главы Днепропетровской обладминистрации, позволяющей решать многие вопросы дистанционно.

В 2014 г. у жителей региона возникало больше всего вопросов в связи с проблемами в сфере коммунального хозяйства (39,1 % от всех запросов). Далее шли вопросы, касающиеся благоустройства и строительства (11,9 %), проявлений коррупции (4,3 %), оплаты труда (4,3 %), соцзащиты населения (4,1 %).

Ранее Депутаты Днепра попросили Кабмин не «душить» людей тарифами на ЖКХ.

В ОГА также отметили, что жители области все чаще стали отдавать предпочтение именно электронному общению с областной властью. По данным заведующей сектором обеспечения доступа к публичной информации управления организационной работы аппарата ОГА Л. Романюк, за I квартал 2015 г. в обладминистрацию поступило 96 запросов, касающихся деятельности местных органов исполнительной власти, транспорта и связи, реализации жилищной политики и строительства (например, получение копии распоряжения руководителя департамента и т. д.). «При этом 62 % запросов были получены по электронной почте, еще 32 % обратившихся воспользовались традиционной почтой, и лишь 5 % граждан пришли лично», – привела статистику Л. Романюк.

Электронные заявки

Практически при каждом департаменте и управлении обладминистрации работают горячие линии, позвонив на которые можно получить консультации. Причем некоторые из них, отвечая спросу людей, работают в четком режиме – звонить можно в любой рабочий день с 9:00 до 18:00. В частности, всегда можно проконсультироваться по вопросам несвоевременной выплаты и погашения задолженности по зарплате – (056) 726-75-26 (28), а также узнать о жилищных субсидиях и пенсионной реформе – (056) 713-66-18, 713-65-60, 713-63-09.

Кроме того, электронные заявки на решение вопросов, связанных с ЖКХ, земельных вопросов, запросы о деятельности правоохранительных органов, благоустройстве и других проблемах можно оставить на сайте «Відкрита влада» – openpower.dp.gov.ua. На заполненное там электронное обращение обязаны ответить в течение 14 дней.

Помощь через соцсеть

А вот департамент коммунального хозяйства и капитального строительства Днепропетровского горсовета осваивает общение с горожанами в соцсети Facebook. Сотрудники департамента активно реагируют на заявки, оставляемые на странице facebook.com/departkomuna.

«С января после урагана дерево возле дома находилось в аварийном состоянии. Жильцы обращались в ЖЭК, но реакции никакой не последовало. А в конце марта я случайно наткнулся на департамент в соцсети и решил попробовать там оставить заявку. К моему удивлению, мне сразу же ответили, и уже через день дерево убрали. Сейчас я обратился с просьбой залатать дыры в асфальте, но этот вопрос уже серьезнее, и мне сказали, что нужно привезти официальное заявление непосредственно в департамент», – рассказал житель ул. Евпаторийской Евгений.

В начале апреля также на Facebook появилась страница Управления жилищного хозяйства горсовета, где можно задавать свои вопросы ***(В Днепре городские проблемы решают через Фейсбук // Днепропетровская Панорама (http://dnpr.com.ua/content/v-dnepre-gorodskie-problemy-reshayut-cherez-feysbuk). – 2015. – 22.04).***

***

Адміністратори найбільшої кіровоградської спільноти «Кировоград ВКонтакте» провели опитування щодо можливого перейменування обласного центру, варіант «Єлисаветград» – на другому місці.

Результати опитування можна переглянути на сторінці «Кировоград ВКонтакте». Станом на момент написання цієї новини участь у ньому взяли 1325 учасників спільноти віком від 18 до 55 років.

Більшість респондентів – 54,6 % (723 голоси) – на сьогодні виступають проти перейменування Кіровограда.

На другому місці за кількістю відданих голосів (29,4 %, 390 голосів) – перейменування міста в Єлисаветград.

Третє місце (7,8 %, 104 голоси) посіла назва «Златопіль». Інші варіанти поки не набрали навіть більше 3 % голосів ***(Учасники найбільшої кіровоградської спільноти у ВК висловилися за Єлисаветград // novosti.kr.ua (http://novosti.kr.ua/news/uchasniki-najbilsho-kirovogradsko-spilnoti-u-vk-vislovilisya-za-elisavetgrad.html). – 2015. – 16.04).***

***

Науковці вирішили за допомогою Twitter розвінчати міф про те, що наука – нудна. Вони почали ділитися цікавими фотографіями зі своїх польових досліджень із хештегом #BestFieldWorkPic.

Про це пише dailydot.com.

Першою використала хештег зоолог та блогер М. Джевелл. 20 квітня вона запропонувала за допомогою #BestFieldWorkPic позначати цікаві світлини з польових мандрівок.

Першим дослідниця опублікувала фото пораненої качки в коробці, пізніше – смішного пінгвіна.

Далі до її ініціативи приєдналися інші науковці й почали оприлюднювати свої світлини з робочих поїздок.

За даними сервісу Topsy, від початку Twitter-кампанії хештег #BestFieldWorkPic було використано 925 разів. Дописи з ним продовжують з'являтися у Twitter ***(Науковці спростовують стереотип про занудність науки за допомогою Twitter // MediaSapiens (http://osvita.mediasapiens.ua/web/social/naukovtsi_sprostovuyut_stereotip_pro_za_nudnist_nauki_za_dopomogoyu_twitter/). – 2015. – 23.04).***

***

Мэр испанского городка Хун уже четыре года управляет всеми муниципальными службами при помощи сервиса микроблогов Twitter.

Повсеместное внедрение Twitter в качестве средства связи с мэрией Х. Салас начал в 2011 г.

В городе живёт около 3 тыс. человек, и все они через Twitter могут полноценно взаимодействовать с мэрией – предварительно, горожане подтвердили свои учётные записи в мэрии, чтобы власти знали, с кем общаются.

Теперь сетью микроблогов пользуются все: от электриков и дворников до школьных учителей. Общение властей с горожанами выглядит следующим образом: вечером житель пишет мэру, что на улице перегорела лампочка в фонаре. Тот делает соответствующую отметку в Twitter электрика. Тот уже на следующий день выкладывает в сети фотографию отремонтированного фонаря.

Мэр Х. Салас отмечает, что такая «взаимная прозрачность» работает как кнут и пряник. Если власти не будут делать свою работу, жители сразу об этом узнают. При этом жители видят, что чиновники и коммунальные службы действительно работают и могут даже похвалить работника ***(Мэр испанского городка управляет всеми службами через Twitter // InternetUA***

(http://internetua.com/mer-ispanskogo-gorodka-upravlyaet-vsemi-slujbami-cserez-Twitter). – 2015. – 27.04).

***

Реагуючи на гуманітарну катастрофу в Гімалаях, де від наслідків землетрусу, за даними CNN, загинуло близько півтори тисячі людей, Facebook запровадила новий сервіс. Про це на своїй сторінці зазначив засновник мережі М. Цукерберг.

Послуга «Перевірка безпеки у Facebook» спрямована на користувачів, які перебувають у зоні стихійного лиха. Завдяки їй можна знайти та зв'язатися з друзями з Facebook у Непалі та відзначити друзів як таких, що перебувають у безпеці.

Мета послуги – «повідомити родину та друзів, що ти в порядку», зазначив М. Цукерберг.

Нагадаємо, 25 квітня в Непалі стався потужний землетрус магнітудою 7,9 – найсильніший за останні майже 80 років. Унаслідок стихійного лиха постраждалі місцеві мешканці, альпіністи, туристи. Замлетрус завдав шкоди будівлям, аеропорт у Катманду було зачинено.

У Непалі перебуває український журналіст і блогер Є. Іхельзон. Світлини з місця трагедії він публікує на своїй сторінці у Facebook ***(Facebook запровадив сервіс сповіщень про безпеку для користувачів у Гімалаях // Телекритика (http://www.telekritika.ua/svit/2015-04-26/106473). – 2015. – 26.04).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

В ближайшее время Twitter закроет доступ к своим данным для реселлеров, включая DataSift и NTT. Теперь компания намерена работать с потребителями напрямую, пишет searchengines.ru.

Twitter зарабатывает, продавая свои данные сторонним компаниям, таким как маркетинговые и рекламные агентства.

Для этого Twitter заключила партнёрские соглашения с реселлерами (перекупщиками) данных, включая DataSift, NTT и Gnip, которым было позволено перепродавать данные Twitter.

Год назад компания приобрела одного из своих партнёров в этом направлении – Gnip и начала напрямую продавать данные компаниям. Теперь Twitter намерена полностью сосредоточить это направление бизнеса на себе. Компания прекратит оптовую продажу данных DataSift и NTT и будет продавать их самостоятельно в розницу.

«После приобретения Gnip в мае 2014 г. мы приняли решение включить продажу данных в пакет услуг Twitter с целью обеспечения лучшего

обслуживания наших клиентов и партнёров», – сообщил пресс-секретарь компании редакции Re/Code.

Бóльшую часть дохода Twitter получает от рекламы, но продажа данных – это также значительная часть его бизнеса. В прошлом году компания заработала на ней 147 млн дол.

DataSift и Twitter сотрудничают с 2011 г. Клиенты DataSift будут иметь доступ к данным Twitter до 13 августа 2015 г. ***(Twitter прекратит продажу данных реселлерам // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43084/118/lang,ru/). – 2015. – 14.04).***

***

Foursquare монетизирует свои данные о местонахождении пользователей с помощью платформы Pinpoint. Новый продукт будет работать в Интернете и мобильных девайсах.

Pinpoint – это новое рекламное предложение, помогающее компаниям таргетировать своих пользователей исходя из того, где они были, используя данные о местонахождении.

Ранее компании могли таргетировать свох пользователей на других сайтах и в приложениях с помощью продукта под названием Foursquare Audience Network. С помощью Pinpoint они могут использовать данные компании, чтобы таргетироть не пользователей Foursquare в Интернете и на мобильных девайсах.

«Мы верим, что места, где вы бываете, это лучший индикатор того, кто вы и мы можем помочь компаниям таргетировать правильную аудиторию», отметил представитель Foursquare.

Чтобы гарантировать точность, Foursquare планирует сотрудничать со сторонней экосистемой приложений, бирж и издателей, чтобы получить доступ к GPS данным потребителей. Компания сравнит эти данные с собственными для создания гео-очертаний, чтобы создать профили потребителей в масштабе.

Pinpoint уже привлек внимание нескольких партнеров, включая Google, AT&T, Choice Hotels, Coors Light, FedEx, Jaguar Land Rover, Olive Garden, Samsung Galaxy и Wild Turkey. Программа будет открыта для других компаний в мае ***(Foursquare запустила новую рекламную платформу Pinpoint // Marketing Media Review (http://mmr.ua/news/id/foursquare-zapustila-novuju-reklamnuju-platformu-pinpoint-43974/). – 2015. – 15.04).***

***

Спикер Н. Хорген, представитель дублинского офиса Twitter, в котором он отвечает за связи с коммерческими партнерами в Европе и Африке, выступая в рамках iForum-2015, рассказал о том, что делает платформу уникальной, и как она может помочь брендам расширить свое присутствие в социальных медиа. MMR предлагает выдержки из его доклада:

Три компонента делают платформу уникальной – он живой, доступен для широкой публики и способствует общению.

672 млн твитов было отправлено во время чемпионата мира по футболу.

Большое количество твитов были сделаны во время полуфинального матча между Бразилией и Германией. Количество твитов возрастало по мере забивания голов Германией. Twitter стал платформой, которая объединила пользователей со всего мира вокруг матча.

Количество мобильных устройств стремительно растет, и они уже стали нормой жизни пользователя.

Средний пользователь разблокирует свой телефон 110 раз в день.

По статистике, около 80 % пользователей отправляют твиты с мобильных девайсов. 40 % пользователей заходят в Twitter, когда просыпаются утром, вероятность использования Twitter возрастает в три раза, когда пользователь добирается на работу или с работы, в два раза больше вероятность использования платформы на работе и в три раза возрастает использование Twitter во время похода за покупками.

Twitter – это платформа, которая используется в течение всего дня, на которой пользователь проводит по 10/15/20 минут при каждом заходе. Каждую неделю на Twitter появляется 3,5 млрд твитов – это огромное количество контента, но мы это рассматриваем, как 3,5 млрд моментов, которые происходят на платформе.

Как бренду, как рекламодателю, воспользоваться этими моментами:

Первое, необходимо понять, почему пользователи находятся на платформе. Исследования показали, что есть три основных причины:

Самовыражение. Пользователи заходят на платформу, чтобы выразить себя, что они думают, что чувствуют.

Для общения. Twitter помогает пользователям общаться со своими друзьями, близкими, соединяет с людьми, которые находятся по другую сторону земного шара.

Чтобы открыть для себя что-то новое.

Поэтому, если в маркетинговых кампаниях вы покажете закулисный взгляд на продукт, на то, что вызывает интерес к вашему продукту или услуге, пользователям платформы это понравится.

66 % пользователей отправляют поисковые запросы в Twitter каждый день. 62 % отмечают, что Twitter – это самый быстрый источник новостей.

В Румынии Кока-Кола интегрировала Twitter в тв-кампанию. Если во время тв-ролика, пользователь отправлял твит, то был шанс, что этот твит появится на экране. В рамках этой кампании Кока-Кола с помощью Twitter объединяла зрителей. В этом было главное сообщение кампании.

Самые эффективные способы планирования вашей кампании в Twitter:

Все 3,5 млрд твитов, которые отправляются в течение недели, помогают определить шаблоны пользовательского поведения.

Определенное количество твитов делается за день, когда люди голодны. И этим могут воспользоваться такие компании как McDonald’s.

Часть твитов посвящена тому, когда пользователи собираются заняться пробежками. В понедельник, вторник все очень активны, но к концу недели все становятся очень ленивыми. Это огромная возможность, если это ваша целевая аудитория.

Пользователи также пишут много о том, что им скучно. Можно запустить кампанию, которая будет развлекать пользователей.

Большее количество пользователей пользуются Twitter во время просмотра ТВ. Хороший пример этому – сериал «Игра престолов». Когда вышла последняя серия предыдущего сезона, она собрала порядка 11 млн твитов. Этой возможностью также можно воспользоваться. Так как данный сериал снимается в Ирландии, много сообщений были направлены ЦА о том, чтобы приехать и посетить Ирландию. В Польше Nokia провела похожую кампанию «Игра телефонов», они изъяли фото героев и вставили фото телефонов. Эти кампании можно спрогнозировать.

Можно также быть непредсказуемым, спонтанным на платформе. Возьмем, к примеру, запуск iPhone 6, многие писали о том, что он гнется. Многие бренды воспользовались этим событием просто для развлечения.

Можно использовать событие, которое точно произойдет, но вы не знаете, что именно на нем случится. К примеру, Евровидение.

И последнее относительно спонтанности. Не переживайте, если произойдет что-то негативное.

Если вы храбры и спонтанны и отвечаете с юмором, то вы будете успешны. Чем больше твитов пользователь видит о вашем бренде, тем больше вероятность, что он совершит покупку ***(Найл Хорген, iForum -2015: как проводить успешные кампании в Twitter // Marketing Media Review (http://mmr.ua/news/id/najl-horgen-iforum-2015-kak-provodit-uspeshnye-kampanii-v-twitter-44016/). – 2015. – 17.04).***

***

Девять распространённых ошибок соцмедиа-маркетинга

Советов о том, как продвигать бизнес в социальных сетях и строить SMM маркетинг, – бесконечное множество. Тем не менее, многие компании продолжают снова и снова наступать на одни и те же SMM-грабли. Давайте рассмотрим девять самых распространённых ошибок SMM из инфографики предпринимателя Д. Сквайрса – и не будем больше их совершать.

Гнаться за количеством подписчиков (фолловеров).

Число подписчиков не имеет значения. Отдача от SMM будет намного выше, если сосредоточиться на точном попадании в потребности пользователей, а не на их количестве.

Публиковать нерегулярный и непривлекательный контент.

176 млн человек ежегодно покупают товары онлайн, но если вы размещаете нерегулярный и неинтересный контент, то они выберут не вас.

Не конвертировать подписчиков в платящих клиентов.

Популярные посты, получившие много повторных публикаций, приносят пользу только в том случае, если они конвертируются в продажи.

Фокусироваться на всех каналах сразу.

Новые быстрорастущие сервисы (вроде Snapchat и Ello) появляются, как грибы после дождя, и кажутся очень активными. Но всё-таки Facebook ещё никто не отменял – с их 1,23 млрд пользователей, проверенной и реальной аудиторией.

Не придавать бренду личностные черты.

Бренд печенья Oreo получил грандиозный отклик (больше 15 тыс. ретвитов) на свой молниеносный, остроумный маркетинг во время финала Национальной футбольной лиги 2013 г. в США (Супер Боул). При этом почему-то всего лишь 22 % компаний видят смысл в формировании личности своего бренда.

Спамить.

Эта практика не требует большого ума. Но спам все ненавидят.

Делать всё вручную.

При наличии инструментов планирования публикаций пытаться вручную управлять кучей кампаний или десятком страниц – пустая трата потенциала.

Транслировать одно и то же сообщение по всем каналам.

Для разных социальных сетей требуется разный стиль контента. Кроме того, если ваши подписчики пересекаются в нескольких соцсетях, то дублирование сообщений может их раздражать.

Не иметь стратегии вообще.

У 90 % компаний есть соцмедиа-стратегия (география не уточняется; в России эта цифра явно намного меньше – Прим. ред.), так что вести кампанию без осмысленного анализа и поставленных целей – может оказаться напрасной тратой энергии ***(9 распространённых ошибок соцмедиа-маркетинга // Marketing Media Review (http://mmr.ua/news/id/9-rasprostranennyh-oshibok-socmedia-marketinga-infografika-44012/). – 2015. – 17.04).***

***

В этом году рекламодатели во всём мире потратят 23,68 млрд дол. на рекламу в социальных медиа, сообщает аналитическое агентство eMarketer. В целом, рекламные бюджеты на этот канал возрастут на 33,5 % по сравнению с 17,74 млрд дол. в 2014 г. В 2015 г. расходы на социальные медиа составят 13,9 % совокупных затрат на цифровую рекламу в мире. Об этом пишет searchengines.ru.

