СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(5–21.06)

2015 № 11

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(5–21.06)
№ 11

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

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

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Компания Facebook выпустила мобильное приложение, разработанное специально для медленных сетей и недорогих смартфонов под управлением Android. Об этом сообщил основатель и гендиректор компании М. Цукерберг на своей странице, передает Lenta.ru.

Размер приложения Facebook Lite, равный всего 1 мегабайту, позволяет скачать его с использованием не самой современной сотовой сети. Внутренняя оптимизация делает программу менее требовательной к скорости мобильного Интернета за счет сжатия контента на стороне сервера. Вторым значимым преимуществом для владельцев недорогих смартфонов является облегченный интерфейс.

Приложение уже доступно в ряде стран, где пользователи часто испытывают проблемы с доступом в Интернет. По словам М. Цукерберга, новинка пройдет открытое тестирование в Азии, Африке, Латинской Америке и Европе.

О том, что Facebook тестирует лайт-приложение для медленных Android-смартфонов, стало известно еще в январе этого года. Тогда клиент Facebook Lite был замечен в Google Play.

Это не первая инициатива Facebook привлечь жителей стран третьего мира в Интернет ***(Facebook выпустил облегченное приложение для медленных телефонов и сетей // From-ua (http://from-ua.com/news/349453-facebook-vipustil-oblegchennoe-prilozhenie-dlya-medlennih-telefonov-i-setei.html). – 2015. – 6.06).***

***

Все россияне, кому надоел vk.com, могут строить радужные планы – в рамках рынка стартапов в России презентовали новую соцсеть.

Сеть микроблогов будет называться Factcloud и представлять собой нечто вроде Twitter – только краткие факты и никакого информационного мусора (хотя с Twitter получилось как раз наоборот).

Разработчик ресурса С. Мельников обещает, что его Factcloud обеспечен возможностями фильтрации, оценки, сортировки поступающих сведений, определения их тематики и группирования по направлениям. То, что это не «ВКонтакте», понятно сразу – формат у соцсети твиттеровский, а дизайн – как у Pinterest ***(В России пытаются создать еще одну соцсеть // GlavPost.Com (http://glavpost.com/post/8jun2015/Nets/41439-v-rossii-pytayutsya-sozdat-esche-odnu-socset.html). – 2015. – 8.06).***

***

Один из самых популярных интернет-сервисов для ведения микроблогов различной тематики Tumblr представил функцию поиска по GIF-изображениям,

обещая, что это будет «определенно весело», пишет Marketing Media Review (http://mmr.ua/news/id/tumblr-zapustil-poisk-po-gifkam-44666).

Нововведение позволит зарегистрированным пользователям Tumblr быстро и удобно находить картинки в формате .gif, которые, по словам компании, «приходят на смену устаревшему многословию».

Когда определенная «гифка» будет выбрана кем-то для использования, ее «владелец» получит соответствующее уведомление любым способом, предусмотренным в настройках сервиса, – на телефон, в панели уведомлений и т. д.

Для встраивания GIF в Tumblr-пост необходимо нажать значок «+» в левой части экрана, далее – кнопку GIF, чтобы найти нужную картинку ***(Tumblr запустил поиск по gif-изображениям // Marketing Media Review (http://mmr.ua/news/id/tumblr-zapustil-poisk-po-gifkam-44666). – 2015. – 8.06).***

***

В Украине появилась новая социальная сеть Kozakam. Патриотическая социальная сеть, может быть, станет конкурентом «ВКонтакте».

Основателем сети стал 19-летний житель Киева Ю. Казински. Он объяснил, что «миссия проекта – это объединение всех жителей Украины в одной сети, так как во “ВКонтакте” становится небезопасно сидеть из-за тотального контроля ФСБ».

В настоящее время в сети зарегистрировано всего 10 человек. В Kozakam можно загружать пиратские копии песен в формате .mp3, а видео заходит по ссылкам с YouTube, RuTube, Vimeo.Com, Smotri.Com.

Внутрисетевая валюта Kozakam – «яныки», за которую можно покупать подарки и дарить их друзьям. Каждому пользователю начисляются 10 «яныков» за приведённого с собой пользователя ***(В Украине появилась новая социальная сеть Kozakam // Соціальний захист громадян (http://soc-in.com/component/content/article/4-news/8754-v-ukraine-poyavilas-novaya-socialnaya-set-kozakam.html). – 2015. – 9.06).***

***

Веб-версия Instagram обновилась и получила новый дизайн.

Ее функциональность практически не изменилась: можно просматривать свою ленту, отдельные профили, комментировать и лайкать отдельные снимки. Дизайн стал «чище». Лента обновлений теперь имеет более широкую колонку. Как и фотографии во время их просмотра. Примерно на 8 % больше, чем в предыдущей версии. Также переработано меню настроек ***(Instagram обновил дизайн // GlavPost.Com (http://glavpost.com/post/10jun2015/Nets/42585-instagram-obnovil-dizayn.html). – 2015. – 10.06).***

***

В середине мая 2015 г. Facebook запустила собственный мобильный агрегатор для статей из крупных СМИ, работающий для смартфонов на iOS. Но

месяц спустя ни одного нового материала не было опубликовано – приложение, судя по всему, провалилось.

Новинка Facebook Instant Articles вызвала ряд обсуждений в профильной блогосфере о том, станет ли новое начинание компании М. Цукерберга проблемой для СМИ или возможностью для завоевания новой аудитории.

При запуске Facebook обещала отдавать издателям 100 % рекламной выручки от реклам внутри публикаций в мобильном приложении и брать себе 30 % от объявлений между публикациями. На момент запуска социальная сеть заключила партнерство с девятью крупными контент-проектами и СМИ, включая BuzzFeed, The Atlantic, The New York Times и National Geographic.

Однако обещанного ажиотажа не произошло. Каждое из изданий опубликовало в приложении по одной-две статьи, а издания The Guardian, BBC, Spiegel Online и Bild вообще не выпустили ни единого материала за месяц ***(Facebook Instant Articles оказался невостребованным сервисом для СМИ // Блог Imena.UA (http://www.imena.ua/blog/facebook-instant-articles-fail). – 2015. – 11.06).***

***

Приложение Facebook Messenger загрузили в Google Play более миллиарда раз. Об этом сообщил возглавляющий Messenger Д. Маркус. Помимо Messenger, по миллиарду загрузок набрали Facebook, WhatsApp (оба выпускаются Facebook), а также Gmail, YouTube, Search и Maps (все от Google).

Отметим, что, помимо основной функции обмена сообщениями, Facebook также имеет возможность интеграции сторонних приложений. Это, в частности, спортивный сайт ESPN, сайт для создания смешных видео и открыток JibJab и поиск анимированных изображений в формате .gif Giphy. Кроме того, через мессенджер можно общаться с техподдержкой магазинов и переводить друзьям небольшие денежные суммы.

В 2014 г. Facebook сделала Messenger отдельным приложением, а в апреле того же года убрала возможность отправить сообщение из основного приложения ***(Число дня: сколько раз в Google Play загрузили Facebook Messenger // GlavPost.Com (http://glavpost.com/post/11jun2015/Soft/43059-chislo-dnya-skolko-raz-v-google-play-zagruzili-facebook-messenger.html). – 2015. – 11.06).***

***

Facebook будет учитывать время, которое пользователи тратят на прочтение постов, для улучшения качества новостей в ленте. Об этом сообщается в блоге одного из разработчиков компании Анши Ю.

В сообщении отмечается, что иногда пользователи соцсети не делятся новостью и не ставят отметку «мне нравится», но при этом тратят на изучение поста определенное время. Разработчик уверена, что читатель не всегда хочет поделиться контентом, но при этом проявляет интерес, который можно учитывать при составлении персональной ленты.

Кроме того, отмечается, что новая функция будет иметь ограниченные возможности, поскольку пользователь может потратить 10 сек на прочтение поста из любопытства, но при этом долгое пребывание на странице может быть связано и с плохим интернет-соединением ***(Facebook научится анализировать потраченное на чтение постов время // InternetUA (http://internetua.com/Facebook-naucsitsya-analizirovat-potracsennoe-na-cstenie-postov-vremya). – 2015. – 15.06).***

***

Как растет мобильная аудитория «ВКонтакте» в Украине – статистика за начало 2015 года

Запуск в Украине нового стандарта мобильной передачи данных, более известного как 3G, сулит выгоду не только пользователям и операторам сотовой связи, но и бизнесу – в особенности в сфере IT и Интернет. Смартфон становится полноценным устройством, с которого можно продавать товары, услуги и, конечно же, рекламу. Поэтому популярная в Украине социальная сеть «ВКонтакте» с большим оптимизмом наблюдает за тем, как растет ее мобильная аудитория. Уже на сегодня во «ВКонтакте» с мобильных устройств заходят около 7,6 млн украинцев еженедельно, а когда развертывание 3G будет завершено, руководство соцсети ожидает усиление миграции пользователей в мобильное пространство. О том, как это происходит в настоящее время, расскажет более подробная аналитика от компании на AIN.UA (http://ain.ua/2015/06/15/586025).

