СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(22.06–12.07)

2015 № 12

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(22.06–12.07)
№ 12

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

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

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

За даними компанії Gemius, аудиторія соціальної мережі «Одноклассники» в Україні продовжує знижуватись. Компанія оприлюднила результати свого щомісячного дослідження української аудиторії Інтернету.

У травні 2015 р. трійка лідерів не змінилася – Google, «ВКонтакте» і Mail.Ru:

Згідно з даними gemiusAudience, розмір ПК інтернет-аудиторії в травні 2015 р. – 18,3 млн осіб (Real users, 14+). Соц-дем. звіт складений на підставі 8308 анкет software-панелістів та 45 170 анкет cookie-панелістів ***(«Одноклассники» продовжують втрачати українську аудиторію // UkrainianWatcher (http://watcher.com.ua/2015/07/06/odnoklassnyky-prodovzhuyut-vtrachaty-ukrayinsku-audytoriyu/). – 2015. – 6.07).***

***

ТОП-5 українських соціальних мереж, щоб спілкуватися з друзями

З 1 серпня федеральні спецслужби матимуть вільний доступ до російських соціальних мереж, персональні дані перевірятимуться силовиками. Тож українцям рекомендують переглянути свою присутність у багатьох популярних соцмережах – «ВКонтакте», «Одноклассники», «Мой Мир» і багатьох інших. Як альтернативу можна розглядати новостворені українські аналоги. «Стик» підготував рейтинг найпопулярніших.

«Друзі» – http://druzi.org.ua. Створена в березні 2014 р. Для реєстрації в соцмережі необхідно внести персональні дані: ім'я, прізвище, дату народження, пошту, країну проживання або увійти через акаунт у інших соцмережах.

«Це Україна» – https://ц.укр. Перша українська соцмережа. Для реєстрації необхідно ім'я, прізвище, дату народження. Насторожує лише, що, крім звичної кнопки «увійти», є «увійти через VK».

UKRFACE – http://ukrface.com.ua – проект створений для об'єднання і спілкування українців. Тут обіцяють щоденне оновлення функцій. Для реєстрації необхідно зазначити ім'я, прізвище, електронну пошту, дату народження, країну проживання.

«Всі тут» – http://vsitut.com – соціальна мережа для знайомства патріотів України. Спілкування на стіні, створення сторінок за інтересами, публікація блогів, форум, галерея. Реєстрація на ресурсі мінімальна – ім'я, прізвище, а також ім'я англійською мовою, поштова електронна адреса.

UA Modna – http://www.uamodna.com – інформаційно-розважальна веб-платформа, що об'єднує людей з усього світу. Тут можна знайти статті, інтерв'ю, фото, відео, дослідження, висвітлення соціальних питань, авторські погляди на актуальні події, творчі та наукові доробки сучасників. Реєстрація мінімальна, окрім того, можна увійти через Facebook ***(ТОП-5 українських соціальних мереж, щоб спілкуватися з друзями // Інформаційний портал «Стик» (http://styknews.info/novyny/sotsium/2015/07/08/top-5-ukrainskykh-sotsialnykh-merezh-shchob-spilkuvatysia-z-druziamy). – 2015. – 8.07).***

***

Многие пользователи утверждают, что до сих пор не удалились из «ВКонтакте» только из-за возможности слушать музыку. Рады сообщить, что теперь они могут отбросить этот аргумент, поскольку потоковый музыкальный сервис стал доступен и в Facebook. Конечно, его реализовала не сама социальная сеть – плагин MusekBox создали украинские разработчики из компании StepInMobile, которые ранее рассказали на AIN.UA свою историю переезда из Донецка во Львов (http://ain.ua/2015/06/22/587486).

Плагин доступен для браузеров Chrome, Mozilla и Internet Explorer. После его установки в интерфейсе Facebook появятся элементы управления музыкальным плеером. Он сможет искать музыку прямо в строке поиска Facebook, добавлять ее в плейлист и делиться с друзьями. При желании, можно импортировать уже готовый плейлист из «ВКонтакте», однако для этого нужно дать плагину доступ к вашему аккаунту в российской соцсети.

Примечательно, что сервис проигрывает музыку из YouTube, таким образом, по факту пользователь слушает клипы артистов. Сбоку в плеере можно увидеть небольшое окошко с видеорядом. Очевидно, таким образом разработчики преодолели строгое ограничение на пиратский контент в Facebook.

Пока, как сообщают разработчики, сервис находится в бета-версии, однако по отзывам пользователей, все работает стабильно ***(Украинцы создали плагин для браузера MusekBox, который позволяет слушать музыку в Facebook, как во «ВКонтакте» // AIN.UA (http://ain.ua/2015/06/22/587486). – 2015. – 22.06).***

***

Фахівці зі штучного інтелекту в компанії Facebook вивели алгоритм, здатний визначити особу людини на фотографії, навіть якщо вона стоїть спиною.

Програма здатна аналізувати зачіску, одяг і навіть жести користувачів по вже завантажених раніше фотографіях, пише «Дождь».

Фахівці розробили процес розпізнання на прикладі 40 тис. фотографій із сайту Flickr. При цьому на деяких кадрах обличчя були добре видно, на інших – ні. Навчена нейронна мережа змогла правильно розпізнати вже знайому людину на фотографії, де не видно її обличчя, у 83 % випадків.

Раніше Facebook випустила додаток Moments, який здатний аналізувати фотографії на пристрої користувача і розпізнавати там друзів із соціальної мережі. Очікується, що новий алгоритм зможе знайти комерційне застосування в подібних програмах. Також зі зростанням точності розпізнавання такі нейромережі зможуть допомагати силовим структурам у пошуку злочинців ***(Facebook навчився впізнавати людей на фото зі спини // Інформаційна агенція «Вголос» (http://vgolos.com.ua/news/facebook_navchyvsya_vpiznavaty_lyudey_na_foto_zi_spyny_184078.html). – 2015. – 23.06).***

***

LinkedIn существенно переработала приложение для чтения новостей Pulse. Теперь оно предлагает пользователям персонализированные новости, подобранные с учётом их сферы работы и сети контактов.

В старой версии приложения читатели могли лишь подписаться на конкретные публикации или категории. У них не было возможности каким-то образом персонализировать ленту.

Обновлённое приложение использует технологию машинного обучения, чтобы понять, в каких типах контента заинтересован читатель. Подобный механизм уже используется в новостной ленте LinkedIn.

«Вместо добавления нового функционала в старую версию приложения, мы решили полностью переработать механизм его работы», – пояснил соучредитель Pulse А. Котари.

«Новое приложение Pulse сфокусировано на предоставлении персонализированных новостей – новостей, которые подбираются в соответствии с профессиональным миром конкретного пользователя».

Новый интерфейс на основе карточек был разработан для того, чтобы пользователи могли быстро просмотреть большое количество материалов. Если новость не интересна, её можно отклонить. Если нет времени на чтение, её можно сохранить. Если понравился автор, на него можно подписаться. Все эти действия будут улучшать будущие рекомендации контента для конкретного пользователя.

Напомним, что в октябре 2014 г. социальная сеть для профессионалов LinkedIn запустила ленту новостей LinkedIn Pulse. Обновление было призвано увеличить шеринг, количество просмотров каждого сообщения и в итоге количество пишущих пользователей ***(LinkedIn Pulse стал персонализированным дайджестом бизнес-новостей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/linkedin_pulse_stal_personalizirovannym_daydzhestom_biznes_novostey). – 2015. – 24.06).***

***

С 24 июня пользоваться приложением Messenger можно даже тем, у кого нет аккаунта на Facebook. Об этом сообщает lenta.ru.

Теперь не зарегистрированному в социальной сети пользователю на стартовой странице Messenger доступна опция Not on Facebook. Выбрав ее, можно создать аккаунт, предоставив только имя, телефонный номер и фотографию, которая будет отображаться напротив его имени. Пока опция доступна в США, Канаде, Перу и Венесуэле. О датах запуска в других странах не сообщается.

Новый пользователь Messenger может перенести в приложение все контакты со своего телефона, а затем система сверит их с номерами телефонов уже зарегистрированных в приложении аккаунтов и установит соединение. Это не означает, что теперь сервис работает полностью автономно от соцсети: у новичков есть возможность добавлять друзей в свой контактный лист, используя поиск Facebook.

По мнению Tech Crunch, в странах, где Facebook появилась раньше, например в США и Великобритании, возможность использовать мессенджер без привязки к социальной сети поможет вернуть пользователей, которые покинули соцсеть. В то же время для развивающихся рынков Messenger может стать достойной альтернативой SMS и первым шагом к использованию социальной сети.

Глава Messenger Д. Маркус настаивает, что возможность пользоваться приложением без привязки к Facebook нельзя рассматривать как попытку социальной сети выйти на рынок Китая, где доступ к ней заблокирован. Так как в Поднебесной заблокированы все IP-адреса, связанные с Facebook, то и Messenger не пропустят, рассказал он Tech Crunch.

По данным на июнь 2015 г., Messenger насчитывает 700 млн активных пользователей в месяц ***(Приложение Messenger заработало без привязки к Facebook // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43819/118/lang,ru/). – 2015. – 25.06).***

***

В Instagram з'явилися нові функції – пошук за геотегами і актуальні новинні тренди. Останні оновлюються в режимі реального часу. Про це повідомляється в офіційному блозі соцмережі.

В оновленій версії Instagram 7.0 для iOS і Android з'явився інструмент Places Search, який дає можливість шукати фото і відео не тільки за іменами користувачів і хештегами, але і за географічними точками.

Тепер користувачі можуть сортувати фото та відео за назвою місця.

У свіжій версії Instagram також з'явилася вкладка Explore, що дає можливість переглядати підбірки знімків, які вручну компілює команда редакторів проекту. «Це те, до чого ми прагнули з самого початку. Цей інструмент дасть змогу тримати руку на пульсі подій у світі», – каже співзасновник соцмережі Instagram К. Сістром.

Тренди оновлюються в режимі реального часу.

Оскільки за своїми характеристиками Explore дуже схожа на нещодавно анонсований сервіс Lightning, то видання Wired висловило думку, що Instagram прагне обігнати Twitter і стати майданчиком номер один для тих, хто хоче через соціальні мережі в режимі реального часу стежити за актуальними подіями.

Twitter обіцяв запустити сервіс Lightning у своєму мобільному додатку до кінця літа. Натиснувши на відповідну кнопку, користувач перейде до списку найбільш важливих на даний момент тем, про які пишуть інші користувачі. Відбором найбільш цікавого контенту займеться внутрішня команда редакторів Twitter. Про новий формат роботи з новинами представники Twitter повідомили 20 червня.

Нині сервіс Explore від Instagram доступний тільки в США, однак Instagram обіцяє незабаром надати цю функцію користувачам по всьому світу, починаючи з Європи ***(В Instagram з'являться підбірки фото за актуальними темами // MediaSapiens (http://osvita.mediasapiens.ua/web/social/v_instagram_zyavlyatsya_pidbirki_foto_za_aktualnimi_temami/). – 2015. – 25.06).***

***

Пользователи и администраторы сообществ в социальной сети Facebook получат возможность ставить срок для просмотра загруженных видеороликов. Помимо этого, у людей будет возможность задать условие, по которому видео будет удаляться с аккаунта вместе с публикацией после истечения установленного срока. Информация с этой записи удаляется, в том числе, из журнала действий, статистики и прочих источников.

В компании отмечают, чтобы выставить срок действия для только что загруженного ролика, требуется разрешить использовать новую функцию в «Настройках» личной страницы. Опция находится в разделе «Срок действия публикации».

Порядок действий для внесения изменений таков:

– загрузить ролик в Хронику;

– в списке «Опубликовать» выбрать графу «Запланировать публикацию»;

– выбрать графу «Запланировать дату истечения срока действия» и установить число, до которого ролик должен быть доступен на странице;

– выбрать «Запланировать».

Отмечается, что установить функцию можно и для тех видеороликов, которые были ранее опубликованы на странице ***(Facebook вводит ограничение на срок хранения видеороликов // IT новости (http://itnovosti.org.ua/2015/06/internet/socialnye-seti/autodel-video-in-fb.html). – 2015. – 26.06).***

***

Блогоплатформа Tumblr запустила сервис беспрерывного просмотра гифок под названием Tumblr TV. Об этом сообщает TechCrunch.

Несмотря на то что гифки обычно обладают небольшим разрешением для экономии трафика, на Tumblr TV они проигрываются в полноэкранном разрешении. В случае, если анимацию не получается растянуть на весь экран, для неё делают дублирующую подложку – приём, популярный на телевидении со времён появления YouTube.

В отличие от обычного ТВ, пользователь может смотреть гифки без перерывов на рекламу. Каждая анимированная картинка проигрывается несколько раз, прежде чем сменится другой, а управление осуществляется тремя кнопками: «пауза», «вперёд» и «назад».

Сервис предназначен для увеличения активности пользователей блогохостинга, поэтому под «экраном» можно найти кнопки для лайка и репоста. Сохранять гифки на компьютер напрямую из Tumblr TV нельзя.

У каждой гифки можно найти источник (оттуда можно скачать картинку) и посмотреть, под какими тегами она опубликована, а нажатие на тег приводит к «переключению каналов». Поиск по некоторым из тегов заблокирован: например, в фильтре «телевидения» находятся запросы [sex], [bdsm], [licking], а также [deep penetration], хотя последний доступен через обычный поиск. Вместо них Tumblr предлагает посмотреть на котов, покемонов или что-нибудь смешное.

Tumblr TV пока существует только в настольной версии, но в компании заявили, что работают над мобильным направлением.

Как отмечают авторы TechCrunch, бесконечный поток гифок отражает одну из самых популярных сторон Tumblr, опираясь на анонсированный в начале июня сервис поиска анимаций. Всего на Tumblr существует более 112 млрд записей в более чем 239 млн блогов ***(Tumblr создал «телевидение»***

из гифок // InternetUA (http://internetua.com/Tumblr-sozdal--televidenie--iz-gifok). – 2015. – 27.06).

***

В Facebook появился новый редактор фотографий – пока он работает в тестовом режиме в iOS-приложении.

Новый фоторедактор позволяет накладывать сверху на снимки различные фильтры (сейчас их всего семь, переключаются свайпами), а также цветной текст и стикеры. Здесь также есть функция обрезки фотографий и волшебная палочка, автоматически улучшающая изображение. Обрабатывать снимки в Facebook можно было и раньше, однако возможность накладывать сверху текст – фирменная опция Snapchat – появилась только в настоящее время.

Очевидно, таким образом Facebook пытается заменить собой набирающий популярность Snapchat – после того как у компании не получилось приобрести его, а попытки создать собственный мессенджер для обмена фотографиями вроде Poke и Slingshot провалились ***(В Facebook появился редактор, позволяющий накладывать текст на фотографии // Glavpost.com (http://glavpost.com/post/29jun2015/Nets/49539-v-facebook-poyavilsya-redaktor-pozvolyayuschiy-nakladyvat-tekst-na-fotografii.html). – 2015. – 29.06).***

***

Всё, что вы хотели знать о новой ленте публикаций в Facebook

Facebook, кажется, только то и делает, что вносит изменения в механизм дистрибуции контента. Не так давно соцсеть выпустила отдельное мобильное приложение для СМИ, желающих продвигать собственные статьи среди мобильной аудитории. И практически сразу изменила алгоритм выдачи новостей в общей ленте для пользователей и страниц. Чем вызваны изменения и что конкретно они из себя представляют?

Первое – если раньше детище М. Цукерберга хотело конкурировать с новостными агрегаторами, то теперь внезапно решено сосредоточиться на противостоянии с YouTube. Главное изменение коснётся видеоконтента: теперь лента сама будет «подсовывать» вам видео, даже если накануне вы ничего не смотрели, не «лайкали» и не комментировали из видеороликов.

В основе того, какие видео предлагать в новостной поток, а какие – нет, лежит механизм «самообучения», созданный командой Facebook. Подробности о нём не раскрывают, но зато сообщают, что он уже обеспечил 4 млрд просмотров в сутки.

Второе изменение – длительность чтения материалов. На самом деле, второе изменение в новостной ленте «выросло» из первого. Только в Facebook решили, что к текстам можно применить тот же механизм, что и к видеороликам. Кстати, о видеороликах: недостаточно просто забить всю ленту на своей странице или в профиле видеоклипами. Если люди не досматривают ваш контент до конца, толку от этого будет не слишком много: Facebook

учитывает только те видео, которые вы досмотрели до самого конца (ещё и отдаёт предпочтение материалам в HD-качестве).

В дополнение к первым двум изменениям в Facebook представили отдельную аналитику видео для страниц. Раньше для этого приходилось экспортировать данные в Excel или другой табличный процессор. Теперь же есть встроенная панель для трекинга видеороликов, сравнения частоты кликов, периодов просмотра и другой работы с видео (что-то вроде встроенной аналитики в YouTube для аккаунтов).

И третье – рекомендации по видео и по текстовому контенту теперь друг друга дополняют в ленте (по крайней мере, задумка такова). Анализ поведенческих особенностей пользователя составляется в том числе и на основе того видео, которое он просматривает – и повышается общая релевантность всех тем (и видео, и ссылок, и текстов), которые появляются в ленте новостей Facebook.

Четвёртое изменение уже не такое очевидное и касается скорее работы и возможностей самой соцсети и рекламодателей, которые размещают свои материалы в Facebook. Расширенная аналитика и сбор данных из обновлённой новостной ленты позволяют собрать огромный массив информации, крайне необходимой контент-маркетологам и видеопродакшну. Эта информация пригодится для принятия решений о таргетировании конкретных кампаний, где основным носителем является видео ***(Всё, что вы хотели знать о новой ленте публикаций в Facebook // Блог Imena.UA (http://www.imena.ua/blog/facebook-newsfeed-changes/). – 2015. – 30.06).***

***

Facebook начала не только следить за тем, как долго пользователи смотрят видеозаписи, но также стала отслеживать другие действия, такие как повышение громкости и вход в полноэкранный режим.

По результатам опроса соцсети, это показывает, насколько аудитории нравится просматриваемый контент. Если человек совершает данные операции, сервис покажет ему больше похожих видео в ленте новостей. Нововведение должно появиться в ближайшие недели.

Facebook провела исследование, опросив аудиторию, как соцсеть может улучшить свои алгоритмы. Компания выяснила, что лайки, репосты и комментарии – не единственный показатель того, что человеку нравится просматриваемый контент. Значительно важнее те действия, которые он совершает при просмотре: вывод видео на полный экран и увеличение громкости.

Facebook и раньше следила за тем, как пользователи просматривают видеозаписи – соцсеть определяла, какой контент они смотрят и как долго. Теперь, по словам компании, люди, привыкшие часто смотреть ролики, увидят больше релевантных видео на площадке.

Доступ к данным появится у администраторов страниц, которые смогут отслеживать всю статистику: какое количество видео проигрывается

автоматически, а какое – с помощью кликов пользователей, в какие периоды времени аудитория смотрит видео. Также компании увидят топ роликов по популярности (уже с учетом новых алгоритмов). При этом соцсеть отмечает, что большинство страниц не заметят существенных изменений в связи с новой функциональностью.

29 июня 2015 г. количество просмотров видео в Facebook достигло 4 млрд в день ***(Facebook покажет пользователям больше релевантных видео на основе новых алгоритмов // Цукерберг Позвонит (http://siliconrus.com/2015/06/fb-video/). – 2015. – 30.06).***

***

Facebook тестирует плавающее видео

В ленте некоторых пользователей появилась новая опция, благодаря которой видео «выскакивает» из новостной ленты и занимает нижний левый угол на экране, позволяя пользователю одновременно листать ленту и смотреть видео. Его можно переместить в другое место на странице, лайкнуть и поделиться с ним друзьями. К сожалению, при переходе на другую страницу, видео за пользователем не последует. В последнее время Facebook все глубже заходит на территорию YouTube, предложив поделиться с создателями видео доходами и увеличив количество видео в ленте ***(Facebook тестирует плавающее видео // Marketing Media Review (http://mmr.ua/show/facebook_testiruet_plavayushtee_video). – 2015. – 8.07).***

***

Социальная сеть Facebook в следующем месяце откроет африканский офис для расширения присутствия на континенте, сообщает IT Expert со ссылкой на Газету.ру и The Telegraph.

Офис разместится в пригороде Йоханнесбурга и займется повышением доступности Facebook для жителей Нигерии, Кении и ряда других африканских стран с растущим интернет-рынком. Социальная сеть также будет налаживать партнерство с мобильными операторами для улучшения доступа клиентов к проекту доступного Интернета Internet.org.

На сегодня число африканских пользователей Facebook превышает 120 млн человек ***(Facebook открывает офис в Африке // IT Expert (http://itexpert.org.ua/rubrikator/item/41140-facebook-otkryvaet-ofis-v-afrike.html). – 2015. – 30.06).***

***

Ученые из Университета Сан-Паулу, Бразилия, создали алгоритм для автоматического обнаружения пожаров на фотографиях в соцсетях. Данная работа была частью проекта Rescuer, в рамках которого планируется создать систему быстрого реагирования на чрезвычайные происшествия по данным из социальных сетей. Препринт исследования выложен на arXiv.org.

Ученые пользовались методами машинного обучения и классификации изображений. Для этого из социальной сети Flickr было взято 5962 фотографии, которые пользователи отмечали тегами, содержащими слово «огонь». Далее при помощи добровольцев из всех фотографий отбирались те, где на снимке отчетливо видно пламя.

По имеющимся фотографиям авторы составляли соответствующие им вектора признаков. В них входили значения, определяющие расположение и температуру цветов, а также характерную текстуру изображения. На основании этих данных ученые обучали программу определять наличие пламени на произвольно заданной фотографии.

Результаты работы нового алгоритма авторы сравнили с данными ручной классификации изображений. Эффективность программы оказалась сопоставима с «ручной» классификацией: совпадение результатов наблюдалось в 85 % случаев.

Авторы отмечают, что одной из ключевых особенностей их программы являются сравнительно низкие вычислительные затраты, что позволяет использовать ее на персональных устройствах. В планах проекта Rescuer лежит создание аналогичных приложений для определения других потенциальных источников опасностей помимо пожаров ***(Алгоритм научили искать пожары на снимках в соцсетях // InternetUA (http://internetua.com/algoritm-naucsili-iskat-pojari-na-snimkah-v-socsetyah). – 2015. – 1.07).***

***

Социальная сеть Facebook сменила логотип впервые с 2005 г., пишет «Обозреватель» (http://tech.obozrevatel.com/news/61548-facebook-smenil-logotip-vpervyie-s-2005-goda-fotofakt.htm).

Так же, как и прежний логотип, новая эмблема представляет собой надпись белым шрифтом на синем фоне.

Д. Хиггинс, креативный директор Facebook, рассказал, что перед компанией стояла задача сделать логотип «более дружелюбным и доступным». Команда дизайнеров решила обновить старую эмблему, а не создавать новую, передает Siliconrus.com ***(Facebook сменил логотип впервые с 2005 года // Обозреватель (http://tech.obozrevatel.com/news/61548-facebook-smenil-logotip-vpervyie-s-2005-goda-fotofakt.htm). – 2015. – 2.07).***

***

Глава Facebook опубликовал на своей странице в социальной сети информацию о том, что компания работает над технологией передачи данных при помощи лазера, и показал прототип устройства.

1 июля 2015 г. М. Цукерберг ответил на вопросы пользователей в очередном Q&A. Во время сессии вопросов и ответов М. Цукерберг упомянул, что Facebook работает над некой лазерной системой передачи данных, использовать которую планируется там, где сетевая инфраструктура плохо развита. Над проектом трудятся инженеры из подразделения Connectivity Lab,

чья задача – провести Интернет даже в самые глухие уголки планеты, если нужно, то и посредством инновационных технологий.

На следующий день М. Цукерберг дополнил информацию, разместив на своей странице фотографии лазерной установки. Глава Facebook пишет, что в жизни лазерные лучи не видны глазу, их сделали видимыми для фото. По словам М. Цукерберга, скорость передачи данных на большие расстояния «значительно возрастает» с использованием этой технологии.