По прогнозам eMarketer, к 2017 г. доход от рекламы в социальных медиа достигнет 35,98 млрд дол., 16 % совокупного мирового рынка цифровой рекламы. По оценкам агентства скорость роста мировых расходов на рекламу замедляется. В 2014 г. она составляла 56,2 %, в этом году она упадёт до 33,5 %, в 2016 – до 26,3 %, в 2017 – до 20,3 %.

Рекламодатели в США и Канаде остаются ведущими драйверами этого рынка. В этом году их расходы на рекламу возрастут на 31 % по сравнению с

прошлым годом и достигнут 10 млрд дол. Рекламодатели в Азиатско-Тихоокеанском регионе потратят 7,4 млрд дол., в Западной Европе – 4,74 млрд дол. Североамериканские страны также лидируют по расходам на одного пользователя, которые составляют 50,42 рекламных доллара. В Западной Европе эта сумма составляет 25,26 дол., в Азиатско-Тихоокенском регионе – 8,04 дол.

По прогнозам eMarketer, в ближайшие годы США и Китай будут лидировать по расходам на цифровую рекламу в мире. На долю этих стран будет приходится бóльшая половина мирового рынка цифровой рекламы в течение прогнозного периода.

В этом году рекламодатели в США потратят 9,59 млрд дол. на рекламу в социальных медиа, что на 31 % выше, чем в 2014 г., и более чем в два раза превышает их расходы на этот канал в 2013 г. К 2017 г. расходы на рекламу в социальных сетях в США достигнут 14,4 млрд дол. – около 20 % совокупных расходов на цифровую рекламу в США. В Китае расходы на этот канал достигнут 3,41 млрд дол. в этом году, а в 2017 – 6,11 млрд дол., составив 12,5 % совокупных расходов на цифровую рекламу в стране.

Неудивительно, что большая доля затрат на рекламу в социальных медиа будет приходиться на Facebook. В 2015 г. доход компании от рекламы достигнет 15,5 млрд дол. и 65,5 % всех рекламных затрат на социальные медиа в мире. В 2014 г. доля Facebook на этом рынке составляла 64,5 %.

Twitter заработает на рекламе 2,09 млрд дол. в 2015 г, что составит 8,8 % мирового рынка рекламы в социальных медиа ***(eMarketer: Мировые расходы на рекламу в социальных медиа достигнут $23,68 млрд в 2015 году // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43136/118/lang,ru/). – 2015. – 20.04).***

***

Компания Buzzstream и диджитал-агентство Fractl провели совместное исследование, которое показало одну из сторон тесной взаимосвязи эмоционального вовлечения пользователей, их активности в социальных сетях и виральности брендированных историй, пишет Marketing Media Review (http://mmr.ua/news/id/potrebiteli-ohotnee-pokupajut-tovary-brendov-kotorye-postjat-klientoorientirovannyj-kontent-44039/).

Эксперты провели опрос среди 900 интернет-пользователей, чтобы выяснить, как они реагируют и насколько подвержены влиянию клиентоориентированных историй, которые придумывают крупные бренды для удержания или возврата покупательского спроса. Исследователи также составили инфографику по пяти крупным компаниям – Amazon, The Ritz-Carlton, Lego, разработчик игр Bungie и сеть британских супермаркетов Sainsbury’s, – в которой отразили взаимосвязь вирусного контента, транслирующего позитив, и вовлеченности аудитории.

Респонденты разделились на две группы: одни признались, что брендированный сторителлинг, направленный на поддержку интереса покупателя, так или иначе влияет на них, другие – что не влияет. 29 % опрошенных из второй группы определили пять компаний из списка как «очень хорошие», в то время как 42 % высказались более нейтрально. В первой группе 37 % показали положительное отношение к пяти названным брендам, и только 33 % заняли нейтральную позицию.

На вопрос о том, хотели бы они приобрести товары представленных компаний, 18 % опрошенных ответили, что сделали бы это охотнее, если бы не видели позитивные истории, а 37 % – наоборот, если бы прочитали такие посты ***(Потребители охотнее покупают товары брендов, которые постят клиентоориентированный контент // Marketing Media Review (http://mmr.ua/news/id/potrebiteli-ohotnee-pokupajut-tovary-brendov-kotorye-postjat-klientoorientirovannyj-kontent-44039/). – 2015. – 20.04).***

***

Видео в Facebook становится все популярнее. Согласно результатам исследования от SocialBakers, в декабре 2014 г. пользователи соцсети разместили на своих страницах на 20 тыс. больше Facebook-видеороликов, чем YouTube-контента, пишет Marketing Media Review (http://mmr.ua/news/id/kak-poluchit-maksimum-ot-video-v-facebook-44048/).

Разумеется, для успеха маркетинговой кампании бренду важно использовать все каналы связи со своей аудиторией, но загружая видеоролики непосредственно в Facebook, они рискуют получить поразительные результаты. Давайте разберемся, как сделать это правильно.

1. CTA-кнопки

Видео – это всего один из множества инструментов, который призван увеличить количество лайков и расшариваний брендового контента. Хорошо, когда есть лайки, а если видео еще и обсуждают, при этом активно, то это просто великолепно. Чтобы подписчики не проходили мимо и не забывали о видеоролике сразу после просмотра, нужно добавить к видео CTA-кнопку, предлагающую, к примеру, поделиться им с друзьями. Такие ролики лучше всего размещать в хронике, потому что в разделе видео они рискуют остаться незамеченными.

Компания Diamond Candles, опубликовав видео, демонстрирующее их продукцию, попросила своих подписчиков поставить отметку «мне нравится», если они хотели бы себе что-то из товаров бренда. В результате видео посмотрели около 25 тыс. пользователей, а лайкнули 1836 раз.

Однако не стоит забывать, что Facebook-видео нельзя поделиться в других соцсетях. Так что вам придется загрузить его еще и в YouTube, но эта мера точно не будет лишней.

2. Будьте в теме

Все еще помнят то самое платье? О нем говорили везде, где только можно, и оно успело надоесть всем буквально за день. Примерно то же самое

случилось и после выхода нового трейлера «Звездных войн». Многие бренды не растерялись и успели в очередной раз привлечь к себе внимание на волне всеобщей радости.

В общем, если вы еще не поняли, суть такова: нужно не просто публиковать контент, но еще и знать, чем живет ваша аудитория. Смотрите, что интересует ваших подписчиков не только в Facebook, но и в Twitter и Instagram. Они поддержали Ice Bucket Challenge? Прекрасно, и вы поддержите. Им интересен футбол? Очень хорошо, пора бы и вам обратить на него внимание.

Прошлой осенью компания 24Hr HomeCare опубликовала видео, которое было посвящено популярной акции «Небритый ноябрь». Пользователи это оценили, а компанию заметили не только в контексте ее деятельности.

Создавая трендовые видеоролики, не забудьте убедиться, что такая же идея не пришла в голову кому-то еще.

3. Размещайте видеоролики длиной не больше двух минут

Согласно данным The Verge, 30 % пользователей Facebook заходят в соцсеть исключительно с мобильных устройств. Помимо этого, мобильное видео тоже переживает революцию: результаты исследования, проведенного Business Insider, показали, что 15 % всех просмотров онлайн-видео приходится на просмотры с мобильных устройств.

Когда пользователи открывают Facebook, они листают новостную ленту, заходят на страницы своих друзей, родственников, смотрят фотографии. Но они идут туда не за длинными видеороликами. Исследование, проведенное компанией Wistia, показало, что чем короче видео, тем лучше. Больше всего просмотров у роликов длиной 30 секунд и менее – их предпочли 80 % респондентов.

Компания The Coffee Bean & Tea Leaf знает, что длинные ролики утомляют, и поэтому все видеоматериалы, размещаемые на ее странице в Facebook, не превышают минуты.

Если вы поняли, что короткие видеоролики – ключ к успеху, не забывайте, что содержание тоже должно быть на высоте.

4. Сделайте кликабельную миниатюру

Боитесь, что ваш чудесный видеоролик пользователи пролистают, даже не посмотрев? Нужно привлечь к нему внимание, выбрав удачную миниатюру. Это можно сделать, загрузив видео. После загрузки кликните кнопку «опции», и отредактируйте миниатюру. Facebook предложит вам 10 вариантов на выбор.

Если не уверены в своих силах, посмотрите, как это делают другие ***(Как получить максимум от видео в Facebook? // Marketing Media Review (http://mmr.ua/news/id/kak-poluchit-maksimum-ot-video-v-facebook-44048/). – 2015. – 21.04).***

***

Исследовательская компания Nielsen на примере Microsoft сделала некоторые выводы относительно того, как ТВ-реклама влияет на присутствие и упоминание брендов в социальных медиа. Об этом пишет cossa.ru.

Проводя прямую зависимость между этими двумя каналами продвижения, эксперты Nielsen в своем новейшем исследовании выяснили, что недавняя ТВ-кампания крупной американской корпорации значительно увеличила ее степень присутствия в социальных сетях.

В течение 30 дней после запуска ТВ-роликов, количество твитов о компании от пользователей, упоминавших хотя бы одно прайм-тайм шоу, в котором была размещена реклама Microsoft, возросло на 41 %. Для контраста, обсуждение бренда среди тех, кто не упоминал телепередачу, снизилось на 38 %.

Кроме того, телевизионная кампания Microsoft была основана на двух различных типах креативной стратегии. Одна поддерживала эмоциональное вовлечение и взывала к «душевным струнам» зрителей, в то время как другая имела более рациональную составляющую и фокусировала внимание на конкурентных преимуществах продукта, таких как, например, стоимость, и содержала призыв к действию. Первый, эмоциональный, подход вызвал значительно больше обсуждений в социальных сетях, чем второй, прагматичный, – выяснили в Nielsen.

76 % респондентов сказали, что считают объединение таких каналов коммуникации, как ТВ и социальные медиа, таким же либо более эффективным, чем традиционная телетрансляция: 51 % не видят разницы, а 26 % считают, что у «подключенного» телесмотрения больше преимуществ.

Исследователи также пришли к выводу, что экспансия ТВ-продвижения в социальные медиа спровоцировала увеличение количества упоминаний о роликах Microsoft в пять раз по сравнению с кампаниями, характеризующимися меньшей степенью интегрированности в соцсети ***(Nielsen изучила влияние ТВ-рекламы на обсуждение брендов в social media // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43170/118/lang,ru/). – 2015. – 22.04).***

***

Чистая прибыль крупнейшей в мире социальной сети Facebook по итогам I квартала 2015 г. сократилась на 20 %, до 512 млн дол., говорится в пресс-релизе компании. Об этом пишет ria.ru.

В пересчете на акцию квартальная прибыль составила 0,18 дол. против 0,25 дол. годом ранее. При этом аналитики ожидали, что прибыль на акцию составит 0,4 дол. Выручка Facebook подскочила на 41 % – до 3,543 млрд дол. При этом объем издержек и расходов увеличился в 1,83 раза – до 2,61 млрд дол. Операционная прибыль сократилась на 13,2 % – до 933 млн дол.

Число ежедневных активных пользователей соцсети в марте 2015 г. увеличилось на 17 % по сравнению с прошлым годом и составило 936 млн человек, 798 млн из которых заходили на Facebook с мобильных устройств (рост на 31 % в годовом выражении).

Число активных пользователей в месяц возросло в годовом выражении на 13 % – до 1,44 млрд пользователей. Число мобильных пользователей Facebook

по состоянию на 31 марта 2015 г. подскочило на 24 % в годовом выражении, составив 1,25 млрд человек.

«Это было сильным началом года…. Мы по-прежнему сосредоточены на обслуживании нашего сообщества и соединении всего мира», – заявил основатель и генеральный директор Facebook М. Цукерберг ***(Чистая прибыль Facebook в I квартале сократилась на 20 % // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43186/118/lang,ru/). – 2015. – 23.04).***

***

В социальной сети «ВКонтакте» появятся рекламные посты, встраиваемые в ленты новостей наподобие promoted posts у Facebook и Twitter. Об этом рассказал на форуме РИФ+КИБ руководитель отдела клиентского сервиса «ВКонтакте» А. Круглов, пишет Marketing Media Review со ссылкой на tjournal.ru (http://mmr.ua/news/id/vkontakte-vstroit-reklamnye-zapisi-v-lentu-novostej-44104/).

В отличие от рекламных постов, размещаемых в сообществах через биржу «ВКонтакте», рекламные записи будут попадать в ленты пользователей без подписки на сообщество, но будут специальным образом помечаться как реклама.

Сами рекламные записи будут выглядеть так же, как и обычные. После встраивания они будут отображаться в одном месте ленты как на десктопе, так и на мобильных устройствах.

По словам А. Круглова, во «ВКонтакте» первая рекламная запись будет появляться в ленте через 6–10 постов, следующие – через 25. У Facebook и Twitter такие рекламные записи начинают показывать уже через три поста с начала ленты и повторяются в несколько раз чаще, у «Одноклассников» это происходит «чуть мягче», считает А. Круглов.

С 1 мая начнётся технический тест функциональности: в ленту пользователей начнут встраиваться невидимые записи для проверки объёмов трафика и настройки цен. С 15 мая начнётся сотрудничество с крупными рекламодателями ***(ВКонтакте встроит рекламные записи в ленту новостей // Marketing Media Review (http://mmr.ua/news/id/vkontakte-vstroit-reklamnye-zapisi-v-lentu-novostej-44104/). – 2015. – 23.04).***

***

Как заставить пользователей смотреть вашу рекламу, да еще и делиться ею с друзьями? Просто! Надо лишь показать ее людям, смотрящим видео на своих смартфонах, пишет Marketing Media Review (http://mmr.ua/news/id/youtube-polzovateli-ljubjat-mobilnuju-reklamu-44094/).

YouTube совместно с Ipsos MediaCT провел исследование, из результатов которого становится ясно – мобильные зрители в 1,4 раза охотнее смотрят рекламу на своих мобильных устройствах, чем на PC или ТВ. И почти в два раза охотнее ею делятся с друзьями.

Мобильное видео стабильно растет на протяжении многих лет, но сейчас оно действительно близко к тому, чтобы оправдать всю шумиху, которая создавалась все это время вокруг него. Мобильная видеореклама в США увеличилась больше чем в два раза с 720 млн в 2013 г. до 1,5 млрд дол. в 2014 г. и достигнет 6 млрд дол. в 2018 г. Это составляет около половины всех онлайн видеообъявлений.

Отчет Medialets за III квартал показывает, что конверсия мобильной рекламы, если ее правильно посчитать, превосходит все ожидания. По данным отчета, конверсия после просмотра (view-through conversion) составляет на смартфонах 58 %, на планшетах – 72 %. То есть большая часть конверсий это не прямые клики и тапы, а просмотр рекламы и потом отложенные во времени действия (где уже играет роль осведомленность о бренде) ***(YouTube: пользователи любят мобильную рекламу // Marketing Media Review (http://mmr.ua/news/id/youtube-polzovateli-ljubjat-mobilnuju-reklamu-44094/). – 2015. – 23.04).***

***

Facebook анонсировала запуск программы Anthology, призванной объединить бренды с медиаиздателями для производства качественной видеорекламы для Facebook, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-programmu-sozdanija-sponsirovannogo-videokontenta-44122/).

Издатели-партнёры предоставят свой опыт и технические возможности, бренды – деньги.

В анонсе Facebook не были указаны детали ценовых условий, но ясно, что программа в первую очередь направлена на крупные бренды.

Партнёрами Facebook выступили такие медиакомпании, как Electus Digital, Funny Or Die, Oh My Disney, The Onion, Tastemade, Vice Media и Vox Media. Кроме того, в программе также будет участвовать собственное креативное подразделение компании Creative Shop.

«Вместе Creative Shop и партнёры Anthology помогут брендам создать контент, который найдёт отклик у аудитории и принесёт бизнесу доход»,– сообщается в официальном блоге Facebook.

Напоминаем, что на днях Facebook заявила, что количество просмотров видео в социальной сети достигло 4 млрд в день. Программа Anthology – это один из способов монетизировать эти просмотры.

О том, что Facebook ведёт переговоры с несколькими издателями контента поводу создания спонсируемых видеороликов, стало известно в прошлом месяце ***(Facebook запустил программу создания спонсированного видеоконтента // Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-programmu-sozdanija-sponsirovannogo-videokontenta-44122/). – 2015. – 24.04).***

***

Чему я научился за год работы с рекламными инструментами Facebook

Последний год я занимался изучением всех существующих вариантов продвижения в Facebook. Хочу поделиться советами по настройке рекламы и рассказать о том, каких результатов они мне позволили достичь, пишет AIN.UA (http://ain.ua/2015/04/25/575497).

У Facebook существует два основных варианта запуска рекламной компании.

Продвижение публикаций на странице

Этот инструмент продвижения удобен, если у вас уже есть готовая аудитория в менеджере рекламы, т. к. по умолчанию он не предполагает детальную настройку кампании. Его также можно использовать для увеличения охвата в рамках своей собственной страницы.

Менеджер рекламы

Здесь у вас есть возможность анализа ваших рекламных кампаний и создания новых. Это основной инструмент для работы с продвижением в Facebook, который я использую.

В менеджере рекламы вы можете создавать и детально настраивать таргетинг на интересующую вас аудиторию.

Сбор данных о вашей аудитории

Если у вас есть сайт, обязательно установите на него код отслеживания пользовательских симпатий от Facebook. Делается это так: Install the Custom Audience pixel.

Это позволит собирать данные о ваших посетителях, и в случае запуска рекламы, вы сможете настраивать показ рекламы только для посетителей вашего сайта, которые также зарегистрированы в Facebook – это существенно повысит эффективность кампании. Также с помощью этого инструмента можно настраивать ремаркетинг.

Кроме этого, ограничить аудиторию помогут другие ваши бизнес-странички в Facebook, данные из которых можно использовать в настройке рекламной кампании. Например, вы хотите продвинуть в Facebook бизнес-страничку мебельной компании (назовем ее Page 1). При этом у вас уже есть популярная страничка, посвященная декору, дизайну и мебели – Page 2. Вы просто настраиваете показ рекламных публикаций Page 1 только для аудитории Page 2, тем самым ориентируясь на уже лояльную публику, которой интересно следить за новостями мебельной темы.