Около 4,5 млн украинцев еженедельно заходят в социальную сеть с настольных компьютеров и мобильных устройств, при этом исключительно с помощью мобильных устройств соцсеть просматривают 3,1 млн в неделю. Только в Киеве исключительно через мобильные гаджеты во «ВКонтакте» заходят более полумиллиона пользователей.

Соотношение платформ

По данным Liveinternet, в мае 2015 г. среднесуточное число уникальных посетителей из Украины, заходивших в социальную сеть с мобильных устройств, составило 5,4 млн (по данным на декабрь 2014 г. их было не более 4,3 млн).

Операционная система Android – вторая по популярности ОС среди пользователей «ВКонтакте» в Украине: 5,9 млн человек в неделю заходит со смартфонов на базе Android (больше украинцев пользуются vk.com только с десктопной Windows 7). На втором месте среди мобильных ОС – платформа iOS (1,1 млн), остальные пользователи посещают социальную сеть с Windows Phone (230 тыс.), Blackberry (около 3 тыс.) и других операционных систем.

Мобильные технологии традиционно выбирает самая активная аудитория возрастом от 18 до 34 лет. Как для iOS, так и для Android соотношение популярности мобильного доступа, исходя из возрастных показателей, примерно одинаковое.

Миграция в мобайл

По охвату сайт ежемесячно уже посещают более 60 % интернет-пользователей из Украины. В процентном соотношении доля пользователей mobile-only от общей недельной украинской аудитории «ВКонтакте» оказалась на уровне 27 %. Остальные 73 % – это приверженцы стационарных компьютеров и пользователи смешанного типа потребления.

«За миграцией пользователей на мобильные платформы мы наблюдаем последние несколько лет. Очевидно, что в дальнейшем число посетителей "ВКонтакте", которые вообще не используют компьютеры, будет только увеличиваться: как в абсолютном измерении (с ростом пользовательской базы), так и в относительном – процент десктопа постоянно будет падать. Современные смартфоны зачастую оказываются мощнее и функциональнее многих компьютеров, а развитие мобильного Интернета позволяет пользоваться всеми возможностями социальной сети со смартфонов и планшетов», – пояснил AIN.UA «операционный директор "ВКонтакте"» А. Рогозов.

Он также заявил, что при разработке новых и оптимизации действующих сервисов «ВКонтакте» этот тренд учитывают: в будущем, вероятно, многие нововведения сначала будут появляться в приложениях, а только потом уже на vk.com.

Напомним, в декабре 2014 г. AIN.UA публиковал итоговую статистику от «ВКонтакте» по Украине не только в мобильном, но и десктопном измерениях. 13 ноября соцсеть установила новый рекорд – за сутки на сайт зашло 12,1 млн пользователей из Украины. Что касается мобильных пользователей, то в прошлом году, по данным LiveInternet, их количество достигало 4,3 млн в день ***(Яровая М. Как растет мобильная аудитория «ВКонтакте» в Украине – статистика за начало 2015 года // AIN.UA (http://ain.ua/2015/06/15/586025). – 2015. – 15.06).***

***

Снова сменился алгоритм выдачи новостей в соцсети Facebook, теперь решающим станет время просмотра материала для того, показываются ли заметки или ссылка в общей новостной ленте максимальному числу пользователей или нет.

Разработчики анонсировали изменения, подчеркнув, что в настоящее время пользователи комментируют, лайкают и повторно публикуют далеко не каждый пост, который для них важен. Поэтому изменения в работе новостной ленты Facebook призваны устранить этот недостаток. Люди, как правило, читают длинные интересные материалы, но далеко не всегда повторно их публикуют – скорее, они предпочитают обсуждать их в комментариях к записи или просто лайкнуть, не делясь публикацией с другими людьми. Новинка заработает для всех пользователей соцсети в ближайшие несколько недель и, как обещают, не затронет особо выдачу материалов от страниц брендов, компаний и СМИ ***(Facebook снова меняет алгоритм выдачи публикаций в***

новостной ленте // Блог Imena.UA (http://www.imena.ua/blog/facebook-news-again). – 2015. – 13.06).

***

Во время интервью каналу CNBC профессор Гарвардской школы бизнеса Б. Джордж сравнил сервис микроблогов Twitter с «BlackBerry социальных медиа».

По словам ученого, эта социальная сеть демонстрирует существенное отставание, по сравнению с конкурентами. Б. Джордж также был одним из критиков бывшего главы Twitter Д. Костоло и призывал к его отставке несколько месяцев назад. «У них даже нет рабочей группы по поиску, – сказал он. – Что они делают? Мир оставляет их позади. <...> Если они продолжат в том же духе, то это не сулит Twitter ничего хорошего. Я вижу, что они чувствуют себя так же плохо, как и последние пять лет».

11 июня стало известно, что Д. Костоло добровольно оставит занимаемую им должность. Главой социальной сети временно станет ее сооснователь Д. Дорси. Он примет новые обязанности с 1 июля. Причин ухода Д. Костоло не называют. Он уточнил, что начал переговоры об уходе в конце прошлого года. Д. Костоло возглавлял соцсеть с октября 2010 г.

К слову, за последний год в Twitter снизилось число новых пользователей. В IV квартале 2014 г. рост упал до 1,4 %, а в I квартале 2015 г. – поднялся до 4,6 %. По итогам этого года в социальной сети с 302 млн пользователей планируется рост в 14,1 %. Для сравнения: в 2013 г. рост достигал 30 %. За 2014 г. в Twitter дважды менялись главы по продукту: весной это место занял бывший сотрудник Google Д. Грэф, а в декабре его сменил К. Вейл ***(Twitter – это «BlackBerry социальных медиа» // iLenta.com (http://ilenta.com/news/company/news_7087.html). – 2015. – 16.06).***

***

Facebook выпустила новое приложение Moments, которое позволяет обмениваться фотографиями, не публикуя их в социальной сети. Программа призвана решить проблему обмена изображениями между пользователями, которые не хотят, чтобы снимки оказались в открытом доступе.

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.

Moments также может автоматически определять, кто запечатлен на снимке, чтобы сразу отправить ее другу. В социальной сети уверены, что им удалось найти «золотую середину» между отправкой фотографий в публичные альбомы в соцсети и сохранением изображений в закрытые аккаунты на фотохостингах.

Приложение Moments является детищем внутреннего подразделения компании Facebook Creative Labs. Ранее студия выпустила новостную читалку Paper и «убийцу» Snapchat – Slingshot.

Приложение Moments уже доступно для загрузки в американском App Store. О сроках выхода программы в других странах пока не сообщается ***(Facebook выпустила новое приложение для обмена фотографиями // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/facebook-vypustila-novoe-prilozhenie-dlya-obme.html). – 2015. – 15.06).***

***

Социальная сеть Twitter снимет ограничение на величину личных сообщений, которая в настоящее время составляет 140 знаков. Об этом сообщил руководитель проекта Direct Messages в Twitter Inc. С. Агарвал, передает пресс-служба микроблога.

Ограничение будет установлено в 10 тыс. знаков. Сообщается, что ограничение будет снято в июле.

При этом С. Агарвал отметил, что длина твитов останется прежней ***(Twitter снимет ограничение в 140 знаков в личных сообщениях // Версии.com (http://versii.com/news/329054). – 2015. – 13.06).***

***

Сервис микроблогов тестирует кнопки загрузок приложений, которые позволяют пользователям устанавливать мобильные приложения известных СМИ непосредственно из профилей в Twitter.

Поначалу функция была замечена на странице профиля The New York Times в Twitter, а затем – в аккаунте The Guardian. В эксперимент также вошли собственные сервисы соцсети – Vine и Periscope. Представители Twitter подтвердили проведение эксперимента, проводимого в рамках улучшения пользовательского опыта, однако отказались предоставить более подробную информацию ***(Twitter тестирует карточки загрузок приложений новостных изданий // likeni.ru (http://www.likeni.ru/events/Twitter-testiruet-kartochki-zagruzok-prilozheniy-novostnykh-izdaniy). – 2015. – 17.06).***

***

Первый инвестор Facebook запустил соцсеть для американских избирателей и политиков. Миллиардер из Кремниевой долины Ш. Паркер представил социальную сеть для политиков – Brigade. Предполагается, что новая сеть поможет людям со всего мира «решать проблемы, которые не способна решить Facebook».

Социальная сеть Brigade подразумевает, что, кроме политических деятелей, в ней сможет зарегистрироваться и рядовой гражданин, чтобы обратиться к чиновнику любого уровня для решения своих проблем.