Facebook планирует использовать лазерную передачу данных совместно с беспилотными летательными аппаратами и спутниками, которые должны проводить в воздухе по несколько месяцев без перерыва, заряжаясь от солнечных батарей ***(Цукерберг продемонстрировал лазерную передачу данных // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/technology/cukerberg-prodemonstriroval-lazernu.html). – 2015. – 3.07).***

***

Группа христиан-евангелистов из Бразилии запустила в Интернете «безгреховный» аналог Facebook, в котором «лайки» были заменены на «аминь». Социальная сеть получила название Facegloria и ряд ограничений, исключающих появление на страницах разнузданных бикини-фото, бранных слов и всякого рода упоминаний о гомосексуализме. Администрация сети намерена бороться за моральный облик своих пользователей, чего, по их мнению, не делает Facebook.

«Мы намерены стать лучше морально и технически, нежели Facebook», – заявил сооснователь Facegloria А. Баррос. За духовной чистотой соцсети следит порядка 20 модераторов, в чьи обязанности входит отслеживание и удаление материалов с намеками на сексуальность, насилие и т. д.

Христиане-евангелисты имеют большое значение в Бразилии – около 42 млн последователей, или 22 % населения страны. В первый месяц функционирования сети ее пользователями стали 100 тыс. человек. За два года планируется собрать аудиторию в 10 млн человек и начать экспансию на международные рынки ***(Бразильские евангелисты создали «непорочный» Facebook // InternetUA (http://internetua.com/brazilskie-evangelisti-sozdali--neporocsnii--Facebook). – 2015. – 7.07).***

***

Instagram повысил разрешение снимков в официальном приложении сервиса. Об этом говорится в официальном блоге разработчиков. Новые снимки, публикуемые на iOS и Android, имеют разрешение 1080x1080 точек вместо 640 x 640 точек.

Ранее Instagram неоднократно критиковали за низкое разрешение фотографий. Изображения шириной в 640 точек уже были ощутимо малы для новых iPhone 6 с дисплеями разрешением 1334 x 750 и 1920 x 1080 пикселей. Смартфоны на Android начали массово получать экраны с высоким

разрешением в 2013 г., когда разрешение фотографий в Instagram составляло и вовсе 612х612 точек. В результате приложение «растягивало» фотографии под ширину экрана, что портило качество снимков.

Слухи о том, что Instagram повысит качество фотографий ходили еще на прошлой неделе. Тогда разработчики заметили, что сервис начал готовить свое ПО и серверы к переходу на снимки разрешением 1080 х 1080 точек. Позже признаки этого внимательные пользователи обнаружили в исходном коде сайта Instagram.com – все указывает на то, что уже сейчас все снимки, заливаемые в Instagram, хранятся с повышенным разрешением.

Изменения в приложениях Instagram уже вступили в силу, без обновления клиентов. Как объяснили разработчики, параметры фотографий является ограничением на серверной стороне.

Отметим, что на экране iPhone 6 Plus с разрешением Full HD по горизонтали умещается как раз 1080 пикселей. Даже для отображения на HD-дисплее (720 пикселей по ширине) «инстаграмовский» квадрат в 640 пикселей ранее приходилось растягивать, что неизбежно делало картинку менее четкой ***(Instagram повысил качество фотографий на iOS и Android // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/instagram-povysil-kachestvo-fotografiy-na-ios-i-android.html). – 2015. – 7.07).***

***

Социальная сеть «ВКонтакте» анонсировала поддержку видео с разрешением Full HD и частотой 60 кадров в секунду. Теперь пользователи могут загружать и просматривать контент в таком качестве.

Переключиться на видео 1080p можно там же, где и на другие разрешения. В плеере появились миниатюры при перемотке и поиске нужного момента. У всех новых видеороликов после этого обновления перемотка будет работать стабильно и с точностью до одной секунды.

«Только что крупное обновление получил видеоплеер «ВКонтакте». Самое главное: социальная сеть теперь поддерживает видео повышенной чёткости 1080p с частотой кадров до 60 fps. Также были изменены некоторые элементы управления и обновлена перемотка видеозаписей: у роликов, которые загружены с текущего момента, перемотка работает стабильно и позволяет перематывать видеозапись в промежутках до одной секунды».

Администрация «ВКонтакте» обещает в скором времени открыть загрузку видеозаписей в 1080p верифицированным сообществам и участникам Видеокаталога ***(«ВКонтакте» добавила поддержку видео с разрешением 1080p и частотой 60 fps // InternetUA (http://internetua.com/vkontakte--dobavila-podderjku-video-s-razresheniem-1080p-i-csastotoi-60-fps). – 2015. – 7.07).***

***

Facebook зазіхає на першість Google в мобільному пошукові статей та відео.

Публікація посилань через мобільні сервіси протягом кількох останніх років істотно покращилась: тепер не треба копіювати і вставляти посилання між додатками чи між додатком і браузером. Нативні клієнти соцмереж та онлайн-сервісів мають підтримку переходів через вбудований браузер або нативний мобільний браузер смартфона / планшета за умовчуванням.

У світлі цих змін Facebook може отримати «ласий шматок» мобільного пошукового трафіку завдяки власному пошуковому механізмові. Компанія М. Цукерберга експериментує з пошуком статей та посилань через нативний додаток. При цьому самі матеріали можуть міститися за межами соціальної мережі.

Ще в травні 2015 р. у низки користувачів iOS-смартфонів та планшетів у додатку з'явилася нова кнопка – Add a Link. За допомогою цієї кнопки можна було швидко прикріпити до свого статусу чи запису в соцмережі релевантні посилання на статті, відеоролики чи інші матеріали із зовнішніх джерел. Сортування пошукових результатів при цьому відбувається залежно від того, де нині перебуває користувач, яким контентом найчастіше діляться всі користувачі в мережі Facebook тощо.

Нову опцію отримала невеличка група користувачів соцмережі на території США. Однак у компанії підтвердили, що в подальшому впроваджуватимуть такий інструмент пошукового маркетингу та додавання матеріалів для усіх.

Коли така опція стане загальнодоступною, це означатиме, що зникне потреба «гуглити» чи гортати стрічку новин Facebook у пошуках потрібного посилання. А це особливо важливо для мобільних користувачів – бо екрани з малою діагоналлю, мобільний Інтернет та обмеженість часу використання не дають можливості довго шукати потрібну статтю, відео- чи аудіозапис.

Для видавців поява такої кнопки означатиме додаткові можливості для просування свого контенту серед мобільної аудиторії та отримання додаткового реферального трафіку. Для порівняння: під кінець 2014 р. Facebook став справжнім «трафікогенератором», даючи до 25 % усіх переходів із соцмереж для сайтів з новинами та статтями (у Twitter цей показник становить менше 1 %).

Нова опція поширення матеріалів також припаде до смаку і рекламодавцям: команда М. Цукерберга має намір віддавати авторам рекламних оголошень 100 % виручки, якщо контент демонструється поруч із посиланням, опублікованим через кнопку Add a Link ***(Facebook зазіхає на першість Google в мобільному пошукові статей та відео // Блог Imena.UA (http://www.imena.ua/blog/facebook-beats-google/). – 2015. – 7.07).***

***

Социальная сеть Facebook расширила набор инструментов управления новостями в своей ленте. Об этом сообщается в официальном блоге компании.

Пользователи смогут выбирать, чьи новости они хотят видеть в первую очередь. Расставить приоритеты и выбрать из списка своих друзей и страниц наиболее интересные можно с помощью вкладки See first.

Изменения коснулись и настройки подписок: Facebook предлагает пользователю отказаться от подписки на страницы тех людей, чьи посты ему неинтересны, и в отдельной вкладке – возобновить подписки, которые ранее были отменены. Отдельная вкладка посвящена рекомендованным социальной сетью страницам. Предложения составляются на основе предпочтений пользователя и анализа понравившихся ему страниц.

«Мы отбираем конвент, основываясь на том, что нам кажется интересным для вас, с кем вы больше общаетесь, какие материалы отмечаете как понравившийся и комментируете», – говорится в сообщении соцсети.

Изменения доступны в приложении Facebook на iOS с 9 июля, а в настольной версии и устройствах на Android – в течение нескольких недель.

Нововведение вызвало опасения экспертов по безопасности. Издание Wired назвало новые настройки ленты «дающими иллюзию контроля». Предлагая пользователям больше инструментов настройки ленты новостей «под себя», Facebook стремится создать впечатление, что читатель способен в большей степени, чем раньше, контролировать то, что он видит. Между тем эти настройки позволят соцсети собрать еще больше информации о пользователе. «Чем точнее будет информация, которую компания получит о вас, тем больше за вас заплатят рекламодатели», – отмечает издание ***(Facebook дал пользователям свободу управления новостной лентой // InternetUA (http://internetua.com/Facebook-dal-polzovatelyam-svobodu-upravleniya-novostnoi-lentoi). – 2015. – 9.07).***

***

Несколько дней назад в сети появился слух о том, что представители Facebook провели беседу с крупными лейблами и начали подготовку к запуску музыкального сервиса. Facebook официально опроверг эти слухи.

В то же время представители соцсети заявили, что Facebook готовит новый, уникальный сервис. Издание Music Alley предполагает, что речь идет о видеосервисе, который будет конкурировать с YouTube. Возможно, разговор с лейблами все же состоялся, и стороны обсуждали, каким образом к этому сервису можно привлечь музыкантов.

На прошлой неделе Facebook запустила партнерскую программу, по которой люди, выкладывающие видео, могут получать деньги за показ рекламы ***(Facebook не планирует запускать музыкальный сервис, но готовит что-то другое // InternetUA (http://internetua.com/Facebook-ne-planiruet-zapuskat-muzikalnii-servis--no-gotovit-csto-to-drugoe). – 2015. – 12.07).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Украинские и российские блогеры создали на портале Change.org петицию, которая призывает прекратить политические блокировки в соцсети Facebook, передает Цензор.НЕТ.

Петиция с момента размещения набрала 14 182 подписи.

«За последние месяцы Facebook превратился в послушный инструмент, с помощью которого враги свободы слова затыкают рты несогласным. Мы призываем администрацию Facebook и лично М. Цукерберга перестать преуменьшать масштабы проблем с модерированием социальной сети и сделать все необходимое для их исправления в кратчайшие возможные сроки», – говорится в петиции.

Авторы обращения также призывают администрацию соцсети разблокировать все заблокированные за последние недели российские и украинские аккаунты и «полностью прекратить блокировки до создания новой, защищенной от атак троллей, системы модерирования, которая не сможет быть использована в политических целях».

Полный текст петиции читайте на сайте ***(«Facebook превратился в эффективное орудие Кремля», – петицию против политических блокировок в соцсети подписали более 14 тысяч человек // Цензор.НЕТ (http://censor.net.ua/news/341970/feyisbuk_prevratilsya_v_effektivnoe_orudie_kremlya_petitsiyu_protiv_politicheskih_blokirovok_v_sotsseti). – 2015. – 30.06).***

***

2 липня Верховна Рада України ухвалила Закон «Про реструктуризацію зобов'язань за кредитами в іноземній валюті». За відповідне рішення проголосували 229 народних депутатів – повідомляє Українська Правда.

Законом передбачено, що виплата кредитів буде здійснюватись за курсом на день отримання кредитів.

Український Twitter і Facebook одразу вибухнули критикою популізму Верховної Ради.

Хештег #ПорошенкоВетуй1588 миттєво вийшов у топи українського Twitter ***(Реакція інтернету на популізм Верховної Ради щодо валютних кредитів // UkrainianWatcher (http://watcher.com.ua/2015/07/02/reaktsiya-internetu-na-populizm-verhovnoyi-rady-schodo-valyutnyh-vkladiv/). – 2015. – 2.07).***

***

Губернатор Одесской области М. Саакашвили, отметившийся публичностью SMM-показателей, опубликовал свежие данные своей страницы Facebook. Согласно последней информации, количество лайков страницы

превысило 555 тыс. (у Президента Украины – 366 тыс. подписчиков). Этот момент М. Саакашвили отметил обновлением cover image в Facebook с комментарием «с детства хотел, чтобы у меня были одни пятерки». Количество новых лайков страницы упало на 3,1 %. Предыдущий бурный рост можно объяснить хитовыми видео на YouTube ***(Саакашвили обошел Порошенко по лайкам // Marketing Media Review (http://mmr.ua/show/saakashvili_oboshel_poroshenko_po_laykam). – 2015. – 28.06).***

***

Харківський районний військовий комісаріат створив в одній із соціальних мереж в Інтернеті власну сторінку. За її допомогою мають надію розшукати юнаків, які ухиляються від строкової служби.

Так, 30 червня в соціальній групі «Люботин» користувач Харьковский-Районный Военный-Коммисариат розмістив три повідомлення. У них автор просить допомоги розшукати трьох хлопців – мешканців м. Люботин, які ухиляються від призову на строкову службу. Думки читачів розділилися порівно щодо такого «ноу-хау» військкомату ***(Військкоми розшукують ухилянтів в соціальних мережах // Газета «Слобідський край» (http://www.slk.kh.ua/news/suspilstvo/vijskkomi-shukayut-ukhilyantiv-vid-armiyi-v-sotsialnikh-merezhakh-foto.html). – 2015. – 30.06).***

***

Медійний саморегулюючий орган Вірменії Єреванський прес-клуб готує рекомендації щодо соціальних мереж для того, щоб їх враховували медіа і журналісти при укладенні трудових договорів.

Про це сказав керівник клубу Б. Навасардян під час міжнародної зустрічі саморегулюючих медійних організацій у рамках спільного проекту ЄС та Ради Європи «Сприяння професіоналізму і відповідальній журналістиці та підтримці органів саморегуляції в ЗМІ», що відбулася 2 липня в Тбілісі.

За його словами, протягом останнього часу були звільнені двоє журналістів за дописи в соціальних мережах. Тому, на його думку, це питання варто унормувати, щоб не порушувалися трудові права журналістів.

Раніше, на початку травня голова Єреванського прес-клубу Б. Навасардян заявив кореспондентові сайту «Кавказский узел», що у Вірменії існує прихована цензура, а редакційну політику визначають власники політичних центрів ***(Вірменський прес-клуб готує рекомендації щодо соцмереж для трудових договорів зі ЗМІ // Media Sapiens (http://osvita.mediasapiens.ua/ethics/standards/virmenskiy_presklub_gotue_rekomendatsii_schodo_sotsmerezh_dlya_trudovikh_dogovoriv_zi_zmi/). – 2015. – 2.07).***

***

Мережа органів саморегуляції в ЗМІ з Азербайджану, Вірменії, Грузії, Молдови, Росії та України вирішили створити робочу групу, яка розглядатиме

скарги, пов'язані з розпалюванням національної ворожнечі і поширенням мови ненависті (домовленість про це була досягнута на попередньому засіданні мережі в Брюсселі восени 2014 р.).

Таке рішення було прийнято на міжнародній зустрічі саморегулюючих медійних організацій у рамках спільного проекту ЄС та Ради Європи «Сприяння професіоналізму і відповідальній журналістиці та підтримці органів саморегуляції в ЗМІ», що відбулася 3 липня в Тбілісі.

Мережа як наднаціональний орган буде розглядати звернення і скарги, які проблематично або неможливо буде розглянути на національному рівні через небезпеку звинувачень у «непатріотизмі». Таким чином, мережа намагатиметься провести максимально об'єктивний розгляд будь-якої скарги.

Крім того, організації, що входять до мережі, вирішили підготувати спеціальні рекомендації для ЗМІ, щоб протистояти найбільш небезпечним проявам пропаганди, яка призводить до розпалювання міжнаціональної і будь-якої іншої ворожнечі.

«Добре, що тепер ми знатимемо, як така група працюватиме. Протягом місяця ми підготуємо базові принципи, згідно з якими будуть розглядатися подібні скарги та звернення. Після їх затвердження національними організаціями саморегулювання (в Україні це Комісія з журналістської етики) – група розпочне роботу. Це дасть можливість об'єктивніше оцінювати матеріали тих журналістів та ЗМІ, які сьогодні піддаються жорсткій критиці з боку політиків, урядів або певних громадських груп. Головне – захистити професійні стандарти і чесну роботу журналістів. Також я сподіваюсь, що ця діяльність мережі дозволить хоча б трохи знизити розповсюдження мови ворожнечі в наших ЗМІ та Інтернеті, яке вже досягло значних масштабів і має катастрофічний вплив на можливість досягнення політичної та економічної стабільності в Україні. Відповідальність журналістів сьогодні колосальна, і дуже добре, якщо мережа та органи саморегуляції допоможуть медійникам втриматися в професійному руслі» ***(Мережа органів саморегулювання в ЗМІ розглядатиме скарги про розпалювання міжнаціональної ворожнечі // MediaSapiens (http://osvita.mediasapiens.ua/media_law/law/merezha_organiv_samoregulyuvannya_v_zmi_rozglyadatime_skargi_pro_rozpalyuvannya_mizhnatsionalnoi_vorozhnechi/). – 2015. – 3.07).***

***

Київська поліція відкрила акаунти в Instagram і Facebook

У числі найбільш популярні хештегів #kyivpolice, пише «Корреспондент» (http://ua.korrespondent.net/kyiv/3536069-kyivska-politsiia-vidkryla-akaunty-v-Instagram-i-Facebook#5).

Новостворена київська поліція, яка вже викликала бум у соцмережах, завела профіль у фотомережі Instagram.

На профіль уже підписалося понад 2000 користувачів. Поліція постить свої фото (з присяги, а також з місця роботи), а також селфі патрульних.

Також на сторінці вже з'явилися перші відео з місць пригод і скріншоти постів у соцмережах, де розповідається про роботу правоохоронців.

Сторінки у Facebook «Патрульна поліція України» лайкнули вже понад 22 тис. осіб.

Нагадаємо, нова поліція вийшла на вулиці Києва 4 липня ***(Київська поліція відкрила акаунти в Instagram і Facebook // Корреспондент.net (http://ua.korrespondent.net/kyiv/3536069-kyivska-politsiia-vidkryla-akaunty-v-Instagram-i-Facebook#5). – 2015. – 6.07).***

***

Юрист із Херсона Є. Єршов уже понад півроку працює над наповненням у соціальній мережі Facebook спільноти-агрегатора новин «Об'єктивний Крим – Obyektiv Qırım – Объективный Крым» про події на анексованому півострові. Про це він розповів «Телекритиці».

В описі спільноти повідомляється, що мета проекту – вчасно повідомити про подію тим, кому це може бути цікаво.

«Виходячи з цього відбір новин і читачів у нас здійснюється індивідуально. У цільову групу новин входить інформація про Крим і його жителів, а також для Криму і знову ж таки його мешканців. Ми не обмежуємося тільки подіями в Криму. Нам цікаво все, що може вплинути на рішення кримського питання, змінити сприйняття цієї проблеми як мешканцями Криму, так і світовим співтовариством», – зазначається в спільноті.

Є. Єршов розповів, що це його особиста ініціатива, і він займається проектом самотужки. «Це особистий проект без вкладень – приватна ініціатива. Почав працювати на повну з листопада 2014 р. Я юрист і мені як жителю Херсона цікава тема Криму. Ось так і з'явилася ця ідея. Хоча напевно нічого в цьому нового немає. Просто є велике бажання допомагати кримчанам отримувати альтернативну інформацію», – каже засновник спільноти.

Окрім повідомлення новин, читачі спільноти – жителі Криму, які є громадянами України, можуть отримати безкоштовну онлайн-консультацію з питань українського законодавства щодо Криму. Корисна інформація для мешканців півострова міститься в колонці «Нотатки». «Об'єктивний Крим» також сприяє заходам, спрямованим на надання допомоги жителям Криму, незалежно від того, де вони перебувають.

«Надаємо журналістам майданчик сторінки для публікації їх матеріалів, які відповідають проблематиці діяльності "Об'єктивного Криму" (авторське право залишається за автором). Залишаємо за собою право відмовити в розміщенні в випадку, якщо стаття носить явно провокаційний характер, підштовхує до національної ворожнечі та інше», – зазначається в спільноті.

З метою сегментації новин та для кращого їх сприйняття на сторінці функціонують додаткові напрями: «Об'єктивний Крим – аналітика» та «Об'єктивний Крим – відео».

«У Криму в мене вже є постійні читачі, з якими я спілкуюся. Допомагаю охочим зв'язатися громадськими активістами в українських містах, щоб

приїхати на їх заходи і розповісти про те, що відбувається в Криму. Надаю юридичну допомогу. Саме в Херсон кримчани приїжджають за адміністративними послугами. Інколи проводжу екскурсії по нашому місту. Вони часто діляться тим, що бачать в Криму, і я викладаю їх матеріали без зазначення імен», – розповів Є. Єршов.

Є. Єршов запрошує читачів підтримати проект, підписавшись на нього, а також ділитися з ним актуальними новинами про Крим. Медіа він пропонує надавати посилання на свої матеріали для публікації в спільноті.

Наразі на сторінку «Об'єктивний Крим» підписано майже 6,5 тис. користувачів.

Нагадаємо, нещодавно Східно-Європейський Демократичний Центр (Варшава, Польща) та громадська організація «Інтерньюз-Україна» оголосили про початок програми надання технічної допомоги для редакцій та окремих журналістів та блогерів, які висвітлюють питання Криму ***(Херсонський юрист започаткував Facebook-сторінку, яка агрегує новини про Крим // Телекритика (http://www.telekritika.ua/rinok/2015-07-08/109021). – 2015. – 8.07).***

***

Украинский Facebook превратился в новую реальность, где пост может заставить действовать Президента

Социальная сеть увлекла уже несколько миллионов самых активных украинцев – представителей среднего класса, политиков и ключевых госчиновников, пишет «Новое время» (http://nv.ua/publications/nv-24-ukrainskiy-facebook-prevratilcya-v-novuyu-realnost-gde-neskolko-postov-mogut-zastavit-deystvovat-prezidenta-58300.html).

Устроившись поудобней за столом возле компьютера, К. Волох, бизнесмен и один из украинских топ-блогеров Facebook (FB), рассуждает о том, во что превратили соцсети своих адептов. «Те, кто постоянно находится в FB, считают, что и вся страна находится там же, – К. Волох говорит, а на мониторе идет постоянное обновление его ленты новостей. – Но огромное количество людей и понятия не имеет, что там происходит».

Если бы эту фразу он не произнес, а написал в соцсети, ее прочло бы примерно 43 тыс. человек – столько пользователей FB подписано на обновления К. Волоха. «Facebook – это огромная песочница, в которой люди дружат и ругаются друг с другом не на шутку», – добавляет он.

«Песочница» по накалу страстей даст фору телевизионным политическим шоу – в соцсети ссорятся, опускаясь до матов, интеллигентные люди, в обычной жизни никогда не практикующие подобное. Зашкаливание эмоций неслучайно – по мнению экспертов, часть пользователей FB буквально живет соцсетью. А потому воспринимает любой негативный отзыв как личный выпад.

Более того, FB влияет уже не только на отдельных индивидуумов, но и на поведение общественных групп, деятельность коммерческих компаний и даже на действия властей. И все потому, что за последние полтора года FB

«завербовал» в свои сети достаточно сторонников, чтобы стать социальным явлением. Часть пользователей сутками сидят в онлайн. Подобная вовлеченность, как считает К. Волох, вводит пользователей FB в «сильное заблуждение» – они воспринимают реальностью то, что читают в соцсети.

Украинская аудитория Facebook с начала 2014 г. возросла на 800 тыс. человек и теперь превышает уровень в 4 млн пользователей. Но реальный охват, по мнению М. Саваневского, главного редактора издания Watcher, специализирующегося на интернет-бизнесе и маркетинге в соцмедиа, составляет около 7–8 млн человек. То есть примерно каждый шестой украинец подвержен влиянию FB.

Чтобы понять величие этой цифры, достаточно вспомнить, что весной 2009 г., когда в Украине фейсбукомания лишь начиналась, вся аудитория сети составляла, по данным Watcher, 62 тыс. человек. Нынче у самых популярных персонажей украинского FB число подписчиков может исчисляться сотнями тысяч.

Причем в украинской соцсети № 1 «обитает» самая активная часть населения – госчиновники высших рангов, политики, активисты, волонтеры, журналисты, эксперты – то есть люди, являющиеся лидерами мнений, имеющие большое влияние на общество.