Увеличение охвата публикации

Если у вас уже есть популярная страница в Facebook, у которой более 10 тыс. подписчиков, не забывайте усиливать каждую свою публикацию – без усиления ваши посты увидит только небольшая часть подписчиков.

Достаточно часто я сталкиваюсь с владельцами популярных страниц, которые занимаются платной публикацией рекламных материалов. Практически все они берут деньги за публикацию, но не выделяют и 1 дол. на

усиление этой публикации – в результате рекламодатель остается не удовлетворен эффектом публикации и повторно не обращается.

Существующие рекламные функции Facebook, с их возможностью четкого отбора любой аудитории, с учетом не только возраста, пола и таргетинга, но и с учетом предпочтений, финансового положения, места работы, и многих других факторов, позволяющих показывать рекламу только вашей аудитории.

Нужен женатый директор туристической фирмы, увлекающийся маркой BMW, который недавно был в Риме и пьет кофе латте? Facebook найдет таких среди своих пользователей и покажет рекламу только им.

Теперь пару о том чего можно достичь – мои кейсы

32 тыс. посетителей сайт + 12 тыс. подписчиков бизнес странички

Рекламная кампания для сайта dekorin.ru и его странички принесла 12 тыс. подписчиков и 32 тыс. посетителей сайта за 3 месяца.

Как этого достигли:

1–2 публикации в сутки, каждая публикация строилась на завлекающем заголовке – ТОП-5 идей для спальни, ТОП-10 новинок дизайна, 5 вариантов обустройства кабинета и т. д.

Контент для проекта было решено брать в Pinterest. Сначала придумывалась тема публикации, потом под тему публикации собирались изображения, на основе которых и составлялся материал.

На каждую публикацию настраивали рекламную кампанию с бюджетом до 5 дол. и настройками таргетинга – Украина, женский пол; интересы – мебель, дизайн, мода.

Более 1 млн просмотров видео в Facebook

Небольшая рекламная кампания по продвижению видео #LikeLife на страничке “Наш Харьков” принесла почти 3 тыс. подписчиков страницы и более миллиона просмотров видео за четыре дня!

Для продвижения видео ставка делалась на женскую аудиторию Facebook, проживающую в Харькове, т. к. эта аудитория чаще репостит информацию в Facebook.

Харьков – студенческий город с большим количеством иностранных туристов. Привлеченные с помощью рекламной кампании 3 тыс. просмотров привели к волне перепостов: через день после публикации видео попало на стены граждан разных стран, проживающих в Харькове, еще через день – стало появляться на стенах пользователей Facebook по всему миру.

При этом стоит отметить, что в разных странах поведение пользователей Facebook отличается. Например, в Сингапуре аналогичная рекламная компания провалилась, а в Дубаи результат получился хуже – всего лишь более 30 тыс. просмотров ***(Сергиенко Ю. Чему я научился за год работы с рекламными инструментами Facebook // AIN.UA (http://ain.ua/2015/04/25/575497). – 2015. – 25.04).***

***

Как использовать Twitter для реализации маркетинговых задач

Twitter – одна из самых популярных социальных сетей в мире. На сегодняшний день число ее пользователей насчитывает порядка 280 млн человек и с каждым из них вы можете связаться в любой момент времени.

Такая возможность делает платформу незаменимым помощником в бизнесе. Скорость и простота отправки сообщений, а также огромное количество полезных функций значительно упрощают процесс привлечения новых покупателей и способствуют улучшению качества обслуживания уже имеющихся клиентов.

Согласно собственным исследованиям сегодня 9 из 10 разговорам в Twitter посвящены темам малого или среднего бизнеса. Более того, 60 % пользователей, подписанных на Twitter-аккаунты мелких предприятий, гарантированно становятся их постоянными покупателями.

Согласно Visually:

– 74 % людей, подписанных на аккаунты мелких и средних компаний, отслеживают в Twitter информацию о новинках;

– 47 % людей, подписанных на аккаунты брендов, с большей долей вероятности хоть раз посещали сайт компании;

– 84 % людей, подписанных на аккаунты компаний малого и среднего бизнеса и имеющих опыт взаимодействия с брендом, оставляют положительные отзывы о его работе и продукции;

– 85 % пользователей считают подписку на аккаунты компаний в Twitter отличным способом оставаться на связи с брендом.

Сегодня многие бренды все еще не до конца используют весь потенциал Twitter. Однако данная платформа обладает огромным количеством возможностей, которые могут значительно обогатить маркетинговой арсенал любой компании. Ниже описаны некоторые из таких полезных функций.

1. Аналитика

Twitter на сегодняшний день – единственная платформа, которая в отличие от остальных социальных сетей предоставляет своим пользователям «интерпретируемую» информацию об их профилях. Это означает, что Twitter Analytics тщательно анализирует все данные и затем подробно разъясняет, о чем говорит значение того или иного показателя.

Дается не просто перечень таких базовых показателей, как

– уровень взаимодействия и впечатление об аккаунте;

– рост числа подписчиков;

– интересы подписчиков;

– местоположение подписчиков

– пол подписчиков.

Предоставляется более значимая информация:

– лучшее время для публикации твитов;

– подписки подписчиков аккаунта;

– наиболее авторитетные подписчики;

– ссылки, дающие максимальный трафик;

– ресурсы, откуда приходит трафик.

Знания о том, какой контент является наиболее эффективным, позволяют своевременно вносить корректировки в маркетинговую деятельность компании в соответствии с ее целями и задачами. @FeedingAmerica, ведущая благотворительная организация в США, использовала аналитику, чтобы определить, какую информацию стоит публиковать в сети, что позволило ей получить прирост трафика на свой сайт в 2,5 раза.

2. Расширенный поиск Twitter

Расширенный поиск Twitter может творить чудеса. Так как это открытая платформа, то расширенный поиск в системе позволяет искать практически любую информацию, обсуждаемую на ней. Одним из важнейших преимуществ является возможность поиска по географическим регионам.

Допустим, компания владеет кофейным бизнесом в Квинсе, Нью-Йорк. Это не очень крупный бренд, и его ежедневный доход зависит от активности местных покупателей. Благодаря расширенному поиску Twitter организация может с легкостью найти людей, проживающих в Квинсе и обсуждающих тему кофе в сети.

Больше нет необходимости платить значительные суммы денег за рекламу, чтобы привлечь внимание покупателей. В отношении той же кофейной компании можно, например, дополнительно выполнить поиск твитов, в которых говорится о том, что человек только что проснулся, и напомнить ему, каким приятным может быть глоток свежесваренного кофе в ранние утренние часы.

Twitter позволяет искать обсуждения в сети на любые темы и мгновенно переключаться между ними.

Для более точного поиска можно использовать специальные ключевые слова, указать свое местоположение и исключить тэг «http» из поискового запроса.

Исключение «http» означает, что поиск будет проводиться только по беседам, не содержащим внутренних ссылок. Это позволяет переходить только на реальные обсуждения и не тратить время на автоматизированные аккаунты, созданные специально, чтобы размещать на платформе ссылки.

Расширенный поиск очень удобен для поиска реальных людей, проживающих в конкретном регионе и имеющих определенный набор интересов.

3. Twitter-списки

Для более организованной работы в Twitter лучше использовать списки. Списки позволяют распределить подписчиков по группам, а также с их помощью можно легко фильтровать новостную ленту в зависимости от того, какую информацию требуется просмотреть в тот или иной момент времени.

На самом деле, у списков Twitter бесконечно огромная сфера применения. С их помощью можно:

– отслеживать действия конкурентов;

– связываться с лидерами отрасли;
– быть в курсе популярных тенденций;
– взаимодействовать с сотрудниками;
– общаться с покупателями;
– следить за новостями блогеров и СМИ.

Кроме того, есть один хитрый трюк, как с помощью списков можно очень быстро найти интересных людей в Twitter. Все, что требуется сделать – это просмотреть списки конкурентов и подписаться на аккаунты, которые в них включены.

Соответственно, чтобы конкуренты не могли поступить аналогичным образом, необходимо сделать свои Twitter-списки приватными.

Если нет времени создавать собственные Twitter-списки, то можно подписаться на списки, которые делают другие пользователи. Это очень удобно, так как нисколько не ограничивает ваши возможности при работе со списком.

4. Пин

Пин твита – очень удобная функция. Она закрепляет пост на самом верху профиля пользователя. Таким образом можно вручную выбрать, какой твит посетители аккаунта будут видеть первым.

Пины позволяют значительно увеличить количество кликов, ретвитов, комментариев и добавлений в избранное в отдельно взятых твитов.

5. Обнаружения

Эта функция говорит сама за себя. Благодаря алгоритму, анализирующему ряд различных показателей, она позволяет быстро определить, что в настоящий момент пользуется наибольшей популярностью в Twitter.

С помощью обнаружений можно узнать, что происходит на местном рынке конкретно выбранной отрасли, а также организовать публикацию популярных твитов в новостной ленте своих подписчиков, что будет значительно способствовать поддержанию их интереса к вашему профилю ***(Как использовать Twitter для реализации маркетинговых задач // Marketing Media Review (http://mmr.ua/news/id/kak-ispolzovat-twitter-dlja-realizacii-marketingovyh-zadach-44136). – 2015. – 27.04).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Молодь воліє уникати інтернет-взаємин із власними батьками, пише The Telegraph. Британські дослідники помітили масову відмову дівчат і хлопців від популярних соцмереж, оскільки те, що вони пишуть, можуть прочитати їхні батьки.

Третина молодих інтернет-користувачів видаляють свої акаунти, коли до соцмережі приєднується тато чи мама. З цієї причини із Facebook довелося видалитися майже 32 % респондентів віком 16–34 років. Тридцять три відсотки зізналися, що блокували когось зі своїх родичів. При цьому кожний десятий молодий інтернет-користувач перейшов до соцмереж, де його дії та коментарі не можуть побачити члени його родини.

На думку експертів, відмова молоді від популярних соцмереж пов'язана з тим, що дедалі більше представників старшого покоління користується смартфонами та планшетами. Якщо в 2012 р. смартфон був лише в 9 % британців, старших за 55 років, то нині такий гаджет є вже в 52 %. Для порівняння, серед молоді ця цифра становить 85 %. Планшети мають 49 % літніх британців. П'ятдесят дев'ять відсотків людей похилого віку в Британії мають акаунт у Facebook, 32 % користуються Skype, а 17 % мають WhatsApp на своєму телефоні ***(Молодь покидає соцмережі // InternetUA (http://internetua.com/molod-pokida--socmerej). – 2015. – 16.04).***

***

Исследование: Facebook делает женщину вещью

Довольно интересное исследование провели британские ученые. Наблюдая за поведением группы девушек в Facebook, они пришли к выводу, что социальная сеть делает их более склонными к сексуальной объективации. Проще говоря, постоянный просмотр картинок из чужой жизни заставляет женщин считать себя вещью.

Авторы исследования проследили за поведением 150 девушек в возрасте от 17 до 25 лет, фиксируя, как различные источники информации влияют на их представления о месте женщины в обществе. При этом использовались различные рекламные видеоролики, фотографии, глянцевые журналы и социальные сети.

В итоге Facebook неожиданно оказался одним из главных факторов, способствующих развитию «самоовеществления» у женщин. Те девушки, которые проводили больше времени за просмотром страничек в соцсети, были более склонны считать физическую привлекательность своим главным

положительным (или отрицательным) качеством, чем остальные участницы эксперимента. К примеру, телевидение, Интернет и музыкальные клипы не оказывали такого влияния и в целом не были связаны с тенденцией к сексуальной объективации.

«Наше исследование показало, что когда девушки проводят больше времени за чтением журналов и просмотром соцсети, то они проявляли большую степень самообъективации по сравнению с другими женщинами. Этот феномен связан с тем, что у женщин есть тенденция сравнивать свою внешность с окружающими людьми, в особенности со сверстницами или знакомыми в Facebook», – уверяет один из авторов исследования Ф. Дидрихс из Университета Западной Англии в Бристоле.

В статье, опубликованной в журнале Psychology of Women Quarterly, говорится о том, что соцсеть Facebook оказалась одним из ведущих факторов в растущей тенденции многих женщин воспринимать себя в первую очередь как объект сексуальных желаний мужчин. К такому выводу ученые пришли, проверяя одну из наиболее распространенных претензий феминисток и борцов за права женщин к миру СМИ и массовой культуры: овеществление женщин (когда их красота и сексуальная привлекательность являются главными и самыми значимыми позитивными качествами).

Данную особенность принято считать одной из основных причин половой дискриминации на работе, в быту и обществе и главной причиной того, что сами женщины во многих случаях овеществляют себя и смотрят на себя по большей части только как на предмет сексуального влечения со стороны мужчин ***(Исследование: Facebook делает женщину вещью // GlavPost.Com (http://glavpost.com/post/20apr2015/Nets/26353-issledovanie-facebook-delaet-zhenschinu-veschyu.html). – 2015. – 20.04).***

***

У Данії негативне враження про взаємодію в соціальних мережах часто базується на поодиноких, маргінальних випадках. Такого висновку дійшли учені з датського Університету Роскілле, що в Копенгагені, пише European Journalism Observatory.

Науковці дослідили регулярні онлайн-дебати протягом одного тижня і виявили, що переважно інтернет-дискусії є нейтральними та не становлять небезпеки.

Дослідження «Залучення громадськості у виробництво новин через коментарі у Facebook» (Agency and Civic Involvement in News Production via Facebook Commentary) базувалося на контент-аналізі. У його рамках учені проаналізували 149 повідомлень із семи Facebook-сторінок датських онлайн-газет, а також 3800 коментарів під ними. Дані зібрані станом на 46 тиждень 2012 р. Щоб уникнути модерації повідомлень, дані були зібрані максимально швидко, у режимі реального часу.

Серед 149 постів найбільш популярними були нейтральні думки (49 %), якими супроводжувався лінк на матеріал видання. Другий за популярністю –

пост-запитання (30 %). Як зазначають експерти, обидві стратегії позитивно впливають на залучення користувачів до обговорення, однак запитання переважно викликають ширшу дискусію.

Дослідники, за результатами роботи, зробили такий головний висновок: у Данії інтернет-дебати є нейтральними. Більшість коментарів (73 %) не були чітко позитивно чи негативно забарвленими. Принизливими були тільки 21 % з них, схвальними – 6 %.

Під час дослідження не аналізували зміст дебатів, а лише кількісні показники. Однак встановлено, що дискусії не були беззмістовними. У 82 % випадків коментарі стосувалися теми обговорення. У 68 % випадків користувачі висловлювали свою думку.

Попри пересторогу медійників про те, що соцмережі можуть перейняти основні функції журналістики, автори дослідження дійшли висновку, що інтернет-дебати не загрожують наявним медіа.

Лише 5 % аналізованих коментарів пропонували нову точку зору й тільки 11 % коментарів мали антиурядову спрямованість. Тобто в контексті впливів на громадськість онлайн-дебати ще не стали надто потужними, зазначають автори ***(Негативне враження про дискусії у соціальних медіа базується на поодиноких випадках – дослідження // MediaSapiens (http://osvita.mediasapiens.ua/mediaprosvita/research/negativne_vrazhennya_pro_diskusii_u_sotsialnikh_media_bazuetsya_na_poodinokikh_vipadkakh_doslidzhennya). – 2015. – 21.04).***

***

Як комп’ютерні технології та інтерфейси впливають на освіту

Клавіатура, стилус, сенсорний екран, жести, диктування – вводити інформацію в сучасні гаджети можна багатьома способами. Однак не всі ці інтерфейси однаково корисні: дослідження Microsoft показує, що деякі з них заважають опановувати нові знання та навички, а інші, навпаки, спрощують навчання.

У статті «Комп’ютерні інтерфейси та їхній вплив на навчання» професор Ш. Овіат дослідив, які результати мають учні, коли користуються тим чи іншим способом вводу інформації у свій комп’ютер. Від цього інтерфейсу напряму залежить їхнє вміння думати та вчитися.

Один з найпопулярніших засобів вводу інформації – клавіатура – не є найкращим. Хоча користуватися нею досить просто, вона знижує здібності студентів. Учні краще розвиваються, коли використовують, наприклад, стилус. У них виходить ліпше генерувати нові ідеї, правильно розв’язувати проблеми та запам’ятовувати матеріал під час його занотовування. Клавіатура погіршує результати учнів приблизно на 9–38 % проти стилуса. Це відбувається при вивченні як математики і точних наук, так і гуманітарних предметів.

При роботі зі стилусом учні можуть створити на 56 % більше діаграм, ніж із клавіатурою. Вони також генеруватимуть на 9–38 % більше ідей.

Дослідження також розкриває те, як саме та чому зі стилусом учні показують кращі результати порівняно з використанням клавіатури. Одна з причин полягає в більших можливостях першого.

Зі стилусом, наприклад, простіше створювати безсловесний контент – діаграми, символи, знаки. З таким інтерфесом учні можуть гнучкіше висловлювати свої думки, швидше писати формули та пояснювальні малюнки. На математиці, наприклад, 80 % змісту – це безсловесний матеріал, який незручно вводити з клавіатури.

Опановувати новачкам також простіше стилус, оскільки багато дій з ним аналогічні роботі з ручкою чи олівцем. Усе це, як стверджує дослідження, зменшує когнітивне навантаження на учнів і дає змогу їм зосередитися на розв'язанні поточних завдань. Крім того, стилус зменшує розрив між студентами з різним рівнем підготовки.

Ефективність стилуса в навчанні також підтверджують нейробіологи. Вони з'ясували, що написання літер ефективніше розвиває мозок та його здібності до запам'ятовування, ніж друкування на клавіатурі. Сам процес письма також інтенсивно стимулює різні частини мозку. Постійне повторення одних і тих же форм літер створює довготривалу моторну пам'ять ***(Як комп'ютерні технології та інтерфейси впливають на освіту // InternetUA (http://internetua.com/yak-komp-uatern--tehnolog---ta--nterfeisi-vplivauat-na-osv-tu). – 2015. – 25.04).***

Маніпулятивні технології

Учёные Корнелльского университета (США) разработали компьютерный алгоритм, который может точно идентифицировать интернет-тролля менее чем по 10 постам.