Кроме того, на базе социальной сети существует платформа для обсуждения изменений законодательства. Пользователи могут голосовать за те или иные инициативы, которые, как им кажется, должны быть введены в стране. Например, в настоящее время в социальной сети обсуждается вопрос платного обучения. Активисты из США предлагают сделать его бесплатным для студентов, которые вынуждены совмещать учебу с работой, чтобы содержать семью.

На сегодняшний день в Brigade зарегистрировано около 13 тыс. тестовых пользователей, которые сформировали примерно 90 групп по интересам. В перспективе такое объединение может стать активной группой с четкими убеждениями или даже превратиться в новую политическую силу.

Для политиков, считает Ш. Паркер, участие в специализированной социальной сети станет не только способом рекламировать свои достижения и демонстрировать на публике свою работу, но и даст возможность собирать мнения избирателей, чтобы корректировать политический курс страны.

Также данная социальная сеть позволит обзавестись необходимой поддержкой политикам, которые предлагают непопулярные, но нужные меры ***(Первый инвестор Facebook запустил соцсеть для американских избирателей и политиков // Блог Imena.UA (http://www.imena.ua/blog/brigade). – 2015. – 19.06).***

***

23 червня всі сайти, на яких встановлений плагін Facebook Like Box, автоматично переключаться на новий плагін сторінки Facebook Page Plugin. Крім того, Facebook додав у плагін сторінки кілька нових функцій: поліпшену підтримку ширини блоку й кнопки, що містять call-to-action.

«На прохання нашої спільноти розробників ми оновили плагін сторінки, тепер він підтримує як широкі блоки розміром 500px, так і вузькі – 180px, – пояснюють в Facebook. – Зверніть увагу, що ви можете побачити незначні зміни макета через брак місця при роботі з вузьким блоком. Наприклад, при розмірі в 180px ви не побачите кнопку Share.

Плагін тепер підтримує кнопки, що містять заклик до дії, як на сторінці. Наприклад, якщо на сторінці є кнопка “зареєструватися” або “зв’яжіться з нами”, то вона з’явиться і в плагіні сторінки на сайті і буде працювати так само. Це не вимагає яких-небудь змін в конфігурації плагіна користувачами».

Фахівці Facebook представили плагін сторінки в березні поточного року на конференції розробників. Плагін, який прийшов на зміну блоку Like для веб-сайтів, дає можливість сайтам просувати свою сторінку в Facebook, при цьому відвідувачі ставлять лайк і діляться сторінкою, не покидаючи сайт.

Плагін дає змогу підвищити впізнаваність сторінки і залученість користувачів. Люди можуть швидко побачити, хто з їхніх друзів поставив лайк сторінці ***(Facebook замінить Like-бокс для сторінок на спеціальний плагін // UkrainianWatcher (http://watcher.com.ua/2015/06/15/facebook-zaminyt-like-boks-dlya-storinok-na-spetsialnyy-plahin). – 2015. – 15.06).***

***

Twitter запустил новый интерфейс отображения диалогов в хронике. Нововведение призвано сделать их чтение более удобным.

«Обсуждения, окружающие твиты, особенно если они включают множество ответов и отдельные разговоры, сложно читать, – отметил продакт-менеджер компании А. Кумар. – Поэтому мы внедрили несколько изменений, призванных облегчить этот процесс: сгруппировали диалоги и выделили наиболее интересные ветки прямо под твитом. Для этого учитывался такой фактор, как ответы автора твита».

Твиты, относящиеся к отдельным веткам обсуждений, объединены линией. Чтобы увидеть больше твитов в каждой ветке, нужно нажать на ссылку «посмотреть другие ответы».

Новый функционал запускается в десктопной версии сервиса. В будущем он также будет внедрен в мобильных приложениях. Конкретные сроки представитель компании не назвал.

Напомним, что последний раз Twitter вносил изменения в отображение обсуждений в хронике в 2013 г. ***(Twitter изменил отображение диалогов в хронике // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_izmenil_otobrazhenie_dialogov_v_hronike). – 2015. – 17.06).***

***

Найвідоміший сервіс мікроблогів готує власний агрегатор новин та тематичного контенту під назвою Project Lightning. Запуск новинки очікується до кінця 2015 р.

У межах цього агрегатора відбиратиметься контент за конкретними подіями, опублікований у Twitter, а також додаватиметься відео та фото. Усі матеріали в тематичних потоках можна буде інтегрувати зі сторонніми сайтами чи додатками.

Повідомляється, що в мобільному додатку Twitter з’явиться нова кнопка. При натисканні на неї користувач потраплятиме на сторінку вибору конкретної події – там демонструватимуться усі твіти, фотографії та відео з конкретного заходу чи місця.

Діапазон подій буде доволі широким – від музичних фестивалей чи вручення нагород у змаганнях і на престижних кінопреміях до надзвичайних подій на кшталт ураганів та повеней. Стрічка контенту в подіях оновлюватиметься автоматично, а також буде реалізовано підтримку автоматичного відтворення для відеороликів ***(Twitter готує власний агрегатор контенту // Блог Imena.UA (http://www.imena.ua/blog/twitter-lightning). – 2015. – 21.06).***

***

Популярний відеосервіс YouTube запускає одразу три тематичні відеоканали, присвячені новинам і пов'язаному з ними відеоконтенту – YouTube NewsWire, First Draft та Witness Media Lab.

Повідомляється, що YouTube NewsWire створюватиметься спільно з агенцією новин Storyful і до нього ввійдуть найбільш цікаві відео з місця подій, зроблені очевидцями. Перевірка достовірності та відбір найкращих роликів здійснюватимуть співробітники Storyful.

FirstDraft шукатиме відеоконтент із соціальних мереж, а також перевірятиме його достовірність і відповідність етичним стандартам. Компанія обіцяє восени запустити спеціальний сайт, де будуть надані поради та роз'яснення щодо того, як створювати подібне відео.

Witness MediaLab буде присвячено боротьбі за права людини, у чому допомагатиме відео порушень громадянських прав і свобод. Серед перших тем, висвітленням яких займатиметься канал, стане надмірне насильство з боку поліції та силових структур у США ***(YouTube запускає тематичні відеоканали з новинами // Блог Imena.UA (http://www.imena.ua/blog/youtube-channels). – 2015. – 21.06).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Департамент госзакупок Министерства обороны Украины будет публиковать информацию о планируемых закупках для нужд ВСУ на своей странице в Facebook. Об этом сообщила волонтер Д. Яровая, передает «Цензор.НЕТ».

«Прошу обратить внимание на данную страницу в Facebook. Это страница департамента государственных закупок Министерства обороны.

На этой странице будет публиковаться информация о ближайших планируемых закупках Министерством обороны. Просьба всех производителей, заинтересованных в работе с Министерством обороны, подписаться на страницу, а также максимально ее распространить», – просит волонтер ***(Департамент госзакупок Минобороны будет сообщать о планируемых закупках в Facebook // Цензор.НЕТ (http://censor.net.ua/news/339208/departament_goszakupok_minoborony_budet_soobschat_o_planiruemyh_zakupkah_v_facebook_volonter_dana_yarovaya). – 2015. – 8.06).***

***

Компания Brand Analytics опубликовала исследование социальных сетей в России за 2015 г. Примечательно, что в рейтинге топ-20 блогеров рунета половина – украинцы. Возглавил рейтинг Б. Филатов, а на втором месте расположился оппозиционный журналист А. Шарий. Об этом пишет Ain.ua.

Также среди лидеров рейтинга такие известные общественные и политические деятели, как А. Геращенко, С. Семенченко, Д. Тымчук, Р. Шрайк, А. Мочанов, Б. Береза и др. Рейтниг «ВКонтакте» представлен преимущественно российскими видеоблогерами, артистами и светскими львицами.

Сами фигуранты рейтинга не скрывают удивления. «Согласно презентации Brand Analytics проекта российской компании “Ай-Теко”, ваш покорный слуга является лидером всего (!) русскоязычного Фейсбука (по степени вовлеченности). На втором месте, с большим отрывом гадкое животное по кличке Шарик. Такие дела… Но больше мое самолюбие тешит то, что я живу на нашей, Богом нам данной, земле. Україна понад усе. Слава нації», – прокомментировал свою «победу» Б. Филатов.

Не остался в стороне и Р. Шрайк: «Я не знаю что такое “русскоязычный сегмент Фейсбука”, но половина из топ-20 в нем – украинцы». Что касается А. Шария, его, очевидно, не удивило попадание в данный рейтинг, пусть и не на первое место. Он не стал благодарить россиян за доверие, а вместо этого акцентировал внимание на своем “толерантном” ответе Б. Филатову, который упомянул Анатолия в неуважительной манере».