На что способна сегодня соцсеть и самые влиятельные адепты этой «секты по интересам» в новом номере журнала Новое Время – № 24 от 10 июля ***(НВ №24: Украинский Facebook превратился в новую реальность, где пост может заставить действовать Президента // Новое время (http://nv.ua/publications/nv-24-ukrainskiy-facebook-prevratilcya-v-novuyu-realnost-gde-neskolko-postov-mogut-zastavit-deystvovat-prezidenta-58300.html). – 2015. – 9.07).***

***

Недавно в журнале Forbes вышла занятная статья, посвященная образовательному буму. В ней приводятся не самые очевидные факты и цифры: уже сейчас видеолекции и другие просветительские видео по многим параметрам превосходят ролики о животных, сообщает IT Expert со ссылкой на Edutainme.

Также статистика говорит о том, что количество просмотров резко возрастает в периоды сессии и подготовки к ней.

Видео от Khan Academy или CrashCourse собирают миллионы просмотров и увесистые гранты от известных организаций – например, от Фонда Билла и Мелинды Гейтс. Часть образовательных роликов помещается на центральный канал YouTube EDU channel, призванный помочь студентам всех возрастов разобраться в многообразии ресурсов. Уже сейчас YouTube служит хорошим дополнением к традиционному образованию.

По словам основателя сверхпопулярного канала CrashCourse, в этом мае удалось установить новый рекорд и набрать миллион просмотров: студенты готовились к экзаменам и смотрели десятки эпизодов подряд ***(В YouTube***

учителя обогнали котиков // IT Expert (http://itexpert.org.ua/rubrikator/item/41131-v-youtube-uchitelya-obognali-kotikov.html). – 2015. – 26.06).

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Бренди переносять свою активність із Facebook у Instagram. 98 % брендів вже є присутніми у Facebook, але зростання їхньої бази прихильників припинилося. Натомість, в Instagram цей процес набирає обертів – про це йдеться в дослідженні Yes Lifecycle Marketing.

Головна причина припинення зростання – низька ефективність Facebook, через це рітейлери переходять на нові канали та використовують нові інструменти – ідеться в дослідженні.

91 % брендів уже присутні у двох або більше соціальних мережах (у дослідженні розглядалися Facebook, Twitter, YouTube, Instagram і Google+). Найвищий рівень присутності у брендів одягу: 86 % представлені на чотирьох соціальних каналах, 60 % – на всіх п'яти. Зростання бази прихильників брендів одягу в Instagram минулого року становило в середньому 417 %.

91 % брендів присутні у Twitter, 79 % – на YouTube, і тільки 43 % – в Instagram, незважаючи на його потенціал. Середній темп зростання прихильників брендів в Instagram становив 237 %.

Зростання бази прихильників припинилося не лише у Facebook, але і у Twitter ***(Бренди переносять свою активність з Facebook у Instagram // UkrainianWatcher (http://watcher.com.ua/2015/06/23/brendy-perenosyat-svoyu-aktyvnist-z-facebook-u-instagram/). – 2015. – 23.06).***

***

Как используют соцсети на Ближнем Востоке и в Африке. Наблюдения Н. Мендельсон из Facebook

Вице-президент соцсети Facebook Н. Мендельсон два года отвечает за развитие компании в Европе, Ближнем Востоке и Африке. Она часто ездит в командировки, знакомится с людьми и изучает, как в разных странах пользуются социальными сетями и мобильным Интернетом. Для Business Insider она привела несколько примеров того, как по-разному люди пользуются гаджетами и технологиями. «Секрет» выбрал самые важные тренды.

Мобильные платежи – это не так сложно

Число пользователей Facebook из Ближнего Востока и Африки в настоящее время 191 млн человек, из них 85 % посещают сайт с мобильных устройств. Н. Мендельсон рассказывает о поездке в столицу Кении, город Найроби. Там люди делают покупки с помощью мобильных телефонов, даже

если не имеют счёта в банке. Помогает сервис M-Pesa, поставщик платёжных услуг для абонентов мобильных операторов. Он позволяет мгновенно осуществлять денежные переводы с телефона на телефон по всей стране, даже не имея счёта в банке. «M-Pesa – это что-то невероятное. Вы можете идти по рынку в Найроби, такому же, каким он был тысячу лет назад. Но вся торговля там ведётся через мобильные телефоны. Вы думаете: "Как странно, на рынке в Лондоне, я не могу сделать подобного". Многому можно научиться, побывав там».

Раз десктоп не нужен пользователям, он не нужен и рекламщикам

Не секрет, что в развивающихся странах у людей нет денег на покупку ноутбука или домашнего компьютера, поэтому смартфон заменяет пользователям десктоп. Н. Мендельсон утверждает: в первую очередь эту особенность должны учитывать рекламщики, когда придумывают контент. В 2015 г. Facebook запустил программу Creative Accelerator, чтобы дать возможность агентствам и брендам создавать рекламные объявления для размещения в сети прямо со смартфона. Она рассказывает об опыте работы с компанией Coca-Cola в Кении, там производитель газировки запустил рекламную кампанию в Facebook со слоганом «Делись своей историей». Пользователи без труда могли поучаствовать в ней с любого устройства, это подняло узнаваемость бренда на 18 %.

Instagram – двигатель бизнеса

В Кении Н. Мендельсон встретила женщину по имени Изабелла, владелицу модного бутика Fashion254. Предпринимательница вовсю использует Instagram для продажи платьев, хотя в регион ещё не пришла возможность рекламы в этой соцсети. На страничке «О себе» Изабелла предлагает связаться с ней по телефону или в WhatsApp, чтобы договориться о доставке. Фермеры в Кувейте тем временем используют Instagram для продажи овец. С ними Н. Мендельсон познакомилась ещё в 2013 г. Тогда на аккаунт @sheeps_sell (ныне неактивный) было подписано 2500 человек.

Женщины мусульманских стран находят себя в сети

Организация Glowork, которая помогает женщинам в Саудовской Аравии найти работу и построить карьеру, познакомила Н. Мендельсон с женщинами-предпринимателями, которые используют Facebook как площадку для продажи своих товаров. «В этой стране множество правил и запретов, и для женщин там Интернет стал способом связи с внешним миром. Facebook дал возможность быть в контакте с друзьями, семьёй, узнавать о бизнесе, который им интересен. Женщины рассказали о том, как Facebook открыл им двери в мир, который раньше был бы недоступен». Facebook помогает предпринимательницам из Аравии экспортировать товары за рубеж.

«Пропущенные звонки» в Индии тоже способ рекламы

В Индии и в других развивающихся странах люди часто звонят друзьям и близким и вешают трубку, не дожидаясь ответа. Так они приветствуют друг друга, сообщают, что всё благополучно или просят перезвонить. Это способ сэкономить деньги на телефоне. В 2014 г. Facebook запустила в Индии проект

«Пропущенный вызов». Индийский пользователь видит рекламу в Facebook со своего телефона и получает возможность нажать на иконку «Пропущенный вызов» в нижнем углу сообщения. В ответном звонке от рекламодателя он услышит, например, музыку, результаты игры в крикет или голосовые сообщения от знаменитостей.

Ближневосточные пользователи – самые большие поклонники групп в Facebook

Группы в Facebook существуют давно и больше походят на доски объявлений. Многие пользователи по всему миру перестали ими пользоваться, когда Pages стало ведущим способом следить за звёздами, музыкантами, фильмами или брендами. Однако люди с Ближнего Востока по-прежнему остаются поклонниками групп в Facebook. Н. Мендельсон призывает учитывать эту особенность в общении с аудиторией из этого региона.

Видео смотрят даже те, у кого медленный Интернет

Более 50 % пользователей Facebook в Великобритании, Израиле и ОАЭ просматривают видео с сайта Facebook ежедневно. Между тем на Ближнем Востоке люди потребляют больше видео из расчёта на человека, чем любой другой регион в мире, сообщает вице-президент Facebook. Недавно соцсеть представила новую функцию, она позволяет рекламодателям ориентировать/таргетировать фото- или видеоролики с рекламой на мобильных пользователей в зависимости от устройства и скорости соединения. Nestle Everyday недавно провела кампанию в Индии, которая работала как на сельских жителей (фотореклама), так и на городское население (видеореклама). Facebook заявляет, что по сравнению с другими подобными кампаниями бренда в регионе эта подняла уровень узнаваемости марки на 9 %, а покупательское намерение – на 5 % ***(Как используют соцсети на Ближнем Востоке и в Африке // InternetUA (http://internetua.com/kak-ispolzuuat-socseti-na-blijnem-vostoke-i-v-afrike). – 2015. – 24.06).***

***

В ближайшие месяцы все инструменты таргетинга в Facebook будут доступны для рекламодателей Instagram. Об этом заявила вице-президент социальной сети К. Эверсон на международном фестивале креативности Cannes Lions 2015, сообщает searchengines.ru

Таким образом, для рекламодателей покупка рекламы в Instagram, нацеленной на конкретные сегменты аудитории, станет проще. Для пользователей реклама в сервисе фотошеринга станет более релевантной их интересам.

В настоящее время рекламодателям Instagram доступен только таргетинг по полу, возрасту и стране. После того как они смогут интегрировать информацию из пользовательских профилей в Facebook, реклама станет более релевантной и, предположительно, эффективной. С учётом этого, Facebook сможет взимать за неё более высокую плату.

Интеграция данных Facebook «должна обеспечить более высокий коэффициент возврата инвестиций, поскольку маркетолог достигает пользователя, который на самом деле заинтересован», – комментирует предстоящее нововведение К. Эверсон.

В настоящее время аудитория Instagram составляет более 300 млн пользователей в месяц и 200 млн активных пользователей в день.

По оценкам аналитиков Canaccord Genuity, в 2016 г. доход Instagram достигнет 1,2 млрд дол., к 2018 г. – около 4 млрд дол.

Аналитики Raymond James, прогнозируют 500 млн дол. дохода в 2015 г.; 1,1 млрд дол. в 2016 г.; 2 млрд дол. в 2017 г. ***(Facebook откроет доступ к таргетингу для рекламодателей Instagram // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43785/118/lang,ru/). – 2015. – 23.06).***

***

Facebook догоняет YouTube на рынке видеорекламы

В 2015 г. число просмотров видео в Facebook составит две трети просмотров в YouTube – два триллиона против трёх соответственно, сообщается в отчёте Ampere Analysis. В целом, оба сервиса имеют сопоставимое число пользователей в месяц. Об этом пишет searchengines.ru

Специалисты Ampere опросили 10 тыс. интернет-пользователей в Европе и Северной Америке и выявили, что 15 % респондентов просматривали видео в Facebook в прошлом месяце. У YouTube дела обстоят хуже: из тех, кто смотрел видео в Facebook, 16,67 % в указанный период не смотрели ничего в YouTube.

Facebook всё ещё предстоит длинный путь, чтобы догнать YouTube по числу просмотров. Однако аудитория социальной сети растёт, и часть пользователей переходит из видеохостинга.

Платформа Facebook располагает значительными возможностями. Зрителями видео в социальной сети являются зарегистрированные и авторизированные пользователи, что говорит о том, что компания обладает большим количеством их данных. Рекламодатели в свою очередь могут использовать эту информацию для таргетинга на нужные сегменты аудитории.

В отличие от YouTube, Facebook пока не предлагает видеорекламу формата pre-load (ролик, который проигрывается перед основным видео). Рекламные видео в социальной сети появляются после основного контента. Кроме того, компания начисляет плату за просмотр видеорекламы после трёх секунд показа, а в YouTube это время больше.

Тем не менее, несмотря на эти недостатки, обе платформы имеют сопоставимые рекламные показатели. Это свидетельствует о том, что рекламодатели действительно ценят аудиторию Facebook.

«Масштаб обоих игроков говорит о том, что быстрой победы не будет ни для одной из сторон. На горизонте – годы конкуренции», – отметил директор по исследованиям Ampere Р. Бротон.

«С точки зрения потребителей, объём видеорекламы на обеих платформах увеличится», – добавил руководитель ***(Facebook догоняет YouTube на рынке видеорекламы // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43782/118/lang,ru/). – 2015. – 23.06).***

***

Twitter установил новый стандарт видимости видеорекламы

Twitter запустил автоматическое воспроизведение видео для всех пользователей. Теперь видеозаписи, шестисекундные ролики Vine и GIF-анимацию можно просматривать прямо в ленте. Функция уже работает на сайте Twitter.com и в мобильном приложении для iOS. Пользователи Android смогут воспользоваться ею в ближайшее время.

Сервис микроблогов начал тестировать автоматическое проигрывание рекламных видеороликов в ленте еще в марте текущего года. Тестирование проходило в ограниченном масштабе на iOS-устройствах.

До этих пор пользователи запускали встроенные в твиты видеоролики вручную. Теперь видео воспроизводится автоматически во время просмотра ленты твитов. По умолчанию звук будет выключен, а при клике по ролику он включится, и запись продолжит воспроизведение в режиме расширенного просмотра. Звук также появляется при переводе видео в ландшафтный режим.

Пользователи могут сами выбирать удобный режим просмотра. Автоматическое проигрывание видео можно отключить и вернуться к воспроизведению видеозаписей по клику. Можно также выбрать режим, при котором видео будет автоматически проигрываться, только если пользователь подключен к Интернету через Wi-Fi. При медленном соединении сервис сам переключится на режим воспроизведения по клику.

В связи с запуском Twitter установил новый порядок оплаты рекламодателями видеорекламы. Теперь компания будет взимать плату за видео, 100 % которого находилось в поле зрения на устройстве пользователя не менее трех секунд. Такая же продолжительность видео считается стандартом видимости в Facebook.

В текущем году Twitter усовершенствовал возможности использования видео в микроблогах. Теперь пользователи могут напрямую загружать в твиты 30-секундные видеозаписи, снятые на камеру смартфона, а также встраивать в сообщения 6-секундные ролики Vine и GIF-анимацию ***(Twitter установил новый стандарт видимости видеорекламы // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_ustanovil_novyy_standart_vidimosti_videoreklamy). – 2015. – 23.06).***

***

Семь любопытных фактов о социальных сетях

Когда лучше всего расшаривать материалы? Все еще думаете, что Facebook – самая популярная соцсеть в мире? Эксперты из Buffer собрали

результаты нескольких исследований, которые ответят на эти вопросы и заставят удивиться. Читаем внимательно.

1. Вы охватите большую аудиторию поздно вечером или ночью.

Компания Chartbeat опубликовала результаты исследования, целью которого было отследить влияние постинга в соцсетях на трафик изучаемых сайтов. Результаты показали, что количество расшариваний и трафик возрастали рано утром, достигали пика в середине дня и сокращались вечером. Однако важно обратить внимание на то, в какое именно время каждый из показателей достигает максимума. Так, трафик из соцсетей оказался выше с 15 ч. до 1 ч. после полуночи.

2. Вовлеченность в Instagram выше, чем в Facebook и Twitter.

В апреле 2015 г. компания Locowise изучила 2500 профилей в Instagram на предмет работы различных маркетинговых ходов и приемов. В ходе исследования выяснилось, что вовлеченность пользователей соцсети в разы выше, чем в Twitter и Facebook.

В среднем, процент вовлеченности в одном посте в Instagram равнялся 2,81 %. В Facebook этот показатель равнялся 0,25 %, в Twitter – 0,21 %.

3. Самые активные пользователи – в Instagram.

Специалисты из Quintly проанализировали 5000 аккаунтов в Instagram и выяснили, что аудитория соцсети невероятно активна. Активность рассчитывалась методом деления количества лайков и комментариев за пост на общее количество подписчиков аккаунта. Оказалось, что показатель активности на 100 подписчиков в Instagram равняется 4,8, в то время как в Facebook эта цифра составила всего 0,72.

4. Facebook – не самая популярная соцсеть.

Исследование, проведенное компанией Global Web Index с целью изучить, как интернет-аудитория использует соцсети, показало, что пользователи чаще посещают YouTube, а не Facebook. Также выяснилось, что у YouTube и Twitter гораздо больше посетителей, чем активных пользователей.

В ходе исследования также выяснилось, что Twitter используют в основном для чтения новостей, а в Facebook предпочитают «лайкать» посты друзей и интересных страниц.

5. Бренды не отвечают на 5 из 6 сообщений в соцсетях.

Компания Sprout Social решила исследовать, как быстро брендовые страницы отвечают на пользовательские сообщения. Оказалось, что бренды стали делать это гораздо быстрее, в сравнении с 2013 г., но процент сообщений, оставшихся без ответа, достаточно велик.

6. Маркетологи заинтересованы в Twitter, YouTube и LinkedIn.

Эксперты из Social Media Examiner расспросили 3700 маркетологов об их планах и стратегиях. В ходе опроса выяснилось, что для них Facebook является лучшей рекламной площадкой. Помимо этого стало известно, что:

Три из четырех маркетологов планируют использовать больше видео в своей работе.

Большинство маркетологов не уверены, что их стратегии в Facebook эффективны.

Опрошенные маркетологи назвали Facebook и LinkedIn самыми важными соцсетями в своей работе.

7. Количество ретвитов возрастет, если добавить картинки.

Исследование, проведенное компанией Stone Temple Consulting, показало, что при добавлении картинки к твиту, вероятность его репоста возрастает в два раза. Аккаунты, имеющие мало подписчиков, смогут увеличить ретвиты от 5 до 9 раз ***(7 любопытных фактов о социальных сетях // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/7_lyubopytnyh_faktov_o_sotsialnyh_setyah). – 2015. – 26.06).***

***

В сервисе микроблогов Twitter появились посты с рекламой продуктов.

Это начало нового проекта, где Twitter планирует развивать продажи товаров с привлечением знаменитостей и брендов ***(Twitter будет развивать коммерцию // GLAVPOST.COM (http://glavpost.com/post/25jun2015/Nets/48466-twitter-budet-razvivat-kommerciyu.html). – 2015. – 25.06).***

***

Большинство сообщений клиентов компаний в Facebook остаётся без ответа, сообщается в новом отчёте Locowise.

Специалисты аналитического сервиса Locowise изучили более 900 публичных страниц и выявили, что клиентский сервис компаний в Facebook – неудовлетворительный.

Наиболее впечатляющим результатом исследования оказался тот факт, что 87 % обращений клиентов остаются вообще без ответа. При этом компании, отвечающие на вопросы клиентов на своей странице в Facebook, делают это выборочно, откликаясь только на 37 % всех постов.

Из тех компаний, которые отключили возможность публикации постов на своих страницах, 65 % не отвечают на любые сообщения клиентов.

С другой стороны, если компании отвечают на вопросы клиентов, они делают это быстро. По всем компаниям, отвечающим на обращения клиентов в Facebook, 33 % ответов поступили в течение 60 минут после публикации вопроса; 12 % – в период от 1 до 2 часов; 15 % – от 2 до 4 часов.

Как отмечают специалисты Locowise, полученные данные дают компаниям информацию о текущем состоянии клиентского сервиса в Facebook. Если организация относится к числу 87 % компаний, не отвечающих на обращения клиентов, её сотрудникам следует рассмотреть вопрос организации обработки сообщений или же вообще отключить возможность публикации постов на странице ***(Locowise: Компании игнорируют 87 % обращений клиентов в Facebook // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/locowise_kompanii_ignoriruyut_87_obrascheniy_klientov_v_facebook). – 2015. – 30.06).***

***

Глобальная социальная сеть Facebook начала поощрять публичные страницы компаний специальным значком, символизирующим оперативность откликов на публикации и вопросы подписчиков.

Новая иконка присваивается корпоративным аккаунтам, администраторы которых успевают отвечать на 90 % запросов в течение 5 минут после их поступления. Если это условие соблюдается в течение недели, значок прикрепляется к обложке профиля.

В информационной панели, доступной только владельцам страниц, в отдельной графе также появилась оценка скорости и объема ответов на пользовательские сообщения. Таким образом администраторы могут узнать, какие усилия им нужно приложить, чтобы активировать значок.

В социальной сети считают, что индикатор скорости отклика поможет брендам, которые оперативно реагируют на пользовательский фидбек, привлечь больше лояльной аудитории, и заодно простимулирует «медлительных» ***(«Фейсбук» стимулирует бренды быстрее отвечать пользователям // Состав.ру (http://sostav.ua/publication/fejsbuk-stimuliruet-brendy-bystree-otvechat-polzovatelyam-67323.html). – 2015. – 25.06).***

***

Facebook запустила приложение «Менеджер рекламы» (Ads Manager) для Android, чтобы маркетологи могли на ходу создавать и отслеживать кампании.

Приложение позволяет создавать новые объявления с текстом и изображениями, редактировать существующие объявления и настраивать выбранные настройки аудитории и бюджет.

Кроме того, приложение присылает уведомления о том, что срок размещения объявления подходит к концу или превышен доступный лимит затрат. Также с его помощью можно узнать, сколько денег на рекламу было потрачено.

Android-приложение ничем не уступает iOS-версии «Менеджера рекламы», запущенной в феврале ***(Facebook запустил «Менеджер рекламы» для Android // Likeni.RU (http://www.likeni.ru/events/Facebook-zapustil-Menedzher-reklamy-dlya-Android/). – 2015. – 30.06).***

***

Администрация сервиса обмена фотографиями Instagram обновила мобильное приложение, добавив новые возможности для рядовых пользователей и маркетологов.

Для начала в версии 7.0 была полностью переделана вкладка «Поиск и интересное». Здесь пользователи отныне могут подбирать себе новые материалы с популярными хэштегами, местами и актуальными подборками фото и видео. Коллекции составляются командой Instagram и посвящены людям, природе, архитектуре и многому другому.

Специалисты считают данное решение более чем удачным, поскольку сами пользователи зачастую не хотят тратить часы на просмотр тысяч фотографий ежедневно.

Выборки «лучших из лучших», позволяющие включать в них ориентированную на аудиторию рекламу, дают брендам возможность получать практически гарантированный отклик от потенциальных покупателей.

В сервисе заработал улучшенный поиск, чтобы искать и рассматривать во всех подробностях кадры с мероприятий, путешествий и т. д. Встроенная функция «Лучшее» позволяет искать среди людей, локаций и хэштегов одновременно.

Рекламодатели получили от Instagram полный набор таргетирования материалов благодаря интеграции с Facebook – заинтересованные пользователи увидят только релевантные объявления.

В свою очередь, введение функции Shop Now чтобы прямо из Instagram оформить покупку понравившегося бренда призвано повысить продажи компаний и упростить жизнь покупателям, которые хотели бы приобрести увиденные на фото товары или услуги.

Принимая во внимание рост индустрии электронной коммерции, новая система существенно улучшит процесс трансформации «последователей» в «покупателей» брендов в социальной сети ***(Instagram добавил новые инструменты для пользователей и рекламодателей // Блог Imena.UA (http://www.imena.ua/blog/instagram-new-for-users-ads/). – 2015. – 30.06).***

***

«ВКонтакте» запустив платні пости в стрічці. Про це розповів генеральний директор соцмережі Б. Добродєєв, передає Еспресо.TV із посиланням на «Газету.ру».

На відміну від реклами в групах, промопости будуть вбудовуватися безпосередньо в стрічку користувача незалежно від того, чи підписаний він на паблік з близькою тематикою. Зовні рекламний пост буде схожий на звичайний, однак він буде позначений як реклама. Подібне нововведення націлене на збільшення виручки Mail.ru Group від соціальної мережі.

Поки подібний формат реклами доступний тільки в десктопній версії, надалі планують ввести його і в мобільний додаток «ВКонтакте» ***(«ВКонтакте» запустив платні пости в стрічці // Еспресо.TV (http://espreso.tv/news/2015/07/02/quotvkontaktequot_zapustyv_platni_posty_v_strichci). – 2015. – 2.07).***

***

Pinterest запустил анонсированные месяц назад пины с возможностью покупки. Новый функционал доступен пользователям iOS-устройств в США, а позже будет выкачен и для Android. Пользователи смогут приобретать товары прямо в приложении, пишет likeni.ru.

В настоящее время сервис предлагает около 30 млн пинов с возможностью покупки. Новые пины появятся в ленте, на досках, в результатах поиска и будут включать в себя цену товара и кнопу «Купить».

В меню приложения для iOS теперь есть категории Shop и Shop our picks, отображающие пины с возможностью покупки. В категорию Shop войдут новые пины, а в категорию Shop our picks войдут пины, отобранные Pinterest «вручную».

Товары в приложении можно будет приобрести с помощью кредитной карты или Apple Pay.