В ходе разработки алгоритма специалисты изучали интернет-форумы и в общей сложности рассмотрели поведение более 10 тыс. «пользователей, предрасположенных к банам».

Как выяснилось, подавляющее большинство троллей пишут комментарии с крайне низким уровнем грамотности и ясности изложения. Кроме того, «токсичные» комментаторы предпочитают фокусировать усилия на меньшем количестве тем.

Поведение троллей зависит и от ресурса, на котором они действуют. Так, на новостном портале CNN они предпочитают создавать новые заметки, а на крупных сайтах Breitbart и IGN – комментировать уже существующие ветки.

Все интернет-тролли демонстрируют огромное упорство, назойливость и слабую грамматику. Созданный исследователями алгоритм пока что является, скорее, суммой всех исследований, а не полноценной компьютерной системой.

Тем не менее, исследователи подумывают о подобной разработке, в которой уже заинтересовались представители Google.

Ранее исследователи Университета Дрекселя (США) и Университета Гёттингена (Германия) разработали методику, позволяющую выяснить личность программиста, анализируя созданный им код ***(Компьютерный алгоритм автоматически вычисляет и блокирует интернет-троллей // Блог Imena.UA (http://www.imena.ua/blog/troll-hunting-algorithm). – 2015. – 16.04).***

***

Facebook, Google, Twitter угрожают свободе Интернета

От компаний Facebook, Google, Twitter и им подобных исходит угроза изначально свободному интернет-пространству, заявил на iForum один из его организаторов А.Ольшанский. Об этом пишет delo.ua.

Опасность состоит в том, что крупные сетевые сервисы принадлежат транснациональным корпорациям. «Они втягивают свободный Интернет. Уже растет поколение пользователей, для которых Интернет – это Facebook, и они плохо знают обычный веб», – объяснил А. Ольшанский.

Он подчеркнул, что Facebook, Google и Twitter определяют предпочтения своих пользователей по неизвестным алгоритмам. «Пятерка транснациональных корпораций определяет, что читают и на что реагируют миллиарды людей. Эти сервисы способны искажать нашу реальность», – отметил А. Ольшанский.

По его мнению, второй проблемой правительств, в том числе и украинского, является плохое представление о том, как работает Интернет. Попытки ограничить свободу в Интернете терпят крах. А. Ольшанский привел пример «большого китайского файервола», на который правительство Поднебесной потратило, по официальным данным, 3 млрд дол., а по неофициальным – 20 млрд дол. «Но все китайцы умеют обходить эти запреты», – подытожил соорганизатор iForum. Он подчеркнул, что любая технология по фильтрации в Интернете будет в тысячу раз дороже, чем технология по преодолению любых ограничений.

А. Ольшанский предложил отказаться от «построения стен» в Интернете. Для противодействия информационным атакам, обострившимся из-за войны на Востоке Украины, он посчитал целесообразным создавать много ресурсов, которые бы «вещали правду». В том числе должна быть и площадка, которая бы освещала государственную позицию. В качестве примера он привел британскую BBC.

Появление разнообразных сетевых сервисов позволит также создать конкурентную среду и ослабить влияние таких монстров, как Facebook, Google и Twitter. А. Ольшанский посчитал нужным оказывать на крупнейших игроков давление через международные организации по типу ICANN ***(Facebook, Google, Twitter угрожают свободе Интернета – Александр Ольшанский // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43124/118/lang,ru). – 2015. – 17.04).***

***

21 квітня Facebook заблокував відомого українського письменника А. Бондара через використання мема «Че там у хохлов?».

Адміністрація соцмережі почула скарги користувачів, яким не сподобався пост А. Бондара «Хотел спросить у рыбака, как клев, Но вырвалось: “А че там у хохлов?”».

Перед цим А. Бондар запостив серію двовіршів з використанням мема «Че там у хохлов?» на підтримку користувача Anton Hodza. Його Facebook забанив на 30 днів за фотоколаж з використанням цієї фрази.

Мем «Че там у хохлов?» висміює росіян, які, незважаючи на проблеми у власній країні, найбільше цікавляться новинами з України.

Варто зазначити, що після бану А. Бондара іронічних постів користувачів з «Че там у хохлов?» з’явилося в рази більше.

Нагадаємо, наприкінці серпня користувачі Facebook підтримали ідею звернутися до засновника мережі М. Цукерберга із скаргою на цензуру: акаунти українських активістів мережа блокувала за скаргами так званих «кремлеботів». Суть претензій до Facebook зводилася до того, що в Україні немає офіційного представництва компанії, а в Росії – є, і активісти побоювалися, що рішення про блокування приймалися не за правилами, а з міркувань цензури.

Facebook у відповідь заявив, що не має представників ні в Росії, ні в Україні, а неупереджену підтримку користувачам з України надають співробітники з різних країн, що працюють у штаб-квартирі в Дубліні. Судячи з усього, серед цих співробітників найбільше вихідців з Росії ***(Фейсбук банить українських користувачів за фразу «Че там у хохлов?» // LB.ua (http://ukr.lb.ua/news/2015/04/21/302577_feysbuk_banit_ukrainskih.html). – 2015. – 21.04).***

***

Самая популярная социальная сеть в мире продолжает охоту на популярных украинских блогеров, награждая их многосуточными банами по заявкам «кремлеботов».

Очередной жертвой неадекватного модерирования контента стал популярный украинский блогер А. Заводюк. Карикатуру годичной(!) давности администрация сети расценила в семь суток бана ***(Сумасшедший Facebook: 7 суток бана за карикатуру годичной давности // GlavPost.Com (http://glavpost.com/post/23apr2015/Nets/27179-sumasshedshiy-facebook-7-sutok-bana-za-karikaturu-godichnoy-davnosti.html). – 2015. – 23.04).***

***

Війна за українські душі

Як відомо, практично вся сучасна молодь спілкується в Інтернеті. Про це прекрасно знають і ті, хто використовує можливості соціальних мереж для розпалювання ворожнечі, ненависті, поширення сепаратистських ідей. Одним словом – хто веде проти нашої країни інформаційну війну.

За словами фахівців, у сепаратистських групах, які діють у соціальних мережах, як правило, тільки близько 2-3 % реальних людей, що проживають у Східній Україні. Решта – або фейкові (фальшиві) акаунти, або спеціально найняті російськими спецслужбами люди, яким поставлено чітке завдання: усіма способами розхитувати ситуацію, поширювати антиукраїнські настрої, нагнітати напруженість.

До речі, не так давно в тому ж Інтернеті був опублікований довжелезний список так званих «кремлівських ботів», робота яких полягає в розміщенні коментарів і постів антиукраїнського змісту. І спецслужби агресора виділяють на їхнє утримання надзвичайно солідні суми коштів. Бо наразі доля перемоги вирішується не тільки на фронті, а в соціальних мережах агресія не менша, а часто навіть більша, ніж на лінії зіткнення.

Особливо привільно «кремлеботи» почуваються в російських соцмережах, таких як «Одноклассники» чи «ВКонтакте».

Для завоювання українців у віртуальному просторі використовують і російських (та й не тільки) «зірок». Наприклад, одна з таких «зірок» активно включилася в антиукраїнську пропаганду навзамін обіцянки присвоїти звання народного артиста Росії. І таких випадків досить багато.

Працівники правоохоронних органів Чернігівської області неодноразово звітували про викриття «місцевих» прихильників так званих ЛНР/ДНР, які намагаються популяризувати на Чернігівщині сепаратизм, а також періодично проводять у молодіжному середовищі профілактичні заходи щодо небезпеки потрапляння в сепаратистські й антиукраїнські сіті в мережі Інтернет. Однак важливо й самим усвідомити, що сучасна війна ведеться не тільки за території, але й за душі і свідомість людей. Протидіяти цій агресії може й повинен кожен. Аби «русский мир», який несе ненависть, смерть і руйнування, ніколи не прийшов на нашу землю ***(Коливан І. Війна за українські душі // Сіверщина (http://siver.com.ua/news/vijna_za_ukrajinski_dushi/2015-04-22-16631). – 2015. – 22.04).***

***

Facebook усилил защиту социальной сети от фальшивых лайков. Это стало возможно за счет усовершенствования технологии распознавания паттернов. Улучшенная технология позволила компании утроить количество подложных лайков, заблокированных еще до их попадания на публичные страницы.

В октябре прошлого года Facebook раскрыл некоторые из методов борьбы со спамом и мошенничеством в рамках социальной сети. Теперь компания заявила о том, что обновленная технология распознавания паттернов помогает ей в борьбе против бирж, продающих фальшивые «лайки» из «лайковых ферм», фальшивых аккаунтов или сгенерированные с помощью вредоносного ПО.

В блоге Facebook поясняется: «Проделанная нами работа значительно усложнила фирмам, продающим фальшивые лайки, обеспечение их присутствия на публичных страницах клиентов. По факту, за последние

полгода мы утроили количество лайков, обнаруженных и заблокированных до того, как они попали на страницы. В результате, многие из компаний, продающих подложные лайки, закрыли свои бизнесы.

Кроме того, теперь, когда мы блокируем или удаляем фальшивые лайки со страниц, мы уведомляем об этом их администраторов. С момента запуска этой функции в марте 2015 г., 200 тыс. администраторов публичных страниц были уведомлены о том, что мы защитили их от подложных лайков.

Специалисты компании также создали справочное руководство по фальшивым лайкам. В нем рассказывается о том, как генерируются такие лайки, как Facebook с ними борется, а также о том, как они приносят компаниям больше вреда, чем пользы.

Напомним, что социальная сеть ведет борьбу с фальшивыми лайками уже несколько лет. Команда Facebook нашла способ определять и удалять подложные лайки автоматически летом 2012 г. ***(Facebook ужесточил борьбу с фальшивыми «лайками» // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_uzhestochil_borbu_s_falshivymi_laykami). – 2015. – 23.04).***

***

Учёные из американского университета проанализировали учётные записи в социальных сетях и обнаружили закономерность, которая позволила выявить сеть «российских ботов». На это обратило внимание научно-популярное издание N+1.

Д. Голбек из Мэрилендского университета в США провела исследование, в котором попыталась выяснить, как закон Бенфорда соотносится с социальными сетями. Оказалось, что число подписчиков в социальных сетях должно удовлетворять так называемому «закону первой цифры», который гласит, что цифра 1 встречается на первом месте куда чаще, чем все остальные.

В своей работе американские учёные отобрали пользователей из Twitter, Google Plus и LiveJournal, у которых было минимум 100 друзей или подписчиков, а затем проанализировали полученные данные о социальных связях в соответствии с законом Бенфорда. Выяснилось, что результаты проверки более 91,5 % пользователей Google Plus и 85,5 % аккаунтов в LiveJournal совпадали с теми, которые предполагались на основании закона первой цифры.

Для анализа были взяты 20 988 профилей в Twitter. В них нашли только 170 подозрительных профилей, 168 из которых действительно оказались ботами. Абсолютное большинство из них были замечены в подозрительной активности. Д. Голбек называет их частью «российской сети ботов». Аккаунты публиковали одинаковые случайно выбранные фразы (зачастую вырванные из середины предложений) или изображения с бесплатных фотохостингов.

Согласно полученным показателям, социальные сети прекрасно подпадают под действие закона. Исключением стал лишь Pinterest, где цифра 5 встречалась чаще, чем это прогнозировали специалисты. Объяснением этому

служит необходимость указывать минимум пять сфер интересов при регистрации.

Обнаружить закономерность удалось исключительно благодаря использованию закона Бенфорда, который позволил проанализировать поведение большого количества аккаунтов и выявить те, которые отличались необычными действиями.

Закон Бенфорда описывает вероятность появления определённой первой цифры в различных величинах, которые взяты из реальной жизни. Например, в списке самых высоких строений мира цифра 1 встречается куда чаще, чем 9. Данный закон используют для измерения точности финансовой документации, результатов выборов и множества других показателей. Существует специальный сайт, где можно ознакомиться с другими примерами ***(Учёные выявили сеть ботов в соцсетях по первой цифре числа подписчиков // InternetUA (http://internetua.com/ucs-nie-viyavili-set-botov-v-socsetyah-po-pervoi-cifre-csisla-podpiscsikov). – 2015. – 24.04).***

Зарубіжні спецслужби і технології «соціального контролю»

У соціальній мережі Facebook з невідомих наразі причин видалено сторінку кримськотатарської газети «Янъы дюнья». Про це повідомляє кримськотатарське інформаційне агентство QHA з посиланням на головного редактора видання З. Бекірову.

«З Facebook несподівано, без жодних попереджень видалена сторінка газети “Янъы донья”. Завдяки публікаціям на цій сторінці тисячі передплатників газети, які проживають за кордоном, мали можливість оперативно знайомитися зі змістом газети. Кілька днів не замовкають телефони в редакції. Спасибі за турботу і увагу», – сказала головред.

При цьому З. Бекірова зазначила, що газета не закрита. «У Роскомнагляді обіцяли зареєструвати газету», – додала головред.

Нагадаємо, наприкінці березня повідомлялося, що газету «Янъы дюнья» було перереєстровано в Роскомнагляді відповідно до вимог російського законодавства.

Як повідомляла «Телекритика», Роскомнагляд відмовив у реєстрації майже всім кримськотатарським ЗМІ. З 1 квітня припинили своє мовлення телеканал ATR та інші ЗМІ цього медіахолдингу (телеканал Lale, радіостанції «Мейдан» і «Лідер»), які не пройшли перереєстрацію відповідно до російського законодавства через відмову в ліцензіях від Роскомнагляду.

Інформаційне агентство «Крымские новости QHA» також отримало відмову в реєстрації та було змушене припинити свою діяльність на території Криму й переїхати до Києва.

Керівництво кримськотатарської газети «Авдет» вирішило скоротити тираж видання, аби мати змогу продовжити свою роботу без дозволу Роскомнагляду, який їм не вдалося отримати.

Російськомовна газета «Голос Крыма» отримала свідоцтво про реєстрацію, змінивши назву на «Голос Крыма New». 7 квітня кримськотатарський дитячий журнал «Арманчыкъ» також перереєстрували за російськими законами.

18 березня в доповіді Amnesty International, опублікованій з нагоди річниці анексії півострова, ішлося про те, що влада Криму використовує широкий спектр тактик залякування в боротьбі з інакомисленням. 20 березня Комітет захисту журналістів повідомив, що стривожений погіршенням медійного клімату в анексованому Росією Криму, зокрема відмовою Роскомнагляду реєструвати кримські новинні ЗМІ.

У квітні невідомі організували DDoS-атаки на кримські опозиційні інтернет-видання «Новости Севастополя» та «Меридиан Севастополь», унаслідок чого ресурси певний час були недоступні для інтернет-користувачів ***(Facebook зникла сторінка кримськотатарської газети «Янъы дюнья» // Телекритика (http://www.telekritika.ua/kontekst/2015-04-15/106073). – 2015. – 15.04).***

***

Роскомнадзор опроверг появившуюся ранее информацию о получении ведомством разрешения на чтение личной переписки россиян в социальных сетях. С соответствующим заявлением выступил в эфире радиостанции «Эхо Москвы» пресс-секретарь ведомства В. Ампелонский.

В. Ампелонский: «На периферийных сайтах начали распространять информацию о том, что Роскомнадзору якобы разрешили читать личные сообщения пользователей. Это феерическая чушь, основанная на незнании действующего законодательства».

Как напомнил В. Ампелонский, с 1 августа 2014 г. в России действует так называемый закон о блогерах, который принимался в комплекте антитеррористических поправок. Он отметил, что основными исполнителями этого закона являются правоохранительные органы, которые имеют право осуществлять оперативно-розыскную деятельность, и Роскомнадзор к таким органам не относится.

В. Ампелонский: «Наша функция – контрольно-надзорная и технико-коммуникационная. То есть мы обеспечиваем взаимодействие между правоохранительными органами и интернет-площадками».

Он пояснил, что закон о блогерах обязал интернет-площадки хранить так называемые логи – информацию о действиях пользователей в сети. При этом он подчеркнул, что под это понятие «ни в коем случае не попадает содержание личной переписки». В. Ампелонский: «Площадка хранит метаданные только о том, что вы с кем-то переписываетесь, но не содержание. Такую информацию о действиях пользователей правоохранители вправе запрашивать у нас. При этом ни Роскомнадзор, ни правоохранительные органы по данному закону ни в коем случае не получают доступа к личной переписке граждан».

Отметим, что ранее в некоторых СМИ появилась информация о том, что Роскомнадзор официально получил разрешение читать личную переписку россиян в социальных сетях ***(«Феерическая чушь»: Роскомнадзор не получал разрешение читать переписку россиян в соцсетях // Телекомпанія НТВ (http://www.ntv.ru/novosti/1392840). – 2015. – 13.04).***

***

Минулого року ФСБ Росії отримало можливість за спрощеною процедурою офіційно діставати дані із серверів будь-яких інтернет-служб, що розташовані на російській території.

Однак, незважаючи на факти контролю інформації в мережі з боку Росії, тисячі українських органів влади продовжують надавати спецслужбам країни, що проводить проти України гібридну війну, доступ до своєї електронної пошти – використовуючи поштові скриньки російських сервісів. Про це пише інтернет-видання ТЕКСТИ.org.ua.

Полтавщина разом з Донеччиною посідає третє місце за кількістю використовуваних на її теренах ru-адрес.

Більше тільки в Запорізькій області та Криму.

