СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(10–24.02)

2014 № 4

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(10–24.02)
№ 4

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

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

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2014

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Слухи в соцсетях можно будет проверять на правдивость: международная группа ученых занялась разработкой системы, которая будет определять, какие записи в соцсетях соответствуют действительности, а какие нет.

Программа получила название Pheme, сообщает mainpeople.ua.

По словам К. Бончевой, руководителя исследования из университета Шеффилда, «после беспорядков 2011 г. (в Великобритании. – Ред.) поступали предложения отключать соцсети, чтобы не дать протестующим возможности организовываться через них. Но соцсети также предоставляют полезную информацию – проблема в том, что все происходит очень быстро, и мы не можем оперативно отделять правду ото лжи. Из-за этого, к примеру, экстренным службам сложно реагировать на слухи и отсекать ложь, чтобы держать ситуацию под контролем. Наша система намерена помочь с этим, отслеживая и подтверждая информацию в режиме реального времени».

Pheme будет автоматически сортировать найденные в соцсетях слухи по четырем категориям: «спекуляция», «полемика», «ложная информация, ставшая популярной случайно» и «дезинформация, распространенная намеренно, со злым умыслом».

Очень важный момент: система также сможет определять, какие сообщения рассылаются живыми пользователями, а какие – ботами. Это вполне возможно, если учитывать предысторию существования аккаунта.

Информацию программа сможет проверять благодаря постоянному сканированию первоисточников. Как скоро Pheme появится в доступе, неизвестно, однако центры тестирования системы на сегодня находятся в полной готовности ***(Слухи в соцсетях можно будет проверять на правдивость // Утро.UA (http://www.utro.ua/ru/zhizn/sluhi_v_sotssetyah_mozhno_budet_proveryat_na_pravdivost1392992447). – 2014. – 21.02).***

***

Turkiler.com – социальная сеть тюркских народов в Казахстане. Из названия видно, что основной аудиторией сети будут люди, говорящие на тюркском языке.

Участники сети смогут общаться с близкими по интересам людьми, создавать свои сообщества (улусы), обмениваться фото- и видеоматериалами и находить уникальные материалы тюркских народов. На сайте будет вестись специальная историческая база.

Создатель сети Б. Асенова хочет сделать локальный аналог уже популярных сетей Facebook, «ВКонтакте», «Одноклассники»: «Мы надеемся, что наш проект поддержат граждане из соседних стран бывшего СССР, и новая социальная сеть Turkiler.com сможет стать альтернативой популярных социальных сетей».

Набрать большую базу пользователей в очень узком сегменте представляется очень сомнительным занятием. Скорее всего, сеть преследует какую-то социальную историческую цель поднять исторические или утерянные данные, чтобы в будущем создать архив или выпустить учебник истории ***(Социальная сеть тюркских народов в Казахстане // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/sotsialnaya_set_tyurkskih_narodov_v_kazahstane). – 2014. – 11.02).***

***

Сервис микроблогов Twitter начал тестирование нового пользовательского интерфейса. Как 12 февраля сообщает интернет-издание Mashable, соцсеть планирует в будущем использовать в оформлении пользовательских профилей «плиточный» дизайн.

Обновления в профиле Twitter первым заметил редактор Mashable М. Петронзио. Зайдя в Twitter-аккаунт, журналист обнаружил, что его аватар и раздел «о себе» переместились в левую часть страницы, а к статистике твитов и подписчиков добавился счетчик загруженных фотографий и видео.

Основные изменения, однако, коснулись центрального элемента пользовательской страницы – ленты твитов. Вместо привычного вертикального блока с идущими в хронологическом порядке твитами лента М. Петронзио теперь состояла из «плиток» разной высоты и ширины с помещенным внутрь текстом. Это делало ее похожей на интерфейсы других социальных сетей – Facebook или Google+.

Сколько еще человек наряду с М. Петронзио затронул редизайн, неизвестно. На момент написания этой заметки в соцсети можно было обнаружить несколько скриншотов обновленной версии профиля, сделанных пользователями из США и Великобритании. Представители Twitter пока никак не прокомментировали обновление.

В начале февраля Twitter уже проводил обновление собственной веб-версии. Интерфейс сайта стал соответствовать внешнему виду мобильных приложений соцсети. Несмотря на то что тогда дизайн пользовательских профилей претерпел в основном лишь «косметические» изменения, обновление вызвало бурную реакцию среди пользователей. До этого (в октябре 2013 г.) в ленте Twitter стали отображаться в режиме предпросмотра большие фотографии и видеоролики, загруженные через сервис Vine ***(Twitter начал тестировать дизайн профилей в стиле Facebook // InternetUA (http://internetua.com/Twitter-nacsal-testirovat-dizain-profilei-v-stile-Facebook). – 2014. – 12.02).***

***

Facebook и другие интернет-компании оказывают давление на мобильных операторов для предоставления абонентам специального доступа к их контенту на некоторых рынках, пишет The Financial Times со ссылкой на сообщение оператора Vodafone.

Исполнительный директор Vodafone В. Колао сообщил, что главный операционный директор Facebook Ш. Сандберг во время недавнего разговора просил исключить контент Facebook из подсчета тарифного плана абонента.

В. Колао отклонил просьбу, так как, по его словам, не видит никаких причин предоставлять бесплатно пропускную способность сети.

Представитель Vodafone отметил, что каждый контент-провайдер в мире хотел бы, чтобы мобильные операторы предоставили бесплатный доступ к их контенту, однако назвал такой шаг «принципиально неправильным» для бизнес-модели компании. Facebook отказалась комментировать обсуждение ***(Facebook договаривается о бесплатном доступе к своему мобильному контенту // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_dogovarivaetsya_o_besplatnom_dostupe_k_svoemu_mobilnomu_kontentu). – 2014. – 13.02).***

***

Соціальна мережа Facebook оголосила, що її англомовні користувачі тепер зможуть вказувати свою стать, обираючи з 50 варіантів гендерної ідентичності.

Окрім варіантів «чоловіча» або «жіноча» Facebook пропонуватиме такі терміни на позначення статі, як «андрогін», «бігендер» або «транссексуал», передає ВВС-Україна.

Крім того, користувачі зможуть обрати займенник, який їх найкраще характеризує – «він», «вона» або «вони».

Соцмережа каже, що сформулювала варіанти гендерної ідентичності після консультацій із провідними організаціями, які захищають права геїв і трансгендерів.

Facebook також дає можливість понад мільярду своїх користувачів по всьому світу тримати в таємниці свою гендерну ідентичність.

Коли нові опції будуть доступні для користувачів за межами США, компанія не повідомила ***(Користувачі Facebook відтепер обиратимуть стать з 50-ти варіантів // Інформаційне агентство «Регіональні Новини» (http://regionews.ua/node/128538). – 2014. – 14.02).***

***

Сервис микроблогов Twitter добавил в блок трендов возможность отслеживать самые популярные темы в Риге, Мекке, Медине, Минске и еще 28 городах. Сообщение об этом 14 февраля появилось в официальном блоге соцсети.

Всего обновление Twitter Trends затронуло 20 стран мира. Помимо латвийских, саудовских и белорусских городов в блок также добавили столицу Австрии Вену, столицу Египта Каир, израильские Тель-Авив, Иерусалим и Хайфу и несколько других крупных городов.

Кроме того, возможность отслеживать самые обсуждаемые в соцсети темы получили пользователи из Ливана, Бахрейна, Кувейта, Панамы, Пуэрто-

Рико и Катара. Тем не менее, в этих странах настроить сортировку трендов по конкретному городу нельзя – твиты отслеживаются только по стране в целом.

Раздел Twitter Trends состоит из популярных на текущий момент хэштегов. Кликнув по тому или иному тегу, пользователь может перейти на страницу, собирающую все твиты, посвященные выбранной теме. Возможность настраивать блок трендов Twitter по стране или городу появилась в 2010 г.

Предыдущее крупное обновление списка доступных геолокаций Twitter Trends прошло в августе 2013 г. Тогда в раздел было добавлено в общей сложности более 160 городов, расположенных в Украине, в Бельгии, Греции, Кении, Португалии и других странах. Возможность настраивать тренды для Москвы, Санкт-Петербурга, Новосибирска или по России появилась в соцсети весной 2012 г. ***(Twitter покажет тренды для Риги, Мекки и Минска // InternetUA (http://internetua.com/Twitter-pokajet-trendi-dlya-rigi--mekki-i-minska). – 2014. – 14.02).***

***

В Узбекистане появилась новая социальная сеть, как две капли воды похожая на Twitter. Создатели микроблога Bamboo.uz предлагают жителям страны писать в нем все, о чем они думают, чем занимаются, что у них интересного, что они чувствуют и о чем мечтают. Об этом пишет bbc.co.uk

Страна, которой бессменно правит бывший функционер КПСС, а ныне президент И. Каримов, отличается жестким – даже по азиатским меркам – контролем Интернета и подавлением свободы слова в целом.

В рейтинге свободы Интернета за 2013 г., составленном неправительственной организацией Freedom House, Узбекистан занимает шестое место с конца.

Хуже, по версии Freedom House, дела обстоят только в Иране, Сирии, Китае, Эфиопии и на Кубе.

Патриотический сервис

Bamboo.uz является практически клоном Twitter – в его интерфейс входят точно такие же изображения пользователей, хэштеги, набор поисковых и навигационных кнопок. И даже шрифт, похоже, тот же самый.

Но есть и несколько отличий: например, сообщения могут быть длиной 700 символов – ровно в пять раз больше, чем у Twitter.

Но главная особенность национальной соцсети состоит в том, что если Twitter создан для всех без исключения, то узбекский Bamboo, как подчеркивают разработчики, «исключительно для жителей Узбекистана».

«Одна страна – одна сеть», таков его девиз.

Интернет-пользователи Узбекистана, где медиа-ландшафт жестко регулируется, восприняли приглашение писать в новом микроблоге все, о чем думается, с большим скептицизмом.

На этой неделе международная организация «Репортеры без границ» подвергла резкой критике Узбекистан за строгую цензуру, заявив, что в

настоящее время там находятся под стражей как минимум 10 журналистов и блогеров.

Нелегкая задача

Микроблог Twitter, происхождением которому обязан его национальный близнец, обрел огромную популярность в Узбекистане в прошлом году – после того как старшая дочь президента И. Каримова, Гульнара, начала выкладывать в нем закулисную информацию о своей семье. В 2012 г. Г. Каримова, которая до недавнего времени считалась одной из самых влиятельных фигур в окружении отца, попала в опалу: у бизнес-леди стали возникать большие и разнообразные проблемы, принадлежавшие ей благотворительные фонды, предприятия, магазины, радио и телевизионные станции начали закрываться один за другим.

И тогда она через Twitter принялась публиковать потоки беспрецедентных обвинений в адрес узбекских спецслужб и ближайшего окружения президентской семьи.

Судя по всему, откровения дочери президента не добавили узбекским властям нежных чувств по отношению к социальным сетям.

По мнению наблюдателей, появление Bamboo.uz – не что иное как попытка местных спецслужб полностью взять под свой контроль медиа-пространство.

Но задача это нелегкая. Предыдущая попытка запустить клона сайта Facebook, UzFacebook, провалилась – зарегистрироваться в нем пожелало всего несколько человек.

В субботу утром на сайт Bamboo.uz попасть было невозможно – во всяком случае, находясь за пределами Узбекистана ***(В Узбекистане появился свой Twitter // Mediabusiness (http://www.mediabusiness.com.ua/content/view/38328/126/lang,ru/). – 2014. – 17.02).***

***

Аккаунты умерших пользователей не будут подвергаться изменениям. Об этом заявили в компании Facebook.

«С сегодняшнего дня мы будем оставлять публичные аккаунты умерших людей открытыми, что позволит пользователям сделать профиль памятным. Мы относимся с уважением к выбранным настройкам пользователя, которые были сделаны еще при жизни», – отметили представители соцсети.

Напомним, что раньше родственники покойных могли запросить сеть закрыть страницу умершего пользователя ***(Facebook не будет удалять страницы умерших людей // InternetUA (http://internetua.com/Facebook-ne-budet-udalyat-stranici-umershih-luadei). – 2014. – 23.02).***

***

Соцсеть «Одноклассники» запустила сервис Magisto по созданию фильмов из фотографий и видеопользователей, сообщила пресс-служба соцсети.

Сервис Magisto, как показало тестирование Digit.ru, предлагает пользователю выбрать фото и видео, из которых следует создать фильм. Это могут быть как изображения, ранее размещенные пользователем на своей странице в соцсети, так и загруженные специально для фильма. Бесплатно для создания фильма разрешается использовать до 15 фото и 10 видео. Платный аккаунт «Премиум» увеличивает количество фото, используемых для фильма, до 30, а видеофайлов – до 25. Стоимость такого аккаунта составляет 80 рублей в месяц или 260 р. в год.

Вторым шагом создания фильма в «Одноклассниках» является выбор темы оформления, среди которых «Будь со мной», «Путешествие», «Ритмы улиц» и «Вечеринка». Заключительный шаг в Magisto – выбор музыки. Ее можно выбрать из предложенных композиций или загрузить свой трек. Обработка данных и создание фильма из 12 фотографий, как показало тестирование Digit.ru, заняло около минуты.

Фильмами, созданными в бесплатном аккаунте, можно только поделиться в соцсети и на других ресурсах, в то время как платный «Премиум» позволяет их скачать.

По данным соцсети, сервис Magisto умеет распознавать лица, а также различать людей, животных, пейзажи и другие объекты, выстраивая их в связную историю. Музыка в ролике может подстраиваться под сюжет, например, ускоряясь при прыжках с трамплина. В ближайших обновлениях в Magisto, как сообщают в «Одноклассниках», появится возможность создавать видео в формате HD ***(«Одноклассники» запустили сервис по созданию пользовательских фильмов // InternetUA (http://internetua.com/odnoklassniki--zapustili-servis-po-sozdaniua-polzovatelskih-filmov). – 2014. – 22.02).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Украинские маршруточники теряют работу из-за жалоб в соцсетях

После жуткой аварии, когда маршрутка с пассажирами попала под поезд, в Сумах из-за жалоб в соцсетях стали увольнять водителей-нарушителей.

Напомним: ЧП произошло 4 февраля возле села Выры Сумской области – на железнодорожном переезде поезд протаранил маршрутку. После столкновения 12 пассажиров погибли, еще шестеро пострадали, и только водитель, 27-летний Б. Лопатка, не получил травм. Об этом пишут Вести.

«После аварии был всплеск жалоб на водителей маршруток, которые нарушают ПДД, курят или отвлекаются. В соцсети появилась жалоба на одного такого – он резко тормозил. Его уже уволили, – говорит начальник логистики сумской мэрии Г. Грызодуб. – Еще двое водителей получили выговор».

Кстати, вместе с водителем маршрутки в суде будет отвечать и перевозчик. Об этом сообщили в прокуратуре Сумской области.

«8 февраля было возбуждено уголовное дело против перевозчика по статье "Грубое нарушение законодательства о труде" (может грозить запретом заниматься перевозками до трех лет или штрафом в 850 грн. – Авт.). За то, что перевозчик пустил в рейс водителя, с которым не заключили договор, – говорит руководитель пресс-службы прокуратуры А. Деревянко. – Водитель же признал свою вину, ему грозит до 10 лет».

В реанимации до сих находятся четверо человек, пострадавших в аварии. Состояние еще двоих пассажиров злосчастной маршрутки врачи оценивают как стабильное.

«Нашему Саше и, как мне известно, еще одной женщине уже чуть лучше. Саша потихоньку встает, общается, с ним работает психолог», – говорит Н. Заговора, мама 15-летнего Саши, единственного ребенка, выжившего после ДТП. Женщина уверяет: за лечение сына не платит, но и обещанную компенсацию от государства (100 тыс. грн) пока не получала. Глава сельсовета Выров С. Шкурат в свою очередь сообщает: всем пострадавшим жители поселка пожертвуют свою дневную зарплату ***(Украинские маршруточники теряют работу из-за жалоб в соцсетях // From-UA. Новости Украины (http://www.from-ua.com/news/438bc46f74f1d.html). – 2014. – 11.02).***

***

Популярный сервис SMM-аналитики SocialBakers опубликовал свежий отчет по самым популярным страницам медиабрендов в Facebook, пишет AIN (http://ain.ua/2014/02/12/512626).

Евромайдан заметно изменил расстановку сил среди украинских медиа. ТСН вытеснил с первого места «1+1», страница «5 канала» за месяц нарастила 21 тыс. подписчиков и вытеснила из первой пятерки «Лига.net», а «Интер» опустился в хвост. «5 канал» занял третье место по динамике роста базы подписчиков. Лидирует здесь «Украинская Правда», на которую в январе подписались более 25 447 фанов, а на втором месте Hromadske.tv – 25 200 новых подписчиков ***(Топ-5 медиабрендов в украинском Facebook за январь 2014 года // AIN (http://ain.ua/2014/02/12/512626). – 2014. – 12.02).***

***

У Facebook з'явилася сторінка з новинами регіональних «Майданів». Сторінка висвітлює протестний рух у регіонах України.

За кілька днів існування сторінка вже зібрала близько 500 лайків, повідомляє Еспресо.TV.

За останню добу на ній з'явилась інформація про акції протесту в Одесі, Вінниці, Львові, Івано-Франківську, Чернігові, Дніпропетровську, Херсоні, а також у менших населених пунктах – Рахові, Краматорську, Калуші, Хусті тощо.

Окрім того, на сторінці присутні повідомлення про діяльність київського Майдану та пітримку протестного руху за кордоном ***(У «Фейсбуці» з'явилась сторінка з новинами регіональних Майданів // Espreso.tv (http://espreso.tv/new/2014/02/12/u_feysbuci_zyavylas_storinka_z_novynamy_rehionalnykh_maydaniv). – 2014. – 12.02).***

***

Користувачі Facebook та «ВКонтакте» мають можливість визначати лідерів Майдану за допомогою соціальних мереж. Проголосувати можна за через спеціальний додаток «Лідери Майдану».

Взяти участь у голосуванні може кожен користувач, який зареєстрований у Facebook або «ВКонтакте».

Голосувати можна, як за запропонованих кандидатів, так і додати кандидатуру власного лідера, натиснувши кнопку «Запропонувати лідера».

Щоправда, голосування не є репрезентативним, бо користувач може проголосувати необмежену кількість разів за різних лідерів. Можна проголосувати за когось одного або за 5 чи 10 людей, яким довіряєш.

Розробники, які створили цей додаток, стверджують, що не мали на меті жодних політичних мотивів.

«Головна мета – продемонструвати настрої, які нині є в українському суспільстві. Спроба знайти нових та неординарних лідерів як серед політиків, так і громадських діячів», – ідеться в повідомленні компанії.

Встановити цей додаток можна на будь-яку сторінку у Facebook ***(Українцям пропонують вибрати лідерів Майдану у соціальних мережах // iPress.ua (http://ipress.ua/news/ukraintsyam_proponuyut_vybraty_lideriv_maydanu_u_sotsialnyh_merezhah_46560.html). – 2014. – 14.02).***

***

В преддверии Дня святого Валентина фирма Jana провела опрос среди пользователей Интернета в возрасте от 18 до 30 лет, чтобы узнать самый популярный сайт знакомств. Как сообщает The Next Web, лидером в данном направлении оказалась социальная сеть Facebook.

Статистика была составлена на основе ответов пользователей Интернета из самых разных стран мира. Несмотря на то что существуют специализированные сайты, созданные исключительно для знакомств (Badoo, Match), Facebook всё равно оказался на первом месте.

Самым большим конкурентом соцсети М. Цукерберга в этом направлении является Twitter. Сервис микроблогинга помогает сближаться людям из стран Африки, Латинской Америки и других. Статистика также

показала, что в некоторых местах планеты до сих пор остаётся актуальным MySpace, а жители Индии активно пользуются супружеским сайтом Shaadi ***(Facebook стал самым популярным сайтом знакомств // Mediabusiness (http://www.mediabusiness.com.ua/content/view/38309/126/lang,ru/). – 2014. – 14.02).***

***

У соціальній мережі Facebook з'явилася сторінка під назвою «Кіберсотня», учасники якої називають себе «об'єднанням українських кібербунтівників та інтернет-активістів».