Во «ВКонтакте» и Instagram россияне преимущественно интересуются страницами культурных деятелей и светских львов/львиц своей страны, а вот в Twitter среди страниц с самыми большими рейтингами вовлеченности россиян также встречаются оппозиционные. Например, на шестом месте аккаунт А. Навального, а на 12 – телеканала «Дождь» ***(Украинцы Филатов и Шарий возглавили рейтинг самых популярных блогеров русскоязычного Facebook // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43608/118/lang,ru). – 2015. – 5.06).***

***

Міністерство закордонних справ у партнерстві з «Європейською правдою» готують зустріч глави МЗС П. Клімкіна з його Twitter-фоловерів. Про це йдеться в матеріалі «ЄвроПравди» та МЗС «Павло Клімкін: розвіртуалізація».

«Настав час вийти в офлайн і познайомитися», – ідеться в повідомленні міністерства для ЗМІ.

П. Клімкін зустрінеться з декількома фоловерами, які нададуть найцікавіші відповіді на розміщені в Twitter запитання.

Детальний опис того, як відбуватиметься відбір, подав у своєму твіті П. Клімкін, також ця інформація наведена на сторінці ЄП з описом проекту.

Фоловери обговорять з міністром зовнішню політику та будуть запрошені на екскурсію по міністерству. «Розмова не буде обмежена 140 знаками», – зазначили в міністерстві.

Слід зазначити, що аудиторія Twitter-акаунта П. Клімкіна за рік зросла з трохи більше тисячі до 96 тис. фоловерів ***(Клімкін зустрінеться зі своїми твіттер-фоловерами // Media Sapiens (http://osvita.mediasapiens.ua/web/social/klimkin_zustrinetsya_zi_svoimi_tvitterfoloverami). – 2015. – 10.06).***

***

Люди объединяются для поисков и досуга

Районы Киева все больше замыкаются на себе, превращаясь в своеобразные информационные анклавы. Благодаря развитию инфраструктуры открываются кинотеатры, супермаркеты, фитнес-центры, у многих жителей отпадает нужда выезжать за пределы родного массива, кроме как на работу, пишет «Сегодня» (http://kiev.segodnya.ua/kpeople/kievlyane-v-socsetyah-v-soobshchestvah-rayona-nahodyat-ugnannye-avto-razyskivayut-zhivotnyh-i-dazhe-vlyublyayutsya-622920.html).

Кроме того, соседей сближает Интернет. Причем каждый район столицы обзавелся своими сообществами – специальными группами в социальных сетях. В них можно узнать о последних локальных событиях, новых заведениях, открывшихся поблизости, найти попутчика для велопрогулки или даже отыскать любимого человека. Например, на Березняках пытаются создать первое районное интернет-телевидение, сюжеты для которого будут снимать сами зрители. «Сегодня» пообщалась с создателями пяти самых крупных пабликов, посвященных жизни киевских районов, и узнала, как они помогают своим соседям-подписчикам.

«Троещина ВК». Каждый 20-й житель Троещины подписан на это сообщество. В общей сумме набегает более 40 тыс. человек. Сперва группа задумывалась для общения и знакомств местных жителей, но со временем переросла в координационный центр жилмассива. Он занимается поиском пропавших животных, предупреждает о мошенниках, организовывает субботники, информирует о разных мероприятиях.

«Неделю назад наш подписчик увидел запись об угоне авто, а потом обнаружил его у себя во дворе. Три дня назад в группу написала девушка о пропаже собаки. Через 5 мин животное нашлось», – хвастается айтишник С. Полоз, основатель «Троещина ВК».

Кроме того, в группе некоторым даже удается найти свою любовь – парни выкладывают свои фотографии и предлагают познакомиться. Есть и фотографии сложившихся пар – тех, кто встретился в реальной жизни после переписки и начал отношения. Группа немало зарабатывает на рекламе – деньги идут на поддержку сообщества и зарплату трем модераторам. До конца этого года С. Полоз планирует дорасти до 50 тыс. подписчиков.

«ПОХ». Три массива Дарницкого района объединяет группа «ПОХ» – Позняки, Осокорки, Харьковский. В 2008 г. ее основал киевлянин А. Травкин. В настоящее время группа насчитывает 30 тыс. подписчиков.

«В современном мире коммуникация между людьми минимальная. Я решил собрать на одной площадке всех, кто живет по соседству. Кто-то находит напарника для игры в сквош, кто-то для прогулки на велосипеде», – рассказывает А. Травкин. К примеру, в группе искали хозяев ручной вороны и лабрадора. Еще делились информацией о пляжах «на районе», где можно купаться.

«Типичное Голосеево». Группа ориентирована сразу на несколько соцресурсов и насчитывает около 11,5 тыс. подписчиков «ВКонтакте», 4,5 тыс. на Facebook, 2,5 тыс. в Instagram. В основном это местные жители, но немало людей из других районов, которым интересен контент.

Группа освещает локальные проблемы: сомнительные застройки, нелегальные МАФы, установленные на газоне и т. д. «Через подписчиков мы собираем макулатуру, а вырученные деньги отправляем на помощь нашим солдатам. Также сотрудничаем с райвластями – анонсируем их мероприятия. Может, когда-то нам грамоту за это вручат», – улыбается основатель сообщества К. Рухлов.

«Я люблю Оболонь». Сообщество насчитывает около 7 тыс. подписчиков. Они делятся между собой информацией о разных находках и пропажах, организовывают флешмобы и критикуют городскую власть. Например, недавно разместили фото матраса в дорожной яме с подписью «матрасное латание». К слову, дорожники на следующий день убрали матрас, а яму лишь щебнем засыпали...

«Городские СМИ нередко берут у нас новости, благодаря огласке наши проблемы быстрее решаются. Кроме того, сообщество помогает самоорганизоваться жителям района, а коллективно отстаивать свои права проще», – считает общественный активист Г. Антоненко, основатель группы «Я люблю Оболонь».

«Welcome to Борщага». Группа основана в прошлом году, поэтому у нее пока менее тысячи подписчиков. Тем не менее, сообществу уже удается собирать людей для решения общих проблем: провели несколько субботников, отремонтировали детскую площадку и посадили деревья.

«Борщага всегда считалась бандитским и не самым благополучным “спальником” Киева. Но, несмотря на это, мы искренне любим свой район. В одиночку бороться сложно, а объединившись, можно сделать его лучше и дать отпор тем, кто мешает нам спокойно жить», – заявляют организаторы ***(Одаренко С. Киевляне в соцсетях: в сообществах района находят угнанные авто, разыскивают животных и даже влюбляются // Сегодня (http://kiev.segodnya.ua/kpeople/kievlyane-v-socsetyah-v-soobshchestvah-rayona-nahodyat-ugnannye-avto-razyskivayut-zhivotnyh-i-dazhe-vlyublyayutsya-622920.html). – 2015. – 11.06).***

***

17 червня міністр інформаційної політики України Ю. Стець і заступник міністра А. Біденко зустрілися з директором з питань громадської політики Facebook у Скандинавії, Центральній і Східній Європі та Росії Т. Крістенсеном та керівником напряму громадської політики Facebook у Центральній та Східній Європі Г. Чех. Про це повідомляє прес-служба міністерства.

Під час зустрічі було обговорено політику Facebook щодо контенту користувачів, а також процедури подання, розгляду та реагування на скарги. Зокрема, міністр інформаційної політики порушив питання блокування акаунтів українських політиків, громадських діячів, експертів, а також звернув увагу на проблематику оцінки контенту в соціальній мережі.

Представники Facebook підтвердили, що розпочинають з українською стороною діалог щодо більш ретельних і виважених підходів до моніторингу українського сегмента Facebook. Вони запевнили, що весь моніторинг та аналіз українського сегмента відбувається винятково в операційному офісі в Дубліні (Ірландія) на засадах аполітичності та дотримання стандартів соціальної мережі.

Крім того, ішлося про можливість відкриття офісу компанії Facebook у Києві. «Звичайно, я розумію, що ви самостійно оцінюєте ступінь необхідності такого кроку. Однак я впевнений, що, крім мене, цього прагнуть всі користувачі соціальної мережі Facebook в Україні», – зазначив міністр ***(Стець обговорив з керівництвом європейського офісу Facebook політику щодо контенту користувачів // Телекритика (http://www.telekritika.ua/kontekst/2015-06-17/108305). – 2015. – 17.06).***

***

16 червня в Національній раді з питань телебачення і радіомовлення відбулася зустріч голови Національної ради Ю. Артеменка, його заступника Г. Шверка, члена Національної ради О. Ільяшенка, а також працівників апарату регуляторного органу з представниками компанії Facebook Т. Крістенсеном, директором з питань громадської безпеки Facebook у Скандинавії, Центральній і Східній Європі та Росії, С. Алдоус, менеджером із громадської політики підрозділу Facebook у Великій Британії, Г. Чех, керівником напряму громадської політики в Центральній і Східній Європі. Ішлося про особливості модерування контенту компанією, повідомляє сайт Нацради.