Видання зібрало такий собі реєстр ru-адрес українських органів влади, що є користувачами російських поштових скриньок, до яких мають повний доступ російські спецслужби та контролюючі органи. Серед них:

– Фінансові управління Полтавської, Великобагачанської, Зіньківської, Новосанжарської, Хорольської та Шишацької райдержадміністрацій;

– Регіональна державна лабораторія ветеринарної медицини в Полтавській області та вісім районних державних ветлікарень;

– Управління агропромислового розвитку Семенівської та Глобинської райдержадміністрацій (у реєстрі «Текстами» на Полтавщині зафіксовані російські адреси чотирьох управлінь. Вірогідно, два з них змінили їх на українські вже після обробки даних аналітиком видання);

– Полтавська та Кременчуцька міські санітарно-епідеміологічні станції та ряд районних;

– Відділ охорони здоров’я виконавчого комітету Кременчуцької міської ради;

– Управління з питань надзвичайних ситуацій та цивільного захисту населення виконавчого комітету Кременчуцької міської ради.

Також ряд відділів культури та туризму РДА, сільських і селищних рад, райвідділів Держкомзему та соцстраху та ін.

Щоправда, деякі органи влади змінили електронні адреси, але вони не внесені до офіційного реєстру електронних адрес українських органів влади. Зокрема, на сайті Полтавського міського управління юстиції адреса polupr@just.gov.ua, а в офіційному реєстрі – polupr@mail.ru ***(Електронне листування низки державних органів Полтавщини є доступним для російських спецслужб // Полтава Сьогодні (http://today.pl.ua/suspilstvo.html?new_id=5296). – 2015. – 16.04).***

***

16 квітня співробітники СБУ в Харківській області провели обшук і вилучили серверне обладнання та роутери в харківського дата-центру SteepHost.

Дата-центр надає послуги хостингу, а також здає сервери в оренду, пише AIN.UA.

За словами голови компанії А. Кисельова, усього силовики вилучили близько 130 серверів, через що близько 1 тис. сайтів «пішли» в офлайн. Причина візиту СБУ – справа про фінансування тероризму.

Як зазначає видання, обшук і вилучення техніки проводилися під час розслідування кримінальної справи за ч. 2 ст. 110-2, що стосувалося фінансування так званих ЛНР/ХНР через сервіс change-wm.com.

Слідство встановило, що сервери, «на яких розміщується автоматизована система для поширення матеріалів, у яких присутні заклики до збору грошей на ЛНР і ХНР, розміщуються в дата-центрі SteepHost».

Глава SteepHost повідомив, що адвокати компанії наразі працюють над скаргами до прокуратури та СБУ, а також позовами до суду.

Нагадаємо, трохи раніше співробітники СБУ вилучили сервери великого хостера та реєстратора NIC.UA.

На сьогодні компанія спілкується з представниками СБУ з приводу повернення обладнання, але поки що прогресу в цьому напрямі мало ***(СБУ вилучила 130 серверів у харківського дата-центру: в офлайн пішла тисяча сайтів // Osp-Ua.Info (http://osp-ua.info/politicas/47928-sbu-viluchila-130-serveriv-u-kharkivskogo-data-tsentru-v-offlayn-pishla-tisjacha-saytiv.html). – 2015. – 19.04).***

***

Гомельчанин К. Сілівончик засуджений у Росії до двох років в’язниці за заклик у соціальних мережах повернути Крим Україні. Про це повідомляє Еспресо.TV з посиланням на радіо «Свобода».

«22-річний айтішник з Гомеля працював в Нижньому Новгороді системним адміністратором», – повідомив громадський активіст П. Юхневич, який отримав інформацію від родичів і дівчини засудженого білоруса.

18 грудня К. Сілівончика затримали в Нижньому Новгороді разом із друзями, які є громадянами Росії. Проти К. Сілівончика порушили кримінальну справу за російською статтею «Публічні заклики до здійснення терористичної діяльності». «Підставою стали повідомлення на підтримку України, які К. Сілівончик розміщував в соціальній мережі “ВКонтакте”. У тому числі він нібито закликав “вбивати москалів”, “повернути Крим Україні” тощо. Один з малюнків був такий, де український солдат рве російський прапор і зневажає герб», – ідеться в повідомленні.

9 квітня Московський окружний військовий суд засудив К. Сілівончика до двох років у колонії-поселенні.

Як повідомляє видання, нині він перебуває в одному із СІЗО Нижнього Новгорода й чекає відправки в колонію ***(В Росії білорусу дали два роки колонії за заклик повернути Крим Україні // Espreso.tv (http://espreso.tv/news/2015/04/21/v_rosiyi_bilorusu_daly_dva_roky_koloniyi_za_zaklyk_povernuty_krym_ukrayini). – 2015. – 21.04).***

***

Руководитель Роскомнадзора А. Жаров сегодня заявил, что сложности с Twitter периодически урегулируются, но так же периодически накапливаются из-за бюрократизма. Об этом пишет vedomosti.ru.

«У Facebook и Twitter несколько миллионов пользователей в России, и мы ведем себя в отношении них терпеливо. Вы знаете, что я направил письмо администрации Twitter, в котором выразил недоумение по поводу их позиции в отношении игнорирования наших запросов. После этого Twitter заблокировал 55 аккаунтов», – отметил А. Жаров. По его словам, сейчас опять «накапливается некая отрицательная статистика». «Однако сказать, что появилась негативная отрицательная информация, пока нельзя», – заявил он.

А. Жаров отметил, что в данных компаниях «чрезмерно забюрократизирована система принятия решений». «У нас с ними активное взаимодействие, мы общаемся по почте и Skype. Принятие решений длится в этой компании достаточно долго, с первого раза не получается, но раз в полтора месяца противоправный контент они удаляют», – отметил А. Жаров.

Он уже говорил, что Twitter систематически не выполняет требования российского законодательства. При этом глава ведомства привел данные официального отчета компании, согласно которым социальная сеть в прошлом году удовлетворила почти 3 тыс. запросов правительства США о раскрытии личной информации пользователей, а из российских запросов – ни один ***(Роскомнадзор посетовал на бюрократизм Twitter и Facebook // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43145/118/lang,ru). – 2015. – 20.04).***

***

Компания Mozilla призывает Конгресс США принять закон, который остановит программы массовой слежки за пользователями.

В рамках данной кампании представители Mozilla обратились за подписями к пользователям браузера Firefox. Mozilla настаивает на отказе от законодательного запрета на использование технологий шифрования в социальных интернет-сервисах.

Помимо этого, в петиции содержится требование предоставить широкой общественности подтверждение того, что власти не будут создавать новые надзорные органы, предоставлять полномочия или инициировать другие аналогичные программы.

Руководство Mozilla считает, что массовая слежка несёт прямую угрозу конфиденциальности и безопасности огромного количества людей, пользующихся Интернетом.

Ранее стало известно, что Mozilla готовится внедрить технологии, используемые в анонимной сети Tor во встроенную поисковую систему Firefox. Подобные меры будут предприняты для повышения анонимности пользователей.

Речь идёт об интеграции систем шифрования передаваемых данных Tor. К слову, собственный браузер Tor является одной из версий браузера Firefox с открытым исходным кодом ***(Mozilla призывает Конгресс США прекратить слежку за пользователями // Блог Imena.UA (http://www.imena.ua/blog/mozilla-secure-data). – 2015. – 20.04).***

***

Друзі оператора кримськотатарського каналу ATR Е. Небієва, який був затриманий окупаційною владою Криму після обшуку, вважають, що непрямою причиною дій щодо нього міг стати запис у соціальній мережі про перемогу сімферопольського боксера О. Усика. Про це повідомляє портал «События Крыма».

Уранці 19 квітня телеоператор залишив пост на своїй сторінці в Facebook: «Пропоную зустріти Усика з Києва! З квітами, плакатами... Давайте покажемо, що Сімферополь пишається ним, що ми його любимо і цінуємо».

Цей допис не став популярним у користувачів: його «лайкнуло» 19 людей.

Видання «События Крыма» нагадує, що ввечері 18 квітня О. Усик здобув перемогу над чемпіоном WBO Oriental росіянином А. Князєвим. Після цього глава Кримського регіонального відділення партії «Справедлива Росія» О. Юр'єв запропонував заборонити боксеру О. Усику, який не визнає анексії Криму, в'їзд на півострів.

Як повідомляла «Телекритика», 20 квітня в окупованому Російською Федерацією Криму провели обшук помешкання оператора кримськотатарського телеканалу ATR Е. Небієва, а його затримали. Інший журналіст О. Пашаєв підтвердив, що Е. Небієв був затриманий Слідчим комітетом Росії ***(Друзі оператора ATR вважають, що причиною його затримання міг стати запис в соцмережі про боксера Усика – ЗМІ // Телекритика (http://www.telekritika.ua/pravo/2015-04-21/106297). – 2015. – 21.04).***

***

Twitter анонсировал несколько нововведений, призванных сделать борьбу с интернет-троллями и оскорбительным поведением в рамках платформы более эффективной. Об этом пишет searchengines.ru.

В первую очередь компания обновила свою политику в отношении оскорбительного поведения и расширила список угрожающего и ненадлежащего контента, запрещённого к публикации в рамках сервиса.

Изначально политика сервиса микроблогов запрещала «прямые и конкретные угрозы применения насилия по отношению к другим людям». В новой версии документа слова «прямые» и «конкретные» опущены. Это нововведение позволило Twitter расширить понятие угрожающего контента в рамках сервиса.

Новая политика даёт модераторам сервиса большую свободу в интерпретации контекста твитов. Документ запрещает «угрозы применения насилия или пропаганду насилия по отношению к другим людям».

Специалисты сервиса также добавили новые инструменты, призванные остановить троллей. Первый – «заморозка» аккаунта – таймаут, в течение которого тролль, отправляющий угрозы или публикующий ненадлежащий контент, не сможет получить доступ к своей учётной записи.

Twitter уже поступает подобным образом, блокируя пользователей, публикующих ненадлежащий контент. Они не могут получить доступ к своему аккаунту до тех пор, пока запрещённые материалы не будут удалены. «Заморозка» аккаунта продлит штрафное время после выявления нарушения.

Компания также тестирует новый алгоритм, призванный идентифицировать ненадлежащий или угрожающий контент и не допустить его появление в хронике пользователя. Например, тролль угрожает конкретному пользователю. После того как алгоритм определит твит как угрозу, он не будет показан в уведомлениях пользователя.

В прошлом Twitter не удавалось справиться с наиболее агрессивными пользователями. Благодаря элементу анонимности сервиса микроблогов, интернет-тролли могли преследовать других людей и угрожать им, используя несколько аккаунтов и создавая новые, когда старые блокировались администрацией ***(Twitter ужесточил борьбу с интернет-троллями // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43182/118/lang,ru). – 2015. – 22.04).***

***

Найбільша у світі соціальна мережа Facebook записує кожне слово, яке користувачі вводять на її сторінках. Це відбувається навіть тоді, коли допис видаляється або взагалі не публікується. Про це інформує портал Information Age.

Facebook завжди заперечував, що використовує подібну технологію. За словами розробників порталу, сервіс фактично записував дані, які стосувалися видалення посту перед його публікацією, але не зберігав його змісту. Подібно справа виглядає в разі повідомлення.

Ірландський програміст Príomh Ó hÚigínn проаналізував дані, які збирає Facebook. «Виявилося, що все, що вписане до поля статусу, відсилається на

сервери Facebook навіть тоді, коли я не натискаю кнопки “опубілкувати”», – пише на своєму блозі програміст.

Щоб доказати це, він опублікував запис, який доводить, що найбільша соціальна мережа дійсно збирає всю введену в неї інформацію ***(Facebook записує навіть ті слова, які користувачі вводять, але не публікують в мережі // iPress.ua (http://ipress.ua/news/facebook_zapysuie_navit_ti_slova_yaki_korystuvachi_vvodyat_ale_ne_publikuyut_v_merezhi_120450.html). – 2015. – 23.04).***

***

Член коллегии МВД Украины А. Геращенко обнародовал информацию о масштабных операциях украинских волонтёров и спецслужб против сторонников пророссийских террористических групп ДНР/ЛНР в Интернете.

По его словам, одна из спецопераций проводилась для «выманивания» активистов террористического движения и сбора информации о российских и украинских террористах, военнослужащих российской армии и прочих лицах, которые воюют в зоне АТО или ведут информационную войну на территории Украины. К настоящему времени в базах данных сайта «Миротворец» собрано 32 тыс. аккаунтов тех, кто активно участвовал или участвует в таких противоправных действиях, а по результатам работы ещё трех дней база пополнится ещё на несколько десятков тысяч таких профилей.

Вторая спецоперация в интернет-пространстве носила название «Разводной ключ» и ставила своей целью раскрытие схемы лиц, финансирующих террористические пророссийские группировки в Украине, и подмену реквизитов на те, которые позволили бы получить деньги, предназначенные для ДНР/ЛНР, украинским военнослужащим. В числе лиц, установленных в ходе этой операции, – пророссийский журналист А. Шарий, находящийся в розыске уже несколько лет по обвинению в других преступлениях: «Если операция “Гюльчатай” ставила перед собой задачу собрать воедино данные о десятках тысяч российских и украинских террористов, их местонахождении и IP-адресах, то операция “Разводной ключ” ставила перед собой задачу собрать деньги, которые предназначались для финансирования терроризма на укрепление материальной базы украинских Вооружённых сил.

Всех лиц, занимавшихся перечислением денег на финансирование терроризма и сепаратизма, попрошу занять места в кинозале, запастись попкорном и кока-колой. Вы узнаете, как и куда пошли ваши денежки, перечисленные на финансирование преступных действий против Украины.

В сетях “ВКонтакте”, “Одноклассники”, Facebook наблюдается массовое закрытие аккаунтов антиукраинских элементов. Оно и правильно. Хватит гадить в Интернете. Его не для того создавали» ***(Проект «Миротворец» и МВД Украины провели операции против пророссийских кибертеррористов // Блог Imena.UA (http://www.imena.ua/blog/mirotvorec). – 2015. – 22.04).***

***

Правовласники підготували список з понад 700 сайтів і домагатимуться їх «довічного» блокування, якщо вони не припинять порушувати авторські права. Про це пишуть «Известия».

Блокування здійснюватимуть у рамках розширеної версії антипіратського закону, яка набуває чинності з 1 травня.

На сьогодні цей закон працює тільки щодо фільмів. Якщо суд визнає сайт порушником, цей ресурс вносять у чорний список Роскомнагляду, він стає недоступний для росіян. Але після видалення незаконного контенту сайт покидає чорний список.

Із травня за піратство каратимуть за всіма видами контенту, крім фотографій. Крім того, у правовласників з'явиться можливість закривати сайти назавжди за неодноразові порушення.

Серед укладачів чорного списку сайтів є асоціація «Інтернет-відео», яка об'єднує найбільші онлайн-кінотеатри Рунету. «Асоціація "Інтернет-відео" як одна з найбільш зацікавлених сторін в антипіратському процесі виступає координатором у роботі з блокування піратських ресурсів. Позови подаватимуть правовласники та підрядники, які займаються антипіратською діяльністю за довіреностями від правовласників», – розповів голова асоціації О. Бирдін.

У списку нині є понад 700 сайтів. Однак розкривати його повністю О. Бирдін відмовився. Він назвав лише п'ять сайтів, проти яких позови буде подано в першу чергу: kinogol.net, bobfilm.net, kinozal.tv, zerx.tv, intv.ru.

Чи ввійшли до списку соцмережі «Одноклассники» і «ВКонтакте», які періодично зазнають нападів з боку правовласників, О. Бирдін також відмовився сказати.

Свій список піратських сайтів підготували й музичні компанії. Гендиректор Національної федерації музичної індустрії (об'єднує Sony Music, Universal Music, Warner Music тощо) Л. Агронов розповів, що в їхньому списку на сьогодні є 23 ресурси-порушники. На ці сайти, за його словами, припадає 95 % усіх завантажень і прослуховувань піратської музики в Рунеті. Перші позови буде подано проти rutor.org, primemusic.ru, buffa.ru тощо ***(У Росії заблокують 700 сайтів: серед них, можливо, й «Одноклассники» та «ВКонтакте» // Інформаційна агенція «Вголос» (http://vgolos.com.ua/news/u_rosii_zablokuyut_700_saytiv_sered_nyh_mozhlyvo_y_odnoslassnyky_ta_vkontakte_178464.html). – 2015. – 22.04).***

***

Google будет защищаться шифрованием от массовой слежки АНБ

Во время проходившей в Сан-Франциско конференции BoxDEV исполнительный директор Google Э. Шмидт заявил, что использование в интернет-сервисах надежных стандартов шифрования является одним из наиболее эффективных методов противостояния правительственной слежке.

Отвечая на вопрос главы Вох А. Леви о текущем состоянии кибербезопасности в США, Э. Шмидт отметил, что был очень расстроен разоблачениями Э. Сноудена. «Они (АНБ) не сотрудничали с нами, – подчеркнул руководитель поискового гиганта. – Нам никто ничего не рассказывал, но мы работаем над тем, чтобы полностью зашифровать и обезопасить всю информацию, предоставляемую нашими клиентами для обработки».

По словам Э. Шмидта, безосновательный массовый мониторинг сетевой активности и скрытное вторжение в частную жизнь американских граждан не может являться нормой, и избежать этого поможет шифрование ***(Google будет защищаться шифрованием от массовой слежки АНБ // InternetUA (http://internetua.com/Google-budet-zasxisxatsya-shifrovaniem-ot-massovoi-slejki-anb). – 2015. – 27.04).***

Проблема захисту даних. DDOS та вірусні атаки

Компания FireEye, работающая в сфере защиты информации, опубликовала отчет, в котором уличила китайское правительство в бесчисленных хакерских атаках на правительства и корпорации различных стран Азии.

В документе сказано, что властями КНР были санкционированы атаки на виртуальные объекты в Индии, Малайзии, Таиланде, Непале, Сингапуре, на Филиппинах, в Индонезии и ряде других стран. Как отметил портал Tech Crunch, атаки периодически совершаются в течение 10 лет – первые взломы были проведены еще в 2005 г.

По словам Б. Боланда, генерального директора FireEye, Китай заинтересован в подобного рода атаках, поскольку страны Азии накопили значительную интеллектуальную собственность, за счет которой могут стать серьезными конкурентами КНР в различных сегментах деятельности. Власти Китая не могут этого допустить.