«Ми, небайдужі патріоти, які з різних причин не можуть бути присутніми в рядах самооборони Майдану чи волонтерів на самому Майдані у Києві фізично, вирішили створити громадянську спільноту "Кіберсотня"», – ідеться в повідомленні на сторінці спільноти у Facebook.

Адміністратори сторінки пишуть, що спільнота складатиметься з «інтернет-активістів, які готові гуртуватися, координуватися з представниками самооборони Майдану та інших громадських об'єднань». У «Кіберсотні» зазначать, що їхня головна мета – зміна влади в Україні і «здобуття чесності, поваги та справедливості для кожної людини».

Із 11 лютого, коли була створена сторінка у Facebook, на спільноту підписалися вже понад 3 тис. користувачів цієї соціальної мережі ***(Тепер сотні Майдану не тільки на вулицях, але і в Інтернеті // Коломия ВЕБ Портал (http://kolomyya.org/se/sites/ko/54775/). – 2014. – 14.02).***

***

Министерство юстиции Украины создало аккаунт в социальной сети Twitter, передает корреспондент proIT со ссылкой на пресс-службу ведомства.

«Теперь в Twitter от @minjust_gov_ua украинцы смогут получать информацию об изменениях в сфере правового образования, законодательные изменения и анализ их влияния на жизнь населения, важные новости из сферы права, свежую статистику», – сообщает Минюст на своем официальном сайте ***(Минюст выходит в Twitter // proIT (http://proit.com.ua/news/internet/2014/02/17/122402.html). – 2014. – 17.02).***

***

Група молодих учених зі Львова виступила з ініціативою: використати можливості соцмереж для висвітлення досягнень і проблем вітчизняної науки. Один із них, аспірант-археолог Є. Ткач, розповідає: «Ми знаємо обличчя й імена половини депутатів Верховної Ради. А чи відомі широкому загалу наші науковці? Навіть ті, що мають світове ім'я? Над чим вони працюють? Які відкриття зробили? Про це постійно ведуться розмови, нібито робиться безліч спроб та започатковується ініціатив для популяризації науки. Але поки що похвалитися немає чим. Це виклик усім нам. Потрібно змістити

акценти в суспільстві. Маємо пишатися нашою наукою, усвідомлювати, що без неї немає майбутнього. І ініціювати зміни».

У чому суть ідеї?

«У соцмережах є сторінки окремих людей, є групи, що об'єднують однодумців з якоїсь певної тематики. Але все це обмежені аудиторії. Вашу сторінку і допис на стіні у групі прочитає лише невелике коло людей. А тим часом є можливість зробити будь-яку публікацію у соцмережах доступною для необмеженої аудиторії – усієї мережі. Для цього біля публікації ставиться спеціальний символ # (так званий хештег) і якесь кодове слово. Наприклад, дописи в мережах, пов'язані з Євромайданом, позначаються #Євромайдан, з Автомайданом – #Автомайдан, з Олімпіадою в Сочі – #Сочі. Якщо ви хочете побачити всі публікації в мережі, присвячені, скажімо, Автомайдану, – вводите у пошуковику комбінацію #Автомайдан і отримуєте всі дописи, позначені цим символом.

Ми подумали, що таким чином можна сформувати в соцмережах контент, присвячений вітчизняній науці. Пропонуємо всі дописи, статті й повідомлення, пов'язані зі сферою науки і освіти, позначати хештегом #розумні», – розповідає Є. Ткач.

Чому не #наука або #science?

«По-перше – слово "розумні" милозвучне, викликає гарні асоціації. По-друге, ми хочемо, щоб за цим хештегом відфільтровувався лише український контент, який не перетинатиметься з відповідними англомовним і російськомовним сегментами мережі. Тому уникали збігів з іншими мовами. Нам, українцям, потрібно формувати свій науковий і суспільний простір. Наука – це наше майбутнє», – каже науковець.

Інформація, позначена #розумні, буде цікава насамперед науковцям, зазначає Є. Ткач. Вони зможуть значно розширити коло спілкування, отримувати найсвіжішу інформацію від колег у різних куточках країни, брати участь у дискусіях, продукувати ідеї, поширювати інформацію про себе і свої досягнення. Звісно, у нас є наукові фахові видання. Але ж інформація цих видань призначена для обмеженої аудиторії. І таких можливостей для комунікації, як у соцмережах, вони не створюють.

Відфільтрована і скомпонована інформація під хештегом #розумні буде цікава й освітянам. Популяризація наукових досягнень, повідомлення про найсучасніші з них – усе це оперативно можна буде побачити в соцмережі. Так, про це розповідають науково-популярні журнали, які видаються в Україні. Але вони здебільшого мають певну спеціалізацію і не є універсальними. Немає в нашій країні наукового видання, яке охоплювало б багатющий спектр тематики настільки ж масштабно, як це робить, наприклад, The Telegraph.

У всьому світі популярні Science Reports або New Science. У нас є не гірші за контентом видання. Але широкий загал мало про них знає. А тим часом гарну статтю можна позначити хештегом, вона піде в мережу, і її побачить величезна аудиторія.

Хештег #розумні може бути корисний і для наукових інститутів та вишів. Звісно, у них вже є свої веб-сайти й сторінки в соцмережах. Але здебільшого там просто викладено якусь інформацію. Роботу варто вести в напрямі популяризації власної діяльності. Як це роблять усі поважні наукові установи – починаючи від NASA і закінчуючи Американською ботанічною радою.

У нас іще немає розуміння того, що інституції повинні не просто нести інформацію, а згуртовувати навколо своєї ідеї людей. А от у Європейському контенті соцмереж відбувається обмін інформацією і про студентів, і про наукові досягнення – це живі сторінки.

Важливо, щоб науковці й освітяни могли не лише обмінюватися інформацією, а й скоординувати свої дії для розв'язання спільних проблем. Це можуть бути найрізноманітніші питання – новий порядок захисту дисертацій, педагогічне навантаження на викладача, адміністративний тиск на інституції (як це було з Інститутом українознавства), фінансування державою науки тощо. Наукова і освітянська спільнота повинна активно комунікувати між собою і з усією країною, вести публічні обговорення.

Така ініціатива важлива і для наших ЗМІ. Вона дасть змогу якісно моніторити новини світу науки, визначати пріоритетні теми (їх видно за кількістю коментарів, перепостів, лайків), бачити коло експертів (активних коментаторів, розповсюджувачів новин, авторитетних фахівців) і спостерігати відверті дискусії. Навіть якщо хтось не наважується висловити відкрито свою точку зору, він може просто поставити лайк біля близької йому публікації. Коли ти не один, коли ти відчуваєш підтримку однодумців – це дуже важливо. Великим плюсом соцмережі є й те, що її неможливо цензурувати й контролювати.

«З того, що спостерігаємо нині, – активність з професійних питань у соцмережах невелика. Та вона є. Зауважу, що існують професійні соцмережі для науковців – такі як мережа academia.edu. В ній зареєстровано понад 7 млн науковців, серед яких багато й українців. Але, звісно, хотілося б, щоб вони активно спілкувалися і поза межами професійного кола. Наша ініціатива якраз і покликана змінити ситуацію», – зазначає Є. Ткач.

Ініціатори проекту – група молодих учених, які працюють над львівським едукаційним проектом «Академ Парк Вернадського». «У рамках проекту ми спільно з Львівським палацом мистецтв організовуємо для зацікавленої громадськості науково-популярні лекції. Є визначена тематика, і нам потрібні фахові лектори-науковці. Як виявилося, знайти їх неабияка проблема. Необхідність комунікувати й отримувати якомога більше інформації і спонукала нас ініціювати #розумні».

Завдяки цій ініціативі буде створено унікальний український контент, великий простір розумників, які матимуть умовний майданчик для спілкування. Це буде інформаційний потік, насичений цікавими темами, подіями. І всі зацікавлені сторони його наповнюватимуть, говоритимуть про Україну для України. Оперативно реагуватимуть на виклики суспільства й відчуватимуть його потреби. А головне – наука відчуватиме, що потрібна

суспільству й державі. Наразі ж вона не може похвалитися суспільною увагою ***(Ткач Є. Соцмережі поРОЗУМНІшають / Бесіду вела О. Онищенко // Дзеркало тижня. Україна (http://gazeta.dt.ua/science/socmerezhi-porozumnishayut-_.html). – 2014. –14– 21.02).***

***

У всіх районах Києва в останні дні було організовано багато груп самооборони. Свою діяльність вони координують через соцмережі та сервіс голосових повідомлень Zello.

Zello – це програма, яка працює як рація, але через Інтернет. Вона може працювати як через стаціонарний комп'ютер, так і через смартфони.

Найпопулярніші канали Zello зараз на Троєщині та Оболоні – мають по кілька тисяч людей.

Через сервіс люди повідомляють що зараз відбувається в різних частинах їх районів – особливо вночі. Підозрілий рух груп людей, спроби підпалів авто чи мародерства.

Щоб знайти групу свого району, введіть у пошуку назву району або «самооборона» ***(Кияни організовуються в групи патрулювання своїх районів та координують діяльність через Zello // UkrainianWatcher (http://watcher.com.ua/2014/02/21/kyyany-orhanizovuyutsya-v-hrupy-patrulyuvannya-svoyih-rayoniv-ta-koordynuyut-diyalnist-cherez-zello/). – 2014. – 24.02).***

***

Кількість прихильників сторінки Євромайдану у Facebook перевищила 250 тис. За цим показником сторінка стала найпопулярнішою в Україні.

Сторінці Євромайдану була запущена 22 листопада 2013 р., їй знадобилось усього три місяці для того, щоб стати найпопулярнішою українською сторінкою у Facebook. До цього найпопулярнішою сторінкою була «Чернігівське».

Варто зауважити, що є ще дві сторінки, які мають більше прихильників, ніж Євромайдан – «ФК Шахтар» та «Брати Клички». Обидві ці сторінки мають більше мільйона прихильників, але українських серед них лише кілька десятків тисяч (у «Шахтаря» – 50 тис. і понад півмільйона бразильців) ***(Сторінка Євромайдану стала найпопулярнішою українською сторінкою у Facebook // UkrainianWatcher (http://watcher.com.ua/2014/02/24/storinka-yevromaydanu-stala-naypopulyarnishoyu-ukrayinskoyu-storinkoyu-u-facebook/). – 2014. – 24.02).***

***

Представители Госдепартамента США: соцсети помогают США продвигать свободу слова в мире

В Нью-Йорке, в Центре для иностранной прессы, в рамках недели социальных медиа состоялось обсуждение вопросов использования

американским правительством социальных сетей для продвижения свободы слова и национальных интересов США в мире.

Участники дискуссии – представители Госдепартамента США – пришли к выводу, что для «народной дипломатии, то есть для взаимодействия с самыми разными группами населения в разных странах мира, социальные СМИ являются незаменимым инструментом».

Круглый стол назывался: «Цифровая дипломатия: как приблизить внешнюю политику».

«Более половины населения планеты сейчас моложе 30 лет, – отметила участница круглого стола, помощник Госсекретаря США по вопросам образования и культуры Э. Райан. – Эта молодежь "живет" в соцсетях, и именно до этих людей мы пытаемся дотянуться и привлечь для участия в наших программах. Чтобы достичь успеха, мы должны активно использовать новые медиа».

Еще один участник дискуссии, координатор Бюро международных информационных программ М. Филлипс, считает, что из-за социальных сетей институты и организации становятся менее влиятельными, а отдельные люди, индивидуумы, получают все больше влияния. «Большим организациям, таким, как Госдепартамент США, к этому бывает трудно приспособиться», – отметил он.

М. Филлипс также предостерег от опасности чрезмерного увлечения соцсетями и различными гаджетами, с ними связанными. Он рассказал, что работал в предвыборной кампании Б. Обамы в 2008 г. Уже тогда кандидат на пост президента Б. Обама, по словам М. Филлипса, очень хорошо понимал, как должны работать социальные медиа для его предвыборной кампании. «Дело в том, что он до выборов был общественным организатором и знал, как работать с общинами, – рассказал М. Филлипс. – Тот же самый принцип применим и сегодня: сначала должна быть разработана стратегия взаимодействия и вовлечения общин, а уже потом ее можно проводить при помощи социальных медиа».

Модератор дискуссии Э. Паркер – старший научный сотрудник мозгового центра «Новый американский фонд» и автор книги о современном «медиа-подполье» в странах с низким уровнем свободы слова – задала представителям Госдепартамента вопрос о влиянии дела Э. Сноудена на их работу и репутацию США в мире.

После его разоблачений не стало ли международное сообщество более скептически относиться к усилиям Госдепартамента продвигать свободу слова в других странах, в то время как сами США готовы серьезно наказать человека, раскрывшего общественности секретные программы американских спецслужб? Не могут ли другие страны усмотреть в этом лицемерие?

«Нельзя сравнивать яблоки с апельсинами, – ответил Д. Франц, помощник Госсекретаря США по связям с общественностью. – Э. Сноуден говорит о работе секретных служб, а то, что Госдепартамент делает в сетях, наше продвижение принципов свободы слова, – мы это делаем открыто, мы транспарентны. Но, конечно, в реальность после дела Э. Сноудена работать

стало сложнее. Однако наш месседж о важности свободы слова не изменился. В результате дела Э. Сноудена у нас в США состоялось честное обсуждение того, не зашли ли новые технологии слишком далеко и не вторгаются ли они в частное пространство граждан. И президент об этом открыто высказывался. Такое честное обсуждение было бы невозможно ни в России, ни в Китае, ни на Кубе, ни в любой другой стране мира, где нет свободы слова».

После обсуждения корреспондент «Голоса Америки» задала помощнику Госсекретаря США Д. Францу вопрос: являются ли легитимными жалобы некоторых государств, когда они утверждают, что при помощи социальных медиа Госдепартамент в некоторых странах способствует усилению протестных настроений, которые, по мнению этих государств, могут привести к смене там режима? Д. Франц считает, что эти обвинения беспочвенны.

«Миссия Госдепартамента США – продвигать открытость, транспарентность и свободу слова, – сказал он “Голосу Америки”. – Мы все время этим занимаемся во многих странах и в отдельно взятой стране. Это не имеет ничего общего со сменой режима. Например, вы уже не слышите про смену режима в Иране от представителей администрации Б. Обамы. Администрация, наоборот, хочет быть вовлеченной в диалог с официальными лицами Ирана, а также хочет взаимодействовать с гражданами Ирана. То же самое с Россией. Я не думаю, что кто-то в Госдепартаменте продвигаем смену режима в России. Но мы прекрасно понимаем, что в России и во многих других странах у людей нет свободы слова, которую мы считаем универсальным правом человека. Так что именно это универсальное право на свободу слова мы и продвигаем в мире» ***(Купчинецкая В. Соцсети и национальные интересы США // Голос Америки (http://www.golos-ameriki.ru/content/social-media-and-diplomacy/1854400.html). – 2014. – 19.02).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Как работать с бесплатным трафиком из социальных сетей. Проверьте пять позиций

Для всех сайтов в целом и для сайтов коммерческих тематик в особенности всё важнее становится трафик из социальных сетей и социальные сигналы. Допустим, вы активно занимаетесь контентом, обновляете новости и статьи на своём ресурсе, ими делятся люди в социальных сетях. Вопрос: вам известна точная цифра – какое количество пользователей возвращаются к вам на площадку после этого? Данные по Share, Like, числу посетителей, пришедших из социальных сетей на каждую станицу сайта – если иметь такую тонкую статистику перед глазами, из нее можно извлечь массу полезных вещей: проанализировать и увеличить поток

бесплатного социального трафика, пишет AIN (http://ain.ua/2014/02/10/512235).

Собирайте статистику социальной активности

Чем больше вы знаете о поведении посетителей сайта, тем эффективнее сможете укрепить социальный профиль ресурса. Соберите данные за несколько месяцев и анализируйте: какие страницы привлекают больше трафика, какие материалы получают больше лайков и шеров, какой процент посетителей возвращается, какие заголовки самые привлекательные, какие акции оказались самыми эффективными.

Хороший инструмент в помощь – модуль социальной активности UpToLike. Удобнее всего его использовать, просто установив на сайт красивые, кастомизированные кнопки, которые будут собирать информацию о поведении пользователей. UpToLike также можно использовать для опросов, конкурсов и прочего интерактива на площадках.

Экспериментируйте с кнопками на сайте

Расположение кнопок, их размер, форма, цвет – эти факторы влияют на кликабельность. Например, динамическая панель слева дает гораздо больше кликов, чем кнопки снизу (по разным данным, от 50 % до 170 %). Малозаметные кнопки в левом нижнем углу вряд ли вообще получат клики, чего нельзя сказать о ярких стилизованных кнопках в поле зрения читателя. Для экспериментов с расположением кнопок отлично подойдёт бесплатный тул Google Website Optimizer, он позволяет быстро и удобно выполнять сплит-тесты.

Создавайте трендовый контент

Следите за тем, что в тренде, и учитывайте это при написании контента. Статьи, видео и иллюстрации на трендовые темы, будь то обновление алгоритма Google, Олимпиада, продажа Motorola китайцам, новый iPad, получают, как правило, больше лайков и шеров, а также приносят трафик. Для отслеживания трендов удобен тул Google Trends, также недавно Facebook запустил секцию трендов.

Следите за социальными сигналами сторонних сайтов, где размещается ваш контент

Если помимо контент-маркетинга вы занимаетесь ссылочным продвижением сайта, обращайте внимание на социальные сигналы доноров. Все внешние ссылки на сайт должны давать переходы реальных пользователей. Это возможно, только если на сайте присутствует настоящая, активная аудитория. Таким образом, ресурс необходимо оценивать по социальным и поведенческим профилям. Это самый свежий тренд поискового маркетинга, под который уже начали перестраиваться некоторые ссылочные и статейные биржи. Например, Система SeoPult, а вслед за ней – статейная биржа WebArtex ввели новый параметр оценки донора – по поведенческим и ссылочным профилям. Что такая технология дает рекламодателю? Прежде всего, стабильность поискового маркетинга, который уже не будет так сильно зависеть от экспериментов поисковых систем, потому что ссылочный профиль сайта выглядит абсолютно

естественно. Помимо этого – дополнительный бесплатный непоисковый трафик. И всё это вместе работает на скорость достижения результатов, в том числе высоких позиций.

Не накручивайте поведенческие факторы!

Накрученные поведенческие факторы не дают ничего хорошего и очень опасны: если поисковая система заподозрит сайт в накрутке, он сразу будет пессимизирован или исключен из индекса ***(Как работать с бесплатным трафиком из социальных сетей. Проверьте 5 позиций // AIN (http://ain.ua/2014/02/10/512235). – 2014. – 10.02).***

***

Маркетинг и аналитика – фундамент успеха на YouTube

Согласно данным Nielsen, на середину 2013 г. охват YouTube в возрастной группе 18–34 был выше, чем у любой кабельной сети. И что еще важнее, на YouTube люди не просто потребляют контент, но и обсуждают, делятся им и создают собственный, пишет Marketing Media Review (http://mmr.ua/news/id/marketing-i-analitika-fundament-uspeha-na-youtube-38287/).

По данным на март 2013 г., каждый месяц на YouTube 1 млрд пользователей смотрел 7 млрд часов видео, а каждую минуту пользователи загружали на видеохостинг 100 часов видео.

Многие люди знают о существовании брендов типа Evian или грузовиков Volvo лишь благодаря YouTube. Казалось бы, сочетание огромного количества контента и большого числа заинтересованных пользователей должно гарантировать успех на YouTube любому бренду мира. Но нет, ничего подобного не происходит.

Проблема YouTube: А что это вообще такое?

Большинство брендов понятия не имеют о том, что им делать на YouTube. У некоторых компаний там есть каналы, куда они изредка что-то публикуют или используют их в качестве хранения всех своих рекламных роликов. Некоторые покупают там рекламу, но не уверены в том, что получают от этого какой-то эффект. Многие бренды экспериментируют с виральностью (кейсы Pepsi Test Drive или Dove Beauty), но уникальность не всегда приносит результат – некоторые создавали оригинальный контент (например GoPro), но оригинальность без интеграции в общую маркетинговую стратегию бренда нельзя назвать супер эффективным инструментом.