Ю. Артеменко окреслив головні виклики, що постають перед Україною в рамках боротьби з інформаційною агресією Росії. Він звернув увагу на те, що останнім часом частішають випадки блокування у Facebook акаунтів тих користувачів, які вирізняються активною антиросійською позицією. Голова Нацради навів конкретні приклади спланованих атак спеціальними службами.

Т. Крістенсен зі свого боку докладно розповів про організаційну структуру Facebook, принципи й механізми, за якими відбувається модерування контенту. За його словами, компанія має чіткі правила, які передбачають можливість блокування контенту, тимчасового карантину і як останній захід –

видалення акаунта в разі порушення вимог щодо допустимих матеріалів. Останні не можуть містити мови ненависті, прямих погроз, зневаги й приниження за ознаками статті, раси, національності тощо.

За словами Т. Крістенсена, працівники компанії, які реагують на скарги користувачів щодо контенту, дуже добре навчені, причому їхнє навчання триває постійно. У разі потреби вони звертаються за допомогою до інших фахівців. Тож сама система розгляду скарг достатньо складна. Він також запевнив, що в команді Facebook є фахівці, які розуміють і українську мову, і українську специфіку.

Водночас, зважаючи на реальні факти блокування акаунтів українців, представники Facebook обіцяли вивчити й проаналізувати цей матеріал. Вони також погодилися обдумати ініціативну пропозицію Ю. Артеменка щодо можливості зустрічі експертів обох сторін, аби докладніше обговорити питання модерування контенту.

У червні соціальна мережа Facebook відповіла на петицію користувачів і пояснила блокування акаунтів популярних українських користувачів. Відповідь опублікована на сервісі Change.org, де була створена петиція. На думку Facebook, соцмережа не порушувала власних стандартів, розроблених компанією ***(Члени Нацради теж обговорили з менеджерами Facebook модерування контенту в соцмережі // Телекритика (http://www.telekritika.ua/kontekst/2015-06-17/108317). – 2015. – 17.06).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Компания Pinterest объявила о запуске пинов с возможностью покупки – простого и безопасного способа приобретать товары прямо в социальной сети. Функция станет доступна американским пользователям iOS в конце этого месяца, позднее появятся версии для десктопов и Android.

«Pinterest является каталогом идей, – говорит представитель компании. – Наша миссия заключается не только в том, чтобы показать идеи, но и помочь воплотить их в жизнь. Пины с возможностью покупки – следующий шаг в этом направлении, так как мы приносим радость открытия товаров в ваших любимых магазинах оффлайн и онлайн».

Пользователи смогут покупать товары на Pinterest, когда они увидят синюю цену и кнопку «купить». В поисковых фильтрах также появится фильтр по цене. Это сделает новый функционал более полезным, а сам Pinterest – более эффективным.

Когда пользователь хочет совершить покупку, он может нажать кнопку «купить» и оплатить товар с помощью Apple Pay или кредитной карты. Личную информацию следует ввести один раз. Так как Pinterest сотрудничает с платежными системами, он не будет хранить информацию о кредитных картах. Одним из партнеров является Stripe.

В настоящее время Pinterest работает только с несколькими крупными брендами и двумя коммерческими платформами. Если компания использует Shopify, в аккаунте можно добавить канал Pinterest. После этого компания сможет запустить пины с возможностью покупки с помощью нескольких кликов.

Shopify – в настоящее время единственный способ для малого и среднего бизнеса продавать товары с помощью новых пинов. Все заказы, товары и клиенты компании в Pinterest будут автоматически синхронизироваться с Shopify. В ближайшие недели смогут запустить пины с возможностью покупки пользователи Demandware.

Всем остальным компаниям следует зарегистрироваться в списке ожидания. В компании стремятся установить высокую планку для функции, поэтому не будут делать ее доступной мгновенно для всех сразу.

Pinterest также работает над новым материалом для своей платформы для разработчиков, которая даст новые возможности для покупок и продаж.

О том, что Pinterest готовит запуск кнопки buy («купить»), стало известно в феврале текущего года ***(Pinterest запускает пины с возможностью покупки // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/pinterest_zapuskaet_piny_s_vozmozhnostyu_pokupki). – 2015. – 9.06).***

***

Что делать b2b-бренду в Instagram?

Instagram занимает все больше места в работе маркетологов. Но, кажется, это утверждение имеет отношению только к сфере b2c.

Недавнее исследование Social Media Examiner показало, что маркетологи примерно одинаково симпатизируют YouTube, Google+ и Pinterest, если речь идет о сфере b2c, и практически не проявляют там активности, работая со сферой b2b.

Можно подумать, что b2b-маркетологи не считают Instagram эффективным инструментом. Но есть один момент. Да, b2c все еще доминирует в этой социальной сети, но 40 % b2b-маркетологов планируют увеличить свою активность в Instagram.

Известный западный SMM-специалист Б. Рейнман рассказала, для чего b2b-компании могут использовать Instagram. Например, здесь они могут рассказывать историю бренда, устанавливать долгосрочные связи, демонстрировать навыки, очеловечивать бренд и создавать сообщество.

Ключ к эффективному использованию Instagram как маркетингового инструмента для b2b-брендов – не думать о нем как о маркетинговом инструменте вообще. Вместо этого нужно воспринимать Instagram как способ рассказать вашу историю в рамках большой маркетинговой онлайн-стратегии. Fedex (американская компания, предоставляющая почтовые, курьерские и другие услуги логистики по всему миру. – Прим. ред.) делает это очень хорошо. Их лента в Instagram полна красиво скомпонованных фото, на многих из

которых изображены легко узнаваемые грузовики и самолеты Fedex. Когда вы просматриваете ленту Fedex, то невольно чувствуете, что пока вы лениво скролите, они активно работают. Складывается впечатление, что грузовики Fedex всегда куда-то едут, всегда что-то доставляют, всегда есть. Для компаний, которые полагаются на своевременные поставки, это действительно важное сообщение.

PR-менеджер сервиса Mention.com Б. Бергер рекомендует использовать Instagram, чтобы показывать историю компании, продвигать демоверсии и руководства, делиться корпоративными новостями, распространять контент с других каналов, улучшать ситуативный маркетинг, запускать конкурсы и транслировать корпоративную культуру.

Эксперт по работе в Instagram Г. Джордан дал следующие рекомендации по успешному развитию бренда в соцсети: «Вы должны развивать беседу между брендом/бизнесом и вашими подписчиками/клиентами. Чем ближе они к бизнесу, тем больше шансов, что они станут супер-поклонниками. Это легко сделать в Instagram, просто лайкая и комментируя контент других пользователей и делая репосты их интересных фотографий у себя в ленте.

Еще один хороший способ поддержания вовлеченности – предложить подписчикам показать вам свои лучшие фотографии, которые имеют отношение к вашему бизнесу, в обмен на возможность быть размещенными у вас на странице. Сохранить все материалы поможет специальный хештег, который будут использовать ваши подписчики» ***(Что делать b2b-бренду в Instagram? // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/chto_delat_b2b_brendu_v_instagram). – 2015. – 8.06).***

***

10 главных законов маркетинга в социальных сетях

Используя возможности контента и SMM, вы можете расширить свою аудиторию и клиентскую базу. Но начинать работу, не имея опыта или понимания принципов, может оказаться не так уж и просто.

Если вы решили расширить возможности своего бизнеса и заняться продвижением в социальных сетях, важно понимать основы работы с ними. Улучшение качества вашей работы в сети поможет построить фундамент, который будет направлен на вашу аудиторию, бренд и, главное, на результат вашей работы.

Предлагаем 10 законов SMM, которые немного упростят вашу работу.

1. Закон «Слушать»

Успех работы в социальных медиа заключается в том, что нужно больше слушать и меньше говорить. Читайте информацию, которую публикуют ваши потенциальные клиенты, интересуйтесь, о чем они дискутируют. Это важно для того, чтобы узнать, что для них важно. Только тогда вы сможете создать контент, который на самом деле будет ценным для вашей аудитории, а не принесет еще больше беспорядка в ее жизнь.

2. Закон «Узкая специализация»

Лучше быть хорошим специалистом в одной сфере, чем быть мастером на все руки, но не доводить ни одного дела до конца. Целенаправленная стратегия в социальных сетях и активная деятельность, направленная на построение сильного бренда, имеет больше шансов на успех, чем всеобъемлющий замысел, который пытается удовлетворить максимум запросов.

3. Закон «Качество»

Качество должно превосходить количество. Суть этого принципа заключается в том, что лучше иметь 1 тыс. подписчиков, которые читают, обсуждают и делятся со своей аудиторией вашим контентом, чем 10 тыс. подписчиков, которые исчезнут после того, как впервые установят контакт с вами.

4. Закон «Терпение»

Социальные сети и контент-маркетинг не станут успешными в один миг. Конечно, вы можете получить моментальный успех, но, скорее всего, вам все же придется долго трудиться, чтобы достичь результатов.