Для того чтобы найти пины от конкретной компании, пользователю нужно будет посетить профиль нужной компании и нажать на кнопку Shop Pins, расположенную справа ***(Pinterest объявил о запуске пинов с возможностью покупки // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43861/118/lang,ru/). – 2015. – 1.07).***

***

Facebook работает над созданием новых форматов мобильной рекламы. Новый функционал призван обеспечить лучший опыт для пользователей и более высокую эффективность рекламы. Об этом рассказал директор по продуктам Facebook К. Кокс в интервью The Wall Street Journal.

Компания презентует новинки на международном фестивале креативности Cannes Lions 2015.

Ранняя версия нового функционала предлагает возможность создания брендированной интерактивной рекламы в Facebook, которая включает полноэкранное видео, информацию о продукте и другой контент.

«Вы увидите много новых интеракций на мобильных устройствах. Мы пытаемся определить некоторые из этих трендов и представить, как они будут выглядеть несколько лет спустя», – заявил К. Кокс во время интервью.

Предстоящий запуск – попытка привлечь рекламные доллары от крупных брендов, использующих в основном ТВ-рекламу для продвижения своих товаров.

К. Кокс отметил, что новый функционал – ответ на запросы рекламодателей, которые заинтересованы в предоставлении более богатого и интерактивного опыта на мобильных устройствах. Facebook хочет создать такие форматы рекламы, которые выглядят естественно на смартфонах и используют возможности этого типа устройств для привлечения внимания пользователей по мере прокрутки ими новостной ленты.

Новые форматы мобильной видеорекламы помогут маркетологам более эффективно доставлять свои сообщения до целевой аудитории. Они также дадут возможность специалистам, работающим в области маркетинга прямого отклика, лучше презентовать свои продукты. Например, используя интерактивные карусели.

По словам К. Кокса, перед запуском нового функционала Facebook планирует протестировать его на небольшой группе рекламодателей, а затем доработать его, исходя из полученной обратной связи.

Кроме того, компания также намерена разрабатывать рекламные продукты, предназначенные специально для развивающихся рынков. Как известно, они характеризуются более высокой стоимостью данных и медленным интернет-соединением.

«Мы пытаемся стать отраслевым лидером в предоставлении отличного опыта для сетей и устройств с ограниченными возможностями», – отметил К. Кокс ***(Facebook анонсировал новые форматы мобильной рекламы // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_anonsiroval_novye_formaty_mobilnoy_reklamy). – 2015. – 2.07).***

***

Twitter добавил в свои мобильные приложения возможность контролировать и корректировать рекламные кампании прямо на ходу.

Некоторые пользователи уже заметили графическую иконку в своем профиле в мобильном приложении. Нажатие на иконку переносит пользователя в интерфейс Twitter Ads, где показаны результаты рекламной кампании, вовлеченность, общие расходы, стоимость вовлечения и уровень вовлеченности.

Также нововведение позволяет корректировать бюджеты и ставки и менять сроки кампании прямо в приложении. Однако новые кампании могут быть запущены только через веб-интерфейс на ads.twitter.com.

По словам представителя Twitter, в настоящее время функция находится на этапе тестирования ***(Рекламный кабинет Twitter стал доступен на мобильных приложениях // LIKENI.RU (http://www.likeni.ru/events/Reklamnyy-kabinet-Twitter-stal-dostupen-na-mobilnykh-prilozheniyakh/). – 2015. – 2.07).***

***

Соцсеть Facebook запускает новую опцию для рекламодателей, взимая плату за ролики, которые пользователи посмотрели хотя бы 10 секунд. В настоящее время бренды платят за то, что пользователи пролистнули видео или бегло просмотрели его в новостной ленте. 10-секундный порог позволит сети дороже продавать рекламную возможность, так как рекламодатели получат гарантию, что хотя бы часть видео была просмотрена. Платформа к тому же начинает делиться доходами с некоторыми создателями видео. Принцип такой же, как и на YouTube: 55 % получит создатель видео, а 45 % Facebook. По словам вице-президента по сотрудничеству Д. Роза, «партнеры будут размещать больше контента, если выиграют от дистрибуции и к тому же заработают» ***(Facebook поделится доходами с авторами контента // Marketing Media Review***

(http://mmr.ua/show/facebook_podelitsya_dohodami_s_avtorami_kontenta_). – 2015. – 2.07).

***

Twitter обновил панель сведений об аудитории (Audience Insights) и представил рекламодателям усовершенствованный способ таргетинга демографических групп (Persona Targeting).

Панель сведений об аудитории предоставляет данные о доходах и интересах пользователей, а также о поведении покупателей. Бренды могут применять эти данные для своих рекламных кампаний с учетом аудитории. Демографическую информацию Twitter собирает с помощью партнеров – Datalogix и Acxiom – и отображает без указания идентификации отдельных пользователей.

Менеджер Twitter по продукту Э. Брэгдон объясняет:

«Обновление поможет вам лучше понять, кого вы достигаете с помощью ваших рекламных кампаний. В вашей панели кампании вы можете просто кликнуть «Посмотреть сведения об аудитории», чтобы больше узнать о вашей платной аудитории, а затем использовать эту информацию для оптимизации таргетинга и рекламного контента.

Вы также можете легко сравнить данные достигнутой и вовлеченной аудитории. Ваша достигнутая аудитория – пользователи, которые просматривают вашу кампанию; ваша вовлеченная аудитория – пользователи, которые активно взаимодействуют с вашими объявлениями (отвечают, запоминают в избранном и размещают ретвиты).

Если у вас включено отслеживание конверсий, сведения о кампании покажут вам больше информации о пользователях, которые конвертировались в прошлом. Вы даже можете сравнить сведения о достигнутой и конвертированной аудитории для выявления новых способов контакта с аудиторией, наиболее склонной к конвертированию».

Twitter также добавил новую функцию фильтрации в панели сведений, которая содержит уточненные категории аудитории: родители, поколение Миллениума, малый бизнес, выпускники колледжей и т. д. Рекламодатели могут таргетировать категории непосредственно в панели.

«У вас также есть возможность добавить дополнительные типы таргетинга для уточнения своей аудитории, – написал Э. Брэгдон. – Например, если вы хотите достичь поколение Миллениума, которое использует iOS, вы можете просто выбрать Millennials и iOS в качестве мобильной платформы, чтобы узнать больше об этой конкретной группе пользователей».

Сведения о кампаниях доступны по всему миру для всех рекламодателей Twitter. Возможность таргетирования по уточненным группам пользователей ограничена территорией США.

Twitter представил новый инструмент аналитики «Сведения об аудиториях» (Audience Insights) в конце мая текущего года. Нововведение призвано помочь маркетологам лучше понимать свою аудиторию в социальной

сети ***(Twitter обновил сведения об аудиториях и запустил таргетирование на уточненные группы пользователей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_obnovil_svedeniya_ob_auditoriyah_i_zapustil_targetirovanie_na_utochnennye_gruppy_polzovateley). – 2015. – 7.07).***

***

Согласно исследованию, проведенному командой Acquity Group – подразделения крупной американской компании Accenture Interactive – которая опросила 2000 респондентов в США, потребители считают Facebook самым авторитетным источником контента, создаваемого брендами и бизнесом.

У интернет-пользователей спросили об их привычках и предпочтениях в сфере диджитал-медиа. Среди прочих каналов, таких как ТВ, email, новостные ресурсы, социальная сеть показала самое высокое значение по шкале доверия, опередив Instagram, Pinterest, Twitter и Snapchat, при этом в самом «низу» оказались YouTube и блогохостинги.

Исследователи выяснили, что молодое поколение в большей степени склонно доверять информации в социальных сетях. Так, из всех опрошенных респондентов, 29 % пользователей от 18 до 22 лет и 32 % миллениалов (23–30 лет), признались, что Facebook лидирует в их иерархии надежных social media источников, в то время как только 16 % бэби-бумеров (возрастная категория 52–68 лет) ответили так же.

Остальные покупатели сказали, что до сих пор предпочитают доверять традиционным медиа, таким как печатная пресса (27 %) или даже онлайн-новости (20 %). В целом 23 % опрошенных подтвердили, что на них оказывает влияние брендированный контент.

Несмотря на высокие показатели пользовательского доверия, social media все еще отстает от других каналов в покупательском намерении и реальных покупках. Эксперты Acquity обнаружили, что реклама на ТВ и в печатных СМИ до сих пор является главным драйвером рынка по привлечению новых клиентов ***(Покупатели больше всего доверяют брендам на «Фейсбуке» // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/pokupateli_bolshe_vsego_doveryayut_brendam_na_feysbuke). – 2015. – 8.07).***

***

Facebook перестанет брать плату с рекламодателей за лайки. Теперь, покупая рекламу на основе цены за клик (или CPC), компании будут платить за переход пользователя по ссылке на приложение или вебсайт. В случае лайка, комментария или шейра пользователя, цена за рекламный пост взиматься не будет. Скорее всего, цена за клик увеличится, но вырастет и ROI. В целом, рекламодатели позитивно оценивают этот шаг сети ***(Facebook перестанет брать плату с рекламодателей за лайки // Marketing Media Review (http://mmr.ua/show/_facebook_perestanet_braty_platu_s_reklamodateley_za_layki_). – 2015. – 9.07).***

***

Facebook обновила панель администрирования страниц, добавив новый раздел «Видео» (Videos). Администраторы страниц получат доступ к информации о просмотрах, самых популярных роликах за определенный период времени, а также к данным о видеороликах, которые были добавлены с других страниц.

Рекламодатели смогут быстро переключаться между органическими и платными, общими и уникальными типами просмотров, автопроигрываемыми видео и теми, что требуют нажатия кнопки воспроизведения.

Функция будет выкачена для рекламодателей по всему миру в течение нескольких недель ***(Facebook расширил статистику видеозаписей для публичных страниц // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_rasshiril_statistiku_videozapisey_dlya_publichnyh_stranits). – 2015. – 6.07).***

***

Facebook: как улучшить органический охват страницы

Сооснователь ресурсов KISSmetrics и CrazyEgg Н. Патель опубликовал инфографику, которая призвана помочь владельцам страниц в Facebook увеличить их органический охват.

По данным агентства Ogilvy, органический охват страниц снизился с 49 % в октябре 2013 г. до 6 % в настоящее время. Основной причиной этого является перенаселенность социальной сети: за внимание пользователей борются более 18 млн бизнес-страниц. Кроме того, Facebook стремится зарабатывать на рекламе.

Увеличить охват поможет:

1. Анализ стратегий компаний из списка Fortune топ-100. Такие компании обычно:

– показывают, что происходит внутри компании;

– демонстрируют доступность для пользователей и подписчиков для охвата и взаимодействия с компанией;

– создают положительный пользовательский опыт.

2. Размещение сообщений в непиковое время (с 22:00 до 3:00), так как в пиковое время (с 6:00 до 15:00) сообщение в новостной ленте быстро затеряется среди других.

Чтобы найти собственное пиковое время бизнес-страницы, следует воспользоваться инструментом статистики Facebook Insights.

3. Регулярная публикация фотографий команды в нерабочей обстановке.

4. Вовлечение пользователей с помощью вопросов, которые не подразумевают продвижение или продажу товаров.

5. Публикация поясняющих фотографий и инфографики.

Использование Facebook для анализа подписчиков помогает получить сведения для роста охвата. Например, с помощью Facebook Insights Н. Патель

обнаружил, что большинство его подписчиков посещает его страницу в 13:00. По этой причине большинство обновлений публикуется именно в этом время.

При этом для анализа успешности бизнес-страницы Н. Патель рекомендует использовать не охват, а трафик и объем продаж из Facebook.

Данные отчёта аналитической компании SocialBakers за период с октября 2014 по февраль 2015 г. показали, что фотопосты – самый худший способ получения значительного органического охвата публикаций на бизнес-страницах в Facebook.

Компании, продвигающиеся на Facebook должны уделять максимум внимания качеству контента, не размещать его слишком часто и не переполнять рекламой. Сообщения на странице должны быть интересными и информативными. При этом продвигать за деньги следует лишь самые интересные сообщения ***(Facebook: как улучшить органический охват страницы // Sostav.ua (http://sostav.ua/publication/facebook-kak-uluchshit-organicheskij-okhvat-stranitsy-67430.html). – 2015. – 6.07).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Ученые из Университета Южной Калифорнии обнаружили в социальных сетях «эффект большинства». Он заключается в том, что некоторая информация может казаться широко распространенной нормой для большинства пользователей, тогда как на самом деле она представлена лишь среди небольшого числа популярных аккаунтов. Подробности исследования приведены в препринте на arXiv.org.

Авторы строили искусственные социальные сети с заданными параметрами распределения числа связей. Некоторым узлам сети (аккаунтам) присваивался бинарный атрибут, например «владеет iPhone/не владеет iPhone». После этого ученые следили за тем, как информация об этом распространяется по сети.

В том случае, когда атрибут присваивался узлам с большим числом связей, оказалось, что большинство других узлов в среднем считала его «нормой». При том, что в общем по сети его распространенность была мала.

При исследовании реальных социальных сетей оказалось, что в них наблюдаются аналогичные явления. Эффект большинства пропадал только тогда, когда среди узлов сети не было большого различия по числу связей, чего практически никогда не наблюдается в реальном случае.

Авторы отмечают, что эффект близости не зависел от конкретной топологии сети, а определялся лишь тем, от каких узлов поступала исходная информация. По мнению ученых, эффект большинства может представлять определенную опасность, так как из-за него те идеи, которые на самом деле присущи меньшинству, могут выглядеть в глаза большинства нормой. Например, подростки могут посчитать пристрастие к алкоголю нормой среди своих друзей, хотя на самом деле лишь небольшое число популярных персонажей обладают этим атрибутом.

Эффект большинства во многом схож с «эффектом друга», хорошо известным в статистике. Согласно нему, для большинства аккаунтов в социальных сетях число друзей будет меньше, чем среднее «число друзей у друзей». Такой перекос возникает из-за того, что одни и те же популярные аккаунты с большим числом друзей и подписчиков оказывают слишком большое влияние на статистику для каждого отдельно взятого аккаунта ***(«Мнение большинства» в социальных сетях оказалось иллюзией // InternetUA (http://internetua.com/mnenie-bolshinstva--v-socialnih-setyah-okazalos-illuaziei). – 2015. – 3.07).***

***

Ученые определили, что во время просматривания Facebook-ленты зрачки испытуемых расширялись – это может свидетельствовать о том, что они испытывали чувство счастья. Ну, или это уже связано с некой зависимостью, пишет «Обозреватель» (http://tech.obozrevatel.com/hi-tech/85961-sotsialnaya-zapadnya-pochemu-lyudi-lajkayut-kommentiruyut-i-postyat-v-facebook.htm).

Психологи проделали большую работу и определили основные моменты нахождения в социальных сетях. Почему пользователи что-то лайкают, комментируют и шерят, а что-то – нет?

Ученые виделяют несколько причин поставить лайк:

– быстрый и простой способ выразить одобрение;

– подтвердить какую-то информацию, имеющую к нам отношение;

– выразить виртуальную поддержку;

– из практических соображений. Например, лайкают статусы известных брендов и посты с купонами.

Публикация и чтение комментариев приносят больше положительных эмоций пользователям. К тому же постинг уменьшает чувство одиночества.

Инфографику исследования можно посмотеть на сайте ***(Социальная западня: почему люди лайкают, комментируют и постят в Facebook // Обозреватель (http://tech.obozrevatel.com/hi-tech/85961-sotsialnaya-zapadnya-pochemu-lyudi-lajkayut-kommentiruyut-i-postyat-v-facebook.htm). – 2015. – 23.06).***

***

Что делают пользователи в Facebook

Практически половина пользователей Facebook заходят на сайт, чтобы просто посмотреть новости в ленте, не публикуя и не комментируя ничего самостоятельно. К такому выводу пришла компания GlobalWebIndex, задав пользователям соцсети простой вопрос – «Что вы делаете в Facebook?».

Самые популярные действия:

– нажимают кнопку «Мне нравится» – 68 % всех пользователей;

– отправляют сообщения друзьям – 54 % пользователей;

– читают статью – 52 % пользователей;

– комментируют фото и видео друзей – 52 % пользователей;

– просто заходят в соцсеть, чтобы узнать, произошло ли что-нибудь интересное – 47 % ***(Что делают пользователи в Facebook // LIKENI.RU (http://www.likeni.ru/events/Issledovanie-chto-delayut-polzovateli-v-Facebook/). – 2015. – 24.06).***

***

По данным, полученным от ВЦИОМ, стало известно, что большинство россиян заходят в Интернет только ради социальных сетей «ВКонтакте» и «Одноклассники». Социологам удалось установить частоту выхода в глобальную сеть ради социальных сетей.

Как оказалось, более 50 % опрошенных заходят в Интернет, чтобы пообщаться с друзьями в известных социальных сетях. Наибольшей популярностью среди россиян пользуются российские социальные сети «ВКонтакте» и «Одноклассники».

По данным опроса, всего 15 % пользователей глобальной сети Интернет не посещают социальные сети. В опросе приняли участие 1600 человек со всей России ***(Россияне выходят в Интернет ради «ВКонтакте» и «Одноклассников» // Газетёнка (http://gazetenka.com/news/tech/Rossiyane_vykhodyat_v_Internet_radi_VKon_4227/). – 2015. – 26.06).***

Маніпулятивні технології

Секретар РНБО РФ процитував фразу, яку поширили в Інтернеті тролі Кремля. Він заявив, що США нібито хотіли б, щоб Росії і зовсім не існувало.

Про це на сторінках Gazeta Wyborcza пише В. Радзівіновіч.

За словами секретаря РНБО Росії М. Патрушева, американцям нібито заздрісно з того, що саме росіяни володіють такою великою кількістю природних багатств.

«Ви, напевно, пам’ятаєте слова колишнього Держсекретаря США М. Олбрайт про те, що Росії не належить ні Сибір, ні її Далекий Схід», – сказав М. Патрушев. Проте журналісти заперечили, оскільки одразу почали шукати, коли ж це вона таке сказала.

Як виявилося, ніколи. Цю фразу присвоїли колишньому Держсекретареві США і поширили в Інтернеті тролі Кремля.

В. Радзівінович іронізує, що, можливо, примітивні писаки-пропагандисти і не придумали цитату «підступної баби з США». Оскільки ще в 2006 р. тодішній глава ФСБ генерал-майор Б. Ратников розповів державній «Російській газеті», що «чекісти сканували думки М. Олбрайт».

«В думках пані Олбрайт ми виявили патологічну ненависть до слов'ян. А ще її ображало те, що Росія володіє найбільшими у світі запасами корисних копалин. Вона б хотіла, щоб у майбутньому російськими запасами володіла не одна країна, а ціла купа народів, які всі будуть підпорядковані США», – розповідав тоді Б. Ратников.

Оглядач продовжив: «І тут виникає складна проблема. Приписав собі генерал чекістів-окультистів вигадки інтернет-тролів Кремля? Чи все сталося навпаки? Може це його люди по секрету розповіли тролям, яку думку треба поширити серед росіян».

«Мене часто питають, чи треба боятися Росії. А я відповідаю, що самої країни не треба. Але боятися варто психічного стану людей, які нею керують і придумують різні жахи, щоб потім самим же в них повірить», – ідеться в статті.

У будь-якому разі від того, що чиновники цитують вигадки з Інтернету, стає дедалі важче зрозуміти, хто кому насправді замилює очі в Росії ***(Gazeta Wyborcza: Російські чиновники почали цитувати інтернет-тролів Кремля // Media Sapiens (http://osvita.mediasapiens.ua/print/1411980895/gazeta_wyborcza_rosiyski_chinovniki_pochali_tsituvati_internettroliv_kermlya/). – 2015. – 25.06).***

***

Лидер каховской ячейки партии «Оппозиционный блок» П. Филипчук продолжает транслировать в Facebook российскую пропаганду.

Вслед за восхищением В. Путиным, П. Филипчук начал репостить экс-нардепа, украинофоба А. Журавко.

Об этом сообщает каховчанка Ю. Зеленчук.

«Пост который перепостил П. Филипчук создал А. Журавко бывший регианал, ярый коллаборационист, сепаратист, поклонник рускава мира и враг Украины, который в настоящее время находится в москве, который ранее принимал участие в митинге в московском Антимайдане с пособниками террористов» – пишет Ю. Зеленчук.

«То что написал товарищ Журавко приложив к посту 13 фото погибших детей, с диким текстом о том, что мы Украинцы убиваем собственных детей, чтобы украинские матери не пускали своих детей убивать, и прочая ересь которую он просит распространять, лично у меня вызывает приступы негодования», – сообщает каховчанка.

Скриншоты репоста можно найти на страницы Ю. Зеленчук в Facebook ***(Лидер каховского оппоблока транслирует антиукраинские месседжи // Мост***

(http://most.ks.ua/news/url/lider_kahovskogo_oppobloka_transliruet_antiukrainskie_messedzhi). – 2015. – 2.07).

***

Итальянские исследователи выяснили, что в социальной сети Instagram 8 % аккаунтов создано для рассылки спама, а 30 % пользователей проявляют активность не чаще одного раза в месяц.

Такие данные могут оказаться помехой при продлении контрактов между рекламодателями и площадками. Первыми являются компании, предоставляющие услуги и продающие товары. Вторыми в этой социальной сети давно стали популярные блогеры.

Сообщая численность своей аудитории, владельцы площадок не делают поправку на спам-ботов и малоактивных пользователей.

Вместе с результатами исследования его авторы опубликовали примененную для выявления ботов методологию. Поведение программ, имитирующих действия реальных пользователей, сводится к публикации пяти-шести видео или фотографий и подписке на 41 пользователя.

Представители Instagram отказались комментировать эту информацию. Однако отмечается, что борьбу с ботами в соцсети начали еще в декабре 2014 г.

8 % выявленных ботов – это остаток от гораздо большей доли, которая была актуальна прошлой зимой. Некоторым создателям ботов с тех пор удалось модифицировать алгоритмы работы таким образом, что теперь их сложно отличить от реальных людей в автоматическом режиме ***(38 % аудитории Instagram составляют боты и неактивные пользователи // iLenta.com (http://ilenta.com/news/internet/news_7294.html). – 2015. – 3.07).***

***

У російській соціальній мережі «ВКонтакте» з’явилася група під назвою «Александрия Радикальная». Судячи з невеликої кількості учасників, група нова, проте її досить активно наповнюють. Переважно фотографіями, іменами та телефонами кіровоградських воїнів, які беруть участь в АТО на Сході України.

В описі групи написано: «ТРИБУНАЛ возмездие настанет. Мы здравомыслящие люди и не сдадим Нашу Родину! Личные данные подававших документы на получение удостоверений участников АТО (подробности в ленте)».

Серед фотоальбомів цієї сепаратистської групи є, наприклад, такі: «Бойцы Кировоградської области. Ликвидированные АТОшники» або «Правий сектор Олександрія» ***(До уваги СБУ: в мережі «ВКонтакте» з’вилася сепаратистська група, в якій викладають фото та телефони кіровоградських воїнів // Весь Кіровоград (http://www.kirovograd.net/shortly/2015/7/3/do_uvagi_sbu_v_merezhi_vkontakte_zvilasja_separatistska_grupa.htm). – 2015. – 3.07).***

***

Російська компанія «Интернет-исследования» з Петербурга, відома як «фабрика тролів», незважаючи на недавні заяви про те, що компанія зараз не має ні офісів, ні штату співробітників, вербує нових працівників.

ТОВ «ГлавСеть» (за даними ЗМІ, юридична особа агентства) дає оголошення про вакансії для веб-програмістів (зарплата від 50 тис. р.), випускових редакторів (від 45 тис. р.), контент-менеджерів (40–50 тис. р.), копірайтерів (від 32 тис. р.). Робота обіцяється поруч зі станцією метро «Старе село».

Раніше на суді з колишньою співробітницею представник організації К. Чернишов заявив, що у компанії зараз немає ні офісу, ні штату. Однак чи звільнили її співробітників, невідомо. До офісу на Савушкіна компанія розміщувалася в Ольгіному, звідки переїхала в жовтні 2014 р.

«Фабрика тролів» зараз судиться зі своєю колишньою співробітницею Л. Савчук, яку звільнили без остаточного розрахунку, дівчина вимагає виплатити їй заробітну плату за лютий і компенсувати моральну шкоду, додає LB.ua.