Корень всех проблем в том, что большинство брендов не знает, как им думать о YouTube. Этот сервис сложен из трех вещей – это социальная сеть (вроде Facebook), рекламная платформа и контент-платформа. Эта тройственность часто сбивает с толку руководство крупных компаний. Они любят простые вещи.

Мне нужен охват – я иду на ТВ, на Facebook мы общаемся с клиентами, мы размещаем рекламу в Vogue, потому что его читает моя жена, в Google я ищу информацию. А зачем мне YouTube? У меня нет видео с котами.

Поскольку они не понимают ценностью YouTube с точки зрения бизнеса/маркетинга, у большинства брендов в мире нет YouTube-стратегии. И их трудно в этом винить.

Кроме того, каждая компания находится на определенной ступени своего развития, и это касается всего, от маркетинга до продаж. Этот факт также нужно учитывать.

Существует и проблема измерения. Раз YouTube так многолик, и так много брендов не могут с ним разобраться, как вообще там можно измерять успех или неуспех?

Итак, мы имеем две проблемы. Что делать? И как измерять успешность своих усилий? Рассмотрим подробнее первый вопрос.

Что самое главное на YouTube? Аудитория, связи и Вы

Главное на YouTube – это глобальный охват аудитории, построение платформы и вовлечение этих людей с помощью тех самых платформ для создания связей.

Охват, построение, вовлечение.

В зависимости от размера вашей компании, YouTube-стратегия может отличаться. Предположим, что вы компания среднего размера. В этом случае, на стадии «Охват» YouTube будет использоваться как обычная рекламная платформа.

#1. С помощью пререоллов на YouTube вы можете охватить огромную аудиторию.

Это то же самое, что реклама на ТВ (и измерить ее эффективность также трудно).

#2. Следующий шаг – выделение аудитории, которая наиболее релевантна для ваших продуктов и услуг.

На YouTube есть несколько видов рекламы, и в каждой из них можно настраивать таргетинг по типу контента, ключевым словам, демографическим и психографическим показателям.

И в этом случае не нужно чрезмерно напрягать руководство лишними описаниями. Надо показать им, что покупка такой рекламы, это то же самое, что и размещение в крупных изданиях, у которых есть определенная аудитория.

#3. Еще одно пересечение YouTube с реальным миром – это спонсорство.

Ваша компания наверняка спонсирует разные мероприятия, спортивные команды и т. д. На YouTube можно делать все то же самое, но только для в десятки раз более целевой аудитории. На концерте, проходящем на стадионе, вы можете охватить рекламой пару десятков тысяч человек, а с помощью видеосервиса – сотни, если не миллионы. Здесь есть сотни каналов, спонсорами которых вы можете стать. Почему ваша компания еще не спонсирует Vsauce или Veritasium? На каждый из этих каналов подписана целая куча людей, которые напрямую относятся к вашей целевой аудитории.

Теперь, когда мы шаг за шагом смогли охватить рекламой самую широкую аудиторию на планете, пора двигаться дальше и заняться

контентной стратегией. На стадии «Построения» мы будем использовать YouTube в качестве медиаплатформы.

#4. Собственный канал

Создайте и настройте собственный канал YouTube, свое пространство на этом сервисе, которое вы полностью контролируете: внешний вид, наличие комментариев и так далее.

#5. Использование контента

Теперь у вас есть свое представительство на YouTube, и самое время для следующего шага. Обычно этот шаг как раз и пугает руководство компаний, потому что кто-то им говорил, что надо с первого же дня стать круче Michelle Phan, Dollar Shave Club или Mentos Coke. А раз это сделать очень трудно, то они предпочли бы пока отмолчаться и подождать какого-то сногсшибательного повода, чтобы триумфально разорвать YouTube.

Этого делать нельзя!

На этом этапе вам нужно взять уже имеющийся контент и загрузить его на свой новый, красиво оформленный канал. Последние телевизионные ролики, видео-уроки с форума поддержки, промо-видео с дисков, которые вы раздаете вместе со своим продуктом. Все это можно использовать. Возьмите видео с отзывами пользователей и залейте на свой канал.

Так как здесь мы используем уже имеющийся контент, данный этап не будет стоить практически ничего. Никакого риска.

#6. Начало построения отношений

Пришла пора создать первое видео именно для YouTube. Если вы уже рекламировались на ТВ, а ваши продукты заинтересовали потребителей, то они наверняка ищут их в Google и на YouTube, так почему бы не взаимодействовать с ними и там?

Все, что вам нужно будет сделать, это немного загрузить уже имеющуюся команду, которая работает над рекламными видео. Может быть, снимать более длинные версии ТВ-роликов для YouTube или делать behind-the-scenes видео. Дайте людям, которые смотрят вашу рекламу, больше возможностей взаимодействовать с вами.

Для руководства это будет первым шагом к построению отношений с аудиторией, а затраты по-прежнему останутся минимальными.

Что еще круче, с каждым вашим шагом «вглубь» стадии построения отношений будет увеличиваться и охват. А значит, результаты, которые YouTube приносит бизнесу, также будут становиться все лучше.

На стадии «Вовлечения» мы будем использовать YouTube как настоящую платформу для построения отношений. Мы уйдем от «маркетинга выкриков» (как с ТВ-рекламой) к «маркетингу диалога».

#7. Короткие видео, учитывающие интересы зрителей

Создавайте небольшие видео, которые предназначены именно для YouTube, именно для аудитории этого видеосервиса. Ваши усилия должны быть направлены на создание историй о вашем бренде – о ваших ценностях, достижениях в области благотворительности (jetBlue рассказывает о том, как

строит детские площадки). Если вы делаете что-то хорошее, почему бы об этом не рассказать?

#8. Создавайте полезный контент

Отличный способ завоевать популярность на YouTube – создавать разные обучающие видео, руководства, инструкции и т. п. Такой контент – один из самых востребованных аудиторией, его больше всего ищут. Вдохновляйтесь примерами других брендов, например тем, как Bank of America повышает финансовую грамотность людей, Google дает советы об использовании Google Glass.

Высший пилотаж – это сделать такое how-to видео, после просмотра которого, клиенты смогут использовать ваши продукты каким-то новым образом, что еще больше облегчит и улучшит их жизнь. Фокусироваться на том, чтобы сделать счастливыми уже имеющихся клиентов – очень важно.

#9. Вовлекайте аудиторию

Есть способы, которые позволяют без особых затрат получить новый контент для своего канала. Организуйте конкурсы, соревнования, устройте опрос или сбор идей. Такой подход позволяет организовать двустороннее общение, что в случае бренда очень важно. Отличный пример (правда, не из мира бизнеса) – это Conan's Video Responses. Благодаря подобной стратегии вы делаете шаг от «покупки» внимания своей аудитория к тому, чтобы заслужить это внимание.

Почему бы не использовать членов коммьюнити в качестве евангелистов вашего бренда? Опыт компаний из мира моды показывает, что это может дать хороший результат.

Отлично получается, например у TRESemme – на их канале много уникального и полезного контента, с помощью которого зрители могут улучшить свой имидж.

Высший пилотаж в использовании YouTube – это превратить его в медиа-платформу, когда ваша компания превращается из продавца серверов, софта, обуви или напитков в настоящую медийную компанию. Отличный пример того, как компания «зарабатывает» внимание пользователей, а не покупает его – это Red Bull.

Компания не продвигает свой напиток стандартными способами. Канал на YouTube является верхушкой всей медиа-системы бренда.

Значительная часть вашей целевой аудитории уже привыкла к не-телевизионному контенту. Почему бы и вам не уйти от создания ТВ-рекламы к созданию контента, который принадлежит только вам, которым вы можете управлять и вокруг которого строить сообщество преданных клиентов?

Итак, Охват, Построение и Вовлечение. Три простых пошаговых стратегии, которые помогут вам запустить свой YouTube-канал и начать получать от него отдачу уже в ближайшем будущем.

Если вы являетесь крупной компаний, то вам стоит в точности следовать описанным выше шагам.

Не всем повезло быть большим бизнесом, да и далеко не всем это нужно. Что, если вы маленькая компания?

В таком случае вам определенно не следует тратить деньги на рекламу. Вы можете начать с самого просто и дешевого – с контента.

Создайте и оформите канал, загрузите туда уже имеющийся контент, а затем переходите сразу к созданию полезного контента.

Ошибка многих маленьких компаний в том, что они создают контент, а потом ждут, что он станет популярным. Такого не произойдет – вспомните, сколько часов видео загружают пользователи за одну минуту. Нужно регулярно создавать контент, набрать начальную аудиторию, затем понять, какой контент ей нравится. А затем вложить немного денег в рекламу и расширение аудитории. Такую же стратегию можно применять и компаниям среднего размера.

Теперь, когда у вас есть общая схема действий, ее можно адаптировать практически к любой жизненной ситуации.

Например, у вас крупная компания, но менеджмент не очень хочет ввязываться в работу с коммьюнити – они боятся разговаривать с людьми, им не нужен диалог. Зато они достаточно умны, чтобы понимать – игнорировать миллиардную аудиторию YouTube просто глупо. И что же делать в такой ситуации?

Руководство по измерению успеха на YouTube

Вот ключевые KPI, которые можно использовать для измерения успешности своих действий в рамках стратегии «Охват-Построение-Вовлечение».

В случае если мы просто используем YouTube как площадку для показа ТВ-рекламы, то все, что нам нужно знать – это количество показов (impressions). От телевизионщиков вы не получите никаких других данных, значит, и здесь ничего более не требуется (хотя по факту есть возможность измерить сотни показателей).

Для дисплейной рекламы подходят стандартные аналитические метрики: CTR, и финансовая отдача (макро и микро доход, полученный благодаря digital-присутствию на десктопах и в мобильной среде).

В случае спонсорства, можно измерять количество эфиров и считать удержанную аудиторию (Retained Audience).

На стадии «Построения» можно анализировать показатель вовлеченности (Engagement Score). Он вычисляется на основе времени просмотра (функции от общего числа просмотров и процента полных просмотров видео) и взаимодействий (общее количество комментариев, лайков и расшариваний). Если у вас есть человек, ведающий аналитикой аккаунтов в Google, вы можете запросить эти данные у него. Эта метрика толком ничего не значит, но ее очень любят боссы, так что покажите им красивые цифры.

Другие метрики – куда более полезные – это Усиление (Amplification), Аплодисменты (Applause) и Показатель общительности (Conversation Rate). Их можно использовать для понимания того, действительно ли ценный контент вы создаете. А на стадии вовлечения уже понятно, какие метрики использовать.

Заключение

Присутствие на YouTube – это отличная возможность охватить огромную и крайне ценную аудиторию, построить собственную медиа-платформу, которую можно использовать как для простой трансляции своих идей и ценности, так и для зарабатывания внимания потенциальных клиентов.

Да, здесь есть определенный риск. Но большая часть всех рисков сводится к незнанию того, что вообще делать. Еще одна проблема – отсутствие понимания того, что и в каком порядке надо делать на YouTube. Благодаря всему, что написано выше, эти вопросы больше не должны вас беспокоить ***(Маркетинг и аналитика – фундамент успеха на YouTube // Marketing Media Review (http://mmr.ua/news/id/marketing-i-analitika-fundament-uspeha-na-youtube-38287/). – 2014. – 11.02).***

***

Instagram выпускает англоязычное пособие для брендов о том, как грамотно использования визуальный контент в продвижении, пишет Marketing Media Review (http://mmr.ua/news/id/instagram-vypustil-rukovodstvo-dlja-brendov-po-effektivnomu-ispolzovaniju-servisa-38341/).

Книга Handbook for Brands (Руководство для брендов), адресованная SMM-специалистам, будет включать истории успеха крупных компаний, которые эффективно используют картинки для привлечения аудитории. Среди успешных американских брендов, которые знают, какие фотографии нравятся их фанам, есть кейсы @patagonia, @disneyland, @chobani, а всего их 11.

В руководстве будет глава, посвященная ценностям Instagram и 10 популярным хэштегам вроде #chasinglight или #thingsorganizedneatly, которые наиболее вдохновляли пользователей добавить свои изображения.

Дата публикации, тираж, стоимость и подробности распространения книги пока неизвестны, но, по словам редакции Instagram, она будет доступна не для всех. Тем не менее, желающие могут получать полезные советы по теме, регулярно заходя в блог компании ***(Instagram выпустил руководство для брендов по эффективному использованию сервиса // Marketing Media Review (http://mmr.ua/news/id/instagram-vypustil-rukovodstvo-dlja-brendov-po-effektivnomu-ispolzovaniju-servisa-38341/). – 2014. – 13.02).***

***

Какой должна быть длительность идеальной рекламы на YouTube?

Сколько должна длиться моя реклама? Этот вопрос обязательно должен задать себе любой рекламодатель, который хочет использовать платформу YouTube для продвижения своих товаров и услуг, пишет Marketing Media Review (http://mmr.ua/news/id/kakoj-dolzhna-byt-dlitelnost-idealnoj-reklamy-na-youtube-38335/).

В зависимости от целей, которые преследует ваша реклама, верный ответ может отличаться.

Специалисты Econsultancy недавно проводили сплит-тестирование для одного из своих клиентов. Главной целью теста было выявление «правильной» длины рекламного ролика, которая принесла бы наибольшее число онлайн-конверсий.

Что думают пользователи?

О длине рекламы на YouTube не особенно много пишут, а между тем, это одна из важнейших тем, над которой необходимо задуматься всем потенциальным рекламодателям видеосервиса.

В 2012 г. опрос американских пользователей, проведенный Mashable, показал, что большинство пользователей не прочь посмотреть рекламу длиной до 15 секунд, а уже потом перейти к контенту YouTube.

Интересный момент – то время, которое люди, по своему мнению, готовы потратить на просмотр рекламы, и ее реальная оптимальная длина – это две большие разницы (с).

Не так давно Д. Уотерхаус из Unruly Media выяснил, что средняя длительность 10 самых расшариваемых реклам за все время составляет 4 мин. и 11 сек., а в прошлом году Г. Жарбо представил обзор популярных YouTube-реклам 2013 г. – их средняя длительность составляла 1 мин. 44 сек.

Вышеприведенные цифры означают, что если вы можете развлечь пользователя, рассказать ему увлекательную историю, то они вполне могут смотреть рекламу значительно дольше, чем сами думают.

При этом чаще всего успешность YouTube-рекламы оценивают по числу лайков и шейров, которые она получила, и по тому, стала ли она вирусной.

Быть популярным хорошо, но большинство клиентов рекламных агентств хотят не популярности, а чтобы реклама генерировала продажи с хорошим ROI.

Учитывая этот факт, Econsultancy разработали тест для проверки того, оказывает ли длина рекламного ролика влияние на конверсию и ROI.

Специалисты компании создали две рекламы, которые были практически идентичны на протяжении первых 15 секунд видео, но первый ролик по истечении этого времени заканчивался, а второй длился в общей сложности 30 секунд.

Затем был проведен A/B тест на YouTube длительностью в один месяц, а затем результаты были собраны и проанализированы.

Прежде всего, тест показал, что люди с большей вероятностью смотрят видео дольше, если его длительность не очень существенна.

34 % зрителей досмотрели 15-секундный ролик до конца, в то время как лишь 32 % добрались до середины видео 30-секундного видео.

Что впечатляет еще больше, несмотря на довольно равномерное распределение показов между двумя видео, число Earned Views (когда пользователь после просмотра рекламы идет смотреть другое видео на вашем

канале) в случае более короткого видео было в три раза выше, чем у 30-секундного ролика.

Если посмотреть на показатели конверсии, разница становится ощутимее. Более короткая реклама получила 51 % всех показов двух видео, но принесла 83 % всех конверсий.

Более того, 15-секундный ролик показал такие результаты при CPA в четыре раза ниже, чем у 30-секундного конкурента. В деньгах это 45 фунтов против 169.

Важный момент: конверсии на YouTube считают не для переходов на сайт, а для просмотров видео.

Конечно, вы можете возразить, что показатели короткого видео лучше, лишь благодаря тому факту, что короткие ролики проще досмотреть до конца, и ничего удивительного здесь нет.

Но конверсия у 15-секундного ролика была в три раза выше, а это значит, что в случае короткого видео выше было не только общее число «сконвертировавшихся» людей, но и вероятность конверсии при просмотре не такого длинного видео была выше.

И, наконец, один из самых впечатляющих статистических показателей заключается в том, что у короткого видео CTR был выше, чем у длинного: 0,84 % против 0,72 %.

Это довольно неожиданно, потому что от длинного видео можно было ожидать больше кликов только благодаря тому, что оно находится на экране зрителя дольше, но, оказалось, что пользователи склонны взаимодействовать с более короткой рекламой.

Конечно же, длина вашего рекламного видео будет в немалой степени зависеть от его содержания и рекламных целей, но (хоть аккаунт-менеджеры в агентствах могут поспорить), если вы еще не проводили тесты эффективности на YouTube, Econsultancy рекомендует стартовать с 15-секундными рекламными роликами ***(Какой должна быть длительность идеальной рекламы на YouTube? // Marketing Media Review (http://mmr.ua/news/id/kakoj-dolzhna-byt-dlitelnost-idealnoj-reklamy-na-youtube-38335/). – 2014. – 13.02).***

***

Социальная сеть Facebook в 2014 г. не будет увеличивать количество рекламных объявлений в новостной ленте пользователей. Об этом 12 февраля сообщает TechCrunch, ссылаясь на слова финансового директора соцсети Д. Эберсмана.

«Реклама в Facebook, в особенности мобильная реклама, в 2013 г. принесла нашим клиентам хороший доход и отлично себя зарекомендовала. Тем не менее, в этом году мы не будем увеличивать ее количество в пользовательских лентах», – заявил Д. Эберсман, выступая на технологической конференции Goldman Sachs Technology and Internet Conference.

По словам топ-менеджера социальной сети, то, что реклама в Facebook становится для ресурса надежным источником дохода, еще не означает, что нужно постоянно наращивать ее объемы. С другой стороны, как отметил Д. Эберсман, если бы в компании все же захотели это сделать, на вовлеченности пользователей это никак не отразилось бы. «Количество платных постов оказывает крайне незначительный эффект на то, как часто пользователи заходят на сайт. Реклама их не отпугивает», – подчеркнул Д. Эберсман.

В конце января Facebook опубликовал очередной квартальный отчет, показавший, что более 50 % рекламного дохода приносят социальной сети пользователи ее мобильных приложений. За IV квартал 2013 г. на мобильной рекламе соцсеть заработала более 1,3 млрд дол. Общая рекламная прибыль за тот же период составила 2,59 млрд дол.

Новостная лента социальной сети Facebook является одним из основных мест, в которых пользователям показывается та или иная реклама ***(Facebook пообещал не забивать новостную ленту рекламой // Версии (http://www.versii.com.ua/news/297115/). – 2014. – 13.02).***

***

Компания Facebook в ближайшее время не намерена внедрять рекламу в принадлежащее ей приложение для чтения новостей Paper, пишет CNN со ссылкой на операционного директора Facebook Ш. Сандберг. Об этом сообщает Digit.ru

Как сообщал Digit.ru, Facebook 3 февраля запустила мобильное приложение для чтения новостей Paper, которое агрегирует контент из самой социальной сети и из новостных ресурсов, для смартфонов iPhone в США. Пользователи могут изучать каждую из историй в ленте новостей либо на интересующем ресурсе в отдельном окне, а также публиковать свои истории. В дальнейшем Facebook планирует выпустить Paper для других платформ и в других регионах.

«Когда мы запускаем продукты, мы готовы долго инвестировать в них, прежде чем начнем размещать рекламу. Можно легко представить, как реклама интегрируется с Paper… но у нас нет причин делать это прямо сейчас – нам еще многое предстоит сделать с монетизацией других наших продуктов», – заявила Ш. Сандберг на конференции Goldman Sachs Technology and Internet Conference.