5. Закон «Ключевые слова»

Если вы публикуете уникальный, качественный контент и стараетесь делать его интересным для других пользователей в сети, то, скорее всего, они поделятся им на своих страничках в соцсетях, блогах.

Такое распространение информации открывает новые возможности для вашего контента в поисковых системах, чему и будут способствовать ключевые слова. Люди получают больше возможностей для поиска вашей информации в Интернете.

6. Закон «Влияние»

Пообщайтесь в сети с влиятельными людьми в вашей сфере, которые имеют вашу потенциальную аудиторию и, возможно, заинтересуются вашей продукцией, услугами или бизнесом. Связывайтесь с этими людьми и старайтесь настроить деловые отношения с ними.

Если вы сможете стать для них источником интересной информации, то они тоже могут рассказать о вас своей аудитории, что позволит вам выйти на новый уровень.

7. Закон «Значимость»

Если вы тратите все свое время на продвижение ваших товаров и услуг, то велика вероятность, что со временем люди перестанут обращать на вас внимание. Вы должны придавать больше значения общению. Сосредоточьтесь на создании уникального контента и общайтесь с влиятельными особами. Со временем такие люди станут сильным маркетинговым катализатором для вашего бизнеса.

8. Закон «Признание»

Вряд ли вы не обратите внимание на человека, который будет обращаться к вам в повседневной жизни, так же не стоит никого игнорировать в социальных сетях. Построение отношений является одной из наиболее важных

составляющих успеха маркетинга в социальных сетях, поэтому всегда отвечайте людям, которые к вам обращаются.

9. Закон «Доступность»

Не исчезайте сразу же после публикации контента. Будьте доступны для своей аудитории. Это значит, что вам необходимо постоянно обновлять контент и участвовать в обсуждениях. Онлайн-аудитория отличается непостоянностью, и если вы исчезните на пару недель, то она моментально переключится на что-то другое.

10. Закон «Взаимность»

Не стоит ожидать, что кто-то поддержит вашу точку зрения и будет говорить о вас, если вы не сделаете того же для него. Находясь в сети, вы должны постоянно стараться обмениваться информацией и обсуждать то, что публикуют другие ***(10 главных законов маркетинга в социальных сетях // GlavPost.Com (http://glavpost.com/post/9jun2015/Nets/42091-10-glavnyh-zakonov-marketinga-v-socialnyh-setyah.html). – 2015. – 9.06).***

***

Яндекс передала соцсеть «Мой круг» Хабрахабру. Теперь за проект будут отвечать издатели «Хабрахабра». Пока что детали сделки не разглашаются.

По словам разработчиков, такое решение было принято для того, чтобы сделать данный сервис еще более привлекательным для пользователей. Предложение о сотрудничестве поступило от компании «Тематические медиа», которая работает над сайтами «Мегамозг», «Хабрахабр» и др. ***(Яндекс передала соцсеть «Мой круг» Хабрахабру // GlavPost.Com (http://glavpost.com/post/9jun2015/Companies/42047-yandeks-peredala-socset-moy-krug-habrahabru.html). – 2015. – 9.06).***

***

В ближайшие месяцы Instagram позволит покупать рекламу большему числу рекламодателей и активирует таргетинг, позволяющий нацеливать объявления на пользователей с конкретными интересами.

Кроме того, на днях сервис начнет тестировать новые форматы рекламы прямого отклика (direct response), которые будут включать ссылки «купить», «установить», «узнать больше» или «подписаться».

Эти нововведения последовали за недавним внедрением рекламных объявлений в виде карусели, которые впервые позволили рекламодателям ссылаться на сторонние сайты в постах в Instagram. Изначально новинка была внедрена в США. В прошлом месяце доступ к ней получили рекламодатели из некоторых других стран.

Анонсированный всплеск рекламной активности – значительное изменение для Instagram, который всегда предельно осторожно относился к вопросу показа рекламы своим пользователям.

После приобретения компании социальной сетью Facebook от Instagram не требовалось больших усилий в направлении монетизации. Это дало возможность сервису неспешно и осторожно внедрять рекламу.

Отдельное внимание уделялось тому, чтобы реклама в Instagram выглядела как нативный контент. Эта стратегия сделала рекламу в сервисе особенно эффективной. Исследование Nielsen Brand Effect, охватившее более 475 кампаний в рамках сервиса в мировом масштабе, показало, что отклик на спонсированные посты в Instagram был в 2,9 раз выше, чем нормы агентства для онлайн-рекламы.

До сих пор рекламу в визуальном сервисе могли покупать только крупные бренды. Теперь она будет доступна более широкому кругу рекламодателей, включая представителей малого и среднего бизнеса.

По данным компании, в ближайшие месяцы рекламу в сервисе можно будет купить через платформу покупки рекламы Facebook и API Instagram, а также через отдельные агентства и маркетинговых партнеров компании ***(В Instagram появится больше рекламы // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/v_instagram_poyavitsya_bolshe_reklamy). – 2015. – 10.06).***

***

Facebook тестирует новую функцию под названием «Сохраненные ответы» (Saved Replies), которая позволяет владельцам бизнес-страниц писать, сохранять и затем повторно использовать шаблонные сообщения при общении со своими клиентами в социальной сети. Функция позволит сэкономить время при обработке входящих запросов. Администраторы страниц могут использовать готовые шаблоны или создать собственные.

«Сохраненные ответы» доступны отдельным компаниям в интерфейсе обмена сообщениями на страницах Facebook. Некоторые администраторы страниц отмечают, что функция не работает на мобильных устройствах.

Ответы можно персонализировать с помощью автозаполнения. Функционал предлагает варианты персонализации, которые позволяют вставить имя и фамилию клиента или администратора страницы, а также адрес сайта.

Представители социальной сети запуск функции не комментируют.

«Сохраненные ответы» помогут, в основном, компаниям малого бизнеса, в том числе стартапам, домашнему бизнесу и прочим магазинам, которые имеют список стандартных ответов для копирования и вставки в сообщения.

В I квартале текущего года общая вовлеченность брендов в Facebook возросла на 43,5 % по сравнению с аналогичным периодом 2014 г. ***(Facebook тестирует функцию «Сохраненные ответы» // ProstoWeb (http://www.prostoweb.com.ua/layout/set/print/internet_marketing/sotsialnye_seti/novosti/facebook_testiruet_funktsiyu_sohranennye_otvety). – 2015. – 11.06).***

***

Доля зарубежных клиентов, которые принесли доход от рекламы компании Facebook, впервые превысила число американских рекламодателей и составила 51 % от мировых продаж. Об этом сообщает gazeta.ru.

Об этом свидетельствуют данные компании за I квартал. Также отмечается, что рост клиентов из Азии составил 57 %. «Следующие 1 млрд клиентов ожидаются именно из этих стран», – добавила вице-президент Facebook К. Эверсон.

Доходы компании от рекламы увеличились на 46 % – до 3,3 млрд дол. По сравнению с аналогичным периодом прошлого года доходы от рекламы возросли на 36 %.

Также К. Эверсон добавила, что в настоящее время мобильная реклама является наиболее привлекательной для рекламодателей и составляет более 70 % от общего дохода компании ***(Facebook удалось увеличить доходы от рекламы вне американского рынка // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43654/118/lang,ru). – 2015. – 11.06).***

***

Компания NewsWhip подобрала самые удачные примеры использования Instagram различными изданиями. Согласно статистике, уже в текущем году пользователями этой платформы станут 27,6 % жителей США.

При этом, с точки зрения издателей, Instagram – не самый удобный ресурс, поскольку он не позволяет размещать ссылки на оригинальные материалы и, следовательно, не ведет к прямому росту трафика. Тем не менее, многие издания научились использовать эту платформу эффективно.

1. Самый простой и очевидный вариант – использование Instagram для создания фотогалерей. Так поступает, например, National Geographic – и ландшафтные снимки, публикуемые изданием, регулярно собирают сотни тысяч откликов.

2. Самостоятельная платформа для дистрибуции контента. Например, NowThis Media не просто размещает в Instagram полноценные новостные ролики, но еще и специально монтирует и оформляет видеоматериалы с учетом особенностей этой платформы. BBC News также готовит для Instagram полноценные самостоятельные материалы.

3. Продолжение уже опубликованных (или готовящихся к публикации) репортажей. Речь идет о размещении в Instagram роликов и снимков, полученных изданиями во время подготовки основного материала, но не вошедших в него. В качестве примера приводится материал The New York Times о подростковой беременности: снимки и фрагменты диалогов с его героинями попали в Instagram.

4. Вовлечение аудитории. Модератор The Huffington Post Canada недавно рассказал NewsWhip о том, что отклики, собранные в соцсетях (в том числе в

Instagram, где пользователи особенно благосклонны), становятся основой для новых материалов. Аналогичный подход использует Chicago Tribune.