Компанія «Интернет-исследования» фігурує в низці журналістських розслідувань як один з головних постачальників платних політичних коментаторів у блогах. Крім того, американський журналіст Е. Чен у своєму розслідуванні дійшов висновку, що пітерська «фабрика» може стояти за серією провокацій в американських соціальних мережах. Зокрема, за інформаційними вкиданнями про витік отруйних речовин на хімзаводі у Луїзіані і про нібито епідемію вірусу Ебола ***(Росії бракує тролів // Експрес online (http://expres.ua/news/2015/07/09/142807-rosiyi-brakuye-troliv). – 2015. – 9.07).***

Зарубіжні спецслужби і технології «соціального контролю»

Двох киян, які пропагандували створення так званої «Київської народної республіки» через соціальні мережі, притягнуто до кримінальної відповідальності.

Про це повідомляє офіційний сайт Служби безпеки України.

«1 липня 2015 р. рішенням Святошинського районного суду Києва двох організаторів фейкових “республік” визнано винними у скоєнні злочинів, передбачених ч. 2 ст. 28 ч. 2 ст. 109 Кримінального кодексу. Зловмисників засуджено до п’ятьох років позбавлення волі з випробувальним терміном три роки», – ідеться в повідомленні.

Слідчі СБУ встановили, що молоді люди створили інтернет-спільноту і поширювали через неї символіку фейкових «республік», що демонстративно нагадує ту, яку використовують бойовики «ДНР» та «ЛНР».

«Експертиза підтвердила, що матеріали, які поширювали молодики, містять антиукраїнські заклики до повалення чинного конституційного ладу», – наголошується в повідомленні.

Нагадаємо, про затримання організаторів спільноти «Київська народна республіка» СБУ повідомила наприкінці квітня.

Вони повністю визнали свою провину і відтоді перебували під вартою. 22 червня прокуратура Києва відправила справу в суд.

Відзначимо, що спільнота і далі діє в соцмережі «ВКонтакте» ***(Організатори «Київської народної республіки» отримали умовні терміни // LB.ua http://ukr.lb.ua/news/2015/07/02/309879_organizatori_kiivskoi_narodnoi.html). – 2015. – 2.07).***

***

Співробітники Управління СБ України в Чернігівській області викрили жителя обласного центру, який через соціальні мережі розповсюджував матеріали сепаратистського змісту.

Про це повідомляє прес-група Управління СБ України в Чернігівській області.

Зловмисник, діючи за завданням представників т. з. ЛНР, розміщував у регіональних та загальноукраїнських об'єднаннях соціальної мережі «ВКонтакте» матеріали пропагандистського характеру із закликами до підтримки та фінансування незаконних збройних формувань, що діють на тимчасово окупованій території, поповнення їх лав новими членами та створення на їх основі «збройних сил» незаконного утворення «новоросія». Крім того, вказані публікації підбурювали до проявів національної нетерпимості, сприяли розпалюванню національної ворожнечі, містили заклики до зміни меж території та держаного кордону України. До своїх публікації автор додавав скріншоти з антиукраїнськими написами та гаслами.

За даним фактом слідчими СБУ відкрито кримінальне провадження за ч.2 ст.110 (посягання на територіальну цілісність і недоторканність України) Кримінального кодексу України. За вчинення такого злочину чинним законодавством передбачено покарання у вигляді позбавлення волі на строк від п'яти до 10 років ***(СБУ викрила чернігівчанина, який розповсюджував у соцмережах інформацію сепаратистського змісту // InternetUA (http://internetua.com/sbu-vikrila-csern-g-vcsanina--yakii-rozpovsuadjuvav-u-socmerejah--nformac-ua-separatistskogo-zm-stu). – 2015. – 30.06).***

***

Руководство Европола намерено создать группу экспертов, которые будут отслеживать страницы пропагандистов ИГИЛ в социальных сетях и при поддержке администрации конкретного ресурса блокировать доступ к учетным записям. Об этом сообщает The Guardian.

По данным правоохранителей, в настоящее время террористы ежедневно публикуют порядка 100 тыс. сообщений в Twitter, привлекая таким образом новых участников группировки из других стран. Согласно предоставленной Европолом статистике, в областях Сирии и Ирака, находящихся под контролем «Исламского государства», уже выехало порядка 700 жителей Великобритании. В РФ, по данным российских правоохранителей, этот показатель составляет 1,7 тыс. человек.

Предполагается, что мониторинг европейских силовых структур начнется с 1 июля этого года. При этом конечной целью специалистов станет блокировка доступа к страницам террористов не более чем через два часа после их создания.

Глава Европола Р. Уэйнрайт также отметил, что все работы будут вестись в тесном сотрудничестве с руководством социальных сервисов, однако не стал уточнять о каких именно компаниях идет речь ***(Европол будет отслеживать пропагандистов ИГИЛ в социальных сетях с целью блокировки // SecurityLab.ru (http://www.securitylab.ru/news/473421.php). – 2015. – 22.06).***

***

Американський ПЕН-центр виступив проти вилучення на сайті соцмережі постів і блокування профілів українських і російських противників режиму президента РФ В. Путіна і закликає Facebook своєчасно відновити весь належний контент.

Про це повідомляє «Українська правда».

Оприлюднена на сайті американського центру заява критикує вилучення політично-забарвленого контенту, блокування і скасування облікових записів.

У заяві йдеться про те, що американський ПЕН-центр і Український ПЕН-клуб серйозно стривожені ситуацією з блокуванням у Facebook. Вони також перелічують випадки, що, на їхню думку, свідчать про цензуру.

Так через підозру в «порнографії» заблокували селфі А. Капустіна з губернатором Одещини М. Саакашвілі.

Поет і блогер А. Бондар потрапив під заборону за критику блокування іншого користувача, а О. Ройтбурда у свою чергу заблокували за незадоволення рішенням щодо А. Бондаря.

Серед інших користувачів, які скаржаться на маркування їхніх постів і наступне блокування, є український політик Б. Береза, російський журналіст А. Красовський, російський бізнесмен і блоггер С. Рабинович та ін.

Водночас американський ПЕН-центр не заперечує потреби у фільтруванні образливих повідомлень і сторінок на сайті соціальної мережі. Він схвалює те, що Facebook заохочує поважну поведінку і вилучає образливий вміст. Разом з тим письменницька організація вітає перші кроки в напрямі більшої прозорості цього процесу, особливо коли запити щодо видалення вмісту надходять від урядів.

Як повідомлялось раніше, Facebook-акаунт Т. Березовця заблокували на добу за те, що він поширив пост про українську націю. Того ж дня був

заблокований акаунт народного депутата Б. Філатова, який перепостив повідомлення нардепа Б. Берези. Окрім того, спільнота «УКРОП – Український Опір» була видалена адміністрацією Facebook.

Також 4 червня А. Бондар опублікував критичну колонку, у якій писав про подвійні стандарти Facebook, які змушують думати про те, що позов на її адміністрацію – єдиний вихід із ситуації, що склалася.

10 червня у відповідь на петицію користувачів, у Facebook пояснили, що соцмережа не порушувала власних стандартів, а тому українців блокують виключно в рамках правил.

18 червня Facebook розпочала діалог з українською стороною та пообіцяла ретельніше моніторити український сегмент соцмережі ***(ПЕН-центр США засудив необґрунтоване блокування акаунтів у Facebook, які критикують Путіна // Media Sapiens (http://osvita.mediasapiens.ua/web/social/pentsentr_ssha_zasudiv_neobruntovane_blokuvannya_akauntiv_u_facebook_yaki_kritikuyut_putina/). – 2015. – 22.06).***

***

Сервис Instagram столкнулся с трудностями в Северной Корее. Как сообщают пользователи, они периодически не могут получить доступ к службе в сети единственного местного оператора, предлагающего 3G-связь.

Пользователи Instagram из Северной Кореи сообщают, что видят уведомление о блокировке ресурса при попытках посетить сервис как с настольного компьютера, так и со смартфона. «Внимание! Вы не можете подключиться к этому веб-сайту потому что он находится в черном списке», – гласит надпись, которую увидели жители Пхеньяна, столицы КНДР. Проблемы при выходе со смартфонов наблюдаются у пользователей оператора Koryolink, который является монополистом 3G в стране.

Само правительство не озвучивало инструкций по блокировке, да и сам оператор не извещал об этом пользователей. Как заверили АР представители Koryolink, никаких новых политик касательно Instagram они не вводили. В отдельных случаях, мобильное приложение все еще можно использовать, несмотря на уведомление, однако отправка снимков и просмотр профиля были недоступны в данном случае. Такое положение вещей наводит на мысль, что все-таки какие-то ограничения появились, раз уж проблемы наблюдаются у конкретного оператора.

Что интересно, социальная сеть Facebook, которой и принадлежит Instagram, все еще исправно работает в Северной Корее в целом, и Пхеньяне в частности. Проблемы же с Instagram наблюдаются уже несколько дней. Согласно одной из версий, блокировка сервиса связана с недавним пожаром в отеле столицы, который часто выбирают туристы и иностранные граждане. Именно через Instagram очевидцы распространили фото с места происшествия, которое не было освещено в местной прессе.

Отметим, что специально для туристов была введена программа доступа к популярным сервисам, которые местным жителям социальные сети

практически недоступны, однако теперь в стране, где крайне чувствительно относятся к внутренней информации, это может измениться. Еще 13 июня, сразу после пожара, Koryolink объявили о невозможности предоставлять открытый 3G для иностранцев в связи с «техническими трудностями», но обещали в будущем вернуть данную услугу ***(В Северной Корее начали блокировать Instagram // InternetUA (http://internetua.com/v-severnoi-koree-nacsali-blokirovat-Instagram). – 2015. – 22.06).***

***

Предупреждение россиян о возможных неприятных последствиях поездки в Крым послужило поводом обращения Генпрокуратуры в Роскомнадзор, информирует «Экономические известия» (http://news.eizvestia.com/news_politics/full/653-zablokirovan-dostup-k-rossijskomu-sajtu-razmestivshemu-pamyatku-o-negativnyh-posledstviyah-poezdki-v-krym).

Роскомнадзор сообщил, что операторы связи в России начали блокировать доступ к сайту общества защиты прав потребителей «Общественный контроль» (ОЗПП). Блокировка производится по требованию Генпрокуратуры, которая ранее обратилась в Роскомнадзор. Поводом для этого обращения послужила памятка, в которой ОЗПП предупредила российских граждан о возможных негативных последствиях поездок в Крым.

«В полном соответствии с требованием 398-го федерального закона сайт направлен в выгрузку операторам связи. Производится его блокировка на территории Российской Федерации», – сообщил пресс-секретарь Роскомнадзора В. Ампелонский.

«Памятка для российских туристов, направляющихся на отдых в Крым» была опубликована на сайте ОЗПП 18 июня. В этом документе присоединение Крыма к России названо «юридической фикцией». ОЗПП считает, что по нормам международного права Крым имеет статус оккупированной территории. Во избежание негативных последствий общество советует туристам въезжать на полуостров только с территории Украины, имея разрешение украинских властей. Кроме того, ОЗПП рекомендует не совершать сделки с недвижимостью в Крыму.

22 июня Генпрокуратура потребовала от следственных органов возбудить уголовное дело в связи с публикацией памятки, а также заблокировать доступ к сайту ОЗПП.

С просьбой провести проверку в отношении ОЗПП к Генпрокуратуре обратились Роспотребнадзор и депутат Госдумы М. Дегтярев. Глава комитета Госсовета Крыма по туризму А. Черняк назвал публикацию памятки «чистой воды провокацией» ***(Заблокирован доступ к российскому сайту, разместившему памятку о негативных последствиях поездки в Крым // Экономические известия (http://news.eizvestia.com/news_politics/full/653-zablokirovan-dostup-k-rossijskomu-sajtu-razmestivshemu-pamyatku-o-negativnyh-posledstviyah-poezdki-v-krym). – 2015. – 22.06).***

***

Роскомнадзор хочет заблокировать сайт фонда «Открытая Россия», созданного М. Ходорковским. 25 июня «Открытая Россия» получила от Роскомнадзора уведомление об ограничении доступа к ее сайту как содержащему призывы к экстремистским действиям.

23 июня «Открытая Россия» опубликовала статью «Что ждет российских туристов на пути в Крым: версия ОЗПП и реальность». В статье рассказывается о памятке, появившейся на сайте Общества защиты прав потребителей и предупреждающей россиян о том, что Украина считает Крым своей территорией и поэтому любой, кто приедет туда без разрешения украинских властей, может подвергнуться уголовному преследованию.

В статье объясняется, что реальность отличается от описания в памятке.

«Смешно, когда юридический анализ и советы пугают "правоохранительную" структуру. Мое отношение к прокуратуре России известно – я считаю это ведомство с его нынешней идеологией "служения государю", а не стране, антиконституционным. Мне знакомы и их методы – силовые, а не правовые. Именно поэтому я предложил редакции сайта убрать материал. Надеюсь, все, кому он интересен, успели его скопировать», – прокомментировал ситуацию М. Ходорковский.

Фонд «Открытая Россия» отмечает, что уведомление Роскомназора датировано 22 июня, а памятка Общества защиты прав потребителей появилась в Интернете 23 июня ***(Роскомнадзор хочет заблокировать сайт фонда «Открытая Россия» из-за статьи о Крыме // Крым.Реалии (http://ru.krymr.com/content/news/27093323.html). – 2015. – 25.06).***

***

Відеохостинг YouTube заблокував акаунт російського співака О. Газманова. Технічні проблеми з доступом на сторінку виконавця, творчістю якого неодноразово обурювалася влада Латвії, з'явилися після розміщення на ній кліпу на пісню «Вперед, Россия!» – пише Корреспондент.net з посиланням на видання Super.

«Напередодні Дня Росії не тільки мій кліп, але і весь мій канал просто перекрили. Офіційна відповідь YouTube була такою: йде перевірка моєї причетності до даного відеоконтенту, мого авторства. Але це і так зрозуміло, що я автор всіх кліпів і роликів», – розповів О. Газманов виданню.

За словами артиста, з моменту блокування його акаунта вже минуло два тижні, хоча зазвичай процедура перевірок займає не більше двох днів.

Повідомляється, що 23 червня YouTube остаточно заявив, що не буде відновлювати відеоканал О. Газманова. Росіянин вважає, що в даному випадку, як і в торішній ситуації із забороною в'їзду артисту в Латвію, замішана політика ***(Youtube заблокував сторінку Олега Газманова // Корреспондент.net (http://ua.korrespondent.net/showbiz/music/3531119-Youtube-zablokuvav-storinku-oleha-hazmanova). – 2015. – 23.06).***

***

На сайті українського парламенту оприлюднено текст законопроекту, який спрямований на чергову спробу врегулювати кіберпростір та посилити контроль за інформаційною безпекою в Україні.

Група депутатів від партій «ВО Батьківщина», «БПП» та «Народний Фронт» пропонує створити додаткові законодавчі норми для посилення контр-розвідки та інформаційного контролю за інтернет-простором. Доручити основні функції моніторингу та боротьби з кіберзлочинами запропоновано СБУ та НКРЗІ.

Зокрема, за цим законопроектом українські силовики отримають можливість отримувати доступ до інформації з державних баз даних, а також із БД мобільних операторів, інтернет-провайдерів та телекомунікаційних компаній; проводити обшуки та виконувати функції нагляду. НКРЗІ здобуде функції державного цензора, який зможе виносити рішення щодо блокування окремих сайтів та моніторингу даних про абонентів мобільних операторів. Витрати на блокування, моніторинг та контррозвідку при цьому пропонують здійснювати самим операторам та телекомунікаційним компаніям.

Нагадаємо, це вже не перша спроба подібного контролю за Інтернетом: раніше подібний законопроект (лишень щодо блогосфери) вже розглядався українським парламентом ***(НКРЗІ та СБУ пропонують стежити за українцями в інтернеті та на мобільних телефонах // Imena.UA (http://www.imena.ua/blog/sbu-nkrsi-hackers/). – 2015. – 25.06).***

***

Депутат Законодательного собрания Санкт-Петербурга В. Милонов требует закрыть социальную сеть Facebook на территории России.

Об этом он заявил «Русской службе новостей», добавив, что уже обратится в Роскомнадзор с соответствующим требованием.

По его словам, соцсеть нарушила законодательство России, запустив функцию окрашивания аватара в цвет ЛГБТ-радуги.

«Это грубое нарушение российского законодательства. У Facebook нет возрастных ограничений, невозможно проконтролировать, сколько там несовершеннолетних пользователей. Поэтому совершенно нормальным будет вырубить Facebook на территории России. Тогда они ради их бога – денег, ради которых они готовы продать и родную мать, моментально исправят это», – заявил В. Милонов ***(В России требуют закрыть Facebook из-за радуги // Подробности (http://podrobnosti.ua/2043425-v-rossii-trebujut-zakryt-facebook-iz-za-radugi.html). – 2015. – 27.06).***

***

Сервіс зберігання копій веб-сторінок The Wayback Machine, який розташований за адресою web.archive.org, заблокований російським наглядовим органом Роскомнагляд.

Про це повідомляє Еспресо.TV із посиланням на Радіо Свобода.

Приводом до блокування стала опублікована на сайті сторінка під заголовком «Одиночний джигад». Згідно з даними на сайті Роскомнагляду, було обмежено доступ тільки до конкретної сторінки. Але, як повідомляють російські користувачі мережі, станом на 12:40 за допомогою звичних інструментів не відкривалася ані адреса сервісу The Wayback Machine (archive.org/web/), ані сайт некомерційної організації archive.org.

The Wayback Machine – сервіс, який протягом 18 років збирає копії веб-сторінок. На сервісі можна подивитися, як виглядала та чи інша сторінка в певну дату. Архів містить понад 485 млрд сторінок ***(Росіянам заблокували архів інтернету // InternetUA (http://internetua.com/ros-yanam-zablokuvali-arh-v--nternetu). – 2015. – 25.06).***

***

Правоохоронці Донецької області під час моніторингу екстремістських веб-ресурсів встановили майже 800 жителів регіону, причетних до участі в незаконних бандформуваннях.

Про це повідомили в прес-службі Головного управління МВС України в Донецькій області – повідомляє Укрінформ.

«На сьогоднішній день в результаті моніторингу соціальних мереж зібрано інформацію щодо 768 учасників незаконних збройних формувань, встановлено їх зв'язки», – ідеться в повідомленні.

Також правоохоронці відзначили, що з початку 2015 р. оперативники припинили протизаконну діяльність семи суб'єктів підприємницької діяльності – за окрему плату зловмисники за допомогою телекомунікаційного обладнання, в обхід правовласників, ретранслювали абонентам понад 500 платних і заборонених телевізійних каналів, серед яких 10 каналів порнографічного характеру і 14 російських.

Правопорушники діяли в Маріуполі, Красноармійську, Краматорську, Слов'янську, розповсюджуючи мовлення на навколишні населені пункти. Усього колаборанти «підсадили на голку» російської пропаганди майже 14 тис. абонентів – це близько 40 тис. жителів.

Телекомунікаційне обладнання, яке використовувалося для протизаконної діяльності, вилучено і направлено на експертизу ***(Міліція почала активно відслідковувати симпатиків терористів в соціальних мережах // UkrainianWatcher (http://watcher.com.ua/2015/06/30/militsiya-pochala-aktyvno-vidslidkovuvaty-sympatykiv-terorystiv-v-sotsialnyh-merezhah/). – 2015. – 30.06).***

***

Держдума прийняла в другому читанні законопроект, що передбачає штрафи до 3 млн р. за відмову пошукових систем припинити доступ інтернет-користувачів до «недостовірної і неактуальної» інформації.

Про це повідомляє «Росбалт».

Законопроект наділяє правом будь-якого громадянина, але в першу чергу політика чи чиновника, вимагати від оператора пошукової системи припинити видачу посилань на поширювану про нього інформацію. Згідно з документом, мова йде про недостовірну інформацію, а також інформацію, поширювану з порушенням закону.

При доопрацюванні проекту до другого читання депутати виключили норму, за якою пошуковики були зобов'язані також видаляти «достовірну інформацію про події, що мали місце і що завершилися більше трьох років тому, за винятком інформації про події, що містять ознаки кримінально караних діянь, строки притягнення до кримінальної відповідальності щодо яких не минули, а також інформації про вчинення громадянином злочину, по якому не знята або не погашена судимість».

Замість неї з'явилася норма, яка зобов'язує пошуковики видаляти «неактуальну інформацію, що втратила значення для заявника в силу наступних подій або дій заявника, за винятком інформації про події, що містять ознаки кримінально караних діянь, строки притягнення до кримінальної відповідальності за якими не минули, а також інформації про скоєнні громадянином злочину, по якому не знята або не погашена судимість», – ідеться в законопроекті.

Однак нова норма викликала нарікання в Правовому управлінні Держдуми, яке у своєму висновку на законопроект вказало на її невідповідність чинному законодавству.

«Якщо інформація втратила значення для заявника, це не означає, що вона втратила значення для інших осіб і суспільства в цілому, у зв'язку з чим спроба обмеження вільного розповсюдження такої інформації може призвести до порушення конституційних прав інших осіб вільно шукати, одержувати, зберігати, використовувати і поширювати інформацію будь-яким законним способом», – заявили в Правовому управлінні.

При доопрацюванні документа депутати зобов'язали заявників самому вказувати посилання, які, на його думку, мають бути видалені з пошуковиків. Також з 3 до 10 днів збільшується термін для розгляду оператором інтернет-пошукачів самої скарги громадянина тощо. Тим часом депутати погодилися не поширювати новий закон на сайти, включаючи ЗМІ, які володіють системою пошуку архівних публікацій ***(Держдума дозволила «зачищати» Рунет від незручної інформації // Західна інформаційна корпорація (http://zik.com.ua/ua/news/2015/07/01/derzhduma_dozvolyla_zachyshchaty_runet_vid_nezruchnoi_informatsii_603503). – 2015. – 1.07).***

***

Парламент Новой Зеландии приравнял угрозы в Интернете к шантажу и попытке физической расправы, сообщает The Verge.

Теперь запугивание пользователей онлайн влечет за собой уголовную ответственность. Законодательство запрещает отправку людям сообщений, которые содержат расистские или сексистские высказывания, а также

оскорбления религии, сексуальной ориентации и инвалидности человека. Если отправивший такие сообщения признается виновным, ему грозит до двух лет тюрьмы.

Новозеландское правительство создаст новое цифровое агентство, которое будет рассматривать жалобы пользователей со ссылками и отслеживать все популярные сети, включая Twitter и Facebook ***(В Новой Зеландии появится уголовная отвественность за оскорбления в интернете // InternetUA (http://internetua.com/v-novoi-zelandii-poyavitsya-ugolovnaya-otvestvennost-za-oskorbleniya-v-internete). – 2015. – 7.07).***

***

Смартфоны Sony будут следить за пользователями

Патент на технологию анализа изображений для определения эмоционального состояния человека, который на них запечатлен, получила компания Sony. Методика предполагает, что селфи смартфоны, планшеты или умные очки будут делать в автоматическом режиме, а затем отправлять их для анализа на удаленный сервер с использованием защищенного сетевого соединения.

Технология также обеспечивает разбивку фотографий на группы, которые соответствуют определенным эмоциональным состояниям: страх, радость, печаль, гнев, отчаяние и т. д. Если же селфи не отражает никаких конкретных эмоций, оно может быть отфильтровано и не использоваться в дальнейшем.

Впрочем, работает система не в полностью автоматическом режиме – пользователю предоставляются возможности поиска по базе данных изображений, которые отображают счастье и сняты в определенный день. Кроме того, в Sony предусмотрели опцию создания графиков и временных шкал различных эмоциональных состояний.

Разработчики отмечают, что селфи могут быть получены автоматически и в ночное время. Специалисты не стремятся подглядывать за вами – снимки помогут проанализировать фазы сна и оценить качество отдыха.

Как именно будут использованы результаты анализа, в Sony не сообщают. Возможно, по результатам анализа на экране смартфона будет выводиться контент, который, к примеру, заставит улыбнуться, если вы грустите.