Ряд функций Paper действительно можно легко представить себе как рекламные форматы категории премиум. Например, панорамный режим просмотра фотографий, а также видеоролики с автопроигрыванием, которые открываются во весь экран, могут в будущем использоваться для продвижения брендов на мобильных устройствах. Кроме того, приложение Facebook Paper может быть привлекательно для продвижения контента медиакомпаний. Напомним, что в 2013 г. на мобильную рекламу пришлось 40 % выручки Facebook ***(Facebook пока не планирует размещать рекламу в приложении Paper // Медиабизнес***

(http://www.mediabusiness.com.ua/content/view/38298/126/lang,ru/). – 2014. – 13.02).

***

Российская социальная сеть «ВКонтакте» остается в числе компаний, попавших в перечень USTR, перечисляющий наиболее злостных нарушителей прав интеллектуальной собственности.

Перечень рынков, где, по мнению Вашингтона, допускаются подобные нарушения, обнародован внешнеторговым переговорным ведомством США (USTR).

По сути, это дополнение к профильному ежегодному докладу, публикуемому тем же ведомством в конце апреля. Общая цель публикаций – привлечь дополнительное внимание к проблеме. «Соединенные Штаты настоятельно призывают соответствующие органы власти усилить борьбу с пиратством и контрафактом и использовать информацию (из данного отчета) для юридических шагов по мере целесообразности», – указывается в новом «черном списке».

Компания «ВКонтакте» находится в нем с 2011 г. Претензии американцев к «бизнес-модели» данной соцсети связаны с тем, что она, «насколько можно судить, допускает несанкционированное воспроизводство и распространение» продукции, защищенной копирайтом.

В новый перечень USTR включены также файлообменник Rapidgator.net, «перебравшийся в Россию после того, как его закрыли власти Великобритании», и компания Rutracker.org, «базирующаяся в России» и именовавшаяся прежде Torrents.ru.

Докладом USTR охвачены практически все страны мира, включая торговых партнеров США ***(США оставили «ВКонтакте» в списке злостных «пиратов» // InternetUA (http://internetua.com/ssha-ostavili-vkontakte-v-spiske-zlostnih--piratov). – 2014. – 13.02).***

***

«Одноклассники» почти полностью, как и их конкурент, забиты пиратскими музыкой и видео. При этом весь этот контент агрессивно монетизируется с помощью рекламы. Более того, наличие нелегальной музыки в описании приложения в App Store выносится на первую строчку.

«Одноклассники» также составляют из этого всего красочные музыкальные альбомы с обложкой, но в случае обращений правообладателей прикидываются незнающими и удаляют загруженную копию (потом на место удаленной встает, естественно, копия песни, загруженная другим пользователем).

Как им удается избегать публичных скандалов с правообладателями?

Комментарий Roem.ru: скорее всего, сказывается пара факторов. Первый – «ВКонтакте» на первом месте по аудитории и трафику. Получает «премию за лидерство».

Второй: Mail.ru активный информационный спонсор огромного количества мероприятий, в том числе и концертов. Если «ВКонтакте» будет со всеми дружить в этом плане – накал борьбы может снизиться ***(Как «Одноклассникам» удается избегать скандалов с пиратским контентом? // InternetUA (http://internetua.com/kak--odnoklassnikam--udaetsya-izbegat-skandalov-c-piratskim-kontentom). – 2014. – 13.02).***

***

М. Цукерберг был бы вдвойне доволен покупкой Instagram за 1 млрд дол. в апреле 2012 г., если бы увидел исследование компании L2 Intelligence, согласно которому именно эта сделка стала самой значимой за последние пять лет на медиа рынке. При этом самая худшая – Tumblr, который в прошлом мае обошёлся Yahoo в 1,1 млрд дол.

В настоящее время эти социальные сети показывают совершенно разный уровень роста, а заодно и удовлетворённости со стороны брендов и рекламодателей.

Компании отказываются от рекламы в Tumblr и всё меньше идут на блог-площадку. А вот Instagram в 2014 г. может заработать 250–400 млн дол., в то время как про доходы Tumblr даже никто не заикается.

Большинство престижных брендов предпочитают рекламироваться именно в Instagram, увеличив свой engagement на 1,53 %. Также именно эта социальная сеть из года в год показывает увеличение количества уникальных пользователей, регулярно попадая в топ-10 мобильных приложений.

За вторую половину 2013 г. коммьюнити Instagram возросло на 23 %, в то время как Tumblr всего на 6 % ***(Instagram назвали лучшей медиа покупкой последних пяти лет // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/instagram_nazvali_luchshey_media_pokupkoy_poslednih_pyati_let). – 2014. – 14.02).***

***

13 февраля в рекламном кабинете социальной сети «ВКонтакте» появился новый инструмент для настроек ретаргетинга: теперь можно таргетировать рекламу по группам пользователей, совершивших на сайте рекламодателя те или иные действия. Например, по пользователям, которые просматривали характеристики определенных групп товаров или заходили на конкретные страницы, пишет AIN (http://ain.ua/2014/02/14/512964).

В дальнейшем собранные группы пользователей можно использовать как один из фильтров при настройке целевой аудитории рекламного объявления. Количество групп в одном рекламном кабинете ограничено сотней штук. Рекламодатель также может импортировать данные о клиентах (email-адреса, номера телефонов, ID «ВКонтакте») в группу ретаргетинга через интерфейс сайта или при помощи API.

Создатели блога о «ВКонтакте» LIVE поясняют механизм работы на таком примере: пользователь сети заходит на сайт по продаже пылесосов, идет в каталог и указывает параметры пылесоса, который он хотел бы

купить. «ВКонтакте» собирает данные о всех его действиях и дает ее рекламодателю (данных он не видит, но может использовать для настроек рекламы). И находясь во «ВКонтакте», пользователь будет видеть рекламу похожих моделей пылесосов.

В «LIVE Экспресс» объясняют еще проще: «…можно рекламировать что-либо той группе людей, которые сами когда-то дали знать, что заинтересованы в этом. Например, заходили на ваш сайт по продаже… молока и регистрировались там. Теперь ваше молоко будет преследовать их даже во “ВКонтакте”».

Напомним, первые возможности ретаргетинга в сети запустили год назад. В компании описывали его так: «Любая компания, собирающая адреса электронной почты и мобильные телефоны покупателей, сможет обратиться к ним со страниц нашей сети, что в разы увеличит эффективность рекламы за счет повторной коммуникации» ***(«ВКонтакте» разрешил рекламодателям отслеживать интересы пользователей // AIN (http://ain.ua/2014/02/14/512964). – 2014. – 14.02).***

***

Twitter насчитывает более 230 млн пользователей по всему миру. И если активное присутствие в Twitter стоит в вашем маркетинговом плане на этот год, или вы просто хотите эффективно его использовать, обновленная шпаргалка с графическими размерами и советами может помочь вам в этом.

В дополнение представляем еще несколько рекомендаций от The New York Times:

Если твит хорошо сработал один раз, попробуйте отправить его снова. Ваша аудитория, какой бы «фанатичной» они ни была, не контролирует ваш канал 24 часа в сутки. Повторные твиты увеличивают число потенциальных пользователей, которые могут увидеть их.

Лучше быть понятным, чем умным, по крайней мере, если в твите вы ставите ссылку на какой-либо материал. The Times обнаружили, что ясное изложение мыслей в твитах, которые описывают суть новости/материала, получает больше ретвитов.

Будьте острожны при использовании инструментов автоматического постинга. Иногда один твит, оставленный не вовремя, может иметь непредвиденные (негативные) последствия.

И бонус совет: по умолчанию Twitter не сокращает ссылки, поэтому используйте такие сервисы, как Bitly ***(Twitter: обновленный гид по размерам изображений // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_obnovlennyy_gid_po_razmeram_izobrazheniy). – 2014. – 14.02).***

***

Крупнейшая в мире социальная сеть Facebook по размерам капитализации обошла крупнейший в мире интернет-магазин. На этой неделе

акции Facebook возросли в цене, и теперь эта компания стоит 170 млрд дол. – на 5 млрд больше, чем Amazon.

В рейтинге самых дорогих компаний Facebook занимает в настоящее время седьмое место, ее обгоняют Apple, Google, Microsoft, Samsung, IBM и Oracle. Большую часть прибыли социальная сеть получает от показа рекламы на мобильных устройствах.

Facebook вышла на IPO в 2012 г. и в то время оценивалась в 100 млрд дол. Через несколько месяцев стоимость акций компании снизилась в два раза и смогла подняться до стартового уровня лишь в августе прошлого года, когда инвесторы поверили, что на мобильной рекламе можно зарабатывать. В 2013 фискальном году Facebook получила выручку в размере 7,8 млрд дол. Выручка Amazon только в IV квартале прошлого года была почти в три раза больше ***(Facebook теперь дороже Amazon // InternetUA (http://internetua.com/feisbuk-teper-doroje-amazona). – 2014. – 16.02).***

***

В декабре Facebook запустил новый алгоритм для формирования News Feed каждого пользователя. Первые итоги его работы оказались не слишком утешающими для брендов, пишет Marketing Media Review (http://mmr.ua/news/id/tjazhelaja-pravda-dlja-brendov-o-rabote-news-feed-v-facebook-38382/).

Маркетологи стали еще более ожесточенно бороться за внимание пользователя в его News Feed, когда в декабре стало известно, что Facebook включает новый алгоритм, способствующий к более качественной трансляции релевантных пользователю новостей.

Так ли это? Агентство Ignite проанализировало около 700 сообщений 20 брендов и выяснило, что всего за одну неделю количество людей, которые видели сообщения этих брендов, снизилось на 44 %. В компании сделали вывод, что новый алгоритм Facebook сделал доступ к пользователям еще сложнее.

Автор Business Insider Н. Карлсон на анонимных условиях опросил людей, близких к разработке News Feed, и вот что выяснил:

- Еще два года назад никто толком не получал новости СМИ в Facebook. Теперь издатели стараются производить контент с учетом того, что это будет показано в социальной сети. В результате контента в News Feed стало на порядок больше, конкуренция возросла, поэтому в настоящее время важно показывать пользователю самые интересные сообщения.
- Руководящий принцип News Feed – это то, что поток новостей должен быть полон вещей, которые пользователь хочет видеть.
- Facebook сместил фокус с брендов на пользователей, поскольку вторые, как выяснилось, не особенно хотят видеть сообщения первых.
- Если бренд рассчитывает привлечь пользователей через News Feed, то ему нужно просто заплатить за promoted объявления, которые гарантируют охват.

- Число подписчиков в группе и число тех, кто будет видеть новое сообщение на странице бренда, не соответствуют друг другу. Это никогда не работало, выбросьте это из головы.
- Facebook выяснил, если новости обновлять чаще, то взаимодействие пользователя с социальной сетью падает, поэтому News Feed имеет собственные темпы обновления. Лучше показать старую, но важную (если пользователь ее еще не видел), чем новую бессмысленную новость, считают в Facebook.

В Facebook понимают, что соцсеть помогает брендам бесплатно достигать своих потенциальных покупателей через News Feed, но соцсеть более не намерена это поощрять и ожидает консолидации, как это произошло на рынке поисковой оптимизации ***(Тяжелая правда для брендов о работе News Feed в Facebook // Marketing Media Review (http://mmr.ua/news/id/tjazhelaja-pravda-dlja-brendov-o-rabote-news-feed-v-facebook-38382/). – 2014. – 17.02).***

***

В этой статье мы рассмотрим 18 способов побороть хитроумную ленту Facebook и улучшить ваши показатели в работе с аудиторией соцсети, пишет Marketing Media Review (http://mmr.ua/news/id/18-sposobov-uvelichit-ohvat-i-povysit-vovlechennost-v-facebook-38385/).

Как формируется охват вашей страницы в Facebook?

Facebook определяет охват как число уникальных пользователей соцсети, которые видят ваши регулярные посты.

Для просмотра этих данных надо перейти в раздел «Статистика» (Insights) и посмотреть данные на вкладке «Охват» (Reach). Здесь вы увидите, как меняется динамика охвата с течением времени.

На охват оказывают влияние одно или несколько следующих действий:

Вы публикуете контент в Facebook на своей странице компании или бренда. Да, большая часть подписчиков не увидят отдельные ваши посты, но вы все же видите определенный охват – его называют органическим.

Пользователи Facebook могут взаимодействовать с вашим контентом (ставить лайки, добавлять комментарии, делать повторные публикации), – информация об этих действиях появляется в лентах новостей их друзей. Такой охват Facebook называется вирусным (или виральным).

Можно перенаправить пользователей на новый пост при помощи маркетинговых каналов. Конкретный новый пост можно привязать к ссылке и разослать по электронной почте. Это тоже будет входить в органический охват.

И наконец, можно купить рекламу в Facebook. Для этого есть множество опций, включая прокачивание постов и покупку целевой аудитории для показа ей постов. Такой охват называется платным.

Все четыре действия относятся к разным итерациям.

Если вы публикуете свой контент (органический охват), то часть ваших подписчиков реагируют на него (вирусный охват). А если охват этот недостаточен, можно продвинуть пост в общей ленте, – это и будет платный охват: через рекламу, продвижение постов и покупку просмотров.

Чем больше разных видов охвата вы используете, тем выше число людей, которые увидят ваш новый пост. И вот еще 18 способов, как улучшить ситуацию.

1. Создайте контент-стратегию.

Вы, наверняка, слышали об этом много раз, но на самом деле ничто не имеет такого значения, как качественный контент с вирусным потенциалом. Вашими публикациями повторно делятся только тогда, когда она интересна, а не потому, что они ее видят в основной ленте или не видят. Без разработки стратегии контент-маркетинга невозможно создавать хороший контент и вести интересную страницу в соцсети или блог.

2. Узнайте, когда ваши поклонники обычно находятся онлайн.

Мы уже рассказывали об этом раньше. Читайте в нашей недавней статье о том, как увидеть динамику активности вашей аудитории Facebook в течение дня и определить наилучшее время для публикации контента в этой соцсети.

3. Выясните оптимальную частоту постов в течение дня.

В той же статье шла речь о нахождении оптимального количества постов в сутки в Facebook.

4. Позвольте людям публиковать контент на вашей странице в Facebook.

Когда пользователи Facebook публикуют посты на вашей странице или упоминают ваш бренд, их активность отображается в лентах новостей их друзей. Это важно для вирусного охвата.

Как только пользователь что-то комментирует или чем-то делится на вашей странице, его друзья по соцсети тоже видят все происходящее в общей ленте.

Если вас беспокоит угроза спама или негативного контента, который заполонит вашу страницу, не стоит драматизировать. Можно настроить фильтры и блокирование для подобного контента по определенным ключевым словам или данным.

5. Проведите конкурс на лучший заголовок или подпись к изображению.

Проведение конкурсов на лучшую подпись к изображению – как ни странно, один из самых простых и самых эффективных способов привлечь внимание широкой аудитории и увеличить вирусный охват.

Такие конкурсы, а также раздача призов за них – способ увеличить вирусный охват сравнительно просто и эффективно. Только выберите те призы и сувениры, которые интересны вашей целевой аудитории.

6. Отвечайте на комментарии.

Чтобы сообщество вокруг вас росло и сохранялось, необходимо регулярно общаться с людьми. Люди используют социальную сеть, потому

что хотят, чтобы их услышали. Вот почему важно отвечать на все комментарии.

У вашей страницы в Facebook есть опция включения комментариев в виде веток – чтобы вы могли отвечать на конкретные комментарии конкретных пользователей.

Как только вы отвечаете, уведомление об этом приходит человеку, который оставил комментарий. Регулярные ответы на комментарии увеличивают частоту повторных заходов на страницу бренда в Facebook.

Для включения древовидных комментариев:

Перейдите на вашу страницу вашего бренда / компании и кликните на «Редактировать страницу» (Edit Page). Выберите пункт «Редактировать настройки» (Edit Settings). Перейдите к пункту «Ответы» (Replies) и нажмите «Редактировать» (Edit). Щелкните на «Разрешить ответы на комментарии на моей странице» (Allow Replies to Comments on My Page). Сохраните сделанные изменения.

7. Отмечайте комментаторов, когда пишете ответ.

Отмечать комментаторов, когда вы даете им ответ на странице на заданный вопрос или сформулированное критическое замечание – не просто правило хорошего тона, но и отличный способ вовлекать их в дискуссию.

8. Отмечайте другие страницы и предлагайте ссылки на них.

Продвигать хорошие идеи и предложения от других людей и проектов – совсем не зазорно. Наоборот: положительная рекомендация всегда окупается для вас плюсами в карму и положительными отзывами.

9. Повторно публикуйте контент, который вызвал много откликов.

Контент-стратегия касается не только создания нового контента, но и умения работать повторно уже с тем контентом, который существует.

Просмотрите все посты, которые уже получили широкий отклик и хорошо зарекомендовали себя. Возможно, есть смысл повторно вернуться к этим постам и создавать аналогичные материалы – а также периодически напоминать читателям о существующих материалах, цитируя «золотую коллекцию».

Толковое использование рефрейминга и повторных публикаций поможет повысить степень вовлечения ваших подписчиков в социальной сети.

Чтобы понять, какие публикации и типы контента пользовались успехом в прошлом, используйте информацию на вкладке «Публикации» (Posts) в разделе «Статистика» и таблицу «Все размещенные публикации» (All Posts Published), где важно обратить внимание на показатель вовлеченности.

Для получения полной картины вам нужен массив данных хотя бы за 6 прошедших месяцев.

Для повторного привлечения подписчиков можно вручную копировать и публиковать ссылки на старые посты, повторно расшаривать их или вносить изменения в существующий пост, а затем публиковать его как новый пост.

Но не слишком увлекайтесь повторными публикациями, иначе у подписчиков возникнет ощущение, что они видят сплошные репосты и повторы.

10. Прокачивайте те посты в соцсети, которые ранее показали наилучший результат.

Если вы серьезно настроены использовать маркетинговые возможности Facebook, надо использовать рекламу для продвижения постов – никуда от этого, увы, не денешься.

Правда, продвигать стоит посты, у которых уже сформировалось достаточно высокое число читательских реакций (лайков, репостов, комментариев) – это окупит затраты на получение платного охвата.

11. Поддержите посты привязкой их к Like Box на вашем сайте.

Помните, что блок-виджет Like box, предназначенный для встраивания на сайтах, оснащен полезной возможностью показа недавних постов?

Показ постов с вашей страницы Facebook в боковой панели вашего сайта поможет вам привлечь больше людей к опубликованному ранее контенту, даже если сами пользователи этот контент пропустили.

Для включения этой опции вам надо перейти на страницу плагина и поставить галочку напротив Show Posts.

12. Встраивайте наиболее популярный контент в посты блога.

Использование популярных постов из соцсети в контексте публикаций в блогах и на страницах сайтов – еще одна дополнительная возможность привлечь внимание аудитории к вашему контенту. Любой пост на вашей странице Facebook можно встроить в блог или на сайт.

13. Общайтесь с вашими друзьями.

Часто поддерживайте контакт с друзьями в соцсетях, при этом предлагая им интересные посты с вашей страницы в Facebook. Силой заставлять их не надо, спамить тоже не стоит – но предлагать и периодически репостить контент все же нужно. Особенно хорошо это срабатывает, если у вас в друзьях есть люди, чья индустрия, текущая работа или сфера интересов пересекается в контентом с вашей страницы.

14. Используйте гостевые посты на сайте для получения дополнительного трафика.

Гостевой блоггинг – достаточно мощная стратегия для привлечения дополнительной аудитории. Гостевые записи также можно использовать и для прокачивания контента на основе возможностей Facebook Insights.

В отчете «Посещения» (Visits) перейдите к секции «Внешние ссылки» (External Referrers). Этот график покажет вам источники входящего трафика с других сайтов. Свяжитесь с администрацией этих сайтов, чтобы договориться о гостевых постах.

Помимо гостевых постов или интервью хорошо также опробовать совместные маркетинговые проекты, которые могут быть взаимовыгодны по трафику и по финансовой отдаче.

15. Наилучшие снимки публикуйте в Pinterest.

При публикации изображения в Pinterest у вас есть возможность привязки интернет-адресов к опубликованному изображению: после щелчка по картинке пользователь будет автоматически переходить по привязанной ссылке. Попробуйте использовать эту тактику для работы с наиболее рейтинговыми изображениями с вашей страницы Facebook.