Б. Боланд отметил также, что отчет о причастности Китая ко взломам в Азии сформирован на основе многочисленных улик и доказательств, собираемых аналитиками в течение многих месяцев. К ним относятся электронные письма и даже куски кода программ, использованных при атаках. Кроме того, были обнаружены некие документы, принадлежащие весьма подозрительной, по мнению экспертов, чайной компании, расположенной в Китае, которые также имеют определенное отношение ко взломам.

Все проведенные взломы были направлены на получение политической и экономической информации, а также сведений, так или иначе относящихся к военной региональной информации. Как отметили специалисты, чаще всего хакеры применяли самый распространенный метод сбора данных – фишинг.

Они рассылали заведомо опасные ссылки или приложения с якобы доверенных адресов электронной почты.

Китайское правительство в настоящее время отказывается комментировать отчет, выпущенный FireEye ***(Китай уличили в многочисленных кибератаках на страны Азии // InternetUA (http://internetua.com/kitai-ulicsili-v-mnogocsislennih-kiberatakah-na-strani-azii). – 2015. – 14.04).***

***

Ежегодное исследование киберугроз компании Verizon, полный отчет о котором будет представлен в скором времени, показало, что в 2014 г. более двух третей из 290 случаев электронного шпионажа включали фишинг. Отправка всего 10 сотрудникам писем с прикрепленными фишинговыми ссылками позволяет злоумышленникам проникнуть внутрь корпоративной сети в 90 % случаев.

Когда СМИ говорят о кибератаках, различные издания часто указывают на сложность того или иного нападения. Если злоумышленники изображаются как хорошо финансируемые гении, то жертвы выглядят менее уязвимыми, разработчики защитных систем могут критиковать свои продукты, а правительственные чиновники – продвигать более жесткое регулирование сферы или дополнительное финансирования киберзащиты. Однако опубликованные на этой неделе отчеты подтверждают менее удобную истину: большинство хакерских атак успешны потому, что сотрудники переходят по вредоносным ссылкам в электронных сообщениях, компании не применяют доступные исправления уязвимостей ПО или IT-специалисты компании не настраивают системы должным образом.

Результаты исследования Verizon показывают, что новые бреши эксплуатируются злоумышленниками крайне редко, в то время как большинство атак в 2014 г. стали возможными благодаря уязвимостям, исправления которых были выпущены в 2007, 2010, 2011, 2012 и 2013 г.

Отчет ежегодного исследования, который опубликовала компания Symantec, показал, что финансируемые государством шпионы также используют фишинг, поскольку менее сложный подход привлекает меньше внимания со стороны специалистов по защите. Проникнув в систему, злоумышленник создает специализированное ПО, предназначенное для избежания обнаружения вне зависимости от того, какие защитные средства установила жертва.

Другой тревожной тенденцией, которую обнаружила Symantec, является использование вымогательского ПО, при помощи которого злоумышленники шифруют файлы на ПК жертвы и требуют выкуп за их расшифровку. В 80 % случаев данные так и остаются зашифрованными, даже после внесения денег на счет злоумышленника ***(В большинстве кибератак злоумышленники пользуются неопытностью пользователей // InternetUA***

(http://internetua.com/v-bolshinstve-kiberatak-zloumishlenniki-polzuuatsya-neopitnostua-polzovatelei). – 2015. – 14.04).

***

Как сообщают ИБ-специалисты из Rapid7, им удалось выявить три уязвимости в маршрутизаторе Moto, комбинированная эксплуатация которых позволяет захватить полный контроль над устройством. Таким образом, злоумышленники могут внести изменения в сетевые настройки и организовать себе подспорье для еще более опасных атак.

Технический руководитель Rapid7 Т. Бердсли утверждает, что указанные бреши затрагивают все Wi-Fi маршрутизаторы ARRIS/Motorola серии SBG6580. Вместе с тем, по его словам, для успешной атаки злоумышленникам необходимо знать внутренний IP-адрес жертвы (по умолчанию это 192.168.0.1).

«Важно подчеркнуть, что по отдельности эти бреши не представляют серьезной опасности, однако их комбинированная эксплуатация позволяет изменять сетевые настройки пользователя», – сообщает Т. Бердсли.

Эксперт также сообщил, что в настоящее время разработчики набора эксплоитов Metasploit уже представили модуль, ориентированный на поиск всех трех брешей (CVE-2015-0965, CVE-2015-0966 и CVE-2015-0964).

Официальное исправление безопасности для маршрутизатора в настоящее время недоступно ***(Бреши в маршрутизаторе Moto позволяют захватить полный контроль над устройством // InternetUA (http://internetua.com/breshi-v-marshrutizatore-Moto-pozvolyauat-zahvatit-polnii-kontrol-nad-ustroistvom). – 2015. – 14.04).***

***

Исследователь безопасности с псевдонимом Craig обнаружил уязвимость в маршрутизаторах Belkin, которая позволяет получить PIN-коды WPS. Об этом эксперт сообщил на сайте dev/ttyS0.

Проблема заключается в том, что уязвимые устройства используют легко обнаруживаемую информацию для создания PIN-кода. Потенциальному взломщику требуется знать MAC-адрес и серийный номер устройства. Выяснить эти данные достаточно просто: маршрутизаторы Belkin передают свой серийный номер в ответе на обычный probe-запрос 802.11, в то время как MAC-адрес устройства можно раскрыть с помощью нескольких достаточно простых операций. Алгоритм генерации PIN-кода использует эту информацию в качестве входных данных.

По данным исследователя, уязвимости подвержены 24 модели сетевых устройств Belkin ***(Уязвимость в маршрутизаторах Belkin позволяет получить PIN-коды WPS // InternetUA (http://internetua.com/uyazvimost-v-marshrutizatorah-Belkin-pozvolyaet-polucsit-PIN-kodi-WPS). – 2015. – 14.04).***

***

Хакеры могут атаковать современные пассажирские самолеты прямо в воздухе, предупредило американское правительственное агентство, исследовав электронику авиалайнеров Boeing и Airbus. Отчет опубликован на сайте Счетной палаты США (Government Accountability Office, GAO).

Эксперты указали, что наибольшей опасности могут быть подвержены новейшие лайнеры – американский Boeing 787 Dreamliner и европейские Airbus A350 и A380, передает CNN. По данным отчета, некоторые электронные элементы кабины пилотов используют для взаимодействия те же коммуникации или беспроводную передачу данных по Wi-Fi, которыми пользуются и пассажиры для выхода в Интернет или игр на индивидуальных экранах.

Представители GAO проконсультировались с экспертами по компьютерной безопасности, которые указали, что в этом случае возможно вмешательство извне в работу авионики. Один из опрошенных экспертов даже предположил, что платформу для проникновения в системы лайнера может предоставить вирус или червь, которого по Интернету случайно скачает кто-либо из пассажиров самолета.

CNN указывает несколько потенциальных зон риска: заражение либо манипулирование бортовыми компьютерами, контроль над системой безопасности или системой навигации или же просто трансляция опасных указаний пилоту.

В отчете GAO подчеркивается, что более старые самолеты меньше интегрированы в Интернет, и их системы управления гораздо лучше изолированы, а значит, что и риск взлома для самолетов «старше 20 лет» меньше.

Reuters сообщает, что на рассмотрение доклада Транспортным комитетом сената был приглашен представитель Федеральной авиационной администрации М. Уэрта, который согласился с выводами GAO. При этом он сообщил, что администрация уже привлекла экспертов Агентства национальной безопасности и работает над перечнем изменений, необходимых для обеспечения безопасности.

Из текстов Reuters и CNN следует, что конкретных «дыр» в электронных системах эксперты не нашли, но указали на растущую опасность сценария проникновения. Пилот Д. Бартон в интервью CNN поделился своими опасениями: «У нас хакеры в Пентагон попадали, так что проникнуть в компьютерную систему самолета, я бы предположил, совсем несложно». Телеканал, впрочем, подчеркивает, что из отчета GAO не ясно, основывались ли эксперты на результатах «полевых» тестов или же выводы базируются на теоретических предположениях.

Д. Бартон также указал, что Boeing 787 Dreamliner и Airbus A350 изначально создавались с опорой на технологию, которая в будущем может позволить перехватывать управление лайнером с земли в случае экстренной

необходимости. Впрочем, по его словам, до практической реализации этой идеи еще очень далеко.

Один из членов Транспортного комитета П. Дефазио заявил Reuters: «Этот отчет выявил реальную и серьезную угрозу кибератаки самолета во время полета. Авиационная администрация должна сфокусироваться на стандартах сертификации, которые предотвратят (действия) террориста с ноутбуком в салоне или на земле по перехвату контроля над самолетом через систему Wi-Fi, которой пользуются пассажиры».

Отметим, что немецкие СМИ не исключали версию взлома в случае катастрофы лайнера Germanwings, разбившегося в Альпах. Однако затем совокупность доказательств в отношении второго пилота А. Любица, по-видимому, намеренно направившего лайнер к земле, заставила забыть об этой гипотезе.

На момент написания заметки Boeing содержание доклада не прокомментировала. Airbus выпустила краткий пресс-релиз, заверяющий, что компания постоянно работает над архитектурой своих электронных систем с целью обеспечения высшей степени надежности и безопасности, но обсуждать детали не намерена, так как это «может быть контпродуктивно для безопасности» ***(Хакеры могут атаковать современные самолеты прямо в воздухе // InternetUA (http://internetua.com/hakeri-mogut-atakovat-sovremennie-samoleti-pryamo-v-vozduhe). – 2015. – 15.04).***

***

Разработчики Google выпустили крупное обновление для 42 версии своего браузера Chrome. В общей сложности бюллетень содержит исправления безопасности для 45 уязвимостей, из которых сразу девять получили «критический» рейтинг опасности.

Среди прочего, была устранена критическая брешь в HTML-парсере, за которую анонимный IT-эксперт получил вознаграждение в размере 7,5 тыс. дол. За все выявленные сторонними исследователями уязвимости (таких насчитывается 12 штук) компания выплатила в целом 21 тыс. дол.

Среди других критических брешей стоит отметить ошибку использования после освобождения в компоненте IPC, а также type confusion в движке V8. Кроме того, позволяющая скомпрометировать целевую систему уязвимость была выявлена в движке Blink.

Стоит отметить, что подавляющее большинство брешей, 33 штуки, были выявлены в рамках внутреннего аудита, проведенного сотрудниками Google ***(Google устранила 45 уязвимостей в Chrome // InternetUA (http://internetua.com/Google-ustranila-45-uyazvimostei-v-Chrome). – 2015. – 15.04).***

***

14 апреля компания Adobe выпустила три бюллетеня безопасности. В них было устранено 24 уязвимости в таких продуктах, как Flash Player, ColdFusion и Flex.

Бюллетень APSB15-06 описывает и исправляет 22 уязвимости во всех поддерживаемых версиях Adobe Flash Player (17.x до 17.0.0.134 включительно, 13.x до 13.0.0.277 включительно, а также 11.x до 11.2.202.451 включительно). Бреши позволяют скомпрометировать систему, раскрыть важные данные и обойти ограничения информации. Известно, что как минимум для одной уязвимости (CVE-2015-3043) существует функциональный эксплоит.

Бюллетень APSB15-07 описывает и исправляет одну уязвимость в Adobe ColdFusion версии 10 и 11. Она позволяет удаленному пользователю осуществить отраженную XSS-атаку.

Бюллетень APSB15-08 описывает и исправляет одну уязвимость в Adobe Flex 4.6 и более ранних версиях. Она позволяет удаленному пользователю осуществить отраженную XSS-атаку ***(Adobe устранила 24 уязвимости в своих продуктах // InternetUA (http://internetua.com/Adobe-ustranila-24-uyazvimosti-v-svoih-produktah). – 2015. – 15.04).***

***

Корпорация Microsoft выпустила очередную порцию обновлений для своих программных продуктов. На этот раз опубликовано 11 бюллетеней безопасности, содержащих сведения о 26 уязвимостях.

Четыре бюллетеня описывают критические «дыры». Такие баги могут эксплуатироваться злоумышленниками с целью получения несанкционированного доступа к удалённому компьютеру и выполнения на нём произвольного программного кода.

Документ MS15-033, в частности, содержит информацию о пяти опасных уязвимостях в приложениях пакета Microsoft Office. Причём одна из этих «дыр» уже используется киберпреступниками с целью проведения атак на системы с Office Word 2010: для реализации нападения достаточно вынудить жертву открыть сформированный особым образом документ в формате .docx.

Бюллетень MS15-032 описывает десять уязвимостей в различных версиях браузера Internet Explorer. Многие баги носят статус критических, другие – умеренно опасных.

Документы MS15-034 и MS15-035 содержат данные о критических «дырах» в компонентах различных версий операционных систем Windows, в том числе серверных модификаций.

Прочие бюллетени получили статус важных. Более подробную информацию об уязвимостях и обновлениях можно найти в центре безопасности Microsoft TechCenter ***(Microsoft устранила критические уязвимости в IE, Windows и Office // InternetUA (http://internetua.com/Microsoft-ustranila-kriticseskie-uyazvimosti-v-IE--Windows-i-Office). – 2015. – 15.04).***

***

Специалисты ИБ-компании «Доктор Веб» обнаружили новую вредоносную программу, способную инфицировать операционные системы, Linux. Функционал трояна позволяет сканировать удаленные ресурсы на наличие уязвимостей, а также атаковать веб-сайты с заданными адресами по протоколу HTTP. Одной из особенностей трояна является возможность управления им посредством протокола для обмена текстовыми сообщениями IRC. Вредонос получил название Linux.BackDoor.Sessox.1 (по классификации «Доктор Веб»).

По словам специалистов, после инфицирования вредонос регистрирует себя в параметрах автозагрузки. Затем он подключается к серверу, на котором работает чат, поддерживающий обмен текстовыми сообщениями по протоколу IRC. В этом чате троян получает команды от преступников, например зайти в чат-канал IRC с заданными регистрационными данными, передать информацию о времени работы зараженного компьютера или отправить на сервер сообщение PONG (в ответ на команду PING).

Помимо прочего, троян может выполнять специальные действия, в том числе атаковать определенный интернет-ресурс путем отправки повторяющихся GET-запросов и просканировать сервер на наличие ShellShock-уязвимости, позволяющей удаленно выполнить на этом сервере код.

Троян способен выполнять сканирование PHP-сценариев с помощью специальным образом сформированных POST-запросов с целью запуска постороннего скрипта на уязвимом сервере. Также атакующий может установить копию трояна в скомпрометированной системе, тем самым обеспечивая его распространение ***(Новый вредонос для Linux атакует web-сайты //InternetUA (http://internetua.com/novii-vredonos-dlya-Linux-atakuet-web-saiti). – 2015. – 15.04).***

***

Для повышения эффективности взлома паролей используется несколько методов: словари, правила для модификации словарной базы, цепи Маркова. Но можно ещё ускорить процесс, если применить новую технику, разработанную хакерами из компании Praetorian. Они предлагают комбинировать несколько известных методов, а также применить статистический анализ, чтобы выявить характерные закономерности.

Во-первых, если правила на сайте требуют, чтобы в пароле была как минимум одна цифра и один символ в верхней раскладке клавиатуры, то многие установят именно такой пароль: с одной-двумя цифрами и одним прописным символом.

Кроме того, есть другие часто встречающиеся паттерны. Например, цифры часто ставят в конце пароля, прописные буквы в начале, а у разных символов разная частота встречаемости в отдельных местах.

Зная эти факты, работа взломщика значительно упрощается. Достаточно составить «маски» с характерными шаблонами, чтобы сильно ускорить брутфорс.

Гипотезы проверили на некоторых открытых дампах с паролями, похищенными у крупных компаний, в том числе на базе Rockyou с 14,3 млн паролей, базе LinkedIn с 8,6 млн паролей и др. В общей сложности для тестирования собрали базу из 34 659 199 паролей.

Эксперимент показал, что 50 % паролей соответствуют всего лишь 13 маскам из набора.

Это доказывает универсальность применения шаблонов при составлении паролей. Статистический анализ показывает, что символы в пароле очень далеки от случайного порядка.

Выявилось также, что если пользователя вынудили использовать в пароле символ в верхнем регистре, до в 90 % случаев это первый символ в пароле!

Относительно цифр самый популярный шаблон – две цифры в конце пароля. Следующий по популярности шаблон – четыре цифры в конце. Часто это предыдущий или текущий год.

Специалисты отмечают, что есть ещё несколько специфичных методов, повышающих эффективность брутфорса. Например, инструменты вроде CeWL умеют собирать слова с веб-страниц, пополняя словарь. Логика в том, что пользователи иногда выбирают для паролей специфические термины по тематике сайта. Есть и такой приём: в словарь добавляют редкие слова, которые уже встретились в ранее взломанных паролях. Логика примерно такая же: таргетирование атаки для конкретного сайта ***(Взлом паролей с использованием статистического анализа // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/vzlom-paroley-s-ispolzovaniem-stati.html). – 2015. – 16.04).***

***

Специалисты по безопасности из американской компании Cylance обнаружили новый метод похищения логинов и паролей с любого компьютера под управлением операционной системы Windows. Используя брешь, злоумышленники могут похитить логины и пароли пользователя.

Обнаруженная уязвимость ставит под угрозу безопасность сотен миллионов пользователей. Помимо продукции Microsoft она распространена и среди программ других разработчиков.

В число затронутых уязвимостью входят такие популярные продукты, как Adobe Reader, Apple QuickTime, Apple Software Update, Microsoft Internet Explorer, Microsoft Windows Media Player, Microsoft Excel, Symantec Norton Security Scan, AVG Free, BitDefender Free, Comodo Antivirus и др.

Уязвимость окрестили Redirect to SMB. SMB – это узел, способный устанавливать соединение по протоколу Server Message Block, предназначенному для обмена файлами. Используя SMB, пользователь получает доступ к файлам и другим ресурсам на удалённом сервере.

Суть уязвимости заключается в перехвате канала с доверенным сервером при помощи атаки типа man-in-the-middle и прокладке маршрута через подставной сервер SMB с программным обеспечением, извлекающим из сетевых пакетов необходимые данные.