Примечательно, что заявка на получение патента была подана Sony ещё в 2013 г., однако одобрена только сейчас. Когда же технология будет реализована, неизвестно, так как это требует решения множество правовых вопросов, связанных с правом на приватность ***(Смартфоны Sony будут следить за пользователями // InternetUA (http://internetua.com/smartfoni-Sony-budut-sledit-za-polzovatelyami). – 2015. – 7.07).***

***

Пользователи iPhone с джейлбрейком рискуют стать жертвой Hacking Team

После взлома хакерами известной итальянской компании Hacking Team, разрабатывающей системы слежки за пользователями в Интернете, были опубликованы 400 ГБ частных документов. Изучившие эти данные эксперты утверждают, что владельцы iPhone и iPad с джейлбрейком подвергают себя дополнительной опасности.

В результате атаки на Hacking Team в сети появились несколько сотен гигабайт внутренних данных компании, включая конфиденциальную информацию о клиентах и исходные коды продуктов. Похищенные сведения злоумышленники распространяют через торрент-сеть. Кроме того, они взломали аккаунт Hacking Team в Twitter, изменили логотип компании, ее описание и опубликовали в блоге скриншоты украденных данных.

Похищенные документы содержат большое количество информации о клиентах Hacking Team, опровергая многократные заявления разработчиков в прошлом. Так, например, Hacking Team утверждала, что не поставляет свои решения «государствам с репрессивными политическими режимами». А благодаря утечке выяснилось, что в числе покупателей были Казахстан, Судан, Россия и Саудовская Аравия, пишет TechCrunch (издание считает их странами с репрессивным режимом).

Выяснилось, что клиентская база вендора включает не только государственных заказчиков, но и частные компании. Ранее Hacking Team утверждала, что не продает ПО частным организациям.

Из документов также стало известно, что Hacking Team располагает инструментами для доступ к мобильными устройствам Apple, подвергнутым процедуре джейлбрейка. Именно таким образом компания осуществляла слежку за пользователями iPhone и iPad.

Установка средств для удаленного мониторинга за iOS-устройствами с джейлбрейком выполняется после подключения к зараженному компьютеру или установки твиков из Cydia. После этого специалисты Hacking Team получают полный доступ к персональным данным пользователей, включая короткие сообщения, переписку в iMessage, WhatsApp или Viber, список звонков, а также сервисы геолокации со историей посещений.

Выполнение процедуры джейлбрейка iPhone и iPad является добровольным выбором каждого пользователя, однако в некоторых случаях последствия могут оказаться дороже, чем полученные блага, говорят эксперты.

Компания Hacking Team основана в Милане. Согласно официальному описанию, она занимается разработкой наступательных технологий для правоохранительных органов и спецслужб. Один из сервисов компании – под названием Davinci – предназначен для взлома SMS-переписок, электронной почты и веб-соединений ***(Пользователи iPhone с джейлбрейком рискуют стать жертвой Hacking Team // InternetUA (http://internetua.com/polzovateli-iPhone-s-djeilbreikom-riskuuat-stat-jertvoi-Hacking-Team). – 2015. – 8.07).***

***

7 липня офіційну сторінку полку «Азов» у Facebook під назвою «Батальон спеціального призначення “Азов” – нова сторінка» було видалено адміністрацією соцмережі без жодних попереджень – про це повідомляє прес-служба полку.

«Наразі невідомо, що стало причиною видалення сторінки, яка нараховує понад 50 тис. передплатників. В даний момент виясняємо причини блокування та видалення сторінки», – ідеться в повідомленні ***(Facebook видалив сторінку полку «Азов» // UkrainianWatcher (http://watcher.com.ua/2015/07/07/facebook-vydalyv-storinku-polku-azov/). – 2015. – 7.07).***

***

Роскомнадзор не собирается закрывать Facebook в России из-за блокировки российских пользователей либо из-за размещения экстремистских материалов. Как сообщил в эфире «Русской службы новостей» пресс-секретарь ведомства В. Ампелонский, чиновники предпочитают договариваться с руководством соцсети по данным вопросам. Об этом сообщает rusnovosti.ru

«Мы не рассматриваем закрытие Facebook в России. Мы с ним взаимодействуем. Если брать противоправный контент, то это достаточно чистая соцсеть. Есть ряд отдельных вопросов, связанных с распространением материалов экстремистского характера, как украинских националистических организаций, запрещённых в РФ, так и исламских террористических группировок. Но эти проблемы решаются. Никто не пляшет под дудку соцсетей. Мы занимаем сдержанную позицию. Язык, который разжигает ненависть между нациями, недопустим. Facebook делает всё правильно, но принцип этот должен быть не избирательным», – сказал он.

Ранее администрация соцсети Facebook заблокировала аккаунты сразу несколько известных пользователей. В частности, на неделю был заморожен аккаунт писателя Э. Багирова за использование выражения «несчастные хохлы». Об этом говорится в ответе Facebook на просьбу Роскомнадзора разъяснить ситуацию с блокировкой. «Слово “хохлы” в такой подаче подпадает под использование таких слов, как “ниггер” и другие, и нарушает правила сообщества», – сообщается в ответе Facebook. До этого его страницу блокировали за слово «укроп». Страницу журналиста и писателя М. Кононенко также заблокировали в Facebook на неделю за слово «хохлы» в опубликованном им стихотворении Пушкина ***(Роскомнадзор не собирается закрывать Facebook в России // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43922/118/lang,ru/). – 2015. – 7.07).***

***

Сотрудники Службы безопасности Украины задержали жительницу Мариуполя, которая вела активную антиукраинскую пропаганду в социальных сетях.

Как сообщает официальный сайт СБУ, девушка модерировала около 500 групп в социальных сетях, которые охватывали почти 1,5 млн фолловеров.

«Она распространяла призывы к насильственному изменению конституционного строя, захвата государственной власти, поддержки террористических действий на Донбассе, публиковала видео в поддержку мобилизации боевиков и тому подобное», – отмечается в сообщении.

Во время обыска у нее изъяли компьютерную технику и электронные носители с материалами, подтверждающие ее деятельность.

Открыто уголовное производство по ч. 2 ст. 109 Уголовного кодекса (публичные призывы к насильственному изменению или свержению конституционного строя или к захвату государственной власти, а также распространение материалов с призывами к совершению таких действий). Ей грозит ограничение или лишение свободы на срок до трех лет.

Также проверяется информация о возможной координации действий злоумышленницы с боевиками так называемой «ДНР» ***(СБУ задержала модератора 500 антиукраинских групп в соцсетях // Лівий берег (http://society.lb.ua/war/2015/07/08/310407_sbu_zaderzhala_moderatora_500.html). – 2015. – 8.07).***

***

Американские и британские спецслужбы хотят получить доступ к зашифрованным мессенджерам для борьбы с преступностью и терроризмом. Но специалисты в области криптографии выступили резко против такого шага. Ведь правительственные ресурсы слишком часто становятся жертвами хакерских атак, и ключи от защищенных чатов могут быть украдены.

С момента разоблачений Э. Сноудена власти США и Великобритании не первый раз пытаются ограничить применение шифрования в Интернете. Премьер-министр Великобритании Д. Кэмерон даже угрожал полным запретом на средства передачи зашифрованных сообщений по всей стране. А директор Агентства национальной безопасности США (АНБ) М. Роджерс недавно предложил технологическим компаниям разработать специализированные правительственные ключи для доступа к зашифрованным данным на их серверах.

Эти предложения были раскритикованы крупнейшими интернет-компаниями, такими как Microsoft, Apple и Google, а также специалистами по кибербезопасности. Эксперты в один голос утверждают, что создание подобных ключей может нанести серьезный вред всему Интернету.

Так, один из отцов компьютерной безопасности П. Нейман заявил, что средства коммуникации сегодня защищены слабее, чем когда-либо, и получить доступ к зашифрованным данным через уязвимости в безопасности спецслужб сможет почти любой грамотный хакер.

Тем не менее главы АНБ, ФБР и министерства юстиции не отказались от своих попыток и запланировали слушания в юридическом комитете сената, на котором представят законодателям причины столь радикальных действий.

Ведомства настаивают, что современные технологии шифрования делают работу правительственных спецслужб неэффективной.

А глава ФБР Д. Коми дополнительно попросил экспертов предоставить доступ к системам шифрования Google, Apple и Yahoo и ряда криптографических приложений, поскольку исламские экстремисты все чаще используют мессенджеры WhatsApp, Apple iMessage и Telegram для координации преступных действий.

Силовики вполне могут вынудить сенат принять соответствующие законы, сославшись на невозможность обеспечения национальной безопасности США.

Это вынудило интернет-отрасль собрать группу крупнейших экспертов в области криптографии и компьютерной безопасности, которая за день до слушаний успела выпустить отчет по зашифрованным коммуникациям и обосновать ошибочность вносимых силовиками законодательных актов.

Их аргументы просты и понятны. Недавние взломы управления кадров государственной службы США, Государственного департамента США и Белого дома ставят под сомнение безопасность хранения информации госструктурами. В этих условиях специальные ключи, по сути, дающие доступ к любой зашифрованной информации в мире, элементарно не будут достаточно защищены.

Кроме того, страны вроде Китая не согласятся с тем, что подобные ключи есть только у США и Великобритании, и потребуют от производителей аналогичных ключей для себя.

Группа экспертов, включая разработчика одного из самых распространенных протоколов шифрования RSA, профессоров в области криптографии и кибербезопасности Массачусетского технологического института, Колумбийского университета, Гарварда, ведущих специалистов по шифрованию и защите персональных данных Microsoft и Google, последний раз собиралась в таком составе еще в 1997 г. Тогда администрация президента США Б. Клинтона попыталась внедрить специальный правительственный чип (Clipper Chip) во все оборудование, обеспечивающее шифрование данных.

По замыслу разработчиков в случае необходимости чип должен был открывать доступ к зашифрованным коммуникациям. Эксперты выступили резко против, так как подобный элемент закладывал в системы защиты неустранимую впоследствии уязвимость.

Специалисты доказали техническую нереализуемость идеи Clipper Chip, а сотрудник AT&T Bell Laboratories поставил жирный крест на этой инициативе, когда обнаружил в правительственном чипе уязвимость. Она давала доступ к конфиденциальным данным практически любому более-менее подкованному техническому специалисту.

Даже в то время история получила большой резонанс, несмотря на то что под угрозу попадали только электронная почта и факсимильные сообщения, которые использовались в то время не так уж и широко.

Сейчас же по защищенным интернет-каналам передается вся финансовая и банковская информация, осуществляется доступ к системам управления ядерными объектами и опасными химическими производствами, почти всем авиационным и транспортным системам, а также энергосетям и другим критически важным объектам.

И разработка универсальных правительственных ключей доступа к зашифрованным каналам коммуникации – слишком опасный и безответственный шаг.

Однако силовики могут добиться законодательного запрета на использование систем передачи зашифрованных сообщений без внедрения правительственных ключей доступа.

Крупнейшие американские интернет-компании будут вынуждены подчиниться, а затем долго судиться и лоббировать принятие поправок и исключений, чтобы не потерять клиентов на международном рынке.

Но в целом интернет-предприниматели не согласны с аргументами спецслужб и видят огромную рыночную перспективу в обеспечении приватности пользователей. Сегодня на рынке уже существует целый ряд подобных приложений.

Прежде всего это Telegram П. Дурова. Месячная аудитория мессенджера уже достигла 62 млн пользователей, которые отправляют 2 млрд сообщений. В приложение постоянно внедряются новые методы защиты и доступа к сообщениям разной степени стойкости и сложности в использовании, от Touch ID до графического ключа.

Сам П. Дуров перевозит команду разработчиков из страны в страну не реже чем раз в три месяца, чтобы избежать риска влияния правительств на мессенджер.

Telegram приобретает все больше известных последователей. Например, один из отцов рунета А. Носик призывает сменить мессенджер Facebook на Telegram.

Другим направлением развития приватности в мессенджинге является так называемое эфемерное общение, то есть отсылка пользователями друг другу сообщений и изображений с ограниченным сроком жизни, которые нельзя сохранить на устройство. Самым известным сервисом из этой группы является Snapchat.

Конечно, можно заставить сервис сохранять копии всех сообщений, однако отправка сообщений в графическом виде и несовершенство систем компьютерного зрения делают перехват сообщений затруднительным.

Наконец, еще одним интересным решением является использование сети BitTorrent для передачи зашифрованных фрагментов сообщений через распределенных пользователей по принципу скачивания файлов через торрент-трекеры. Этот принцип реализован в мессенджере Bleep от создателей BitTorrent.

Приложение использует тот же принцип, что и Tor-браузер, но при этом гораздо проще в использовании и работает на смартфонах ***(Спецслужбы***

захотели в чат // InternetUA (http://internetua.com/specslujbi-zahoteli-v-csat). – 2015. – 9.07).

***

Linux, Apache и MySQL – это все что нужно АНБ для мирового шпионажа

Согласно информации, рассекреченной Э. Сноуденом, используемая АНБ секретная система наблюдения XKeyscore работает на дистрибутиве Red Hat Enterprise Linux. Стоит отметить, что XKeyscore способна собирать данные маршрутизаторов, электронную почту, записи разговоров через Skype и пр.

Об этом сообщает издание The Register со ссылкой на документы, обнародованные Э. Сноуденом.

Британский журналист Г. Гринвальд заявил, что XKeyscore является «частью программного обеспечения Linux, которое, как правило, размещено на серверах Red Hat». Функционал XKeyscore Г. Гринвальд описал следующим образом: «ПО использует веб-сервер Apache и сохраняет информацию в базах данных MySQL. Файловые системы в кластере обрабатываются распределенной файловой системой NFS и сервисом автоматического монтирования файловых систем autofs. Запланированные задачи выполняются с помощью планировщика задач cron».

Не секрет, что АНБ спонсирует проекты с исходным кодом, и Xen Project тому пример. Издание The Register считает удивительным тот факт, что «управлять миром» можно с помощью только Linux, Apache и MySQL ***(Linux, Apache и MySQL – это все что нужно АНБ для мирового шпионажа // Центр Інформаційної Безпеки (http://www.bezpeka.com/ru/news/2015/07/09/nsa-need-Linux-Apache-MySQL.html). – 2015. – 9.07).***

***

Семь хакерских группировок мира, за которыми стоят правительства

Хакерство нынче расценивается всеми законодательствами как вполне реальная угроза. Любой сколь угодно талантливый хакер, как правило, работает на государство. А противостояние стран и хакерских групп в сети уже вполне серьёзно называют «Второй Холодной войной». Предлагаем ознакомиться с её участниками.

«Сирийская электронная армия»

Группировка, о которой мир узнал в 2011 г., была сформирована из студентов сирийских университетов и занимается пропагандой в пользу сирийского президента Б. Асада. На их счету – удары по The New York Times, Twitter и нешуточный переполох в TOR. Их жертвами в разное время стали CNN, Washington Post и Time – а однажды они убедили общественность в том, что в Белом Доме произошёл взрыв, и президент Б. Обама ранен. Эта новость ненадолго нарушила работу фондового рынка, а индекс Dow Jones сильно понизился. Кроме того, «Сирийская электронная армия» занимается

запугиванием людей, которые не поддерживают режим Б. Асада. Группировка добывает информацию о пользователях для последующей передачи её «компетентным органам» Сирии, порой организовывающим исчезновения неугодных.

Tarh Andishan

Tarh Andishan переводится с фарси как «Мыслители», или «Новаторы». Ни умения мыслить, ни новаторства этой группе не занимать. О себе группировка заявила в ходе операции «Топор мясника», которая проводилась в 2012 г. против как минимум 50 различных организаций со всего мира, работающих в военной, коммерческой, образовательной, экологической, энергетической и аэрокосмической сферах. Несколько раз эти хакеры получали полный контроль над инфраструктурой западных аэропортов. Tarh Andishan из Ирана обожает SQL-инъекции, новейшие эксплойты, backdoor и другие подобные инструменты. После некоторой «разрядки» в отношениях между США и Ираном группа свернула свою «антизападную» деятельность и сконцентрировалась на ближневосточном регионе.

Группа «Стрекоза»

Кому конкретно подчиняется «Стрекоза», точной ясности нет. Аналитики склоняются к тому, что группа действует либо в интересах некой восточноевропейской страны, либо находится под командованием политической верхушки Евросоюза. В 2011 г. она заявила о себе мощнейшей атакой против авиакомпаний и оборонных отраслей США и Канады. «Стрекоза» использует трояны – их собственный Backdoor.Oldrea и Trojan.Karagany. Это шпионское программное обеспечение позволяет следить за сферой энергетики и осуществлять акты промышленного саботажа. Кроме того, «Стрекоза» славится тем, что умеет заражать легальное программное обеспечение.

«Индивидуальные операции доступа»

Финансируемая государством группа, находящаяся в подчинении Агентства Национальной Безопасности США. Именно в её рядах работал небезызвестный Э. Сноуден, именно она повинна в прослушивании телефонных разговоров как в США, так и за рубежом. Действия группы не ограничиваются хакерством. Их люди перехватывают поставки персональных компьютеров, на которых размещается шпионское программное обеспечение. Кроме того, группа отвечает за слежку за многими политиками Европы, включая канцлера Германии А. Меркель и президента Франции Ф. Олланда.

«Летающий котёнок», «Аякс»

«Котёнок» интересен тем, что зародился как кружок по интересам для хакеров-самоучек, патриотов, выучившихся программированию, и других непрофессиональных деятелей. От работы на чистом энтузиазме они быстро перешли к кибершпионажу и разоблачению политических диссидентов. Государственную поддержку они отрицают. Однако специалисты считают данную позицию лицемерной. Группа действует исключительно в интересах правящего режима в Иране – одним из крупнейших актов «Аякса» стала

операция «Шафрановая роза». В основе её лежали серия фишинговых атак и попыток изменить веб-доступ к Microsoft Outlook и страницы VPN для того, чтобы получить учётные данные пользователей и информацию об оборонной промышленности США.

«Подразделение 61398»

Команда, более известная в профильной среде как «Панда с клюшкой», только в 2013 г. похитила сотни терабайт (!) данных как минимум из 141 организации по всему миру, включая громкое похищение всей документации по новейшему самолёту-истребителю Министерства обороны США. Масштабы их деятельности настолько велики, что не поддаются никакому описанию. Кроме того, «Панды» лучше других заметают следы, что затрудняет идентификацию полного списка их «подвигов». Общие приметы деятельности китайского «Подразделения 61398» – шанхайские IP-адреса компьютеров, упрощённые настройки китайского языка в атакующих системах и беспрецедентная скорость. Китай, разумеется, всё отрицает.

«Бюро 121»

Можно сколько угодно шутить на тему хакеров в государстве, где нет подключения к Интернету – корпорация Sony Pictures шутку наверняка не оценит. Северокорейское «Бюро 121» стоит за атакой на сервера компании из-за фильма «Интервью», высмеивающего порядки в стране Ким Чен Ына. Считается, что эта команда подчиняется непосредственно Министерству обороны и создана для подкрепления полноценных боевых действий. На их счету – хакерские атаки и саботаж против Южной Кореи и США. На группу возлагают ответственность за атаку на 30 тыс. компьютеров, находящихся в банках и телекомпаниях на территории Южной Кореи ***(7 хакерских группировок мира, за которыми стоят правительства // InternetUA (http://internetua.com/7-hakerskih-gruppirovok-mira--za-kotorimi-stoyat-pravitelstva). – 2015. – 5.07).***

***

Шпионская программа АНБ проще, чем поиск Google

Издание The Intercept опубликовало новые детали, касающиеся работы сервиса XKeyscore. Согласно документам Э. Сноудена, которые он передал журналистам в 2013 г., АНБ использует XKeyscore для слежки за гражданами. Но никто не мог подумать, что это настолько просто.

Согласно данным The Intercept, XKeyscore «кормится» потоками данным, собирая их прямиком с оптоволоконных кабелей по всему миру. Собранные данные хранятся на серверах агентства 3–5 дней, а метаданные и вовсе до 45 дней. XKeyscore позволяет АНБ перехватывать чаты, email, а также: «фотографии, документы, голосовые звонки, нажатия клавиш, логины и пароли, Skipe-звонки, файлы, загружаемые в онлайновые сервисы, фото с веб-камер, истории поисковых запросов, анализ рекламного трафика, трафик социальных медиа, трафик ботнетов, CNE таргетинг». Сообщается, что АНБ

отслеживает даже устанавливаемые с телефонов соединения с Google Play и Samsung's App Store.

Однако теперь выясняется, что XKeyscore, это не только невероятно мощная, но и очень простая система. Глава Toucan Systems и ИБ специалист Д. Броссард рассказывает в статье, что обучить сотрудника работе с XKeyscore можно, в буквальном смысле, за день, а получение доступа к удаленному компьютеру занимает «минуты, если не секунды реального времени». Более того, интерфейс XKeyscore не сложнее интерфейса поиска Google.

Д. Броссард приводит и вполне конкретные примеры. Так сотрудникам АНБ понадобилось всего лишь набрать email-адреса определенных сотрудников ООН в XKeyscore, чтобы получить доступ к их приватным беседам в 2013 г. Благодаря этому АНБ заранее узнало обо всех ключевых аргументах Генерального секретаря ООН Пан Ги Муна на планируемой встрече с президентом США. Б. Обама явился на встречу хорошо подготовленным.

Известно так же о неком лидере Аль-Каиды, который гуглил себя, а АНБ успешно отслеживало его активность посредством XKeyscore.

Разумеется, при этом АНБ не имеет права собирать данные и столь пристально следить за «простыми смертными» в США, без соответствующего судебного ордера. На деле все это может оказаться несколько сложнее. Так представитель Electronic Frontier Foundation К. Обсахл полагает, что отделить «американские» данные от остальных, может быть крайне сложно, так как аналитики АНБ попросту «никак не ограничены технически», они не могут этого сделать.

Само АНБ связалось с изданием CNet и прокомментировало публикацию The Intercept весьма прохладно. По сути, агентство напомнило, что все зарубежные операции разведки такого рода – совершенно легальны, а личные данные граждан в полной безопасности ***(Шпионская программа АНБ проще, чем поиск Google // InternetUA (http://internetua.com/shpionskaya-programma-anb-prosxe--csem-poisk-Google). – 2015. – 5.07).***

Проблема захисту даних. DDOS та вірусні атаки

Мобильное приложение Facebook Moments не будет работать в Европе и Канаде из-за несоответствия требованиям местного законодательства в области защиты личной информации. Запущенный в середине июня сервис призван решить проблему обмена изображениями между пользователями, которые не хотят, чтобы снимки оказались в открытом доступе.

Технология распознавания лиц в Facebook Moments нарушает европейское законодательство о защите личных данных. Так, например, ирландский государственный регулятор заявил, что приложение должно запрашивать разрешение пользователя на обработку его изображений. В Moments такой опции пока нет, и, по словам представителей Facebook, добавлять ее пока не входит в планы компании.

«Нас беспокоит, что Facebook имеет доступ к биометрической информации и возможность сопоставлять ее с колоссальными объемами сведений о пользователях, включая их биографию, местоположение и связи с другими людьми», – говорится в официальном заявлении омбудсмена по защите права частной жизни Канады.

Технология распознавания лиц, которую использует Moments, была разработана лабораторией исследований искусственного интеллекта Facebook. Алгоритм анализирует фотографии друзей в ленте и ищет соответствия в потоке изображений на устройстве с точностью более 97 %.

Помимо этого Moments дает возможность объединять фотографии в альбомы и отправлять их друзьям. Все изображения хранятся в собственном облачном хранилище в Facebook – компания синхронизирует только те фото, которые отправляет пользователь, а не сохраняет весь альбом мобильного устройства.

В 2011 г. разногласия с ирландским государственным регулятором по вопросам защиты персональных данных, в частности, фотографий, привели к тому, что Facebook отключила функцию рекомендованного тегирования на изображениях для всех пользователей на территории Евросоюза. Система анализировала лица на фотографии, сопоставляла их с френдлистом и предлагала пользователю отметить тех или иных друзей ***(Европа испугалась приложения Facebook Moments // InternetUA (http://internetua.com/evropa-ispugalas-prilojeniya-Facebook-Moments). – 2015. – 23.06).***

***

Польская авиакомпания LOT подверглась масштабной атаке хакеров. В результате десятки международных и внутренних рейсов были отложены.