Следите за тем, как меняется трафик в зависимости от использования привязанных ссылок и картинок при помощи графика «Внешние ссылки» (External Referrers) в Facebook Insights.

16. Публикуйте в Twitter ссылки на свои самые успешные посты в Facebook.

Тут все просто и очевидно: ссылки на наиболее резонансные посты из Facebook стоит публиковать в Twitter, но выдержите паузу от 24 до 48 часов между публикацией одного и того же контента на разных площадках.

17. Используйте email-маркетинг для продвижения постов из соцсети.

Эта процедура сравнительно проста и эффективна, и странно, что ею не так часто пользуются. В еженедельной рассылке помещайте по меньшей мере одну ссылку на ваш пост в Facebook. В особенности это хорошо срабатывает в случае проведения пользовательских опросов.

18. Наилучшую тактику ведения страницы определяйте при помощи Facebook Insights.

Все перечисленные выше тактические приемы можно использовать как по отдельности, так и в комплексе. Для понимания того, что работает наилучшим образом, а что не дает особой отдачи, регулярно следите за показателями и различными источниками входящего трафика с помощью Facebook Insights.

Внимательно наблюдайте, какие типы публикуемого контента приносят вам новых поклонников, подписавшихся на вашу страницу. В зависимости от этого корректируйте свою общую контент-стратегию, время выхода постов и каналы распространения ссылок на сам пост.

Надеемся, что все приведенные в этой статье советы помогут вам увеличить аудиторию в соцсети и сделать вашу страницу в Facebook успешной в плане маркетинговой эффективности и вовлечения пользователей ***(18 способов увеличить охват и повысить вовлеченность в Facebook // Marketing Media Review (http://mmr.ua/news/id/18-sposobov-uvelichit-ohvat-i-povysit-vovlechennost-v-facebook-38385/). – 2014. – 17.02).***

***

We are social проанализировали активность брендов в социальных сетях и реакцию пользователей на нее во время Олимпиады в Сочи.

На первый взгляд, спортивное событие столь высокого уровня с таким плотным информационным покрытием и многочисленными обсуждениями в Интернете должно было бы стать идеальным сценарием для маркетологов. Однако, по политическим ли причинам или из-за социальных факторов, одни спонсоры Сочи-2014 с первого дня Олимпиады сталкиваются с проблемами,

тогда как другие преуспевают. Итак, кто же стал победителем в социальных сетях?

Общая картина

Компания проанализировала общение на английском языке между 7 и 18 февраля. Оказалось, что больше всего в контексте партнерства с Олимпийскими играми обсуждалась Visa (49,7 тыс. упоминаний), за ней идет McDonalds (18,8 тыс. упоминаний) и Procter & Gamble (12 тыс.).

McDonald's, может, и занимает второе место по количеству упоминаний, но компания испытывала определенные трудности с выстраиванием убедительного разговора. Для нее все началось хуже некуда, когда ее хэштег #cheerstosochi был спародирован ЛГБТ-активистами, выступающими против пропаганды гомофобии в России.

Возможно, бренд так никогда от этого и не оправится, а несоответствие компании, занимающейся фастфудом, и спортивных соревнований может только усугубить ситуацию. В отличие от конкурентов, McDonald's так и не смог убедить публику в необходимости своего участия в Олимпиаде.

Хотя по числу упоминаний Procter & Gamble находится на третьем месте, у компании больше всего положительных обсуждений (67 %). Ее успех был главным образом создан рекламной кампанией «Спасибо, мама» и стремлением сосредоточиться на спортсменах и их матерях – идеальная площадка для дискуссий со стороны бренда, производящего товары для дома и личной гигиены.

Отказавшись от акцента на своей продукции, Procter & Gamble смогла добиться эмоциональной реакции, по-прежнему привлекая свою целевую аудиторию. К настоящему времени реклама собрала впечатляющие 18,3 млн просмотров ***(Олимпиада в Сочи не принесла брендам большого успеха в социальных сетях // Marketing Media Review (http://mmr.ua/news/id/olimpiada-v-sochi-ne-prinesla-brendam-bolshogo-uspeha-v-socialnyh-setjah-38467/). – 2014. – 24.02).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Разрушители мифов: психологи развенчали популярные заблуждения о подростках в соцсетях

Сотрудники московского института психологии провели масштабное исследование, в ходе которого выяснили, чем привлекают подростков социальные сети. Для этой цели они опросили несколько сотен десятиклассников и их родителей. Кроме этого, психологи провели экспертную сессию с модераторами и администраторами наиболее

популярных сообществ «ВКонтакте», пишет AIN (http://ain.ua/2014/02/14/512649).

Большинство опрошенных подростков призналось, что много времени проводят в социальных сетях. При этом они не считают, что это влияет на их успеваемость. Всего психологи исследовали пять популярных мифов о подростках в социальных сетях. Подтвердились далеко не все.

Миф 1: Подростки сутками сидят в социальных сетях.

Вывод психологов: Не все подростки сидят в социальных сетях круглыми сутками. Больше 12 часов в сутки в социальных сетях проводит только 5 % опрошенных. В среднем же школьники проводят в соцсетях от одного до трех часов в сутки.

Миф 2: Избыточное пребывание в социальных сетях может отрицательно сказаться на их успеваемости в школе.

Вывод психологов: Связь между времяпровождением в соцсетях и успеваемостью все же есть. 11 % школьников признались, что пропускали уроки из-за соцсетей. А практически треть респондентов признались, что иногда засидевшись в соцсетях они даже забывали поесть.

Миф 3: В социальных сетях подростки часто знакомятся с незнакомыми людьми.

Вывод психологов: Большинство подростков заявили, что не добавляют в друзья незнакомых людей и предпочитают переносить в сеть только своих реальных знакомых. У «среднестатистического» школьника в друзьях не больше 300 пользователей, при этом 80 % из них он знает лично.

Миф 4: В социальных сетях подростки часто выдают себя за каких-то персонажей или известных людей.

Вывод психологов: Сами подростки утверждают, что они не выдают себя за других персонажей, но при этом соглашаются, что большинству пользователей соцсетей свойственно такое поведение. Авторы исследования полагают, что подросткам трудно признаться в этом даже самим себе, потому что такое поведение социально не одобряется.

Миф 5: Как правило в социальных сетях подростки постоянно обновляют статусы и выкладывают фотографии.

Вывод психологов: По словам школьников, они довольно редко обновляют статусы и выкладывают фотографии. Школьники скорее потребляют контент (репосты, прослушивание музыки, просмотр фильмов), а не производят его ***(Разрушители мифов: психологи развенчали популярные заблуждения о подростках в соцсетях // AIN (http://ain.ua/2014/02/14/512649). – 2014. – 14.02).***

***

Приближение весны пробуждает чувства, наблюдать за проявлениями которых стало очень легко с помощью социальных сетей. Специалисты компании Facebook подготовили серию отчётов, посвящённых изучению любви на языке цифр.

В одном из исследований с использованием деперсонифицированной информации была проведена оценка динамики взаимодействия между парами до и после начала их отношений. Исследователи утверждают, что за счёт методов анализа «больших данных» они могут увидеть зарождающиеся романтические отношения между пользователями ещё до того, как они станут очевидными для самой пары.

В своём блоге аналитик К. Дьюк пишет, что, когда для двух людей начинается период ухаживания, число их взаимных постов в хронике Facebook увеличивается характерным образом. Пик активности наблюдается за двенадцать дней до начала взаимоотношений, а спад обычно приходится на конец третьего месяца.

«Примерно за сто дней до начала отношений, – пишет К. Дьюк, – мы наблюдаем постепенный рост числа взаимных сообщений между формирующейся парой».

В случае успешного развития отношений за несколько дней до смены статусов в их профилях отмечается всплеск использования эмотиконов и выражений с позитивной эмоциональной окраской. Слово «любовь» и ласковые формы обращения в адрес друг друга звучат значительно чаще.

После того как каждый из пары поставит статус «в отношениях», число записей обычно уменьшается – просто из-за того, что они стали проводить больше времени вместе и нашли занятие интереснее, чем переписка в Facebook.

Поэтому, несмотря на падение числа постов в хронике, их содержание в целом становится гораздо позитивнее.

Facebook скрепляет разбитые сердца

К сожалению, отношения между влюблёнными не всегда приводят к появлению новой счастливой семьи. Иногда любовь угасает, и люди расстаются. Аналитики компании Facebook попытались выяснить, насколько их социальная сеть помогает пользователям преодолеть горечь разрыва отношений.

В какой степени Facebook сегодня выступает в роли средства поддержки со стороны друзей после любовного кризиса? Чтобы ответить на этот вопрос, Э. Фриджери и его коллеги задействовали методы обработки «больших данных».

Они изучили группу людей, чьи близкие отношения продлились не менее четырёх недель, прежде чем закончились разлукой. Сделать такую выборку из полутора миллиардов аккаунтов было довольно легко за счёт инструмента «Хроника» и отслеживания изменений статусов пользователей.

Наблюдения охватывали период, начинавшийся за месяц до предстоящего разрыва отношений и продолжавшийся в течение месяца после этого события. Для каждого человека в группе отслеживалось число сообщений, постов от других людей и количество оставленных на их странице комментариев.

Непосредственно перед разрывом все эти показатели начинают резко расти. Средневзвешенное число взаимодействий через социальную сеть в

день размолвки возрастает более чем втрое. Затем активность постепенно стабилизируется и в течение следующей недели постепенно снижается до уровня, превышающего первоначальный.

По мнению Э. Фриджери, это как раз объясняется поддержкой со стороны друзей, которая приходит от них в виде личных сообщений или ободряющих комментариев.

Можно ли заранее спрогнозировать развитие отношений?

Аналитики Facebook, попытались выяснить это в ходе другого исследования. Принято считать, что прочность отношений определяется их длительностью. Чем дольше двое встречаются, тем меньше вероятность размолвки в паре. Различные жизненные обстоятельства и личностная несовместимость обычно приводят к краху отношений в самом начале, когда люди ещё мало знают друг друга.

На Facebook характер отношений легко проследить по смене статусов. Для исследования были отобраны и подвергнуты процедуре деперсонализации профили всех американских пользователей, которые начали свои любовные отношения в период между январём 2008 и декабрём 2011 г. Среди них учитывались только те, длительность которых продолжалась не менее трёх месяцев. Фиксировались лишь новые пары, где каждый партнёр на момент начала знакомства был старше двадцати трёх лет и не состоял в браке.

Исследования подтверждают жизненный опыт: отношения со временем крепнут, однако шанс на размолвку остаётся всегда.

Возможно, кроме длительности знакомства на динамику отношений в паре влияют и внешние факторы, такие как изменение экономической ситуации в стране или даже просто смена времён года. Отношения крепнут со временем. Чаще всего разрыв возникает в первый год.

Все пары были разделены на когорты в зависимости от того, на какой период пришлась дата начала их отношений. С небольшой натяжкой можно говорить о том, что отношения имеют определённую сезонность. К зиме и в период экономического кризиса вероятность разрыва временно повышается.

Подтвердить это и выявить другие факторы помогли бы более детальные исследования, но здесь гораздо важнее другой вывод. Независимо от того, когда именно начались отношения (в период расцвета или упадка), они крепнут со временем. Внешние факторы не так значимы, как длительность знакомства, а общие трудности молодую семью чаще сплачивают, чем разрушают ***(Васильков А. Facebook замечает, что вы влюблены, быстрее, чем вы сами // Компьютерра (http://www.computerra.ru/94664/facebook-and-love-in-digital-century/). – 2014. – 20.02).***

Как Facebook ворует деньги честных пользователей

С редакцией ProstoWeb связался Э. Рзаев, который платил за продвижение одного-единственного поста, а денег с него взяли гораздо больше. Как оказалось, он такой не один, и эта проблема существует уже довольно давно.

Э. Рзаев кратко обрисовал для нас ситуацию – у него был пост, отмеченный «звёздочкой» (это значит, что конкретно у этой записи есть все шансы «взлететь»), и пользователь захотел его продвинуть. Заплатил деньги картой, причём, судя по СМС от банка, списали 1375 р. вместо 1300 – это его не смутило, мало ли, перекрутилось чуть-чуть.

На следущий день пришло уведомление о том, что с карты сняли ещё 1995 р. То есть 20 января был создан пост, ему купили статус Promoted, через день туда натекло 120 лайков и со счёта сняли 1375 р. А 22 января списались ещё почти 2000 р., хотя пост даже не оброс новыми лайками.

Э. Рзаев пишет, что он решил провести рисёрч и обнаружил, что таких пользователей довольно много.

Если делать запросы по ключевым словам «украли деньги»/«списали деньги»/«верните деньги», то можно отыскать много таких постов, где люди негодуют и гадают, что им делать.

Поддержка на эти вопросы не откликается. К. Скоробогатова, представитель Facebook в России, также не ответила на запрос Э. Рзаева.

Складывается странная картина – вроде бы мегабогатый Facebook может списывать деньги с вашего и так не очень солидного счёта в любой момент, а поддержка молчит. Что делать, обращаться в банк для отмены несанкционированной транзакции или молча терпеть, стиснув зубы?

Редакция ProstoWeb воспользовалась медийным весом и связалась с агентством Grayling, которое обслуживает Facebook в России – там обещали разобраться, но за неделю ответа так и не пришло ***(Как Facebook ворует деньги честных пользователей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/kak_facebook_voruet_dengi_chestnyh_polzovateley). – 2014. – 11.02).***

***

Честность Facebook снова под вопросом. В отличие от недавних обвинений в неправомерном снятии «лишних» денег с рекламодателей, теперь все куда масштабнее, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-obvinili-v-obmane-reklamodatelej-38311/).

Видеоблоггер под ником Veritasium обвинил соцсеть в том, что лайки, которые она предлагает получить, купив рекламу, являются фейковыми. Он снял подробное видео, в котором по пунктам изложил свои обвинения.

Тема вызвала нешуточный резонанс (568 просмотров за сутки – это не шутка).

Прежде всего, надо разобраться с тем, как вообще можно получить лайки за деньги. Прежде всего их можно просто купить – как правило, такие услуги предоставляют разные «фермы», где тусуются пользователи (в основном из развивающихся стран типа Индии), которым платят копейки за то, чтобы они нажимали лайк на тысячах страниц.

Само собой, реальный профит от таких подписчиков стремится к нулю, потому что ваша страница им совершенно неинтересна, и они никак с ней не взаимодействуют.

Такой способ официально запрещен Facebook. Взамен М. Цукерберг предлагает рекламодателям заплатить сотню-другую долларов, чтобы «получить больше лайков от людей, которые действительно важны для вас».

Но насколько «качественных» подписчиков можно получить этим легальным методом? Судя по результатам эксперимента блогера, лайки, полученные с помощью рекламы на Facebook, мало чем отличаются от лайков, купленных на ферме пакетом 1 тыс. штук за 20 дол.

Veritasium заплатил рекламу, которая помогла ему увеличить количество лайков своей страницы с двух тысяч до двадцати. Но активность на странице от этого не увеличилась – комментариев и лайков под постами не стало больше.

Более того, значительное число новых подписчиков страницы оказались, по странному стечению обстоятельств, представителями бедных развивающихся стран, которые, лайкнув страницу, больше не возвращаются на нее.

Такие подписчики особенно бесполезны в условиях, когда Facebook показывает любой пост вашей страницы лишь ограниченному количеству людей, подписанных на нее. Для того, чтобы охватить остальных – надо платить. Получается, чем больше у вас таких мертвых душ, тем меньше вероятность, что ваш пост увидят реальные подписчики. То есть вы платите за рекламу, получаете лайки, а вовлеченность пользователей лишь падает.

Напрашивающийся выход из положения – поточнее задавать таргетинг рекламных объявлений, исключая представителей «кликающих наций». Но не все так просто.

В продолжение своего эксперимента блогер создал совершенно пустую страницу о котах, указав в описании, что только идиот лайкнет такое. Далее 10 дол. были снова потрачены на Facebook-рекламу. Таргетинг был следующий – только любители кошек в США, Канаде, Австралии и Великобритании.

Можно было ожидать, что без помощи индонезийских и индийских пользователей соцсети настолько убогая страница не сможет получить ни одного лайка. Но уже пару часов спустя весь рекламный бюджет был благополучно потрачен, а число подписчиков увеличилось на пару десятков.

Кто же эти люди? Большинство из них оказались из США – то есть настройки сработали. Единственный странный момент – каждого из них можно назвать любителем лайкать все подряд. Они подписаны на сотни и тысячи совершенно разных, никак не связанных друг с другом страниц. Один

такой подписчик был фанатом Verizon, AT&T и T-Mobile одновременно. А это вызывает определенные вопросы.

Но зачем кому-то лайкать тысячи страниц, даже не получая за это деньги? Неужели Facebook сам платит фермам, чтобы те помогали им наращивать прибыль?

Для того, чтобы не попасть под спам-радар Facebook, фермы направляют определенное количество ресурсов на то, чтобы нажимать на рекламу в соцсети, при этом используя профили в разных странах.

Подозрительную активность, исходящую из одной страны, можно легко обнаружить и пресечь. Но если пользователи лайкают кучу разных страниц в разных странах, то как понять, не приплатили ли им за это?

Именно поэтому у многих страниц в последние месяцы значительно увеличилось общее количество лайков. Взглянем, к примеру, на официальную страницу, посвященную безопасности на Facebook. Угадайте, где она популярнее всего? Правильно – в Индонезии!

Другие страницы не являются исключением. Например, Д. Бекхема больше всего обожают в Бангкоке.

Это что же получается? Мы платим деньги за рекламу, получаем бесполезную кучу лайков, реальный охват становится только ниже. Но, может быть, этому видеоблогеру просто не повезло с экспериментами, а Facebook не при делах? Хотелось бы верить, но опыт других пользователей Интернета говорит об обратном.

Вот, к примеру, пост пользователя Hacker News под ником notlisted:

«Все правда. Я проводил тесты с таким же рекламным бюджетом ($20к), нацеливаясь на аудиторию в Facebook и Google+. ROI в Facebook был отрицательным, в то время как в Google+ составил аж 400 %. Единственный способ привлечение подписчиков, который работал, – это реклама».

Это поднимает интересный вопрос об общей ценности/бесполезности мобильной рекламы. Большое число показов (impressions), супер-низкие CTR, с кучей «обманок» от разработчика, например, когда рекламу показывают в случайном месте экрана, закрывая часть интерфейса, которые очень близко располагаются к кнопкам, на которые постоянно нажимают пользователи.

Пример – приложение Reddit in Pictures показывает рекламу то вверху, то внизу экрана. Если бы реклама была статичной, вы не смогли бы ошибочно на нее нажать, но благодаря ее подвижности со мной в последний месяц это случилось раз двадцать.

Короче говоря, как по мне, так единственным нормальным рекламным средством является реклама Google, которая показывается людям, реально заинтересованным темой – ведь они ее ищут. С другой стороны, дисплейная реклама Google – такой же бесполезный шлак ***(Facebook обвинили в обмане рекламодателей // Marketing Media Review (http://mmr.ua/news/id/facebook-obvinili-v-obmane-reklamodatelej-38311/). – 2014. – 12.02).***

***

YouTube обвиняет украинскую милицию в том, что она нарушала правила и воровала чужие видео.

Youtube заблокировал официальный канал МВД за нарушение правил сообщества и/или авторских прав. Канал не работает, при попытке зайти на него появляется надпись: «Действие этого аккаунта приостановлено из-за частых или грубых нарушений Правил сообщества и/или жалоб о нарушении авторских прав».

Как сообщил заместитель пресс-секретаря МВД И. Бабаев, Youtube уже не впервые блокирует канал МВД. Ранее он был заблокирован после опубликования видео, на котором видно, как протестующие пытаются смять грейдером бойцов внутренних войск.

Теперь, по словам И. Бабаева, канал заблокировали после опубликования видео с двумя российскими блоггерами, которые в нетрезвом состоянии находились в здании банка. Ранее блоггеры утверждали, что милиция их избила и похитила.