В ходе экспериментов выяснилось, что злоумышленники могут перехватывать не только запросы из Internet Explorer, но и запросы из установленного на компьютер программного обеспечения к серверам разработчиков.

Сейчас проблема всё ещё не решена. Для защиты от возможного хищения данных эксперты рекомендуют пользователям блокировать исходящий трафик через порты TCP 139 и TCP 445.

Зато недавно Microsoft закрыла уязвимость в Windows под кодом CVE-2015-0057, известную как «обход защиты с помощью одного бита» ***(Опасная уязвимость в Windows позволяет мошенникам похищать логины и пароли // Блог Imena.UA (http://www.imena.ua/blog/windows-resurfaces-to-steal-your-login). – 2015. – 16.04).***

***

Машины для электронного голосования AVS WinVote, которые использовались в нескольких штатах во время трёх президентских выборов в США и на других выборах с 2002 по 2014 г., совершенно ужасны с точки зрения безопасности, считают эксперты.

Д. Эпштейн из Центра по регулированию информационных технологий при Принстонском университете популярно объясняет, почему избирательная комиссия Виргинии недавно лишила модель AVS WinVote сертификата качества и запретила устанавливать подобные устройства в кабинах для голосования.

Система безопасности AVS WinVote просто безалаберно реализована. Уязвимости настолько серьёзны и просты в эксплуатации, что воспользоваться ими может кто угодно, даже школьник средней квалификации. Взломщику не требуется приходить на участок для голосования, он может быть в сотне метров от него, например на парковке. Если же сделать самодельную антенну из цилиндрической банки чипсов – то почти в километре. Подключившись к терминалу, нет проблемы войти в админский аккаунт и изменить статистику по голосованию. Более того, в системе не останется даже следов такого проникновения!

Первые версии AVS WinVote работали под Windows 2000, а современные – под Windows XP Embedded.

Причиной десертификации этих терминалов в Виргинии стало то, что во время выборов в ноябре 2014 г. одна из машин постоянно зависала. После консультаций с экспертами появилась версия, что причиной стало то, что некто в радиусе действия 802.11b пытался скачать музыку со своего iPhone. Отчёт об инциденте опубликован 14 апреля 2015 г. В нём перечислены многочисленные уязвимости AVS WinVote, количество которых не должно удивлять никого, кто

знаком с Windows XP Embedded. На ОС не устанавливались патчи с 2004 г. Уязвимые сервисы работают во встроенном сервере на портах 135/tcp, 139/tcp, 445/tcp, 3389/tcp, 6000/tcp and 16001/tcp. Можно легко получить доступ в консоль. В качестве БД используется Access со слабым криптоключом. USB-порты минимально защищены от проникновения. Беспроводная связь терминала защищена ключом WEP. Используемый пароль – «ABCDE» и т. д.

Избирательная комиссия штата в тот же день лишила AVS WinVote сертификата.

Можно только догадываться, как настолько безобразные устройства вообще допустили для подсчёта голосов и почему их используют уже более 10 лет. Нужно признать, разработчики очень дальновидно отключили логгирование, потому что скандал с подделкой результатов голосования поставил бы крест на их репутации. А так – никаких доказательств ***(Терминалы для электронного голосования может взломать даже ребёнок // InternetUA (http://internetua.com/terminali-dlya-elektronnogo-golosovaniya-mojet-vzlomat-daje-reb-nok). – 2015. – 17.04).***

***

Американский CERT сообщил, что из-за неправильной конфигурации DNS-серверов, злоумышленники имеют возможность получить информацию о внутренней структуре сетевых доменов, что позволяет провести кибератаку. Злоумышленники могут отправить AXFR-запрос на получение зоны DNS с общедоступного DNS-сервера. Если сервер сконфигурирован неправильно, он может отвечать на подобный запрос, предоставляя информацию о запрашиваемой зоне и раскрывая внутреннюю структуру сети, а также конфиденциальную информацию.

CERT отмечает, что AXFR – это протокол «передачи зон» для копирования данных DNS на нескольких DNS-серверах. В отличие от обычных запросов DNS, которые требуют от пользователя предварительного знания некоторой информации о DNS, AXFR-запросы раскрывают имена поддоменов. Поскольку передача зоны – это один запрос, он может использоваться для получения данных DNS.

Хорошо известная проблема DNS – то, что при помощи запросов передачи зон можно получить информацию о домене. Проблема привлекла к себе внимание из-за недавних сканирований Интернета, которые показывают, что большое количество DNS-серверов неправильно сконфигурированы. Открытый исходный код и проверенные сценарии дают возможность поиска брешей, что повышает вероятность эксплуатации.

Проблема широко распространена. В среднем, каждый двадцатый сайт из рейтинга Alexa использует неправильно сконфигурированный сервер. В целом, было сделано 132 854 AXFR-запроса, в результате которых оказалось, что 72 401 уникальный домен подвержен уязвимости. Специалисты рекомендуют пользователям настраивать DNS-серверы таким образом, чтобы они отвечали на AXFR-запросы только от известных IP-адресов ***(Неправильно***

сконфигурированные DNS-серверы подвержены кибератакам // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/04/17/DNS-servers-vulnerable.html). – 2015. – 17.04).

***

Один из самых известных ИБ-специалистов в мире М. Залевски в течение 30 мин обнаружил 22 ошибки в популярной встраиваемой системе управления базами данных SQLite. Стоит отметить, что архитектура SQLite считается относительно простой и при этом достаточно безопасной.

Иногда SQLite применяется в качестве механизма обработки запросов в Web. Например, некоторые браузеры используют механизм WebDB / WebSQL, в данном случае любая уязвимость в анализаторе SQLite может позволить злоумышленникам совершить кибератаку на всю систему.

М. Залевски решил использовать свою технологию поиска ошибок afl-fuzz (American Fuzzy Lop) для тестирования SQLite. В случае с разными SQL-системами подобные технологии приходится настраивать под грамматику конкретной системы, однако ИБ-эксперту потребовалось 5 мин для автоматического извлечения и сортировки ключевых слов из документации SQLite. Следующим шагом стал запуск теста: create table t1(one smallint); insert into t1 values(1); select * from t1.

М. Залевски взял большой набор вручную написанных тестов SQLite, отсортировал их по файлам, 550 шт. по 220 байт, и снова запустил программу. Данная конфигурация позволила обнаружить различные виды ошибок: неинициализированные указатели, разыменование нулевого указателя и пр.

В общей сложности поиск 22 ошибок занял у эксперта полчаса. Исправления были включены в версию SQLite 3.8.9. М. Залевски рекомендует обновить все версии системы ***(ИБ-эксперт обнаружил 22 уязвимости в SQLite за полчаса // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/04/17/SQLite.html). – 2015. – 17.04).***

***

Согласно данным исследования, проведенного ИБ-компанией Norse совместно с Американским институтом предпринимательства (American Enterprise Institute, AEI), Иран в значительной мере увеличил качество и количество своих кибератак. И это несмотря на то, что правительство страны находится в состоянии переговоров с мировыми силами касательно ограничений в использовании своего ядерного потенциала. Полный отчет об исследовании будет опубликован 17 апреля, говорится в материале издания The New York Times.

Сотрудник AEI и руководитель проекта Critical Threats Project Ф. Кеген считает, что киберпространство является для Ирана действенным оружием, предоставляющим больше возможностей, чем ядерные технологии. По его мнению, если с государства будут сняты ограничительные санкции, велика

вероятность, что прибыль от экспорта нефти будет использоваться для разработки кибероружия.

В феврале нынешнего года руководитель Национальной разведки США Д. Клеппер заявил, что за кибератаку на корпорацию Las Vegas Sands в феврале 2014 г. ответственны иранские хакеры. Это один из нескольких случаев, когда американская спецслужба идентифицировала определенную страну, подозреваемую в совершении нападения в политических целях. Первое такое заявление было озвучено в декабре прошлого года президентом США Б. Обамой, обвинившим Северную Корею в осуществлении кибератаки на Sony Pictures.

Специалисты Norse, как и эксперты другой ИБ-компании Cylance, указывают на тот факт, что иранские хакеры перешли от показных атак (обезображивание веб-сайтов или осуществление сбоя в работе интернет-ресурсов) к более сдержанной шпионской деятельности. В некоторых случаях они пытаются прозондировать критические инфраструктурные системы на наличие уязвимых сегментов, которые могут предоставить возможности для проведения разрушительных атак.

Однако компании расходятся во мнениях относительно роста количества нападений иранских хакеров. По данным Norse, в период с января 2014 г. по март 2015 г. число атак, исходящих с иранских IP-адресов, увеличилось на 115 %. В свою очередь исполнительный директор и основатель Cylance говорит о том, что за последние несколько месяцев активность иранских хакерских группировок значительно снизилась ***(Иран увеличивает частоту и сложность своих кибератак // InternetUA (http://internetua.com/iran-uvelicsivaet-csastotu-i-slojnost-svoih-kiberatak). – 2015. – 16.04).***

***

В рамках стартовавшего около года назад проекта под названием IBM X-Force Exchange специалисты компании собрали архив с данными о киберугрозах.

Компания IBM выгрузила в облачное хранилище обширную базу информации о киберугрозах, доступ к которому может получить любой пользователь. IBM надеется в корне изменить методы обеспечения кибербезопасности организаций, предоставив IT-специалистам, администраторам и обычным пользователям доступ к базе. Кроме того, пользователь сможет добавить в архив свою информацию о киберугрозах, если таковая там отсутствует.

В рамках проекта под названием IBM X-Force Exchange, который стартовал около года назад, специалисты компании собрали 700 ТБ данных о киберугрозах. Информация была получена от 270 млн пользователей и собрана на 25 млрд веб-сайтов.

Вице-президент по безопасности IBM К. Барлоу сообщил, что обмен подобной информацией давно обсуждается в кругах законодателей и

специалистов IT-сферы, однако никаких серьезных шагов в этом направлении до сих пор не было сделано.

К. Барлоу заявил, что злоумышленники хорошо образованы и тесно сотрудничают между собой, а совместная работа экспертов по безопасности, тем временем, не осуществляется на должном уровне. К. Барлоу надеется, что другие компании присоединятся к проекту и добавят новую информацию в постоянно растущую базу IBM ***(IBM обнародовала 700 ТБ данных о киберугрозах // InternetUA (http://internetua.com/IBM-obnarodovala-700-tb-dannih-o-kiberugrozah). – 2015. – 19.04).***

***

Bloomberg: хакеры из России искали информацию о санкциях

Хакеры пытались получить информацию о дискуссиях по вопросу введения санкций против России, используя несовершенство программ Microsoft и Adobe, сообщает Bloomberg.

Атаку хакеров зафиксировала 13 апреля американская компания по обеспечению кибербезопасности FireEye. По утверждению специалистов компании, хакеры из организации APT28 использовали уязвимости программы Adobe Flash, которая позволяла при обновлении в ОС Windows получить доступ к данным в компьютерных системах.

Группа APT28 уже атаковала серверы НАТО и правительств Польши, Венгрии и Грузии.

Компания Adobe заявила, что исправила использованную хакерами уязвимость, а Microsoft работает над заплаткой в системе, заявили в FireEye. Проблема не затрагивает пользователей Windows 8 и более поздних версий ***(Bloomberg: хакеры из России искали информацию о санкциях // InternetUA (http://internetua.com/Bloomberg--hakeri-iz-rossii-iskali-informaciua-o-sankciyah). – 2015. – 19.04).***

***

Согласно данным ежегодного исследования киберугроз компании Dell, в 2014 г. возросло количество вредоносного ПО, нацеленного на PoS-терминалы и SCADA-системы. Dell проанализировала данные, собранные глобальной сетью компании в более чем 200 странах. Источники данных включают сетевые экраны, которые собирают информацию о вредоносном ПО, а также отчеты независимых специалистов.

Исследование показало, что за отчетный период 2014 г. атак на SCADA-системы было осуществлено в два раза больше, чем в 2013 г. Большинство атак было зафиксировано в Финляндии, США и Великобритании. Это закономерно, поскольку в этих странах SCADA-системы получили широкое распространение. Чаще всего злоумышленники эксплуатируют уязвимость переполнения буфера.

По данным Dell, большинство атак на PoS-терминалы в 2014 г. были возможны благодаря использованию устаревшего ПО, незащищенности

мобильной сети и недостаточному регулированию доступа сотрудников к Интернету. За 2014 г. Dell собрала 37 млн образцов вредоносного ПО, что почти в два раза больше, чем в 2013 г.

Хорошие новости (хотя Dell преподносит их в негативном свете) заключаются в том, что общее количество HTTPS-подключений возросло на 109 % за 2014 г. Несмотря на распространенное мнение, что дополнительное шифрование никогда не помешает, Dell считает, что оно дает злоумышленникам больше возможностей зашифровать вредоносное ПО в процессе передачи. Такие действия позволяют большему количеству вредоносных программ проникнуть в корпоративную сеть в обход сетевого экрана ***(Количество атак на SCADA-системы удвоилось за 2014 год // InternetUA (http://internetua.com/kolicsestvo-atak-na-SCADA-sistemi-udvoilos-za-2014-god). – 2015. – 17.04).***

***

Китай впервые воспользовался новым кибероружием для DDoS-атак. Действие системы описали канадские исследователи. О наличии у Пекина новейшей киберразработки сообщили эксперты лаборатории Citizen Lab университета Торонто. Так называемая «Большая пушка», по мнению ученых, предназначена для поражения физически недоступных китайскому файерволу порталов и сервисов путем перенаправления на них интернет-трафика, приходящего в Китай извне. Разработка имеет сугубо наступательный характер, причем ее поражающее действие имеет несколько направлений: от рассылки компьютерных вирусов конкретным людям до перехвата электронных сообщений.

По данным канадских специалистов, основной специализацией «пушки» являются DDoS-атаки на удаленные сайты. Первые испытания разработки в реальных условиях уже состоялись: в конце марта «Большая пушка» использовалась для массированной кибератаки на сайт GitHub, которая длилась почти четверо суток. Вредоносный трафик, призванный нарушить работу веб-сайта, исходил от китайского поискового движка Baidu и был нацелен на две страницы, посвященные обходу средств цензуры в КНР.

Канадские исследователи считают, что «расстрел» GitHub стал результатом перенаправления трафика пользователей, находящихся за пределами КНР, которые воспользовались крупнейшим китайским поисковиком Baidu. Представители Baidu в свою очередь заявили, что никакого отношения к атакам не имеют и пообещали разобраться в причинах случившегося, а МИД КНР подчеркнул, что сам постоянно является жертвой кибератак.

Системы, аналогичные «Большой пушке», как утверждается в докладе Citizen Lab, имеют в своем арсенале Агентство национальной безопасности США, а также британская спецслужба GCHQ (Центр правительственной связи). Однако они используют эти инструменты главным образом для сбора информации, тогда как Китай волнует именно цензурирование Интернета.

Напомним, что для фильтрации интернет-трафика КНР использует «Великий китайский файервол» – систему блокировки неугодных сайтов на территории страны. Исследователи Citizen Lab нашли сходство в исходном коде файервола и «Большой пушки», позволяющее предположить, что оба инструмента используются одной и той же структурой ***(Китай выстрелил из «Большой пушки» // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/kitay-vystrelil-iz-bolshoy-pushki.html). – 2015. – 21.04).***

***

1500 приложений для iOS подвержены серьезной уязвимости

В прошлом месяце исследователи сообщили о наличии уязвимости FREAK в криптографическом пакете OpenSSL, предназначенном для работы с протоколами SSL/TLS (Secure Sockets Layer/Transport Security Layer). Эта уязвимость целенаправленно создавалась в 1990-х годах американскими производителями программного обеспечения, поставляющими свои продукты за границу. Благодаря ей можно вынудить приложения использовать 512-битные ключи шифрования вместо применяемых сейчас 2048-битных. В результате такие ключи можно взломать, запустив специальное ПО на публичных облачных сервисах.

Apple уже выпустила патч для своих операционных систем, однако обновления требуются также отдельным приложениям. Компания SourceDNA проанализировала каталог App Store и установила, что из рассмотренных приложений уязвимы около 1500. Часть из них использует стандартную библиотеку OpenSSL, другие – собственные версии.

По мнению исследователей, использование уязвимости FREAK несёт угрозу безопасности и приватности пользователей мобильных приложений. Уязвимость существует в приложениях множества категорий, включая финансы, коммуникации, покупки, бизнес, медицину. Для OpenSSL только за последний год это не первая найденная масштабная уязвимость. До неё были Heartbleed и POODLE.

Компания SourceDNA запустила собственный интернет-сервис, позволяющий определить наличие опасной уязвимости в приложениях. По словам исследователей, чаще всего атакам подвергаются мобильные клиенты, связанные с банковскими и другими финансовыми операциями. Кроме того, особый интерес для злоумышленников представляют медицинские и офисные приложения. Однако целью кибермошенников может стать и «угон» аккаунтов в Facebook, «ВКонтакте» и других социальных сетях ***(1500 приложений для iOS подвержены серьезной уязвимости // InternetUA (http://internetua.com/1500-prilojenii-dlya-iOS-podverjeni-sereznoi-uyazvimosti). – 2015. – 22.04).***

***

В Интернете появился новый черный рынок, который ориентирован на продажу эксплоитов к уязвимостям нулевого дня. Платформа под названием TheRealDeal Market выставила на продажу эксплоит к уязвимости нулевого дня в драйвере Windows HTTP.sys, которая позволяет злоумышленнику удаленно выполнять код.

Продавцы TheRealDeal также предлагают приобрести эксплоиты к уязвимостям в iCloud, Android, WordPress и пр. У покупателя нет никакой возможности убедиться перед покупкой, что эксплоиты могут функционировать в настоящее время. На «черном» ресурсе также можно найти информацию о финансовых махинациях, оружии и наркотиках.