5. Реклама и ознакомление пользователей с брендом. Этот подход работает в первую очередь для изданий, посвященных моде и образе жизни, среди примеров – Vogue и Vanity Fair ***(Пять удачных примеров использования Instagram // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/pyat_udachnyh_primerov_ispolzovaniya_instagram). – 2015. – 16.06).***

***

Twitter объявил о запуске нового вида таргетинга для рекламы мобильных приложений. Нововведение позволяет нацелиться на тех пользователей, кто успешно установил приложения из определенных категорий.

Новый функционал поможет рекламодателям взаимодействовать с теми пользователями, кто наиболее заинтересован в приложениях их компании. С его помощью также можно нацеливаться на пользователей приложений в категориях, релевантных тем, которые установлены на мобильном устройстве. Кроме того, нововведение можно будет комбинировать с другими видами таргетинга.

Twitter также добавил отчетность для категорий установленных приложений на панели управления для рекламодателей. Отчеты будут доступны для всех кампаний по рекламе приложений, даже если они не используют новый вид таргетинга.

Новый функционал доступен всем пользователям iOS и Android-устройств по всему миру ***(Twitter запустил новый вид таргетинга // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_zapustil_novyy_vid_targetinga). – 2015. – 18.06).***

***

Google запустил измерение Brand Lift (повышения узнаваемости бренда) для объявлений, показанных в мобильном приложении YouTube.

Такой шаг связан с тем, что более половины трафика YouTube поступает с мобильных устройств. Обновление призвано дать рекламодателям больше информации о том, как их объявления вызывают отклик у пользователей, в том числе повышают ли они информированность о бренде, а также увеличивают ли намерения приобретения товара.

В Google говорят, что после запуска Brand Lift годом ранее провели более 10 тыс. исследований кампаний YouTube. В апреле текущего года специалисты выпустили агрегированные результаты в своей программе Google Preferred, согласно которым 94 % рекламных кампаний YouTube имели средний уровень запоминаемости 80 %.

Новый отчет eMarketer показывает, что мобильная видеореклама является самым быстрорастущим цифровым рекламным форматом в США, но инвестиции рекламодателей в мобильное видео отстают от десктопного. Доля затрат на мобильную видеорекламу, как ожидается, достигнет 47,7 % к 2019 г.

Год назад Google запустил бета-версию нового продукта BrandLift, бесплатного автоматизированного инструмента для оценки влияния видеорекламы в Интернете на изменение брендовых метрик. Он был призван помочь маркетологам верно определять эффективность рекламных стратегий ***(На YouTube появился параметр повышения узнаваемости бренда // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/na_youtube_poyavilsya_parametr_povysheniya_uznavaemosti_brenda). – 2015. – 15.06).***

***

Кнопка «купить» в соцсетях: выгода или угроза?

Еще год назад почти никто не задумывался о возможности совершать покупки в социальных сетях. Однако уже сегодня Google, Pinterest, Twitter и Facebook надеются, что покупки через профили их ресурсов станут самой распространенной интернет-тенденцией следующего года.

За последние 12 месяцев все четыре цифровые платформы успели объявить о планах протестировать или запустить кнопку «купить» с целью превратить свои площадки в торговые центры онлайн.

Но, несмотря на энтузиазм разработчиков, процесс движется слишком медленно, сталкиваясь со значительными препятствиями:

– необходимость подключения к платформам платежных систем, которыми пользуются ритейлеры. Для больших магазинов, которые никогда не торговали товарами вне своих онлайн и оффлайн площадок, перейти на Facebook будет достаточно сложно;

– постоянный мониторинг соответствия рекламируемых товаров и продукции, которая есть в наличии на складах ритейлера;

– убеждение предпринимателей в необходимости продавать товары на платформе, а покупателей в надежности нового сервиса.

Что заставило соцсети разработать кнопку «купить»?

Существует несколько факторов, которые заставили руководство крупнейших социальных сетей внедрять платежные функции на своих платформах.

Реклама. Неслучайно бизнес всех соцсетей получает львиную долю прибыли из рекламы. Внедрение кнопки «купить» прямо в объявления может увеличить количество кликов по рекламе, следовательно, привлечь больше трафика на сайт рекламодателя и повысить конверсию. Такой результат должен убедить ритейлеров, поддерживающих опцию продажи товара на Facebook или в Twitter, давать больше рекламы. Для соцсетей выгода очевидна. Чем больше рекламы, тем выше прибыли.

Конкуренция. Возможность покупок позволяет соцсетям конкурировать с крупными торговыми площадками и переманивать ритейлеров, которые теряют прибыль на традиционных маркетплэйсах. Исследования показывают, что пользователи соцсетей восприимчивы к рекламе. Так, 87 % подписчиков Pinterest совершают покупки на основании того, что видели на сайте.

Тем не менее, Facebook и Twitter пока не начинают массовый запуск приложения. Несмотря на то, что некоторые товары в микроблоге Twitter с кнопкой «купить» продавались достаточно хорошо, компания не торопится внедрять эту опцию для всей рекламируемой продукции. Руководство соцсети сконцентрировано на сотрудничестве с платежными провайдерами для отлаживания процесса оплаты прямо в микроблоге. Facebook уже 11 месяцев занимается тестированием кнопки и не подключает к услуге известные бренды.

Многие стартапы понимают перспективы нового сервиса, но пока не подключают кнопку «купить», потому что не представляют, как это решение будет работать со всеми магазинами, которые рекламируются в соцсетях.

Соцсети должны создать стандартный механизм подключения и дальнейшего использования кнопки «купить». Более того, чтобы заставить торговцев подключиться, нужно гарантировать им какие-то бонусы. «Необходимо ввести механизм, который будет повышать рейтинг магазинов, которые интегрировали кнопку “купить”, – написал директор торгового стартапа о Google. – Поскольку Google является одним из основных источников трафика, многие торговцы будут вынуждены переходить на продажи в поисковике, спровоцировав своих конкурентов тоже внедрять кнопку “купить” прямо в поисковой ленте Google» ***(Кнопка «купить» в соцсетях: выгода или угроза? // InternetUA (http://internetua.com/knopka--kupit--v-socsetyah--vigoda-ili-ugroza). – 2015. – 17.06).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Британские ученые из Университета Брунел проанализировали, как поведение человека в социальной сети соотносится с его типом личности. Исследователи проанализировали несколько сотен активных участников Facebook, сопоставляя характеристики реальных людей с проявлениями их виртуальных образов. Учитывалось сразу несколько психологических характеристик личности: уровень невротизации, нарциссизма, открытости,

добросовестности, уступчивости, экстраверсии, а также самооценка испытуемого.

В результате исследования ученые сделали несколько выводов. К примеру, если страница пользователя наполнена полезной информацией, заметками или обсуждениями важных событий общественно-политической или культурной жизни, то владелец аккаунта, с большой долей вероятности, открытый и креативный человек. Огромное количество разнообразной «околоспортивной» информации об упражнениях, диетах, фитнесе, как правило, свидетельствует о достаточно высоком нарциссизме пользователя. Обилие же информации о личной жизни человека может свидетельствовать о разном. К примеру, если пользователь делится информацией о своей семье и близких, он, скорее всего, ответственный и добросовестный. А вот множество сообщений об интимных переживаниях пользователя свидетельствует не о старательности и обязательности, а о низкой самооценке.

В последние годы социологи и психологи все чаще обращают внимание на социальные сети как на относительно новую форму общественной коммуникации. К примеру, в 2012 г. ученые из университетов Лунда и Гетеборга (Швеция) проанализировали несколько сотен человек на предмет «темных» сторон их натуры. Исследователи пришли к выводу, что «нарциссы» слишком неразборчивы в знакомствах. Такие люди склонны буквально «коллекционировать» друзей, добавляя к себе даже незнакомцев. Также шведские ученые полагают, что пользователи, которые не афишируют в социальной сети свои эмоции, зато активно размещают на странице провокационные и циничные высказывания и шутки, склонны быть расчетливыми и манипулировать другими. Люди, беззастенчиво делящиеся порно или «жестью», могут быть обладателями психопатических черт характера.

Само собой, все подобные исследования не являются инструкциями по удаленной постановке диагноза. Но в некоторых случаях социальные сети, действительно, становятся основой для формирования первого впечатления о человеке. К примеру, известно, что рекрутеры и работодатели зачастую подробно изучают информацию о соискателе в Интернете. Зная это, человек вполне может заранее сформировать свою страницу таким образом, чтобы заинтересованные лица прочитали между строк именно ту информацию, какую захочет дать пользователь. К примеру, многих менеджеров по персоналу в первую очередь интересует объем контента на странице. Чем больше человек размещает фотографий, картинок, мыслей, тем более он склонен выставлять свои чувства напоказ. Для одних профессий это может быть полезным, для других – совершенно неприемлемым ***(Что можно узнать о пользователе по Facebook-аккаунту // InternetUA (http://internetua.com/cto-mojno-uznat-o-polzovatele-po-Facebook-akkauntu). – 2015. – 21.06).***

Маніпулятивні технології

На канале федерального канцлера Германии А. Меркель в социальной сети Instagram будут удалять кириллические комментарии. Об этом заявила пресс-секретарь федерального правительства Германии в интервью изданию Frankfurter Allgemeine Sonntagszeitung. По ее словам, канал А. Меркель в Instagram запустили 3 июня.