И. Бабаев заявил, что после того как канал МВД блокируют, ведомство обращается в Youtube и доступ к каналу восстанавливают ***(YouTube заблокировал официальный канал МВД за нарушение авторских прав // Левый берег (http://society.lb.ua/accidents/2014/02/12/255156_youtube_zablokiroval_ofitsialniy.html). – 2014. – 12.02).***

***

Всемирная социальная сеть Facebook, фактически ввела цензуру на своем сервисе. Об этом заявил PR-стратег «Ашманов и партнёры Украина» С. Дидковский, сообщает Лига.net.

В частности, он отмечает, что Л. Бекстром, отвечающий в Facebook за развитие новостной ленты в декабре 2013 г., после введения нового алгоритма, сказал, что именно Facebook определяет, какое содержимое видят его пользователи.

Допустим, у вашей организации есть страница в Facebook, где вы пишете о себе, своих проектах, акциях, стремлениях и результатах. Если Facebook посчитает вашу страницу неинтересной, ваши записи увидит всего 5–10 % подписчиков страницы. Вместо этого Facebook покажет страницу другой организации, поскольку посчитает ее более интересной.

Официальная позиция сети звучит так: заменить привычные сообщения и фотографии друзей на сторонний контент – новостной и вирусный, потому что пользователи должны получать «актуальный контент в нужном месте и в нужное время».

Что Facebook считает интересным?

Новый алгоритм – радость для крупных медиаресурсов с обилием вирусного контента. Facebook посчитал их важными и интересными, а потому усилил их присутствие в новостных лентах.

К примеру, BuzzFeed и Bleacher Report существенно нарастили количество переходов на свои сайты из Facebook. Показатель первого сайта возрос на 855 %, а второго – на 1081 %.

Выгоду получат глобальные бренды. Теперь коммерческим структурам с большими бюджетами станет еще проще рекламировать продукцию. Достаточно купить статьи на сайтах, которые Facebook считает «интересными» (те же BuzzFeed и Bleacher Report), и получить еще больше просмотров.

А вот обычные пользователи напряглись. С одной стороны, приятно, когда тебе показывают лишь актуальное содержание. С другой, совершенно неясно, кто дал полномочия третьей стороне (Facebook) становится между двумя знакомыми людьми (друзьями) и определять – что именно им читать и смотреть. К тому же Facebook ведь не может залезть в голову пользователя и точно угадать его потребность.

Как заставить Facebook вернуть вам ленту с сообщениями от друзей?

Если вы обычный пользователь, который хочет самостоятельно выбирать, что ему читать – создавайте отдельные группы друзей. Выберите интересных вам людей. Добавьте их в отдельную новостную ленту. И открывайте ее вместо общей ленты друзей. Ни единое сообщение от важного и интересного человека не пройдет мимо вас ***(Facebook вводит цензуру: что делать пользователям? // ДЕНЬ Запорожья (http://day.zp.ua/news/37873.html). – 2014. – 14.02).***

***

В Интернете появилось необычное приложение, позволяющее блокировать на рабочем компьютере пользователя сайты, принадлежащие Партии регионов.

Приложение размещено на сайте «Бойкот Партии регионов». Разработчики создали робота для браузера Mozilla. Приложение выдает пользователю следующее сообщение: «Ресурс принадлежит члену Партии регионов». В памяти у робота есть список сайтов регионалов. По желанию можно либо перейти на другой сайт, или же продолжать смотреть этот.

«При применении этого приложения вы будете получать предупреждение при пользовании сайтов, принадлежащих членам Партии регионов. Целью кампании участники бойкота провозгласили больше ухудшить финансовое положение членов Партии регионов. Кроме того, активисты призывают членов выходить из партии и публично объявить поддержку Евромайдану», – говорится в пояснении к программе ***(Гундлах А. В Интернете блокируют сайты Партии регионов // 15 минут (http://15minut.org/article/v-internete-blokirujut-sajty-partii-regionov-2014-02-13-14-30-00). – 2014. – 13.02).***

***

Ночью 17 февраля в официальном Twitter-аккаунте программы новостей «Подробности», которая выходит на телеканале «Интер»,

появилось сообщение-признание: «Мы самые лживые новости». За ночь твит собрал более 600 ретвитов и получил большой резонанс в социальных сетях. Похоже, аккаунт был взломан, однако официальной информации по этому поводу пока не поступало.

Спустя час в Twitter появилось еще одно провокационное сообщение следующего содержания: «Д. В. Фирташ, к сожалению, для продолжения вранья в данном блоге на вашем счете недостаточно средств».

В ответах на первый скандальный твит незамедлительно посыпались саркастические ответы и замечания, апогеем стало сообщение о том, что «признание в лживости» попало в тренды Twitter.

Пока неизвестно, удалось ли администрации новостей вернуть контроль над своим Twitter-аккаунтом. Официальных заявлений по этому поводу не поступало.

Напомним, телеканал «Интер» является главным активом медиа-группы InterMediaGroup, которая официально принадлежит В. Хорошковскому, хотя в СМИ фактическим владельцем называют Д. Фирташа. Согласно опросам, телезрители продолжают терять доверие к национальным каналам, поскольку те, якобы, необъективно освещают события «Евромайдана» ***(Twitter новостей канала «Интер» сообщил, что «Подробности» – самые лживые новости // IT Expert (http://itexpert.org.ua/rubrikator/item/33965-twitter-novostej-kanala-inter-soobshchil-chto-podrobnosti--samye-lzhivye-novosti.html). – 2014. – 17.02).***

***

В социальных сетях активизировались мошенники, которые пытаются воспользоваться трагическими событиями в Киеве. В украинском офисе «ВКонтакте» рассказали, что за последнее время появилось невероятное количество сообществ: как в поддержку Евромайдана и «Правого сектора», так и в поддержку Антимайдана и «Беркута».

Во многих таких сообществах время от времени публикуют некие реквизиты с просьбой поучаствовать в добровольном сборе средств, чтобы помочь раненым во время противостояний. Либо поддержать деньгами покупку еды, одежды, лекарств, рассказывает пресс-секретарь соцсети в Украине В. Леготкин. Как правило, это благие намерения, но есть и мошенники, указывающие личные реквизиты и пытающиеся обогатиться на таком поводе.

В сети советуют внимательно проверять такую информацию, к примеру:

– Внимательно смотрите, куда и кому вы перечисляете деньги. Лучше всего пользоваться официальными реквизитами авторитетных благотворительных организаций.

– Если есть серьезные подозрения, лучше обратиться сразу не только в поддержку, но и в правоохранительные органы – например, если деньги вы перечислили, а подробные документы вам предоставить потом отказались.

– Увидели банковский счет в революционном паблике – проверьте, указан ли такой на официальном сайте какой-то партии или организации, связанной с сегодняшними событиями. Если счет там не указан, лучше перечислить деньги на тот, который есть в официальных источниках – на сайте, официальной странице организации «ВКонтакте», а не той, которая создана неделю назад и не совсем понятно, кем именно.

– Одно дело – когда собирают лекарства, еду или вещи, другое дело – когда собирают деньги. В этом случае стоит более внимательно оценивать стиль сообщения, указанные реквизиты.

– Во «ВКонтакте» часто создают страницы для сбора денег на лечение тяжелых болезней или срочную операцию. «Если на таких пользователей идут жалобы, а администраторы не могут предоставить ни документы о том, что кто-то болен, ни чеки или квитанции, то у нас есть все основания закрыть такое сообщество за нарушение правил сайта. Мы пресекаем мошенничество», – сообщают в сети ***(Мошенники пытаются заработать во «ВКонтакте» на пожертвованиях для раненых в Киеве // InternetUA (http://internetua.com/moshenniki-pitauatsya-zarabotat-vo--vkontakte--na-pojertvovaniyah-dlya-ranenih-v-kieve). – 2014. – 20.02).***

Зарубіжні спецслужби і технології «соціального контролю»

Експерти «Лабораторії Касперського» виявили мережу кібершпигунства «Маска». Вона діяла в 31 державі як мінімум з 2007 р. Про це повідомляється на офіційному сайті компанії.

Спеціалісти стверджують, що дії зловмисників були спрямовані в першу чергу на державні органи, дипломатичні офіси, енергетичні компанії, дослідницькі організації та політичних активістів.

У «Лабораторії Касперського» підрахували, що загалом постраждали 380 користувачів у 31 країні. Згідно з аналізом, операція «Маска» активно велася впродовж п’яти років до січня 2014 р. Під час проведення дослідження керівні сервери зловмисників були згорнуті.

Шпигунська мережа містила потужний арсенал шкідливих програм, розроблених для різних операційних систем, у тому числі Mac OS X та Linux.

Метою зловмисників був збір інформації із заражених систем, а саме різноманітні документи, ключі шифрування, налаштування VPN, що використовуються для ідентифікації користувача на сервері, файли, що використовуються програмами для забезпечення віддаленого доступу.

Експерти «Лабораторії Касперського» пояснюють, що шкідливе програмне забезпечення перехоплювало всі комунікаційні канали і збирало найбільш важливу інформацію з пристрою користувача.

За словами керівника глобального дослідного центру «Лабораторії Касперського» К. Райю, є підстави думати, що може йтися про компанію, що мала державну підтримку.

«Перш за все, ми спостерігаємо дуже високий рівень професіоналізму в діях групи, що забезпечує моніторинг власної інфраструктури, приховує себе за допомогою правил системи розмежування доступу, начисто стирає вміст журнальних файлів замість звичайного їх видалення, а також за необхідності припиняє будь-які дії», – пояснює К. Райю.

На думку експерта, кіберзлочинцям невластивий такий рівень самозахисту й, можливо, це найбільш складна загроза такого класу на сьогоднішній день.

Дослідники з «Лабораторії Касперського» помітили також, що для авторів шкідливих програм рідним є іспанська мова, чого раніше не виявляли в такого рівня атаках ***(Експерти «Лабораторії Касперського» виявили глобальну мережу кібершпигунства // Osvita.MediaSapiens (http://osvita.mediasapiens.ua/material/27663). – 2014. – 11.02).***

***

Кілька десятків інтернет-сайтів узяли участь в акції протесту проти масового стеження спецслужб США за користувачами. Акція з назвою The Day We Fight Back («День, коли ми завдаємо удару у відповідь»), яка почалася у вівторок, 11 лютого.

Про це йдеться на офіційному сайті The Day We Fight Back.

В акції протесту беруть участь такі відомі організації, як Фонд електронних кордонів (Electronic Frontier Foundation, EFF), Фонд Mozilla (займається випуском браузера Firefox), анонімний розвідувач DuckDuckGo, а також Greenpeace, Amnesty International і багато інших. Крім того, акцію підтримали чимало інтернет-видань, зокрема Reddit і Boing Boing).

На головних сторінках усіх ресурсів одночасно з'явився великий чорний відмет, на якому відображається посилання на сайт акції і форма, заповнивши яку, можна підписати петицію проти інтернет-шпигунства.

Крім протесту проти діяльності спецслужб The Day We Fight Back також присвячений пам'яті інтернет-активіста А. Шварца, який скоїв самогубство в січні 2013 р. А. Шварц був засновником руху Demand Progress, що виступав проти цензури в Інтернеті, і активним противником антипіратського законопроекту SOPA, від прийняття якого влада Сполучених Штатів відмовилася у 2012 р. під тиском протестів громадськості. Правоохоронні органи звинувачували А. Шварца в незаконному скачуванні наукового архіву Масачусетського інституту. Активістові загрожували 35 роками тюремного ув'язнення.

The Day We Fight Back уперше був анонсований у річницю смерті А. Шварца 11 січня 2014 р. Цього дня прихильники руху Anonymous зламали сайт Масачусетського університету, розмістивши на ньому оголошення про майбутню акцію і фразу, яка стала її гаслом («День, коли ми завдаємо удару у відповідь») ***(У Мережі організували акцію протесту проти інтернет-шпигунства // Західна інформаційна корпорація (http://zik.ua/ua/news/2014/02/12/u_merezhi_organizuvaly_aktsiyu_protestu_proty_internetshpygunstva_459952). – 2014. – 12.02).***

***

Пользователи сервиса микроблогов Twitter из Венесуэлы сообщили об отключении в соцсети всех фотографий и изображений. Недоступны как уже загруженные на платформу фото, так и сама система добавления новых снимков.

Первые сообщения об отключении фотографий появились в венесуэльских Twitter-аккаунтах в ночь на 14 февраля. «Возникла проблема. Twitter не показывает фотографии», – написал один из пользователей, сопроводив пост скриншотом своей новостной ленты (судя по всему, возможность загрузки фотографий тогда еще не была отключена). Ограничения действуют только внутри самой Венесуэлы – проблемы с отображением фото пользователей из других стан не коснулись.

Вскоре пользователи стали также сообщать о полной блокировке Twitter на территории Венесуэлы. Доступ к соцсети для своих абонентов ограничил как минимум один провайдер – государственная компания CanTV. Посты о блокировке Twitter компанией сопровождались хэштегом #13F, который используется микроблогерами для сообщений, связанных с начавшимися в Венесуэле в феврале массовыми акциями протеста.

Официального подтверждения блокировки сервиса в Венесуэле от представителей властей страны не поступало. Администрация Twitter на момент написания этой заметки также никак не комментировала информацию об ограничении доступа к соцсети.

Массовые протесты в Венесуэле продолжаются уже несколько дней. Жертвами протестов за это время стали по меньшей мере трое демонстрантов. Власти страны и лично президент Н. Мадуро выписали ордеры на арест всех лидеров оппозиции, причастных к организации уличных выступлений.

Протесты в Каракасе и других городах стали самыми серьезными акциями против Н. Мадуро с момента прихода его к власти весной 2013 г. За время правления Н. Мадуро экономика страны пришла в упадок. Годовой уровень инфляции превысил 50 %, а из магазинов стали регулярно пропадать необходимые товары. Сам Н. Мадуро объясняет бедственное положение Венесуэлы «происками врагов, внутренних и внешних» ***(В Венесуэле начали отключение Twitter на фоне массовых акций протеста // InternetUA (http://internetua.com/v-venesuele-nacsali-otkluacsenie-Twitter-na-fone-massovih-akcii-protesta). – 2014. – 14.02).***

Проблема захисту даних. DOS та вірусні атаки

Министерство обороны Латвии опубликовало отчёт по итогам расследования кибератак против стран Балтии во время учений НАТО Steadfast Jazz в 2013 г. Тогда в странах Балтии и Польше резко возросло

количество кибератак в отношении государственных структур, в частности против министерств обороны.

Сайт Министерства обороны Эстонии был взломан накануне старта учений и некоторое время не работал. Хакеры оставили от имени НАТО заявление, дискредитирующее Альянс и его учения.

Также от имени Центра киберзащиты НАТО, расположенного в Эстонии, были разослали лже-письма по электронной почте, вводящие в заблуждение госструктуры, в т. ч. и Польши.

Тогда ответственность за кибератаки взяла на себя группа хакеров, называвших себя Anonymous Ukraine. Поле проведенного расследования, министерство обороны Латвии, работавшее вместе с коллегами из Литвы и Эстонии, не установило связь этой группы хакеров с Украиной.

«Было установлено, что нападения были совершены с нескольких IP-адресов в России. Это дает основания для вывода, что организаторы нападения находятся именно в этой стране», – сказано в отчёте ***(Гончарова О. Хакеры «Anonymous Ukraine» имеют россйкую прописку // Новый Регион (http://www.nr2.ru/baltia/484203.html). – 2014. – 11.02).***

***

Эксперт в области компьютерной безопасности Д. Санчес рассказал о том, что сервис мгновенного обмена картинками и сообщениями Snapchat, ставший популярным в США и странах Европы, содержит опасную уязвимость. С ее помощью злоумышленники могут проводить кибератаки на пользователей смартфонов Apple.

Используя уязвимость приложения Snapchat, хакеры могут организовать массированную DDoS-атаку с отправкой тысяч сообщений в секунду. Это приведет к аварийному завершению работы операционной системы iOS и зависанию iPhone. Для восстановления работы понадобится жесткая перезагрузка смартфона. Д. Санчес продемонстрировал пример такой атаки изданию The Los Angeles Times.

«Используя повторно старые токены, можно в больших объемах отправлять сообщения пользователям. Метод может применяться для организации спам-атаки на одного или сразу нескольких пользователей на сервисе», – заявил хакер.

Ранее эксперты рассказали о том, что Snapchat набирает популярность среди спамеров. В новой волне спам-атак используются эротические фотографии в сочетании со ссылками, выглядящими как ссылки на сайты известных компаний. С помощью чужих коротких доменов спамеры создают очень похожие собственные ссылки, вызывающие у пользователей ложное чувство доверия.

Злоумышленники завлекают людей при помощи порнографии и фальшивых сообщений от тайного поклонника. Человеку приходит фотография эротического характера с просьбой изображенной на ней девушки добавить ее в друзья. Затем в дело идет специальный чат-бот.

Напомним, в начале января хакеры выложили в сеть около 4,6 млн учетных записей и телефонных номеров пользователей Snapchat. Доступ к этим данным взломщики получили, используя обнаруженную уязвимость в мобильном приложении Snapchat для iOS и Android ***(Уязвимость Snapchat позволяет удаленно «убить» любой iPhone // InternetUA (http://internetua.com/uyazvimost-Snapchat-pozvolyaet-udalenno--ubit--luaboi-iPhone). – 2014. – 10.02).***

***

Атака хакеров на сайт официальной газеты Никарагуа La Gaceta помешала официальному вступлению в силу поправок в Конституцию страны, снимающих ограничения на число президентских сроков, сообщает El Nuevo Diario.

Планировалось, что поправки в Конституцию, принятые Национальной ассамблеей (парламентом) Никарагуа 29 января, будут опубликованы La Gaceta 10 февраля. Однако сайт официального издания Никарагуа – www.lagaceta.gob.ni – ушел в оффлайн из-за хакерской атаки. Сайт газеты либо недоступен, либо на нем появляется сообщение Hacked By Algerian Ghosts («Взломано Алжирскими призраками»).

Из-за кибератаки редакция La Gaceta также не успела подготовить и выпустить в печать номер за 10 февраля, в котором должны были быть опубликованы изменения в Конституцию.

Поправки в Конституцию, отменяющие ограничения на число президентских сроков, позволят действующему главе государства Д. Ортеге сохранить за собой пост президента. Д. Ортега первый раз занимал пост президента с 1985 по 1990 г. В конце 2006 г. он вновь победил на президентских выборах, а в 2011 г. был переизбран на новый срок ***(Хакеры помешали вступлению в силу поправок в конституцию Никарагуа // InternetUA (http://internetua.com/hakeri-pomeshali-vstupleniua-v-silu-popravok-v-konstituciua-nikaragua). – 2014. – 11.02).***

***

Как сообщили аналитики из компании Emsisoft, им удалось обнаружить деятельность нового вируса-вымогателя под названием Linkup, который блокирует доступ к Интернету и подключает компьютер жертвы к ботнету, генерирующему криптовалюту Bitcoin.

По данным исследователей, вредоносная программа действует не так, как обычные вымогатели, попадающие на компьютер жертвы. Linkup блокирует не саму систему, а доступ к Интернету. Так, вирус отправляет жертве предупреждение, в котором представители Совета Европы якобы обвиняют ее в распространении детской порнографии и требуют выплатить штраф в размере 0,01 евро.

Как утверждают эксперты, Linkup создает свои копии на инфицированном компьютере под поддельными названиями, имитируя привычные для пользователя файлы, после чего создает мьютексы tnd990r

или tnd990s. После этого вредоносная программа отправляет POST-запрос к серверу на получение информации, связанной с компьютером пользователя, а далее перенаправляет все DNS-запросы жертвы, блокируя доступ к Интернету.

На этом деятельность Linkup, являющегося вымогателем, должна бы закончиться. Однако в то время как жертва пытается разобраться с обвинением в распространении запрещенного контента и возобновить доступ к сети Интернет, вредоносная программа осуществляет попытки подключить компьютер к ботнету, занимающемуся генерацией биткоинов ***(Вирус-вымогатель блокирует пользователю Интернет и использует его ПК для добычи Bitcoin // InternetUA (http://internetua.com/virus-vimogatel-blokiruet-polzovatelua-internet-i-ispolzuet-ego-pk-dlya-dobicsi-Bitcoin). – 2014. – 11.02).***

***

9 февраля активисты Anonymous устроили Twitter-шторм на учетные записи правительства Сингапура для привлечения внимания к арестам некоторых представителей движения, произведенным в прошлом году.