Хакерская атака на наземные информационные системы LOT в варшавском международном аэропорте имени Шопена произошла 21 июня. По данным пресс-службы авиакомпании, вовремя не смогли вылететь 1,4 тыс. человек.

Отмечается, что проблема не коснулась самолетов, которые находились в воздухе. Из-за хакеров были отложены рейсы в Краков, Вроцлав и Гданьск, Гамбург и Дюссельдорф, а также в Копенгаген, Стокгольм, Брюссель и Монако ***(Хакеры атаковали польскую авиакомпанию LOT: десятки рейсов отложены // Телекомпанія НТВ (http://www.ntv.ru/novosti/1429276/). – 2015. – 21.06).***

***

Международная антивирусная компания ESET провела исследование, в ходе которого выяснилось, что 2/3 аккаунтов российских пользователей хотя бы раз подвергались взлому.

В результате действий злоумышленников доступ к аккаунту теряли 59 % пользователей, учетная запись 21 % респондентов была взломана несколько раз, а 38 % опрошенных оказались жертвами интернет-мошенников один раз.

40 % пользователей ни разу не теряли доступа к своему аккаунту. И это хороший результат – в 2013 г. этот показатель составил 32 %.

1 % респондентов указали, что не знают, взламывали ли их когда-нибудь и как определить взлом. Здесь тоже наблюдается положительная динамика – 2 года назад таких пользователей было целых 8 %.

Как показало исследование, чаще всего пользователи теряют доступ к аккаунту из-за собственной безответственности и невнимательности. Всего 14 % опрошенных регулярно меняют пароли от учетных записей в социальных сетях, 60 % делают это когда придется, а 26 % и вовсе не считают смену пароля необходимой мерой ***(2/3 аккаунтов российских пользователей хотя бы раз подвергались взлому // LIKENI.RU (http://www.likeni.ru/events/2-3-akkauntov-rossiyskikh-polzovateley-khotya-by-raz-podvergalis-vzlomu/). – 2015. – 24.06).***

***

Антивирусы под прицелом

Месяц июнь оказался богат на новости, посвященные компроментации двух лидеров российского рынка антивирусного ПО. Первую из этих историй рассказала сама «Лаборатория Касперского» (ЛК), не без юмора назвав отчёт Duqu Bet и как бы намекая на израильское происхождение атакующих. Однако два дня назад появились более серьезные материалы на ту же тему: издание Intercept опубликовало очередное откровение Э. Сноудена, в котором рассказывается, что американские и британские спецслужбы ещё в 2008 г. «отчитались о проделанной работе» по взлому анивирусных продуктов Касперского.

Согласно этим документам, британская GCHQ изучала продукты ЛК для того, чтобы помешать антивирусам выявлять атаки спецслужб. А американская NSA искала уязвимости в антивирусе для того, чтобы следить за пользователями благодаря высоким привилегиям доступа, которые получает защитное ПО на компьютерах своих пользователей.

В частности, хакеры NSA обнаружили, что могут перехватить пользовательские данные, которые передаются от клиента-антивируса к серверам ЛК в строке User-Agent в заголовке HTTP-запроса. Издание Intercept утверждает, что месяц назад протестировало эту возможность на продукте Kaspersky Small Business Security 4, и «хотя часть трафика была зашифрована, детальная информация о конфигурации хоста и установленном ПО передавалась на серверы Касперского без защиты».

Эти данные журнал Intercept опубликовал 22 июня. А буквально на следующий день, 23 июня, команда исследователей из Google (Project Zero) опубликовала отчёт о более серьезной уязвимости в антивирусе ESET NOD32. Благодаря данной уязвимости атакующий может обмануть эмулятор, который используется для проверки исполняемых кодов. Атака позволяет читать, модифицировать и удалять любые файлы на компьютерах, где установлен ESET, а также инсталлировать любые другие программы удалённо, получать

доступ к любым периферийным устройствам (камеры, микрофоны), записывать всю системную активность, и т.д.

Угроза затрагивает все версии ESET и все платформы, на которых работает ESET (Windows, Mac, OS X). При этом, как подчёркивают исследователи, эксплуатация данной уязвимости не требует пользовательского участия, зато использует высокие системные привилегии, которые даются сканеру ESET – то есть является идеальным кандидатом для создания самоходного червя (например, почтового). В отчёт включён пример рабочего рутового эксплойта, а также ролик, который демонстрирует атаку на ESET через браузер:

Закрыть уязвимость можно патчем ESET, выпущенным 22 июня – а до этого можно избежать атаки, если отключить всё сканирование в ESET (плановое, в реальном времени и ручное). И хотя данная публикация исследователей из Google произошла уже после выхода патча, всё равно складывается ощущение, что обнародование этой дыры как-то «специально подгадали» к общей кампании против антивирусов из Восточной Европы ***(Антивирусы под прицелом // InternetUA (http://internetua.com/antivirusi-pod-pricelom). – 2015. – 25.06).***

***

Компания Facebook совместно с мировыми производителями сервисов по безопасности начала бороться с вредоносными программами и вирусами, пишет «Обозреватель» (http://tech.obozrevatel.com/hi-tech/27915-facebook-usilil-bezopasnost-sotsseti-i-nachal-borotsya-s-virusami.htm).

Так крупнейшая соцсеть совместно с Лабораторией Касперского, ESET, F-Secure и Trend Micro создали программу, которая находит и чистит ваш компьютер, пока вы находитесь на странице в Facebook, сообщает Zeenews.

«Благодаря сотрудничеству с этими компаниями, в последние три месяца мы помогли очистить более двух миллионов компьютеров людей, где были обнаружены вредоносные программы», – рассказал инженер безопасности Facebook Т. Потингер.

Эксперт сообщил, что программа использует «сочетание сигналов, которые находят вирусы на вашем компьютере, даже если вредоносная программа не активно распространяет спам или вредные ссылки» ***(Facebook усилила безопасность соцсети и начала бороться с вирусами // Обозреватель (http://tech.obozrevatel.com/hi-tech/27915-facebook-usilil-bezopasnost-sotsseti-i-nachal-borotsya-s-virusami.htm). – 2015. – 25.06).***

***

Е. Касперский прогнозирует хакерские атаки на Smart TV

Основатель организации «Лаборатория Касперского» Е. Касперский рассказал, что в настоящее время хакеры нацелились на бытовую технику, которая имеет доступ в Интернет. Программист отметил, что владельцы

современных устройств часто привязывают банковский счет к Smart TV, а это и является основной целью злоумышленников.

Руководитель организации «Лаборатория Касперского» Е. Касперский заявил, что в скором будущем компьютерные хакеры найдут новые объекты, которые будут подвергаться взлому. По словам программиста, основной целью злоумышленников может стать бытовая техника, которая имеет доступ к Интернету.

На сегодняшний день телевизоры, пылесосы, кофеварки и другие устройства не имеют нужной защиты от вирусов и взломов. Е. Касперский добавил, что в настоящее время в мире есть ряд сервисов, с помощью которых для удобства можно привязать номер банковской карты к Smart TV. Программист подчеркнул, что это является главной целью злоумышленников ***(Касперский прогнозирует хакерские атаки на Smart TV // ВладТайм (http://www.vladtime.ru/internet/434598-kasperskiy-prognoziruet-hakerskie-ataki-na-smart-tv.html). – 2015. – 25.06).***

***

Нещодавно невідомі зламали персональний сайт голови Луганської обласної військово-цивільної адміністрації Г. Москаля www.moskal.in.ua. Про це повідомляється на сайті Г. Москаля.

Згідно з повідомленням, у стрічку новин майже півторарічної давнини, за 1 березня 2014 р., було вставлено новину з вигаданими фактами про В. Малікова – нинішнього керівника Антитерористичного центру, заступника голови СБУ.

«Новина з вигаданими фактами про В. Малікова була навмисно вставлена хакерами в розкручений сайт, щоб потім поширити її як компромат у різних ЗМІ з посиланням на моє ім’я, – заявляє Г. Москаль. – Інформаційна “качка” вже видалена з мого сайту, тому я прошу ЗМІ не посилатися на неї й прибрати зі своїх повідомлень»

Г. Москаль стверджує, що сайт зламали представники Служби безпеки України, яким не подобаються нові кадрові призначення в СБУ. «Низька кваліфікація виконання замовлення є зайвим доказом, що його виконували саме в СБУ. По-перше, чужорідна новина настільки різко виділялася за стилем подачі від сусідніх інформацій, що це очевидно навіть для непрофесіоналів. По-друге, 1 березня на моєму сайті була розміщена заява з різкою критикою керівництва МВС через призначення на посаду начальника Кримського главка міліції члена партії регіонів І. Авруцького, котрий здав Крим росіянам без будь-якого опору. Ця заява зникла, а замість неї виставили інформаційну “качку”», – зазначив Г. Москаль ***(Москаль заявляє, що його сайт зламали для дискредитації керівника Антитерористичного центру СБУ // Телекритика (http://www.telekritika.ua/kontekst/2015-06-26/108641). – 2015. – 26.06).***

***

Аналитики компании Incapsula зафиксировали массовое снижение цен на рынке DDoS-атак. Стоимость услуги отныне составляет 38 дол. в час.

При этом хакеры предлагают сервис по подписке – заказчик платит за время атаки. Мизерная стоимость проведения атаки сильно отличается от стоимости защиты от неё, которая обходится на порядки дороже. Таким образом, хакеры часто прибегают к вымогательству, требуя выкуп у жертвы. Размер возмещения обычно составляет несколько тысяч долларов.

Падение цен на чёрных рынках хакерских атак началось с весны 2015 г. и к настоящему времени составляет более 30 %. Кроме того, специалисты фиксируют рост мощности атак – он обусловлен ростом количества заражённых компьютеров, которые входят в ботнеты. За отчётный период 56 % всего ботнет-трафика пришло из США, Китая, Вьетнама, Бразилии и Таиланда. В этих странах количество инфицированных систем значительно больше, чем в других странах мира.

Подавляющее большинство хакерских атак осуществляются на уровне приложения, когда ботнет нацеливается на конкретную функцию сайта, чтобы вывести её из строя ***(«Время sale» – стоимость DDoS-атак упала до $38 в час // Блог Imena.UA (http://www.imena.ua/blog/ddos-sales/). – 2015. – 26.06).***

***

Исследователи из SecureWorks (дочерняя компания Dell) сообщили об активизации трояна Stegoloader, хранящего свои модули в PNG-изображениях. За последние три месяца наибольшее число заражений пришлось на компании в сфере здравоохранения (42 %), финансовые институты (13 %), производственные предприятия (9 %), предприятия в нефтегазовой отрасли и ИТ-компании (по 3 %), согласно Trend Micro.

По данным аналитиков, больше всего заражений зафиксировано в США (67 %), Чили (9 %), Малайзии (3 %), Норвегии и Франции (по 2 %).

Троян Stegoloader (известный также под названием Win32/Gatak.DR и Tspy_Gatak.GTK) распространяется посредством пиратских ресурсов в генераторах ключей к программному обеспечению (например, Avanquest_PowerDesk_9_0_1_10_keygen.exe). После того как Stegoloader попадает в систему, он подгружает с безопасных источников PNG-изображения с модулями, спрятанными в них с помощью техники под названием «стеганография». Различные модули трояна отвечают за его различную функциональность.

Загруженные трояном изображения формата PNG выглядят как вполне обычные, но в их пикселях записан код модулей Stegoloader. Считывая этот код и подключая модули, троян «собирает» себя прямо в оперативной памяти персонального компьютера.

Ход подключения модулей отправляется на командно-контрольный сервер злоумышленников посредством HTTP-запросов. С этого же сервера троян получает команды на выполнение.

После того как троян «собрался», он начинает похищать с компьютера и отправлять на удаленный сервер различную информацию, включая историю веб-серфинга, пароли, списки недавно открытых документов и т. д. Один из модулей предназначен для поиска на компьютере данных об анализе угроз, который специалисты по информационной безопасности проводят с помощью специального ПО.

Stegoloader оснащен множеством механизмов защиты от обнаружения. Перед подключением вредоносных модулей загрузчик проверяет: не находится ли он в среде эмулятора антивирусной программы. Например, он посылает множество запросов к функции определения позиции курсора мыши GetCursorPos. Если значение этой функции константа, загрузчик мгновенно прекращает свою работу. Таким образом, антивирус не видит никакой подозрительной активности, объяснили в SecureWorks.

Специалисты Trend Micro полагают, что техника скрытия вредоносного кода в изображениях (стеанография) со временем будет набирать все большую популярность. В то же время аналитики не думают, что указанный метод будет применяться для широкомасштабных атак.

Троян Stegoloader был впервые обнаружен в 2012 г. и является не единственным в своем роде. В апреле 2014 г. был обнаружен троян под названием Lurk, который также подгружал модули, спрятанные в компьютерные изображения. В начале 2015 г. компанией AVG был обнаружен банковский троян Vawtrak (другие названия – Neverquest и Snifula), также использующий эту технологию ***(В Сети воскрес троян, скрывающийся в картинках PNG // InternetUA (http://internetua.com/v-seti-voskres-troyan--skrivauasxiisya-v-kartinkah-PNG). – 2015. – 28.06).***

***

Інтернет-сайт Канадської служби безпеки і розвідки (СБР) був зламаний хакерами втретє за 24 години.

Про це 30 червня інформував телеканал CTV, повідомляє ТАРС.

Відповідальність за атаку взяв на себе хакер, який діє під ім'ям Aerith, уточнили каналу його джерела в розвідувальному відомстві. Вони також відзначили, що цей же кіберзлочинець 30 червня на деякий час заблокував роботу сайту правлячої Консервативної партії Канади.

Повідомляється також, що Aerith раніше вже робив атаки на веб-сторінки канадської поліції і різних муніципалітетів. Іншої інформації не надходило.

17 червня сайт Міністерства юстиції, СБР і ще однієї секретної служби Канади – Центру безпеки комунікацій – були заблоковані хакерами міжнародної хакерської групи Anonymus. Як заявили представники угруповання, це стало відповіддю на схвалений канадським парламентом новий антитерористичний закон країни.

«Режим (прем'єр-міністра Стівена) Харпера не чує свій народ, а діє тільки у своїх власних інтересах», – говорилося в повідомленні кіберзлочинців ***(Хакери зламали сайт Служби безпеки і розвідки Канади втретє за добу //***

Західна інформаційна корпорація (http://zik.com.ua/ua/news/2015/07/01/hakery_zlamaly_sayt_sluzhby_bezpeky_i_rozvidky_kanady_vtretie_za_dobu_603481). – 2015. – 1.07).

***

Німецькі фахівці з безпеки даних знайшли сліди активності шкідливої програми – «троянського коня» – із налаштуваннями російською мовою на комп'ютери Бундестагу. Відтак, спеціалісти впевнені: за атакою стоять хакери з Росії, і в них може бути тільки один працедавець – російська влада.

У федеральному відомстві з безпеки у сфері інформаційної техніки і Федеральному відомстві з охорони конституції, яке переважно займається контррозвідувальною діяльністю, упевнені, що йдеться про угруповання саме з Росії. Їхню точку зору поділяють і кілька фахівців з інформаційних технологій.

На відміну від хакерів, які базуються в Китаї і вишукують економічні таємниці та цікаві для підприємців Піднебесної наукові патенти, російськомовне угруповання не цікавиться ні здобуванням фінансової інформації, ні інтелектуальною власністю – тільки політичними таємницями.

«Ми спостерігаємо за роботою добре тренованої команди розробників, які збирають розвідувальну інформацію з геополітичних питань і питань оборони – дані, які цікаві лише урядам», – написала у своєму звіті американська компанія FireEye, що спеціалізується на комп'ютерній безпеці. Групу хакерів вона називає APT28 (в інших джерелах – Sofacy).

APT28 за роки активної роботи – перші ознаки її діяльності помітили у 2006 р. – встигла здійснити багато нападів у різних напрямах, причому в першу чергу на ті цілі, які цікаві і владі в Кремлі, помітили в компанії FireEye. Це, передусім, уряди східноєвропейських країн, Грузії, структури НАТО, ОБСЄ, а також інших європейських організацій, які займаються питаннями безпеки.

Хакери, про яких ідеться, дуже дисципліновані – працюють суворо за розкладом. Понад 96 % їхніх атак, які зафіксували фахівці FireEye, відбулися з понеділка по п'ятницю. Затримуватися на «роботі» вони теж не люблять – 89 % атак здійснені з їхніх IP-адрес з 10 до 18 години за московським часом. При цьому понад половина всіх налаштувань у програмах, які шпигували за різноманітними урядами з 2007 по 2014 р., були написані російською мовою.

Фахівці з компанії FireEye упевнені: без постійної підтримки така хакерська діяльність була б просто неможливою. Вони відверто висловлюють підозру, що за хакерами стоїть російська влада.

«У нас немає фото окремих співробітників, їхніх приміщень чи назви держвідомства, але в нас є докази роботи і чітко спланованих операцій, які означають існування державного спонсора, а саме в вигляді керівництва в Москві», – ідеться у звіті FireEye.

Тільки в Бундестазі, за попередніми підрахунками, злочинцям вдалося вкрасти не менше 16 гігабайтів інформації. І це ще, можливо, не кінець. Поки сліди «троянця» зафіксовано на 15 персональних комп'ютерах (ПК) у офісах

депутатів Бундестагу. Усього ж у німецькому парламенті близько 7000 ПК. До пошуку слідів атаки залучили також приватну детективну агенцію.

Остання зафіксована велика атака з почерком групи APT28, окрім Бундестагу, була здійснена на польський уряд 11 серпня 2014 р. Напад виглядав так: працівник уряду побачив у електронній скриньці лист, який не виглядав підозріло, із вкладенням «MH17.doc». MH17 – це номер збитого за місяць до того в небі над Донбасом лайнера «Малайзійських авіаліній». Польський чиновник, нічого не підозрюючи, відкрив файл. У ньому, крім тексту без певного змісту, перебувала частина шкідливої програми. Такі листи отримав не лише він. Як тільки кілька «наживок» проникають у комп'ютер непомітно для антивірусних систем, програма збирає сама себе з частин і починає непомітно для користувача красти його дані.

Інший спосіб виманити обманним шляхом дані – надіслати посилання з фальшивою адресою, яка мало відрізняється від справжньої. Так, хакерам вдалося отримати необхідні їм відомості в Міністерстві оборони Угорщини: співробітниця відомства зареєструвалася для участі в оборонному ярмарку Eurosatory за підробленим посиланням, пише Deutsche Welle ***(У Німеччині впевнені: Атаку на комп'ютери Бундестагу здійснили російські хакери // Західна інформаційна корпорація (http://zik.com.ua/ua/news/2015/07/01/u_nimechchyni_vpevneni_ataku_na_kompyutery_bundestagu_zdiysnyly_rosiyski_hakery_603664). – 2015. – 1.07).***

***

Исследователи одного из бельгийских университетов (Hasselt University) сообщили в Reddit, что им удалось обнаружить опасную уязвимость в стандарте беспроводной связи 802.11n. Эксплуатация бреши позволяет атакующему удаленно скомпрометировать целевую беспроводную сеть.

Стандарт 802.11n предназначен для увеличения пропускной способности беспроводных сетей, расширения диапазона передачи, а также для повышения их безопасности. При этом в нем реализован механизм агрегации фреймов в протоколе media access control (MAC), который увеличивает пропускную способность путем объединения и одновременной передачи двух и более фреймов.

По словам исследователей, этот механизм содержит уязвимость, которую можно проэксплуатировать при помощи техники Packet-In-Packet (PIP) и внедрить таким образом произвольные фреймы в беспроводную сеть. Такая атака позволит злоумышленнику разавторизовать клиент, взаимодействовать со службами внутренней сети, обходить ограничения межсетевого экрана, внедрять beacon-фреймы, проводить сканирование портов и осуществлять ARP-спуфинг.

Опасность бреши заключается в том, что ей подвержены практически все современные чипсеты Wi-Fi, имеющие активное подключение к открытой сети. Более того, для успешной эксплуатации атакующему не нужно находиться в

непосредственной близости от целевой точки доступа, однако в некоторых случаях необходимо знать MAC-адрес атакуемого устройства.

По итогам анализа уязвимости исследователи опубликовали в открытом доступе PoC-код и отчет с техническими подробностями ***(Уязвимость в стандарте 802.11n подвергает беспроводные сети угрозе компрометации // InternetUA (http://internetua.com/uyazvimost-v-standarte-802-11n-podvergaet-besprovodnie-seti-ugroze-komprometacii). – 2015. – 5.07).***

***

Cisco преследуют уязвимости, обусловленные использованием одинаковых ключей и паролей в своих продуктах. На этот раз компания сообщила о бреши в компоненте платформы, предназначенной для управления объединенными коммуникациями.

Критическая уязвимость

Компания Cisco обнаружила критическую уязвимость в продукте под названием Cisco Unified Communications Domain Manager (CUCDM). Представляющий собой компонент платформы для организации совместной работы Cisco Hosted Collaboration Solution, он предназначен для централизованного управления сервисами и приложениями объединенных коммуникаций.

Уязвимость, которой был присвоен номер CVE-2015-4196, позволяет злоумышленнику дистанционно войти в систему через системную учетную запись с правами администратора и целиком захватить контроль над программой, сообщили в компании.

Проблема статичного пароля

Системная учетная запись создается в процессе установки решения. Затем администратор уже не может ее удалить либо изменить, уточнили в Cisco. Проблема заключается в том, что эта учетная запись создается со стандартным статичным паролем.

Уязвимость затрагивает версии Cisco Unified CDM до 4.4.5 и Cisco Unified CDM 8.x. Версии Cisco Unified CDM 10.x ее не содержат.

В компании сообщили, что уже выпустили патч для устранения бреши.

Проблема одинаковых ключей шифрования

Добавим, что это уже вторая уязвимость в решениях Cisco, о которой стало известно за последнюю неделю. В конце июня 2015 г. вендор сообщил об использовании одинакового ключа шифрования SSH в трех различных продуктах – Cisco Web Security Virtual Appliance (WSAv) для защиты от веб-угроз, Email Security Virtual Appliance (ESAv) для защиты от вирусов, распространяемых посредством электронной почты, и Security Management Virtual Appliance (SMAv) для централизованного управления средствами защиты от интернет-угроз.

Похожая уязвимость в SAP HANA

Cisco сообщила о новой уязвимости спустя неделю после того, как представители российской компании Digital Security рассказали об

использовании одного и того же статического мастер-ключа в платформе SAP HANA, который в каждой инсталляции один и тот же во всем мире. Завладев этим ключом, хакер может получить доступ ко всем данным на платформе на любых серверах с SAP HANA ***(«Дыра» в продукте Cisco позволяет получить полный контроль над системой // InternetUA (http://internetua.com/dira--v-produkte-Cisco-pozvolyaet-polucsit-polnii-kontrol-nad-sistemoi). – 2015. – 5.07).***

***

Последняя волна DDoS-атак, затронувшая небольшие маршрутизаторы для офисного и домашнего пользования, была проведена при помощи протокола Routing Information Protocol Version 1 (RIPv1), разработанного еще 27 лет назад. Несмотря на то что стандарт давно устарел, он все еще пользуется популярностью у многих производителей.

По данным исследователей из Akamai Technologies, хакеры начали активно использовать протокол примерно два месяца назад. В настоящее время разработчики уже выпустили более защищенную версию RIPv1, однако на большинстве уязвимых устройств обновления безопасности, как правило, не устанавливаются и большинство из них все еще могут быть использованы злоумышленниками.

Так, на территории США к Интернету подключены порядка 53 тыс. уязвимых маршрутизаторов от Motorola моделей Netopia 2000 и Netopia 3000, а также 2 тыс. маршрутизаторов класса SOHO. Кроме того, RIPv1 используется некоторыми крупными американскими операторами связи, в том числе AT&T.