Сделки на TheRealDeal контролируются с трех сторон: покупателем, продавцом и администрацией сайта. Для успешного перевода денег требуется подтверждение от двух из трех участников сделки. В случае разногласий решающий голос останется за администрацией ресурса ***(На черном рынке продается эксплоит к уязвимости нулевого дня в драйвере Windows HTTP.sys // InternetUA (http://internetua.com/na-csernom-rinke-prodaetsya-eksploit-k-uyazvimosti-nulevogo-dnya-v-draivere-Windows-HTTP-sys). – 2015. – 22.04).***

***

Антивирусная компания «Доктор Веб» обнаружила опасную вредоносную программу, угрожающую владельцам мобильных устройств на базе Android. Троянец под обозначением Android.Toorch.1.origin может незаметно для пользователей устанавливать и удалять приложения, а также выводить рекламу и собирать подробные данные о зараженных аппаратах.

Android.Toorch.1.origin скрывается в приложении для постоянного включения фотовспышки (функция фонарика), может распространяться через популярные сайты-каталоги ПО и загружаться на смартфон или планшет при помощи различных рекламных модулей.

После того как ничего не подозревающий пользователь установил вирус, он подключается к серверу злоумышленников и отправляет туда информацию о зараженном устройстве (текущее время и местоположение, IMEI-идентификатор, наличие root-доступа и пр.).

Троянец также включает встроенную рекламную платформу Adware.Avazu.1.origin, которая предназначена для отображения рекламы на экране зараженных устройств каждый раз, как пользователь выполнит установку той или иной программы ***(Обнаружен новый опасный вирус для Android // InternetUA (http://internetua.com/obnarujen-novii-opasnii-virus-dlya-Android). – 2015. – 22.04).***

***

Оружие будущего уже рядом. Сотрудники компании Skycure обнаружили в iOS 8 уязвимость, которая позволяет хакерам управлять устройствами Apple

через Wi-Fi. Информация была обнародована во время конференции безопасности RSA, которая проходит в Сан-Франциско.

Для демонстрации проблемы работники Skycure настоящую «цифровую бомбу», которая представляет собой специально настроенную точку доступа Wi-Fi. Название «Зона без iOS» она получила за то, что при попадании в ее радиус действия все устройства Apple входят в цикл постоянной перезагрузки. Для этого используется баг, позволяющий управлять iOS с помощью сертификатов SSL, которые передаются по беспроводной сети.

Естественно, что при отключенному Wi-Fi телефон будет работать. Или если у тебя стоит запрет на автоматическое подключения. Вот только iOS запрограммирована автоматически подключаться к беспроводным сетям определенных операторов (например at&t), которые она определяет по названию точки доступа. Значит, единственный способ восстановить работу устройства, если оно попало в подобную ловушку, – покинуть радиус действия устройства.

Компания уже связалась с Apple для устранения ошибки ***(Баг в iOS 8 позволяет создать цифровую бомбу для устройств Apple // InternetUA (http://internetua.com/bag-v-iOS-8-pozvolyaet-sozdat-cifrovuua-bombu-dlya-ustroistv-Apple). – 2015. – 23.04).***

***

Ещё в октябре прошлого года стало известно о наличии в OS X серьёзной уязвимости, которая позволяет злоумышленнику получить полный контроль над системой жертвы без аутентификации. Правда, возможно такое только при наличии физического доступа к компьютеру.

Предполагалось, что выпустив обновление до 10.10.3, Apple уже разобралась с этой проблемой, получившей название Rootpipe. Но как утверждает П. Уарлд, бывший сотрудник NSA (Агентства национальной безопасности) и основатель охранной компании SYNACK, даже последнее обновление безопасности OS X Yosemite не исправляет её полностью. Кстати, предположительно, уязвимость Rootpipe существует ещё с 2011 г., просто долгое время о её наличии никто даже и не подозревал.

По крайней мере, ему без особых усилий удалось обойти все преграды, поставленные Apple на пути взломщика. Естественно, что П. Уарлд не стал публиковать какие-либо подробности о том, как ему это удалось. Однако опытные взломщики смогут разобраться и без этих подсказок. Apple пока воздержалась от комментариев ***(Серьёзная уязвимость в OS X так и не была устранена // InternetUA (http://internetua.com/ser-znaya-uyazvimost-v-OS-X-tak-i-ne-bila-ustranena). – 2015. – 22.04).***

***

Эксперты по безопасности из компании FireEye утверждают, что уязвимость в Android позволяет хакерам получить доступ к отпечаткам пальцев

пользователей Samsung Galaxy S5 и ряда других смартфонов. Об этом сообщает Forbes.

Т. Вэй и Ю. Занг, специалисты по безопасности из американской компании FireEye, рассказали Forbes об уязвимости в операционной системе Android, которая используется в том числе на флагманском смартфоне от Samsung. Несмотря на все усилия производителей телефонов по улучшению безопасности своих устройств, отпечатки пальцев владельцев Samsung Galaxy S5 и некоторых других смартфонов могут стать лёгкой добычей для злоумышленников.

Разработчики программного обеспечения для мобильных телефонов стараются отделить и зашифровать приватную информацию пользователя в специальных «защищённых зонах», но биометрические данные можно получить ещё до того, как они в неё попадут. Затем их можно использовать для дальнейших атак.

Если хакер сможет взломать ядро Android, то ему всё равно не удастся получить доступ к тем отпечаткам данных, которые уже хранятся в «защищённой зоне». Но начиная с этого момента каждый раз, когда кто-либо использует сканер, его отпечаток пальца может попасть в руки злоумышленника.

Для доступа к отпечаткам пальцев владельцев большинства смартфонов хакерам необходимо обладать root-правами, в случае же с Samsung Galaxy S5 им достаточно иметь уровень доступа обычного пользователя. Подобная уязвимость пока не выявлена в Android версии 5.0 и выше, потому в FireEye рекомендуют пользователям обновить свои смартфоны до последних версий программного обеспечения как можно быстрее.

В ответ на информацию, обнародованную Ю. Зангом, представители компании Samsung заявили, что они очень серьёзно относятся к неприкосновенности частной жизни и безопасности личных данных своих пользователей и в данный момент расследуют ситуацію, связанную с заявлениями FireEye.

Т. Вэй и Ю. Занг сказали, что пока тестировали телефоны только на базе Android. Они уверяют, что подобная уязвимость также встречается в HTC One Max, Samsung Galaxy Note 4, Samsung Galaxy S6 и других. Galaxy S6 был представлен 1 марта и в настоящее время является флагманским смартфоном южнокорейского производителя.

В iPhone от Apple образ отпечатка пальца хранится в специально защищенной зоне процессора, и доступ к самим данным о нём на момент написания заметки пока никому получить не удалось. Хотя в 2013 г. немецкому хакеру под ником Starbug удалось обмануть Touch ID и получить доступ к iPhone, для разблокировки которого требовался отпечаток пальца владельца. На это у него ушло более 30 часов, но сам телефон взломан не был, поскольку для большинства операций также используется пароль Apple ID ***(Хакеры могут получить доступ к отпечаткам пальцев владельцев Samsung Galaxy S5 //***

InternetUA (http://internetua.com/hakeri-mogut-polucsit-dostup-k-otpecsatkam-palcev-vladelcev-Samsung-Galaxy-S5). – 2015. – 23.04).

***

Аналитики антивирусной компании «Доктор Веб» обнаружили в сети приложение-фонарик, которое может полностью скомпрометировать любое устройство под управлением операционной системы Android.

Троянское приложение замаскировано под фонарик для смартфонов. Программа позволяет получить root-привилегии на устройстве жертвы, после чего устанавливает на него другие вредоносные приложения.

Программа может передавать злоумышленникам подробную информацию об инфицированном смартфоне и отображать рекламные баннеры. Сам вирус может распространяться также путём отображения в «агрессивных рекламных модулях».

Специалисты отмечают, что вирус Android.Toorch.1.origin может заразить Android-устройство в том случае, если пользователь самостоятельно установит программу. Вероятность такой установки велика, поскольку троянец «прячется» под маской легитимного приложения.

При этом все функции, которые пользователи ожидают получить от программы-фонарика, действительно исправно работают. Это снижает вероятность своевременного обнаружения угрозы.

Кстати, независимая лаборатория AV-Test недавно опубликовала результаты своего исследования надёжности антивирусов для компьютеров под управлением Windows 8.1 ***(Вирусное приложение-фонарик для Android открывает root-доступ к устройству // Блог Imena.UA (http://www.imena.ua/blog/android-light). – 2015. – 23.04).***

***

Защита от хакеров будет встроена в чипы

За последнее десятилетие ученые, занимающиеся вопросами компьютерной безопасности, показали, что хакеры, просто анализируя обращения компьютера к памяти, могут узнать неожиданно много об информации, которая там хранится. Риск таких атак (memory-access attack) особенно велик в облаке: злоумышленник может загружать на облачные серверы небольшие программы, шпионящие за соседями по серверному пространству.

Два года назад исследователи в группе профессора MIT Ш. Девадаса предложили обезвреживать такие атаки, маскируя картину доступа к памяти. Теперь они приступили к воплощению этого метода в кремнии.

В марте, на конференции, посвященной архитектурной поддержке языков программирования и операционных систем, они представили проект заказного чипа, использующего такую схему, который в настоящее время передан в производство. На другом международном симпозиуме (IEEE International Symposium on Field-Programmable Custom Computing Machines), который

состоится в мае, они обсудят некоторые дополнения к своей схеме, проверенные на чипах с программируемой логикой.

Принцип работы предложенной схемы состоит в том, что всякий раз при обращении к памяти также опрашивается ряд ненужных ячеек, чем маскируется интерес к определенному адресу. Разумеется, такой подход снижает производительность, поэтому авторы стремились свести к минимуму количество дополнительных данных, перемещаемых между процессором и памятью. Для этого они сохраняли адреса памяти в древоподобной структуре, и каждому адресу соответствовала произвольная цепочка узлов, протянувшаяся по дереву сверху вниз. Каждое обращение к памяти включало и серию запросов ко всем узлам такой траектории.

В чипе, описанном в их последней работе, сотрудники лаборатории MIT вместе с коллегами из университетов Коннектикута и Калифорнии (Беркли), а также Института компьютерных исследований Катара предусмотрели дополнительные слоты памяти, соотносящиеся с последовательностями узлов любого пути по дереву. Процессор записывает выходящие блоки данных в эту промежуточную память, откуда они считываются по порядку.

Для приложений, эффективно использующих технологии кэширования, поддерживаемые современными чипами, ложные считывания и сохранения данных увеличивают время вычислений лишь на 20 %. В противном случае, работа компьютера может замедляться в пять и более раз.

Важным достоинством метода, как считают его авторы, является возможность просто дополнять чип новыми схемами без углубленного перепроектирования. При этом дополнительный слой защиты можно отключать, активируя его только в тех случаях, когда незначительное снижение быстродействия будет допустимой платой за предотвращение возможной утечки конфиденциальных данных ***(Защита от хакеров будет встроена в чипы // InternetUA (http://internetua.com/zasxita-ot-hakerov-budet-vstroena-v-csipi). – 2015. – 24.04).***

***

Нижняя палата парламента США приняла два новых закона, которые относятся к информационной безопасности: это закон о защите компьютерных сетей (Protecting Cyber Networks Act) и закон о продвижении национальной кибербезопасности (National Cybersecurity Protection Advancement Act). Одновременно Министерство обороны опубликовало официальную стратегию кибербезопасности.

Первый закон описывает правила по обмену информацией между коммерческими компаниями и государственными организациями. Компаниям гарантируется юридическая защита в том случае, если они сообщают властям информацию о взломе. Сообщать о взломах компании должны через специальный «киберпортал», который будет создан на сайте Министерства внутренней безопасности.

Закон вызвал неоднозначную реакцию среди экспертов. Сторонники говорят, что он поможет предотвратить и бороться с последствиями крупных корпоративных взломов, часто сопровождающихся массовой утечкой конфиденциальных данных о пользователях. Критики считают, что он только увеличивает риски утечки данных. Хотя нормативный акт устанавливает процедуру, чтобы личные данные удалялись перед загрузкой на «киберпортал», но риск утечки всё равно существует. Получается, что закон только увеличивает возможности государства для слежки за гражданами.

С призывом голосовать против закона выступала коалиция из 36 правозащитных организаций и 19 специалистов по безопасности. Перед голосованием они опубликовали открытое письмо к парламентариям. Эти действия остались без результата. Результат голосования 307 к 116 за принятие закона.

Закон о продвижении национальной кибербезопасности не вызвал таких споров. Он был принят с большим преимуществом голосов (355 к 63). Хотя эксперты не высказываются против этого закона, но существуют опасения, что его будут применять не совсем корректным образом, в сочетании с вышеупомянутым законом о защите компьютерных сетей.

В официальной стратегии кибербезопасности говорится, что для защиты национальной инфраструктуры создаётся новое подразделение Cyber Mission Force. Представители Минобороны сказали, что сейчас его штат укомплектован примерно на половину, а в полном составе оно будет включать в себя 133 группы с более чем 6000 «бойцов» ***(Пентагон принял стратегию кибербезопасности // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/pentagon-prinyal-strategiyu-kiberbezo.html). – 2015. – 24.04).***

***

В Вашингтоне сообщили о краже «российскими хакерами» писем Обамы

Последствия проникновения «российских хакеров» в компьютерные системы американского Белого дома оказались более серьезными, нежели предполагалось ранее. Об этом сообщает The New York Times со ссылкой на высокопоставленных чиновников, знакомых с ходом расследования инцидента.

Чиновники уточнили, что хакерам удалось получить не только график встреч президента Б. Обамы, но и некоторые почтовые сообщения, отправителем или получателем которых был глава государства.

Хакеры, по всей видимости, так и не взломали особо защищенные сервера, управляющие трафиком сообщений личного смартфона BlackBerry Б. Обамы, который он или его помощник носит с собой постоянно. Однако они получили доступ к архиву электронной почты чиновников Белого дома, а также, возможно, к каким-то еще пользователям вне администрации, с которыми Б. Обама регулярно переписывался. Таким образом, по данным следствия, взломщикам удалось ознакомиться с сообщениями, которые Б. Обама получал от этих людей либо отправлял им.

Представители Белого дома заверили, что ни одного сообщения, которыми чиновники обмениваются через защищенную правительственную сеть, хакерам получить не удалось. Многие представители руководства имеют в своих кабинетах сразу два компьютера, один из которых подключен к защищенной секретной сети, а другой связан с внешним миром – для несекретных коммуникаций.

При этом в администрации признали, что, тем не менее, несекретные письма обычно содержат много важной информации – рабочее расписание, переписка с послами и дипломатами, обсуждение готовящихся шагов в сфере кадров и законодательства, споры о политике.

Чиновники не раскрывают, сколько именно писем Б. Обамы было собрано хакерами, равно как и не уточняют, насколько они были важны. Сам аккаунт электронной почты президента, по всей видимости, взломан не был.

По словам помощников президента, большинство материалов предоставляются на рассмотрение Б. Обамы в устной форме, на бумаге либо на iPad, который подключен к секретной сети.

Вторжение в компьютерную систему администрации Б. Обамы началось с фишинга электронной почты, который был запущен с помощью электронной почты госдепа ***(В Вашингтоне сообщили о краже «российскими хакерами» писем Обамы // InternetUA (http://internetua.com/v-vashingtone-soobsxili-o-kraje--rossiiskimi-hakerami--pisem-obami). – 2015. – 26.04).***

***

Злоумышленники уже начали эксплуатировать исключительно опасную уязвимость SUPEE-5344, которая присутствует почти в 100 тыс. интернет-магазинах, работающих на системе управления контентом Magento.

Magento считается самой популярной CMS для интернет-магазинов. Разработчики выпустили патч ещё в феврале, но до сих пор большое количество торговых площадок не установили его, как это часто бывает. Многие владельцы магазинов просто не знают, что подвергают опасности и себя, и своих пользователей.

О проблеме рассказал голландский хостер Byte, который размещает много сайтов на платформе Magento. Они уже наблюдали использование эксплоита для Magento версий Community и Enterprise.

Информацию подтверждают коллеги из Sucuri. Они говорят, что обнаруженный ими эксплоит осуществляет только одну функцию: создаёт фальшивый админский аккаунт в базе данных Magento.

«Уязвимость на самом деле состоит из цепочки нескольких уязвимостей, которые в итоге позволяют неавторизованному пользователю запустить PHP-код на сервере», – объясняет Н. Рубин из компании Check Point. В частности, используются уязвимости CVE-2015-1397, CVE-2015-1398 и CVE-2015-1399. На сопровождающем видео специалисты Check Point показывают, как заказать дорогие наручные часы, используя SUPEE-5344.

По информации Incapsula, атаки начались в понедельник с IP-адресов 62.76.177.179 и 185.22.232.218 (оба российские) ***(Уязвимость в CMS Magento: пострадали 98 000 интернет-магазинов // InternetUA (http://internetua.com/uyazvimost-v-CMS-Magento--postradali-98-000-internet-magazinov). – 2015. – 26.04).***

***

В ходе конференции RSA 2015 г. исследователи безопасности продемонстрировали метод эксплуатации бреши в библиотеке AdLibr, используемой практически всеми популярными приложениями для мобильных платформ. По предварительным данным, уязвимость подвергает угрозе компрометации не менее 100 млн человек, передает The Register.

По словам экспертов из NowSecure Э. Хуга и Р. Велтона, проблема заключается в том, что библиотека AdLibr выполняет загруженный с сервера код, не проверяя достоверность полученных данных. Таким образом, потенциальный злоумышленник может осуществить атаку типа «человек по середине» и подменить запрос к целевому смартфону или планшету.

«Уязвимость позволяет злоумышленнику получить полный контроль над устройством, – подчеркнули исследователи. – В настоящий момент библиотека установлена и работает на гаджетах примерно 100 млн человек».

Отметим, что AdLibr используется в приложениях для отображения рекламных объявлений на дисплее. При этом, по заверениям разработчиков, пользователи нажимают на размещенные таким образом объявления порядка 27 млн раз в месяц ***(Уязвимость в библиотеке AdLibr затрагивает 100 миллионов пользователей // InternetUA (http://internetua.com/uyazvimost-v-biblioteke-AdLibr-zatragivaet-100-millionov-polzovatelei). – 2015. – 25.04).***