Одним из арестованных является Д. Арокясами, который под псевдонимом Messiah, предположительно, принимал участие во взломе как минимум одного сайта сингапурского правительства. Кроме того, в 2013 г. правоохранители арестовали еще пять человек из группы Singapore 5, которые выразили гражданское неповиновение, нарисовав на стене граффити с упоминанием Anonymous.

Активисты использовали хэштег #FreeAnonsSG с целью сделать его одним из самых популярных в Twitter и призывали создать как можно больше твитов с упоминанием @GovSingapore и @MFAsg (эти имена пользователя принадлежат правительственным организациям Сингапура). В этом месяце это уже второй Twitter-шторм на учетные записи сингапурского правительства.

Активисты заявили, что хотят привлечь внимание общественности к использованию в азиатской стране «варварского» телесного наказания за незначительные правонарушения ***(Anonymous устроили Twitter-шторм на правительство Сингапура // InternetUA (http://internetua.com/Anonymous-ustroili-Twitter-shtorm-na-pravitelstvo-singapura). – 2014. – 10.02).***

***

Крупнейшая в истории DDoS-атака была направлена на сеть доставки контента CloudFlare. Представители компании сообщили, что мощность трафика превысила 400 Гбит/с. Для проведения атаки был использован набирающий популярность в последнее время метод с задействованием серверов синхронизации времени.

Сеть доставки контента CloudFlare сообщила о том, что ее инфраструктура была подвергнута самой мощной в истории DDoS-атаке.

DDoS (Distributed Denial of Service – распределенная атака типа «отказ в обслуживании») – это атака, цель которой заключается в блокировании

доступа пользователей к ресурсу путем отправки огромного числа запросов в короткий промежуток времени. Эти запросы перегружают серверы и в результате значительно замедляют их работу.

«Мы подвергаемся очень мощной атаке в настоящее время. Похоже, что она мощнее атаки на Spamhaus. Пытаемся справиться», – написал в Twitter генеральный директор Cloudflare М. Прайс.

Первые сообщения об атаке относятся к 10 февраля 2014 г. К моменту публикации этого материала она, по-видимому, завершилась: М. Прайс писал о ней в прошедшем времени: «Это была крупная атака».

М. Прайс рассказал, что вредоносный трафик был направлен на одного из клиентов Cloudflare. Он добавил, что атаки были подвергнуты серверы Cloudflare в Европе.

Атака на некоммерческую организацию Spamhaus, занятую борьбой со спамом, с которой проводит сравнение М. Прайс, до сих пор считалась крупнейшей DDoS-атакой в истории. Она была проведена в марте 2013 г., и мощность трафика, направленного на сервера Spamhaus.org, тогда достигала 300 Гбит/с.

При проведении атаки на CloudFlare, для увеличения трафика, был задействован протокол синхронизации времени Network Time Protocol (NTP). Для того чтобы усилить трафик, злоумышленник отправляет на сервер NTP запрос от лица жертвы, с подставным обратным адресом. Получив этот запрос, сервер отправляет на адрес, с которого он поступил, список из 600 последних IP-адресов, с которых были обращения к серверу. Этот метод позволяет легко увеличить трафик в десятки раз ***(Зафиксирована самая мощная DDoS-атака в истории Интернета // InternetUA (http://internetua.com/zafiksirovana-samaya-mosxnaya-DDoS-ataka-v-istorii-interneta). – 2014. – 12.02).***

***

Новый вредонос JackPOS распространяется на территории США, Канады, Бразилии, Индии и Испании. В настоящее время известно о краже данных 4500 пластиковых карт. Об этом сообщает в пресс-релизе А. Комаров, генеральный директор компании IntelCrawler.

Согласно исследованию компании, вредонос поражает терминалы на заправках и в ресторанах. После успешной установки на систему JackPOS перезаписывает файл Java Update Scheduler и маскирует себя под легитимное приложение Java. Согласно анализу, код JackPOS основан на вредоносе Alina.

Предположительно, заражение терминалов началось в конце января. При этом злоумышленники сумели похитить данные 3 тыс. пластиковых карт в Сан Пауло, Бразилия, заразив 12 терминалов. Также известно о хищении данных 412 карт через два терминала в Индии и данных 230 карт в Мадриде, Испания ***(JackPOS заражает банковские терминалы по всему миру // InternetUA (http://internetua.com/JackPOS-zarajaet-bankovskie-terminali-po-vsemu-miru). – 2014. – 12.02).***

***

В Министерстве доходов и сборов заявили о том, что злоумышленники устроили рассылку спама с вирусами с доменного имени ведомства. Об этом говорится в сообщении пресс-службы министерства.

Миндоходов отмечает, что в последние дни зафиксированы случаи рассылки писем с использованием доменного имени министерства – minrd.gov.ua. При этом файлы – спамы направляются на электронные адреса предприятий и содержат вредоносное программное обеспечение.

Письма поступают с поддельного адреса в виде счетов к оплате или жалобы на невозможность получения писем и содержат приложение в виде файла с расширением .doc (на самом деле формат .rtf), при открытии которого, с точки зрения пользователя, будто ничего не происходит.

На самом деле этот документ содержит эксплойты для программного обеспечения MS Office Word, после срабатывания которых автоматизированное рабочее место поражается вредоносным программным обеспечением и начинает относиться к бот-сети.

Министерство считает, что массовая рассылка вирусных спамов является спланированной атакой для дискредитации работы ведомства, и по данному факту уже начато уголовное производство.

Миндоходов призывает всех налогоплательщиков быть внимательными и не открывать подобные письма, а одними из адресов, с которых осуществляется рассылка вредных спамов, являются pjil@minrd.gov.ua и jngr@minrd.gov.ua.

В случае получения подобных писем необходимо уведомить об этом Государственную службу специальной связи и защиты информации по адресу cert@cert.gov.ua ***(Гундлах А. Украинские налоговики признались в рассылке спама с вирусами // 15 минут (http://15minut.org/article/ukrainskie-nalogoviki-priznalis-v-rassylke-spama-s-virusami-2014-02-13-17-30-00). – 2014. – 13.02).***

***

Эксперты вирусной лаборатории Eset обнаружили приложение Fix PC, которое вымогает денежные средства у пользователей под видом платы за антивирусное решение.

Авторы Fix PC развернули в сети рекламную кампанию в поддержку «нового антивируса». В спам-рассылке, которая затронула в основном жителей Польши, они предлагают пользователям сканирование компьютера на предмет измерения его производительности и наличия шпионского ПО. Перейдя по ссылке в письме, получатели запускали красочное анимированное приложение.

По итогам «сканирования» Fix PC сообщает пользователю, что его компьютер заражен вредоносным ПО, угрожающим конфиденциальности данных. Избавиться от угрозы оно предлагало за счет активации антивирусного продукта стоимостью всего 24 гроша (около 3 р.).

Покупка лицензии Fix PC была также хорошо продумана. С помощью SMS можно оплатить лицензию на один год стоимостью 30 злотых (примерно 340 р.). За два таких SMS пользователь получает «пожизненную» лицензию.

«В действительности Fix PC не имеет ничего общего с антивирусным ПО – скорее, это просто анимированное приложение. Хотя оно не наносит серьезного вреда компьютеру пользователя, его авторы зарабатывают на вымогательстве», – отметил К. Садковский, эксперт вирусной лаборатории Eset.

«Это не первый случай, когда киберпреступники пытались замаскировать вредоносное ПО под легальное антивирусное решение. В 2013 г. было зафиксировано несколько случаев распространения угроз под видом обновлений популярных антивирусов. Авторы Fix PC пошли дальше и втерлись в доверие к пользователям, представив свое приложение как новый продукт. Мои советы пользователям просты: выбирая антивирус, просите рекомендации у друзей и анализируйте отзывы в Интернете», – говорил А. Баранов, ведущий вирусный аналитик Eset ***(Хакеры разработали новый способ получения незаконных доходов // InternetUA (http://internetua.com/hakeri-razrabotali-novii-sposob-polucseniya-nezakonnih-dohodov). – 2014. – 13.02).***

***

Хакерская DDoS-атака на сайт Независимой ассоциации банков Украины (НАБУ) является беспрецедентной по своим масштабам. Такую оценку дают представители Службы безопасности Украины (СБУ) и специалисты банков в области информационной безопасности, сообщили корреспонденту IT Expert в пресс-службе Ассоциации.

Напомним, что сайт НАБУ с субботы 7 февраля атакуют хакеры. По сравнению с началом атаки, в пиковые моменты она усиливалась на несколько порядков, а суммарный создаваемый трафик составлял около 30 Гбит/сек.

По оценкам ИТ-специалистов, для организации атаки такого уровня нужно привлекать серьезные технические ресурсы. Масштабность свидетельствует о том, что ее осуществляют не любители, а хакеры с высоким уровнем подготовки, услуги которых стоят очень дорого.

В НАБУ констатируют, что DDoS-атака началась буквально через день после обнародования позиции Ассоциации об угрозах и рисках, связанных с деятельностью незаконных пунктов обмена валюты. Инициатива НАБУ прямо затрагивает финансовые интересы серьезных теневых игроков на валютном рынке. Предлагаемое НАБУ усиление контроля на рынке пунктов обмена валюты, направленное на защиту интересов клиентов, ставит под угрозу незаконные сделки и заработки.

Кроме того, среди приоритетов деятельности НАБУ – проект «Противодействие киберпреступности». Сайт этого проекта www.anticyber.com.ua также атакуют хакеры.

«К сожалению, нам уже несколько дней не удается восстановить работу сайтов НАБУ, из-за чего наши постоянные посетители, которые привыкли получать от нас самую свежую информацию о деятельности банковской системы Украины, испытывают определенные неудобства. Несмотря на это, НАБУ не уменьшает своего присутствия в медиапространстве и оперативно, через другие каналы, информирует общественность о своей деятельности и состоянии дел в финансовой сфере», – подчеркнул исполнительный директор НАБУ С. Мамедов ***(Хакерская атака на сайт НАБУ является беспрецедентной по своим масштабам // InternetUA (http://internetua.com/hakerskaya-ataka-na-sait-nabu-yavlyaetsya-besprecedentnoi-po-svoim-masshtabam). – 2014. – 13.02).***

***

Российская социальная сеть «ВКонтакте» остается в числе компаний, попавших в перечень USTR, перечисляющий наиболее злостных нарушителей прав интеллектуальной собственности. Перечень рынков, где, по мнению Вашингтона, допускаются подобные нарушения, обнародован внешнеторговым переговорным ведомством США (USTR).

По сути, это дополнение к профильному ежегодному докладу, публикуемому тем же ведомством в конце апреля. Общая цель публикаций – привлечь дополнительное внимание к проблеме. «Соединенные Штаты настоятельно призывают соответствующие органы власти усилить борьбу с пиратством и контрафактом и использовать информацию (из данного отчета) для юридических шагов по мере целесообразности», – указывается в новом «черном списке».

Компания «ВКонтакте» находится в нем с 2011 г. Претензии американцев к «бизнес-модели» данной соцсети связаны с тем, что она, «насколько можно судить, допускает несанкционированное воспроизводство и распространение» продукции, защищенной копирайтом.

В новый перечень USTR включены также файлообменник Rapidgator.net, «перебравшийся в Россию после того, как его закрыли власти Великобритании», и компания Rutracker.org, «базирующаяся в России» и именовавшаяся прежде Torrents.ru.

Докладом USTR охвачены практически все страны мира, включая торговых партнеров США ***(США оставили «ВКонтакте» в списке злостных «пиратов» // InternetUA (http://internetua.com/ssha-ostavili-vkontakte-v-spiske-zlostnih--piratov). – 2014. – 12.02).***

***

Международный альянс интеллектуальной собственности повторно рекомендовал признать Украину «пиратом № 1» в мире. Об этом говорится в официальном отчете Международного альянса интеллектуальной собственности.

Организация отмечает в Украине высокий уровень цифрового и физического пиратства.

Как известно, в прошлом году за Украиной закрепили статус Priority Foreign Country, который определяет нашу страну как «самую пиратскую».

В отчете указано, что расследование по делу о нарушении прав интеллектуальной собственности в Украине, инициированное США в прошлом году должно завершиться 28 февраля.

IIPA призывает американские власти приложить усилия по исправлению ситуации с нарушением интеллектуальных прав, а если украинское правительство не исправит ситуацию, принять все необходимые меры в рамках законодательства, чтобы компенсировать экономические потери ***(Украину могут повторно признать «пиратом № 1» в мире // InternetUA (http://internetua.com/ukrainu-mogut-povtorno-priznat--piratom---1--v-mire). – 2014. – 14.02).***

***

Как сообщают исследователи из Sans, им удалось зафиксировать волну вредоносных атак, направленных на различные модели маршрутизаторов Linksys. Устройства инфицирует червь TheMoon, главной особенностью которого является его способность самостоятельно распространяться.

По данным эксперта Й. Ульриха, в настоящее время скомпрометированы не менее тысячи маршрутизаторов по всему миру, однако фактическое количество успешно проведенных атак может быть гораздо выше. Как бы то ни было количество заражений продолжает расти.

«У нас нет списка уязвимых моделей, но в зависимости от версии прошивки скомпрометированными могут оказаться следующие маршрутизаторы: E4200, E3200, E3000, E2500, E2100L, E2000, E1550, E1500, E1200, E1000 и E900», – подчеркивают в Sans.

Интересно, что исследователи не смогли обнаружить у TheMoon наличие связи с каким-либо C&C-сервером, хотя в исходном коде вируса присутствует соответствующий функционал.

Эксперты также отмечают, что Linksys уже была проинформирована о нападении. Необходимые технические данные были переданы разработчикам, а выпуска исправления стоит ждать уже в ближайшее время ***(Зафиксирована атака самокопирующегося червя на маршрутизаторы Linksys // InternetUA (http://internetua.com/zafiksirovana-ataka-samokopiruuasxegosya-cservya-na-marshrutizatori-Linksys). – 2014. – 15.02).***

***

Как сообщают эксперты «Лаборатории Касперского», созданная в компании Absolute Software программа Computrace позиционируется на рынке как механизм отслеживания и защиты своих компьютерных систем. Программа устанавливается в прошивку устройства, что затрудняет ее удаление. По словам исследователей, Computrace использует множество уловок, которые присущи вредоносному ПО. К примеру, агент противодействует отладке, вписывает свою память в другие процессы и сохраняет файлы конфигурации в зашифрованном виде.

При этом сетевой протокол, который используется программой, предлагает основные функции для удаленного выполнения кода. Более того, этот протокол не использует какое-либо шифрование и не требует аутентификации удаленного сервера, что открывает огромную перспективу для совершения атак.

«Несмотря на то что шифрование присутствует на более поздних стадиях обращения к системе, злоумышленник может использовать основный незашифрованный протокол и успешно осуществить атаку, – отмечают в ЛК. – В ходе атаки на локальную сеть, весь трафик пользователя будет перенаправляться на хостинг злоумышленников при помощи ARP-инъекции. Еще одна возможность, открывающаяся перед хакерами, позволяет использовать атаку на DNS-сервисы, чтобы подключить агента к поддельному C&C-серверу».

По мнению экспертов, это только небольшая часть сценариев нападения, которые могут использовать киберпреступники.

Примечательно, что вице-президент по международному маркетингу компании Absolute Software С. Мидгли заявил о необходимости более тщательного изучения отчета экспертов ЛК и отметил, что компания примет все необходимые меры ***(Программа Computrace может использоваться для взлома компьютера // InternetUA (http://internetua.com/programma-Computrace-mojet-ispolzovatsya-dlya-vzloma-kompuatera). – 2014. – 15.02).***

***

Согласно последнему отчету экспертов из подразделения SecureWorks Counter Threat Unit (CTU) компании Dell, наиболее активным трояном в 2013 г. стала разновидность Zeus – Gameover. По данным экспертов, в 38 % исследуемых ими случаев применения банковских троянов в прошлом году встречался именно Zeus Gameover.

Вторым по активности оказался Citadel, обнаруженный CTU в 33 % случаев, третьим – стандартный вариант Zeus, на долю которого пришлось 13 %. Трояны Shylock, Torpig, Gozi, Bugat и IceIX обнаруживались исследователями в 2–7 % случаев.

«Интересно наблюдать, как киберпреступники годами управляли этими ботнетами и адаптировали тактику, техники и процедуры для обхода средств и сервисов безопасности», – цитирует издание SCMagazine старшего исследователя CTU Б. Стоун-Гросса.

По словам эксперта, жертвами троянов являются около 900 финансовых организаций (банков, кредитных союзов, сайтов и т. д.) в более, чем 65 странах мира, преимущественно за пределами США.

Согласно отчету, злоумышленники особенно активно атакуют учреждения в Германии, Италии, Франции, Великобритании, Испании, Канады и Австралии. Кроме того, увеличилось число жертв на Среднем Востоке, а также в Африке и Азии.

Gameover появился в середине 2011 г. и имеет схожие черты с Zeus (например, фиксирование нажатия клавиш на клавиатуре для похищения

учетных данных), но, в отличие от него, обладает рядом вредоносных функций, позволяющих осуществлять DDoS-атаки ***(Самым активным банковским трояном в 2013 году стал Zeus Gameover // InternetUA (http://internetua.com/samim-aktivnim-bankovskim-troyanom-v-2013-godu-stal-Zeus-Gameover). – 2014. – 15.02).***

***

Специалисты компании FireEye зафиксировали масштабную атаку на пользователей веб-браузера Internet Explorer 10, жертвами которой стали сотни тысяч человек. Заражение происходит через уязвимость нулевого дня после посещения веб-сайта с размещенным на него вредоносным кодом. Атака получила название Operation SnowMan («Операция снежный человек») в честь проходящих в США снежных бурь.

Новая уязвимость была обнаружена спустя два дня после выпуска крупного обновления Microsoft, устраняющего 24 уязвимости в различных версиях Internet Explorer, включая 15 в десятой версии.

Как рассказали в FireEye, атакующие выбрали своей целью ветеранов США, поместив вредоносный код на сайт Организации ветеранов иностранных войн (vfw.org).

После того как пользователь заходит на сайт, вредоносный код загружает в фоновом режиме страницу, которая запускает объект Adobe Flash. С помощью кода ActionScript этот объект взламывает встроенный в операционную систему механизм защиты от уязвимостей ASLR (Address Space Layout Randomization), получая доступ к оперативной памяти.

После этого на компьютер жертвы сбрасывается бэкдор ZxShell. Он позволяет злоумышленникам получать удаленный доступ к системе и похищать ценную информацию.

«Бэкдор ZxShell – это общедоступный инструмент, который широко применяется множеством группировок, промышляющих шпионажем», – сообщили в FireEye. Специалисты считают, что атака Operation SnowMan была проведена теми же людьми, которые в августе 2013 г. провели атаку Operation DeputyDog и Operation Ephemeral Hydra в ноябре. Корни этих атак уходят в Китай, сообщил агентству Reuters представитель FireEye Д. Киндлунд.

В Microsoft заявили, что находятся в курсе уязвимости и работают с FireEye над выпуском нового патча.

Согласно StatCounter, доля Internet Explorer 10 на рынке настольных веб-браузеров в настоящее время составляет 4,7 %. Всем версиям IE в общей сложности принадлежит 24,6 % рынка (второе место после Google Chrome с долей 46,6 %) ***(Сразу после выхода патча Internet Explorer сотни тысяч пользователей атакованы через новую «дыру» // InternetUA (http://internetua.com/srazu-posle-vihoda-patcsa-Internet-Explorer-sotni-tisyacs-polzovatelei-atakovani-cserez-novuua--diru). – 2014. – 14.02).***

***

Хакеры взломали сайт Kickstarter, который помогает авторам собрать средства на осуществление своих проектов. Об этом в ночь на воскресенье, 16 февраля, сообщила администрация сервиса в корпоративном блоге.

Как указывается в сообщении, правоохранительные органы известили Kickstarter о взломе в ночь на 13 февраля. Администрация немедленно устранила возможность повторной атаки и приняла меры для усиления безопасности.