В ходе наиболее масштабной DDoS-атаки, зафиксированной в течение последних двух месяцев, злоумышленники генерировали порядка 12 Гбит мусорного трафика в секунду. Эксперты подчеркивают, что с увеличением количества используемых уязвимых маршрутизаторов этот показатель может быть увеличен до 100 Гбит в секунду ***(Протокол маршрутизации 27-летней давности используют для проведения DDoS-атак // InternetUA (http://internetua.com/protokol-marshrutizacii-27-letnei-davnosti-ispolzuuat-dlya-provedeniya-DDoS-atak). – 2015. – 4.07).***

***

DDoS-атаки типа «отказ в обслуживании» заполняют Интернет

DDoS-атаки стремительно увеличивают свои масштабы, частоту и техническую сложность. Неудивительно, что эта тенденция создала для производителей ПО особый (и быстро растущий) рынок продукции, предназначенной для обнаружения и защиты от таких атак. Отраслевые аналитики из компании IDC ожидают, что к концу 2015 г. глобальный рынок решений для защиты от DDoS-атак составит 657,9 млн дол. США, а к 2018 г. возрастет до 944,4 млн, пишет Г. Бронсон, предприниматель из Кремниевой долины.

Производители соответствующего ПО активно борются за свою долю этого рынка. Те из них, кто не имел решений для защиты от DDoS-атак (или

хотя бы отдельных инструментов для этой цели), начали в спешном порядке приобретать нужные технологии.

Любое предприятие, использующее в своей деятельности Интернет, – мишень для злоумышленников, и, скорее всего, оно уже неоднократно подверглось атакам. В прошлом году 38 % из 300 корпораций, опрошенных компанией Arbor Networks, сообщили, что в 2014 г. ежемесячно становились жертвой более чем 21 DDoS-атаки. Специалисты по информационной безопасности из компании Incapsula (разрабатывает продукты для защиты от DDoS-атак, принадлежит компании Imperva) предсказывают, что в будущем любая компания, имеющая отношение к Интернету, будет подвергаться DDoS-атакам несколько раз в году. «Не стоит рассматривать атаки как всего лишь возможное событие – лучше рассматривать их как событие неизбежное», – говорит Т. Мэттьюз, вице-президент компании Incapsula по маркетингу.

DDoS-атаки очень просты в осуществлении. Сначала злоумышленник незаметно заражает и берет под контроль любые устройства с операционной системой, подключенные к Интернету: ПК, планшеты, браузеры, мобильные телефоны, серверы и т. д. Захваченные устройства становятся частью удаленно управляемой сети ботов (сокр. от «робот») – ботнета. После этого владелец ботнета (т. н. «ботовод») заставляет зараженные устройства отправлять огромные объемы трафика (отсюда название: «лавинная атака») на адреса жертв, чтобы заполнить всю полосу пропускания до такой степени, пока не будет исчерпано место для полезной нагрузки.

«Доступность каналов с широкой полосой пропускания, открытый доступ к услугам киберпреступников и вредоносным инструментам через т. н. “темный Интернет” – все это привело к стремительной эволюции технологий DDoS-атак, используемых злоумышленниками всего мира для нападений на организации», – говорит Д. Сталик, вице-президент компании F5 Networks по глобальным услугам.

В последние годы DDoS-атаки стали существенно изощреннее и в то же время проще в реализации. Кроме того, теперь злоумышленники имеют возможность арендовать ботнеты через Интернет за небольшую сумму (всего несколько долларов за час или даже за несколько дней). Таким же образом можно воспользоваться услугами подрядчиков для управления атакой. У таких сделок есть важное преимущество: заказчик атаки не имеет прямого отношения к реализации киберпреступления.

Специалисты по информационной безопасности рекомендуют организациям использовать гибридный подход к противодействию DDoS-атакам, т. е. подход, объединяющий возможности локальных и облачных решений для того, чтобы поддерживать и защищать как входящий, так и исходящий трафик. Локальные (расположенные на территории организации) решения распознают DDoS-атаки на уровне приложений. Как правило, такие атаки осуществляются с применением небольших объемов сравнительно медленного трафика. Атаки на уровне приложений генерируют постоянные обращения к ресурсам предприятия – например, к веб-сайтам, веб-

приложениям, серверам и т. д. В результате приложения значительно замедляют или вовсе останавливают свою работу.

Как только локальные решения начинают под воздействием DDoS-атаки испытывать нехватку полосы пропускания, они могут переключить контроль на облачные службы, способные контролировать значительно большие объемы трафика. Локальные и облачные решения отслеживают резкий рост трафика и различные аномалии на пакетном уровне, что может сигнализировать о возможной DDoS-атаке. Как только подозрительные пакеты обнаруживаются, их тут же отделяют от основного потока трафика для того, чтобы изучить более подробно. Действительно же вредоносные пакеты просто сбрасываются до того, как они достигнут своего назначения.

Поставщики решений для ИБ докладывают, что многие DDoS-атаки демонстрируют постоянное изменение тактик, предусматривают изощренные лавинные атаки, короткие по длительности, зато очень частые. Специалисты по информационной безопасности полагают, что большинство таких атак – просто разведка боем. Тем самым злоумышленники пытаются обнаружить организации со слабой защитой, по-настоящему уязвимые для более агрессивных атак.

Кроме того, DDoS-атаки часто служат отвлекающим маневром. Киберпреступники начинают такую атаку на основные ресурсы организации, чтобы отвлечь внимание персонала, обеспечивающего безопасность. Параллельно осуществляется незаметное внедрение вредоносного кода через совсем другие, вспомогательные интернет-ресурсы организации. Работа вредоносного кода заключается в поиске и краже конфиденциальной информации, например, данных о заказчиках, коммерческих данных и интеллектуальной собственности. Позже злоумышленники могут попытаться продать похищенную информацию на черном рынке или потребовать выкуп у законных владельцев.

«Киберпреступники применяют также упрощенные стратегии атак, чтобы тем самым повысить общую эффективность и отвлечь внимание ИТ-персонала от действительной цели нападения, которая заключается во внедрении вредоносного кода и похищении данных, – говорит Р. Агарвал, директор по маркетингу продукции в компании NSFocus. – Современные киберпреступники активно развиваются и постоянно совершенствуют методы своей деятельности».

Появление распределенной разновидности атак типа «отказ в обслуживании» привело к возникновению новых проблем, поскольку зараженные устройства, участвующие в нападении, расположены буквально по всему миру. Первые ботнеты формировались более 10 лет назад в среде компьютерных игроков, на базе ресурсов игровой индустрии и сайтов электронной торговли. Затем в течение нескольких последующих лет активность DDoS-атак была сравнительно невелика, но с 2012 г. они начали проявлять себя все заметнее и с тех пор лишь укрепляют свои позиции. Игровая индустрия до сих пор остается привлекательным объектом для нападений. В то

же время за последние несколько лет сфера применения DDoS-атак заметно расширилась и теперь включает в себя финансовый, правительственный, технологический секторы, а также сферу развлечений в целом.

Для организаций, полагающихся в своей деятельности на интернет-ресурсы и приложения (например, для предприятий сферы электронной торговли), последствия DDoS-атак могут быть разрушительными. Недоступные веб-сайты и серверы могут стать причиной того, что на репутацию компании будет брошена тень, а заказчики обратятся к ресурсам конкурентов.

При этом для успешной реализации DDoS-атаки не требуются ни особые знания, ни техническая оснащенность. Этот факт очень хорошо иллюстрируется ростом кибератак на образовательные учреждения. Зачастую учащиеся организовывают DDoS-атаки на свои учебные заведения просто самоутверждения ради. Например, не так давно 17-летний студент из штата Айдахо (США) заказал и оплатил злоумышленникам атаку на интернет-портал системы школьного округа West Ada School District. В результате учителя и студенты лишились возможности продолжать удаленную работу, а некоторым учащимся пришлось по нескольку раз пересдавать экзамены. «Для детей это всего лишь игра, но для учреждений образования и коммерческих структур она может очень дорого стоить», – говорит Т. Гаро, главный научный сотрудник компании Nexusguard (работала с учебными заведениями, ставшими жертвами кибератак).

Шквал DDoS-атак побуждает производителей рассматривать возможности сотрудничества в сфере обмена информацией о значимых кибератаках и их организаторах. Вопрос в том, говорит вице-президент компании F5 Д. Сталик, «насколько можно открыться, не рискуя потерять конкурентные преимущества?» ***(DDoS-атаки типа «отказ в обслуживании» заполняют Интернет // InternetUA (http://internetua.com/DDoS-ataki-tipa--otkaz-v-obslujivanii--zapolnyauat-internet). – 2015. – 6.07).***

***

Специалисты антивирусной компании ESET предупреждают об эпидемии мобильного SMS-трояна под видом популярного мессенджера WhatsApp.

Троянский вирус TrojanSMS.Agent.ZS ориентирован на смартфоны и планшеты на базе Android. Злоумышленники маскируют его под WhatsApp и распространяют через неофициальные магазины мобильных приложений.

Загрузив первый apk-файл с поддельным WhatsApp, вредоносная программа предлагает внести плату за использование приложения. После осуществления платежа начинается загрузка второго apk, который содержит дополнительные пакеты.

Затем троян переходит к установке в операционную систему и запрашивает права администратора, включая разрешение на отправку SMS. Разместившись на мобильном устройстве, TrojanSMS.Agent.ZS опустошает мобильный счёт пользователя, рассылая SMS на платные номера.

Кроме этого, вредонос самостоятельно совершает звонки и отправляет на удалённый сервер данные об устройстве и системе.

Последние обновления антивирусов уже научились распознавать этот троян. Тем не менее, специалисты советуют пользователям устанавливать приложения только с официальных площадок.

Аналитики Gartner установили, что недобросовестные компании техподдержки, обманом заставляя клиентов платить значительные суммы за установку ненужных им антивирусных продуктов, зарабатывают на этом миллионы ***(Эпидемия SMS-вируса начала опустошать счета владельцев Android-смартфонов // Блог Imena.UA (http://www.imena.ua/blog/sms-trojan-whatsapp/). – 2015. – 7.07).***

***

ИБ-эксперты предупреждают, что уязвимости в системах Oracle PeopleSoft могут стать причиной утечки персональных данных в бизнес-компаниях, государственных организациях и университетах. Исследователи из ERPScan определили 549 систем Oracle PeopleSoft, доступ к которым можно получить через Интернет. Двести тридцать одна из них уязвима к кибератакам типа TokenChpoken, которую эксперты ERPScan продемонстрировали в этом году.

По словам ИБ-эксперта из ERPScan А. Тюрина, самая критическая уязвимость кроется в некорректной генерации токенов для единого входа в систему. Исследователь создал сценарий, выполняющий брутфорс-атаку на токен и генерирующий новые cookie-файлы, и с успехом использовал его в ходе пентестинга систем PeopleSoft.

Технический директор ERPScan А. Поляков рассказал изданию SCMagazine о том, что многие крупные мировые компании используют платформу Oracle PeopleSoft для управления различными ресурсами организации, включая такую личную информацию, как номера социального страхования и данные платежных карт.

Согласно информации ERPScan, кибератака TokenChpoken может быть осуществлена злоумышленниками для получения доступа к любой учетной записи в Oracle PeopleSoft, в результате чего в руках преступников оказывается полный доступ к системе PeopleSoft.

Из 549 систем Oracle PeopleSoft, доступных через Интернет, 249 серверов принадлежат коммерческим предприятиям (169 компаний находятся в США), 64 сервера относятся к военным и государственным учреждением, а остальные 236 – университетам. Около 80 университетов используют систему Oracle PeopleSoft, которая уязвима к атаке TokenChpoken.

Стоит отметить, что в числе «уязвимых» университетов находится Гарвард, на компьютерную систему которого недавно была совершена кибератака. В результате нападения были скомпрометированы пароли электронной почты некоторых преподавателей, сотрудников и студентов (имена не уточняются) из многочисленных учебных подразделений.

А. Поляков отметил, что системы Oracle PeopleSoft являются сложными, и им недостаточно простого обновления ***(Из-за брешей в системах Oracle PeopleSoft могут быть похищены тысячи пользовательских данных // InternetUA (http://internetua.com/iz-za-breshei-v-sistemah-Oracle-PeopleSoft-mogut-bit-pohisxeni-tisyacsi-polzovatelskih-dannih). – 2015. – 8.07).***

***

Компания ESET обнародовала результаты анализа новой вредоносной программы Dino, использовавшейся в направленных кибератаках на ряд государственных учреждений.

Сообщается, что Dino представляет собой сложный бэкдор, написанный на языке C++ и использующий модульную архитектуру. Зловред может получать и выполнять в заражённой системе ряд команд злоумышленников. Особый интерес представляет команда search, позволяющая осуществлять поиск файлов по задаваемым характеристикам. Эксперты полагают, что основное назначение Dino – кража данных с последующей их отправкой на удалённый сервер.

Исполняемый файл Dino содержит множество информационных сообщений, позволяющих предположить, что программа разработана франкоговорящими специалистами. По мнению ESET, программа Dino создана кибергруппой Animal Farm, на что указывают характерные для данных авторов участки исполняемого кода и используемые алгоритмы.

Сложность вредоносного ПО Dino свидетельствует о высоком уровне технической подготовки его авторов. В частности, атакующие использовали специальные структуры данных и собственную файловую систему.

На сегодняшний день основная часть атакованных Dino государственных учреждений находится в Иране. Среди них – Министерство иностранных дел Ирана, Иранский университет науки и технологий, Организация по атомной энергии Ирана и пр. ***(Новое кибероружие Dino создано для атак на госучреждения // InternetUA (http://internetua.com/novoe-kiberorujie-Dino-sozdano-dlya-atak-na-gosucsrejdeniya). – 2015. – 9.07).***

***

Неизвестные хакеры взломали зенитные ракетные комплексы Patriot, переданные Германией Турции во временное пользование, сообщает Defence Talk со ссылкой на журнал Behoerden Spiegel. Хакерской атаке подверглись комплексы, установленные на границе с Сирией. Злоумышленникам удалось заставить Patriot отработать несколько команд, однако, что это были за команды, не уточняется. Предположительно, взломать комплексы хакеры смогли благодаря двум уязвимостям.

Одна из уязвимостей заключается в системе SSI, осуществляющей постоянный обмен данными в режиме реального времени между пусковой установкой и командным пунктом. Вторым потенциально уязвимым местом может быть система наведения зенитных ракет, обменивающаяся информацией

с боеприпасами. Благодаря недостаткам этих систем хакеры, предположительно, могут либо полностью перехватить управление ракетным комплексом, либо похитить с него всю информацию.

Турция использует зенитные ракетные комплексы Patriot, поставленные Германией, с 2012 г., когда в соседней Сирии началась гражданская война. При этом приграничная турецкая территория периодически подвергалась обстрелам. Ранее в Турции уже размещались подобные системы, разработанные в конце 1980-х годов. Это происходило в ходе двух иракских войн, в 1991 и 2003 г. В настоящее время на турецкой территории помимо немецких комплексов располагаются и Patriot вооруженных сил Нидерландов и США.

Зенитные комплексы Patriot способны обнаруживать цели на дальности до 180 км и вести одновременное сопровождение до 125 из них. При этом Patriot способен обеспечивать одновременный обстрел до шести целей, летящих на высотах от 60 м до 24 км на скорости до 2 тыс. м в секунду. Ранее Германия объявила, что намерена со временем заменить все устаревшие Patriot новыми зенитными комплексами MEADS ***(Хакеры взломали зенитные ракетные комплексы Patriot // InternetUA (http://internetua.com/hakeri-vzlomali-zenitnie-raketnie-kompleksi-Patriot). – 2015. – 9.07).***

***

Началась вторая за неделю волна атаки на систему Bitcoin. Работа пиринговой платежной системы сильно затруднена из-за большого количества транзакций, содержащих в себе минимальные суммы. Об этом сообщается в ленте новостей на blockchain.info

Новая волна атаки по приблизительным оценкам в 10 раз превосходит по нагрузке на сеть предыдущую, которая началась еще во вторник 7 июля. Причина затрудненной работы системы – так называемая «пыль» – спам микротранзакциями размером в 0,00001 BTC. Первую волну «пыли» суммарной стоимостью в 3 BTC почти целиком вычистил из системы китайский пул F2Pool, обработав самую большую в истории bitcoin цепь транзакций размером в один блок.

Портал Motherboard сообщает, что стоимость атаки уже составила 30 BTC и продолжает расти. На момент написания новости атака не прекращена. Многие майнеры обратили внимание, что время обработки транзакций увеличилось с 10 мин. до 14 часов. Один из адресов, использованных в качестве объекта атаки – кошелек портала Wikileaks. Как отмечает Motherboard, злоумышленники легко могут увеличить нагрузку на сеть, добавив вознаграждение за обработку «пыли». Вознаграждение повысит приоритет транзакции, и большая часть пиринговой сети будет занята обработкой спама, в то время как обычные платежи будут ожидать своей очереди долгое время.

Ранее, 6 июня, в системе Bitcoin произошел сбой, который обошелся майнерам в 50 тыс. дол. США и повысил количество подтверждений для каждой транзакции. Это, в свою очередь, создает дополнительную нагрузку на сеть, поскольку каждая транзакция «пыли» тоже обрабатывается дольше

обычного. О том, кто стоит за атакой, на текущее время ничего неизвестно ***(Началась массированная атака на систему Bitcoin // InternetUA (http://internetua.com/nacsalas-massirovannaya-ataka-na-sistemu-Bitcoin). – 2015. – 10.07).***

***

Мессенджер Telegram, созданный основателем «ВКонтакте» П. Дуровым, подвергся DDoS-атаке, которая привела к перебоям в работе сервиса по всему миру. Об этом сообщается на странице приложения в Twitter.

Как сообщают пользователи, приложение перестало работать в пятницу, 10 июля, около 17.30. В частности, оказалась недоступна функция отправки сообщений. «Глобальный DDoS на все датацентры Telegram. Кто-то недоволен», – уточнил в своем Twitter П. Дуров.

Предприниматель также отметил, что за последние два месяца по пользовательской активности Telegram возрос в три раза. «Неудивительно, что конкуренты взбесились», – написал П. Дуров.

Telegram достиг миллиарда отправленных сообщений в сутки в конце прошлого года – через 15 месяцев после запуска сервиса. По словам П. Дурова, мессенджером активно пользуются в Испании, Бразилии, Южной Корее, Мексике, Германии, Малайзии, Сингапуре, Индии, Саудовской Аравии, Италии и США. При этом доля пользователей из России в Telegram составила около 1 % ***(Мессенджер Дурова подвергся массовой DDoS-атаке // InternetUA (http://internetua.com/messendjer-durova-podvergsya-massovoi-DDoS-atake). – 2015. – 10.07).***

***

Более 500 тыс. пользователей загрузили Android-игры, содержащие вредоносный код для похищения логинов и паролей от аккаунтов пользователей в Facebook. Число скомпрометированных учетных записей неизвестно.

Словацкая компания Eset обнаружила вредоносный код в популярной мобильной игре для Android-устройств – Cowboy Adventure, а также еще в одной менее популярной игре – Jump Chess. Обе игры были доступны в официальном каталоге Google Play. Первая была загружена свыше 500 тыс. раз, вторая – свыше 1 тыс. раз.

При запуске Cowboy Adventure и Jump Chess пользователю предлагается ввести логин и пароль от его аккаунта в соцсети Facebook. Пользователь может перейти к игре, не делая этого. Если же он введет данные, они отправятся на неизвестный удаленный сервер. Кроме того, оба приложения взаимодействуют с еще одним сервером, который специалисты Eset классифицировали как командно-контрольный сервер злоумышленников.

«Анализ кода показал следующее: приложение взаимодействует с удаленным C&C-сервером через HTTPS, для сбора данных аккаунтов используется другой сервер (Drop Zone), его адрес программа получает

динамически в процессе работы», – рассказали CNews в российском представительстве Eset.

Сегодня многие мобильные приложения поддерживают обмен данными о достижениях с друзьями через Facebook или «ВКонтакте». Однако для этого пользователю не нужно в приложении вводит логин и пароль – подключение аккаунта выполняется с помощью собственных механизмов соцсетей без указания персональных данных, а лишь с помощью подтверждения. И само приложение доступ к этим данным не имеет.

Как подчеркнули в Eset, в случае с указанными играми от пользователя требуется именно введение логина и пароля.

Специалисты компании предполагают, что в игры Cowboy Adventure и Jump Chess встроен механизм «угона» аккаунтов в Facebook. «Доподлинно установить, сколько аккаунтов Facebook было скомпрометировано, в настоящее время невозможно. Известно, что не все пользователи, установившие игры, скомпрометировали свои учетные данные. Об этом свидетельствуют негативные комментарии на страницах приложений в Google Play», – сказали в Eset.

Примечательно, отметили в Eset, что обе игры были разработаны одной и той же компанией – Tinker Studio. Эксперты сказали, что не могут утверждать, что Tinker Studio – злоумышленники. «У нас нет таких полномочий», – прокомментировали CNews в компании. Тем не менее, оба приложения были опубликованы в Google Play от лица этой компании, и их описание в магазине соответствовала действительному функционалу. Этим они отличались от обнаруженных ранее вредоносных приложений для Android, которые лишь маскировались под легитимные продукты.

На момент публикации статьи оба приложения – Cowboy Adventure и Jump Chess – были удалены из Google Play ***(Google распространил более 500 тыс. приложений для взлома аккаунтов в Facebook // InternetUA (http://internetua.com/Google-rasprostranil-bolee-500-tis--prilojenii-dlya-vzloma-akkauntov-v-Facebook). – 2015. – 11.07).***

***

Каждый день появляются 5 тыс. новых вирусов для Android

Данные от аналитической компании G DATA говорят о стоящих перед мобильной операционной системой Android проблемах с безопасностью. В I квартале был выпущен доклад Mobile Malware, говорящий о появлении полумиллиона образцов вредоносного кода за первые три месяца нынешнего года. Это равнозначно появлению новой угрозы каждые 18 секунд или по 5 тыс. за сутки.

Недавнее исследование Pulse Secure показало, что 97 % разработанных для мобильных устройств вредоносных приложений нацелены на Android. Рост в I квартале по сравнению с концом прошлого года составил 6,4 % и 21 % по сравнению с I кварталом 2014 г. Помимо несовершенства самой Android, злоумышленников привлекает большое количество приложений онлайн-

банкинга и электронной коммерции. Уже 78 % пользователей глобальной сети по всему миру совершают в ней покупки, примерно 50 % пользуются онлайн-банкингом.

В продолжение данной темы, портал pcmag.com пишет о том, что российский мобильный рынок входит в пятёрку самых проблемных в плане распространения вредоносного ПО на Android. Компания Malwarebyte сообщает о новом трояне Android/Trojan.SMS.FakeInst.asy, нацеленном на российских пользователей.

Он выдаёт себя за надёжные приложения, маскируясь под именами вроде ContraCity.apk или Avito.apk. Троян сканирует наличие эмуляторов Android, в которых исследователи сетевой безопасности ведут тестирование подобного вредоносного ПО, стараясь тем самым избежать обнаружения. Программа распространяется через текстовые сообщения со ссылками на свой файл APK. При установке программа автоматически подключается к платным сервисам СМС и получает права администратора.

Эксперты традиционно рекомендуют устанавливать приложения только из надёжных магазинов, в первую очередь Google Play, и не переходить по неизвестным ссылкам, а также пользоваться антивирусами ***(Каждый день появляются 5 тысяч новых вирусов для Android // InternetUA (http://internetua.com/kajdii-den-poyavlyauatsya-5-tisyacs-novih-virusov-dlya-Android). – 2015. – 11.07).***

***

Обнаружен платный вирус для Android

Вредоносные приложения часто маскируются под полезные, предлагают владельцу смартфона / планшета / лэптопа / ПК скачать себя, обычно это бесплатно. Однако доклад Palo Alto Networks рассказывает об уникальном Android-вирусе Gunpoder, маскирующемся под эмулятор Nintendo. После скачивания он – потрясающая наглость – просит купить на себя лицензию! Это стоит от 20 до 49 центов, платёж проводится через сервисы вроде PayPal и Skrill. После покупки вирус начинает красть данные со смартфона (закладки и историю браузера, например), а также отправлять себя другим людям по SMS.

По словам Palo Alto Networks, вирус нацелен на пользователей, живущих в России, Ираке, Таиланде, Индии, Индонезии, ЮАР, Франции, Мексике, Бразилии, Саудовской Аравии, Италии, США и Испании – весьма случайный набор стран, нам кажется. Запомните название Gunpoder и никогда не устанавливайте (и тем более не покупайте) этот «эмулятор Nintendo» ***(Обнаружен платный вирус для Android // InternetUA (http://internetua.com/obnarujen-platnii-virus-dlya-Android). – 2015. – 12.07).***