Несанкционированный доступ к данным о банковских картах исключен, подчеркивается в блоге Kickstarter. Тем не менее, хакеры получили доступ к именам пользователей, электронным и физическим адресам, телефонным номерам и паролям в зашифрованном виде. Сами пароли раскрыты не были, но злоумышленник, обладающий достаточными знаниями, может взломать и зашифрованные пароли, напомнили создатели ресурса.

В связи с этим Kickstarter настоятельно посоветовал пользователям сменить пароли к своим аккаунтам как на этом ресурсе, так и на других, где использовался тот же пароль.

В сообщении отмечается, что администрация сайта приносит глубочайшие извинения за то, что произошло, и делает все возможное, чтобы такого больше не случилось.

Напомним, Kickstarter работает с 2009 г. В 2013 г. количество пользователей, хоть раз материально поддержавших проекты на сервисе, составило 3 млн человек, а общая сумма перечисленных средств достигла 480 млн дол. США. За тот год собрать запрашиваемую сумму удалось авторам 19,9 тыс. проектов ***(Хакеры взломали сайт Kickstarter // «Час Пик» (http://vchaspik.ua/v-mire/239738hakery-vzlomali-sayt-kickstarter). – 2014. – 16.02).***

***

Согласно данным компании Hold Security, на ряде закрытых хакерских форумов появились предложения о покупке архива из 7 тыс. реквизитов от различных FTP-серверов, включая серверы газеты The New York Times. При помощи данных реквизитов потенциальные покупатели смогут загружать на серверы собственные файлы, включая вредоносные PHP-скрипты, подменять HTML-страницы на серверах и выполнять множество других действий.

В Hold Security говорят, что в продаваемых архивах присутствуют реквизиты как от небольших малоизвестных серверов, так и от серверов известных корпораций. В заметке компании не говорится, на каких именно ресурсах идет продажа, а также не сообщается, как именно были добыты реквизиты в столь внушительных объемах.

Сами по себе реквизиты представляют смесь анонимных и дефолтных учетных записей, с паролями от простых до крайне сложных. Резонно предположить, что они могли быть собраны как при помощи неизвестных ftp-эксплоитов для серверов, так и при помощи клиентских вредоносных программ, таких как клавиатурные шпионы, сетевые программы класса man-

in-the-middle и других. Отметим, что в настоящее время многие пользователи уже отказались от использования классического ftp, так как трафик в данном протоколе не шифруется и это создает простор для деятельности потенциальных хакеров ***(На хакерских форумах продается архив с 7000 FTP-реквизитов работающих серверов // InternetUA (http://internetua.com/na-hakerskih-forumah-prodaetsya-arhiv-s-7000-FTP-rekvizitov-rabotauasxih-serverov). – 2014. – 17.02).***

***

Антивирусная лаборатория PandaLabs компании Panda Security, производителя «облачных» решений безопасности, ведущего поставщика программ защиты от вредоносного программного обеспечения и вирусов, обнаружила в Google Play вредоносные приложения, которые способны подписывать пользователей на сервисы дорогостоящих SMS без их разрешения. Эти новые угрозы к настоящему времени уже способны были заразить не менее 300 тыс. пользователей, хотя количество скачиваний этих угроз могло достичь 1,2 млн.

Такие приложения как Easy Hairdo (посвященное прическам), Abs Diets (посвящено диетам), Workout Routines (о фитнесе) и Cupcake Recipes (рецепты) являются одними из наиболее доступных для скачивания на Google Play.

В случае с Abs Diets, например, после установки приложения и при согласии пользователя с условиями использования сервиса, происходит следующее: во-первых, приложение показывает набор советов по избавлению от жира в брюшной полости. Во-вторых, без ведома пользователя приложение проверяет номер телефона мобильного устройства, подключается к веб-странице и подписывает жертву на сервис дорогостоящих SMS. Возникает вопрос: а как мошенники получают номер мобильного телефона? Номер телефона «выкрадывается» из популярного приложения – WhatsApp. Как только пользователь открывает WhatsApp, вредоносное приложение получает номер телефона и сохраняет его как часть необходимых данных для синхронизации аккаунта.

Согласно данным с Google Play, данное приложение было скачено от 50 тыс. до 100 тыс. пользователей. Другие приложения работают точно также, поэтому с уверенностью можно сказать, что четыре вредоносных приложения могли заразить от 300 тыс. до 1 млн пользователей в целом.

«Действительно, мошенники делают безумные деньги на этих премиальных сервисах. По самым скромным оценкам, скажем, если каждый пользователь платит 20 евро, то в результате получается огромная сумма от 6 до 24 млн евро, украденных у жертв» – сказал Л. Корронс, технический директор PandaLabs.

Независимо от решения безопасности, установленного на этих устройствах, пользователи должны всегда читать список прав, запрашиваемых приложениями, прежде чем их устанавливать. Если приложение запрашивает права доступа в Интернет или чтения SMS-

сообщений, но в этом нет необходимости, то такое приложение не следует устанавливать.

Функция «Аудитор конфиденциальности» в Panda Mobile Security (v1.1) выделяет приложения, которые могут подписать пользователя на платные дорогостоящие SMS-сервисы, в отдельную категорию «Платное», откуда они легко могут быть удалены.

«Не каждое приложение, включенное в данную категорию, является вредоносным. Но необходимо сказать, что любое приложение с аналогичными правами может быть опасным. В любом случае, если пользователь видит любые приложения с правами, которых у них не должно быть, то их следует удалить незамедлительно, – объясняет Л. Корронс. – Такие приложения могут оставаться в Google Play достаточно продолжительное время, т. к., в конце концов, сами пользователи согласились с условиями использования сервиса, а это на руку мошенникам. Но в любом случае наше решение Panda Mobile Security обнаруживает и удаляет подобные творения» ***(Новые вредоносные приложения распространяются в Google Play // ITnews (http://itnews.com.ua/news/71654-novye-vredonosnye-prilozheniya-rasprostranyayutsya-v-google-play). – 2014. – 18.02).***

***

«Лаборатория Касперского» обнаружила, что несовершенная реализация сетевого протокола, используемого продуктом Absolute Computrace компании Absolute Software, может стать своего рода «архимедовым рычагом» и превратить полезное ПО в мощное орудие злоумышленников. Этот программный недочет способен потенциально открыть киберпреступникам доступ к миллионам компьютеров по всему миру – и в качестве ключа в этом случае выступит программный агент Absolute Computrace, хранящийся в прошивке BIOS современных компьютеров и ноутбуков.

Анализировать эту особенность защитного ПО Absolute Software специалисты «Лаборатории Касперского» начали после того, как выяснили, что программный агент Absolute Computrace работает на ряде компьютеров без предварительной авторизации. Несмотря на то что этот продукт является легальной разработкой, некоторые пользователи утверждали, что никогда его не устанавливали и не активировали, а в ряде случаев и вовсе не знали о существовании этого ПО на своих компьютерах. В то время как большинство предустановленных программ может быть легко удалено или деактивировано пользователем, Absolute Computrace, располагаясь в прошивке компьютера, продолжает работать даже после тщательной чистки системы или замены диска.

Однако не только эта особенность Absolute Computrace может вызвать подозрение у пользователей. Это ПО применяет технологии, затрудняющие дизассемблирование и анализ, а также другие инструменты, популярные у создателей зловредов, в частности инъекции в память других процессов,

организацию скрытых каналов связи, изменение системных файлов на диске, шифрование конфигурационных данных и создание исполняемых файлов Windows непосредственно из кода прошивки BIOS.

Согласно данным, полученным из облачного сервиса Kaspersky Security Network, программный агент Absolute Computrace функционирует сегодня в системах около 150 тыс. пользователей. Общее же число пользователей с активированным агентом по некоторым оценкам может превышать 2 млн, и не известно, сколько из них знают о существовании этого ПО на своем компьютере. Также эксперты установили, что большинство компьютеров с активно работающим агентом Absolute Computrace находится в США и России.

Сетевой протокол Computrace, предоставляет базовые возможности для удаленного выполнения кода. Он не требует использования каких-либо криптографических механизмов для шифрования данных или проверки удаленного сервера, что дает злоумышленникам возможность для совершения удаленных атак в незащищенном сетевом окружении. В настоящее время нет доказательств того, что Absolute Computrace используется как платформа для проведения атак ***(Обнаружена угроза в BIOS на современных ПК и ноутбуках // InternetUA (http://internetua.com/obnarujena-ugroza-v-BIOS-na-sovremennih-pk-i-noutbukah). – 2014. – 17.02).***

***

Антивирусная компания ESET предупреждила об активизации банковского трояна Win32/Corkow, поражающего системы дистанционного банковского обслуживания. Атаки вредоносной программы направлены на пользователей из России и Украины, на них приходится 86 % заражений.

Win32/Corkow – комплексная вредоносная программа, предназначенная для хищения аутентификационных данных для онлайн-банкинга. Первые ее модификации появились в 2011 г., но, в отличие от широкоизвестного трояна Carberp, Corkow до сих пор не стал настолько известным. Больше всего заражений приходится на Россию и Украину (73 и 13 % соответственно). Неудивительно, что эти страны пострадали больше других, так как Win32/Corkow имеет российское происхождение. Троян содержит вредоносный модуль, нацеленный на компрометацию системы онлайн-банкинга iBank2, которая используется российскими банками и их клиентами.

Подобно другим банковским троянам, Win32/Corkow имеет модульную архитектуру. Это означает, что злоумышленники могут по мере необходимости расширять спектр его возможностей для хищения конфиденциальных данных. В арсенале Win32/Corkow есть также клавиатурный шпион, модуль для снятия скриншотов с рабочего стола, веб-инъекций и кражи данных веб-форм. Кроме того, троян поддерживает удаленный доступ к зараженному компьютеру и установку другой вредоносной программы для кражи паролей – Pony. Еще одна характерная

особенность Corkow – ориентация на веб-сайты и соответствующее ПО, которое относится к виртуальной валюте Bitcoin, а также компьютеры разработчиков приложений для Android. Далее злоумышленники могут получить несанкционированный доступ к аккаунтам счетов Bitcoin скомпрометированных пользователей со всеми вытекающими последствиями ***(Троян Win32/Corkow атакует клиентов украинских банков // InternetUA (http://internetua.com/troyan-Win32-Corkow-atakuet-klientov-ukrainskih-bankov). – 2014. – 18.02).***

***

Мобильная платформа Android страдает от нехватки эффективного механизма обновления ОС. В отличие от iOS ее разработку ведут разные производители, которые не заботятся об обновлении устройств, выпущенных несколько лет назад. Эксперты создали эксплойт, который позволяет хакеру взломать три из четырех устройств на этой платформе, используя уязвимость годичной давности.

Как сообщает Cnews, специалисты по информационной безопасности из компании Rapid7 написали эксплойт, позволяющий взломать 73 % устройств на Android. Примечательно, что уязвимость была обнаружена еще в декабре 2012 г. Она находится во встроенном в Android веб-браузере, в компоненте WebView, и позволяет злоумышленнику исполнить на устройстве произвольный код.

Для заражения устройства необходимо, чтобы его владелец посетил вредоносный сайт. Заставить его сделать это можно различными способами. Исследователи в качестве примера привели вредоносную ссылку, закодированную в QR-коде. Пользователь может считать такой код в любом рекламном объявлении, ничего не подозревая.

Примечательно, что уязвимость, которой воспользовались специалисты Rapid7, касается устройств любых типов, не только смартфонов и планшетов. Пользователь Джошуа Дрейк сообщил в Twitter, что ему удалось запустить эксплойт на очках Google Glass.

Процент устройств аналитики вычислили довольно просто. Дело в том, что уязвимость содержится во всех версиях Android ниже 4.2. Цифра была получена из официальной статистики Google.

Несмотря на то что в Android 4.2 уязвимость была устранена, риску по-прежнему подвержено большинство пользователей. И именно на это эксперты хотели обратить свое внимание. По их мнению, проблема кроется в отсутствии у Google единого центрального механизма распространения обновлений, как, например, в Microsoft Windows: многие производители не заботятся об обновлении устройств, выпущенных несколько лет назад с предыдущими версиями платформы.

Между тем в июле прошлого года сообщалось о еще более масштабной уязвимости – затрагивающей 99 % устройств на Android. Она была обнаружена специалистами компании Bluebox и содержалась во всех версиях Android, начиная с 1.6, выпущенной четыре года назад ***(Новый троян***

поражает три из четырех гаджетов на Android // InternetUA (http://internetua.com/novii-troyan-porajaet-tri-iz-csetireh-gadjetov-na-Android). – 2014. – 18.02).

***

Мошенники из России все чаще используют так называемые частные деньги (private currency) для проведения расчетов друг с другом на разных русскоязычных подпольных форумах, сообщают исследователи безопасности из RSA.

По мнению экспертов, тенденция к появлению новых частных финансовых систем и валют в киберпреступном сообществе России указывает на довольно высокий уровень сотрудничества, кооперации и более сложной организации в сравнении с преступниками других наций.

«С тех пор, как работа Liberty Reserve была прекращена в мае прошлого года, а средства на счетах ее пользователей были конфискованы представителями правоохранительных органов, мошенники были заняты поиском прочной валюты, позволяющей минимизировать риск потери своих финансов», – поясняют в RSA.

Наиболее очевидными вариантами являлись Perfect Money и BitCoin, однако обе валюты имеют неотъемлемые недостатки. К примеру, последняя не предоставляет достаточный уровень анонимности и не застрахована от ареста ***(Российские киберпреступники – двигатель развития криптовалют // InternetUA (http://internetua.com/rossiiskie-kiberprestupniki---dvigatel-razvitiya-kriptovaluat). – 2014. – 18.02).***

***

В Киеве и Киевской области обнаружили 22 банкомата разных финучреждений с вирусами, которые считывают информацию с пластиковых карт. Об этом сказал директор Украинской межбанковской ассоциации членов платежных систем (ЕМА) А. Карпов «Капиталу».

Риску подвергаются карты с магнитной полосой. Украсть деньги с чиповой карточки намного сложнее.

Названия банков и источники заражения не называются. Но по словам сотрудника одного из процессинговых центров, установить вирусное программное обеспечение на банкоматы могли либо с помощью сотрудников банка, либо специалистов сервисной компании, обслуживающей финустройства.

«Основная проблема финструктур в том, что большая часть терминалов работает на операционной системе Windows, в частности XP, а там вирусы широко обитают. Большинство банков не уделяют должного внимания вопросам IT-безопасности, из-за чего страдают клиенты», – сообщил руководитель отдела безопасности одного из крупнейших украинских банков ***(В киевских банкоматах завелись вирусы // InternetUA (http://internetua.com/v-kievskih-bankomatah-zavelis-virusi). – 2014. – 20.02).***

***

Как уберечься от мобильных вирусов

Времена, когда вредоносное ПО писалось исключительно для ПК, давно прошли. В настоящее время мобильные устройства даже более лакомый кусок для злоумышленников, чем компьютер: там можно найти и много персональной информации, и данные о платежных картах (путем кражи логина от магазина приложений), и доставить много других неприятностей. Но и защититься от них можно как с помощью специальных приложений, так и простых советов. Об этом речь и пойдет далее.

Защита для Android

Большинство мобильных вирусов злоумышленники пишут под операционную систему Android. Это и не удивительно: глядя на распространенность платформы и количество девайсов, работающих на ней, невольно вспоминается ситуация 10–15-летней давности, когда львиная доля вирусов писалась под Windows только потому, что у нее не было альтернативы. Соответственно, и защитных решений для Android существует много, причем как платных, так и бесплатных.

Одно из самых простых для пользователя и вместе с тем надежных решений – приложение Bitdefender Antivirus Free. Оно занимает всего полтора мегабайта и имеет две функции – сканирование устройства по требованию (с возможностью удаления вредоносного объекта) и автоматическая проверка каждого устанавливаемого приложения. Антивирус не требователен к ресурсам, умеет экономить батарею при низком заряде и определять угрозы «нулевого дня» (свежие вирусы, которые еще не внесены в базы).

В отличие от продукта Bitdefender, другое защитное решение от известного производителя антивирусного ПО, Comodo Mobile Security, – это целый пакет разнообразных функций и возможностей. Судите сами: в приложении есть сканер работоспособности системы (проверяет целостность компонентов ОС), непосредственно антивирус, менеджер процессов и установленного софта, а также монитор трафика. Последний умеет показывать сетевую активность каждого приложения, причем делает это раздельно для Wi-Fi и GPRS. А с правами суперпользователя его можно использовать даже как брандмауэр, ограничивая и запрещая тем или иным приложениям выход в Интернет.

Что касается непосредственно антивирусного модуля, то он может проверять все устанавливаемые приложения, запускать сканирование всего устройства по расписанию или требованию пользователя, а также перемещать подозрительные объекты в карантин.

Comodo Mobile Security защищает устройство не только от виртуальных, но и от физических угроз. В нем есть модуль «Антивор», при помощи которого можно удаленно заблокировать как SIM-карту, так и все устройство целиком, включить звуковую сигнализацию и удалить информацию со смартфона или планшета. Приложение также позволяет блокировать входящие звонки и SMS, совершать их в приватном режиме (не

оставляя соответствующих записей в телефонной книге), создавать резервные копии данных на устройстве.

Если же хочется пользоваться приложением на украинском или русском языке, можно скачать или купить антивирус Dr.Web для Android. Бесплатная версия приложения имеет только антивирусный модуль, в то время как платная (годовая лицензия стоит 39 грн.) еще и Антиспам, Антивор и URL-фильтр. Продукт заточен в первую очередь под смартфоны: в платной версии компоненты Антиспам и Антивор на планшетах без SIM-карты не работают.

Поиск вирусов в обоих случаях происходит в нескольких режимах. Можно проверять все устройство по расписанию или требованию, а постоянная защита SpiderGuard проверяет все устанавливаемые приложения и дополнительно анализирует карту памяти на наличие файлов автозапуска. Подозрительные файлы можно помещать в карантин. В случае неоправданного удаления восстановить их не составит никакого труда.

В платной версии URL-фильтр проверяет адреса посещаемых ресурсов и определяет, не относятся ли они к мошенническим сайтам. Антиспам защищает нервы пользователя от назойливой SMS-рекламы и даже умеет блокировать звонки с заданных номеров. А Антивор дает возможность дистанционной блокировки устройства, включения звуковой сирены и удаления персональных данных со смартфона.

Антивирусы под iOS

«Яблочная» платформа также не обделена вниманием злоумышленников. Поэтому и для нее существует несколько наименований антивирусных приложений. Здесь, как и на Android, есть совсем простые приложения, а есть и пофункциональнее.

К первому типу можно отнести Intego VirusBarrier – простой, но в то же время надежный сканер файлов и приложений для iOS. Антивирус стоит символические 0,99 дол. и умеет искать вредоносные данные не только на устройстве, но и в облачных хранилищах Google Drive и SkyDrive, а также в почтовых вложениях, расшаренных файлах на Dropbox и FTP.

Ну а приложение Avira Mobile Security – относится к категории более продвинутых. Оно умеет искать угрозы как в автоматическом режиме, так и по требованию пользователя и имеет модуль «Антивор» с базовым набором функций (таких как удаленная блокировка). Приложение следит за состоянием батареи, и если ее заряд кончается, переходит в фоновый режим, практически не потребляя ресурсы. Ко всему прочему, приложение распространяется бесплатно.

Как не подхватить вирус

Вместо того чтобы лечить виртуальную заразу, лучше быть осмотрительным при серфинге и не попадаться на удочку злоумышленников. Вот несколько советов, как уберечься от мобильных вирусов:

1) не устанавливайте приложения, скачанные с непонятных ресурсов. Вместо этого воспользуйтесь официальным магазином вашей платформы, так риск установки зараженной программы сведется к минимуму;

2) не переходите на сомнительные ресурсы в мобильном браузере;

3) если телефон ведет себя подозрительно (просит странные обновления, генерирует большое количество трафика), сразу же проведите сканирование устройства, а до тех пор отключите ему возможность выхода в Интернет ***(Как уберечься от мобильных вирусов // InternetUA (http://internetua.com/kak-uberecssya-ot-mobilnih-virusov). – 2014. – 24.02).***