«После старта канала за считанные часы собралось несколько сотен комментариев кириллическим шрифтом», – отметила представительница правительства.

Сначала группа редакторов-модераторов канала канцлера проверила содержание этих комментариев, большинство из которых оказались полными ненависти к А. Меркель и Украине, отмечает издание. Так как всего несколько сотрудников группы владели русским, поначалу пришлось прибегать к услугам онлайн-переводчиков. Впрочем, наплыв флуда был таким мощным, что было решено вообще больше не допускать русскоязычных комментариев.

Атака троллей

Поскольку размещенный в социальных сетях продукт федерального правительства Германии «обычно немецкоязычный», то «из соображений читабельности» решили удалить комментарии на других языках, пояснила пресс-секретарь немецкого правительства. Исключение составляют только комментарии на английском. Комментарии же кириллицей «постепенно удалили», добавила она.

Несмотря на это, на канале и в дальнейшем появляются комментарии на русском языке, пересыпанные бранными и оскорбительными словами и выражениями. Нередко такие комментарии удаляют только через несколько часов после появления, пишет издание. Причиной этого является отсутствие предварительного фильтра для вычитки и допуска таких комментариев на сайт.

Как выяснило издание, есть немало оснований считать, что речь идет об организованных троллях. Ведь большинство комментариев, по данным газеты, оставляли российские пользователи, зарегистрированные только под именем. Впрочем, правительственный пресс-секретарь заверила, что не владеет информацией о происхождении оскорблений бранных комментариев ***(На канале Меркель в Instagram будут удалять комментарии кириллицей // GlavPost.Com (http://glavpost.com/post/8jun2015/Nets/41414-na-kanale-merkel-v-instagram-budut-udalyat-kommentarii-kirillicey.html). – 2015. – 8.06).***

***

Компанія «Донецьке кабельне телебачення» заблокувала доступ до 39 інтернет-ЗМІ. У переліку цих сайтів – радіо «Собода», «Цензор.Нет», Громадське телебачення Донеччини, Громадське телебачення та інші медіа.

«Шановні абоненти! Уже повідомлялося про обмеження доступу до певних ресурсів мережі Інтернет на вимогу міністерства інформації та зв'язку ДНР. Список заблокованих ресурсів був розширений і зараз виглядає наступним чином...» – ідеться в зверненні донецького провайдера Інтернету й кабельного телебачення ***(У Донецьку заблокували 39 сайтів українських інтернет-видань // InternetUA (http://internetua.com/u-donecku-zablokuvali-39-sait-v-ukra-nskih--nternet-vidan). – 2015. – 9.06).***

***

В российской социальной сети «ВКонтакте» решили творчески подойти к острому политическому вопросу оккупации украинского Крыма Россией, пишет «Обозреватель» (http://obozrevatel.com/crime/54762-i-nashim-i-vashim-vkontakte-sdelali-kryim-ukrainsko-rossijskim.htm).

Так, на вопрос пользователя А. Панычева о том, когда в соцсети украинские города Симферополь и Севастополь будут показываться российскими, судя из скриншота, техподдержка ВК ответила, что «поиск крымских городов для разных стран будет работать по-разному» ***(И нашим, и вашим: «ВКонтакте» сделали Крым «украинско-российским» // Обозреватель (http://obozrevatel.com/crime/54762-i-nashim-i-vashim-vkontakte-sdelali-kryim-ukrainsko-rossijskim.htm). – 2015. – 10.06).***

***

Сервис микроблогов Twitter реализовал новую функцию, которая позволит пользователям помогать друг другу избавляться от неприятных собеседников и спамеров. Для этого достаточно экспортировать список заблокированных аккаунтов и поделиться им, пишут «Экономические известия» (http://news.eizvestia.com/news_technology/full/372-twitter-budet-banit-trollej-i-spamerov-optom).

Теперь для того чтобы забанить троллей или злостных спамеров, не нужно блокировать аккаунты поодиночке. Достаточно импортировать список таких аккаунтов, которым поделился с вами кто-то еще. Экспорт списка блокировок, как и импорт, осуществляются через меню настроек на twitter.com.

Кроме того, доступ к спискам блокировок получают и разработчики, что позволит им интегрировать эту возможность в свои продукты.

Twitter запустил отдельный пункт меню в настройках аккаунта, посвященный блокировкам, в декабре прошлого года. Тогда же заблокированным пользователям закрыли доступ к просмотру профилей тех, кто их блокировал. Twitter часто критикуют за неэффективную борьбу с троллями и спамерами, но сервис, как видно, старается стать лучше и безопаснее для пользователей ***(Twitter будет банить троллей и спамеров «оптом» // Экономические известия (http://news.eizvestia.com/news_technology/full/372-twitter-budet-banit-trollej-i-spamerov-optom). – 2015. – 11.06).***

***

План России по захвату Левобережной Украины, озвученный народным депутатом А. Геращенко в Facebook, вполне может быть реальным. Однако, опубликовав его в личном блоге, нардеп поступил необдуманно и лишний раз продемонстрировал напряженность между различными ветвями украинской власти. Об этом в комментарии изданию «Гордон» заявил общественный активист А. Мочанов.

«Мы обсуждали этот вопрос с людьми из Генштаба. Учитывая, что часть вещей совпадает, включая то же наступление на Марьинку, и точки соприкосновения очевидны, то опубликованный план имеет под собой почву, – отметил А. Мочанов. – Однако в данной ситуации А. Геращенко, помимо погони за лайками на Facebook, надо было бы связаться с Генштабом и обсудить этот вопрос. Меня в большей степени здесь интересует не то, насколько этот план может соответствовать действительности. Он же рассчитан больше на то, чтобы запугать, мы все это прекрасно понимаем».

По мнению А. Мочанова, А. Геращенко мог бы посоветоваться с Генштабом, прежде чем публиковать такие резонансные данные. «Антон как серьезный менеджер, понимая, что это вызовет панику и резонанс в обществе, должен был связаться с людьми из другого политического лагеря и спросить: “Ребята, вот такая информация. Скажите: вброс или не вброс?” Все же бегут за сиюминутной популярностью на Facebook, не понимая, что эта популярность как лампочка для мошки: сел и сгорел», – считает А. Мочанов.

…«Для россиян это шикарный вброс, им же надо все время чем-то кормить свою публику, которая не понимает, куда уходят люди от них и почему они не всегда возвращаются, а если возвращаются, то в холодильнике», – отметил А. Мочанов.

По его мнению, шансы на реализацию подобного сценария есть и армия к нему готова, однако проблемы в системе государственного управления и безразличное отношение к войне со стороны простых людей могут упростить дело агрессору ***(Мочанов: Геращенко погнался за популярностью на Facebook, не посоветовавшись с Генштабом // From-ua (http://from-ua.com/news/350458-mochanov-geraschenko-pognalsya-za-populyarnostyu-na-facebook-ne-posovetovavshis-s-genshtabom.html). – 2015. – 18.06).***

***

Facebook блокує профілі за білоруську мову на прохання російських тролів

Усі адміністратори з Port Europa при вході на свої профілі отримали інформацію про тимчасове заблокування їхніх приватних аккаунтів з огляду на розміщення «недозволених матеріалів». Про це йдеться на порталі Port Europa.

На сайті соцмережі також зазначалося, що у випадку надходження ще скарг «репресії можуть посилитись аж до цілковитого видалення сторінки».

Головний редактор порталу Я. Логінов зауважив, що нині росіянам заважає саме існування білоруської мови. «Як бачите, росіянам вже заважають

не лише пости осіб, щоб підтримують Майдан чи АТО. Росіяни вважають, що стандартам Facebook не відповідає також саме існування білоруської мови і заохочення до її вивчення. Це методи ще зі сталінських часів, коли Москві так само не подобалось, що на території Радянського Союзу були якісь інші мови, крім російської», – розповідає він.

Я. Логінов пригадує, що багато людей тоді потрапили до таборів через те, що писали вірші білоруською чи українською мовою й таким чином намагалися розвивати ці мови, зберегти їх від знищення. «Це страшно, що у XXI ст. адміністрація Facebook іде шляхом Сталіна і блокує профілі з тієї причини, що хтось опублікував статтю, що заохочує українців вивчати білоруську мову», – каже редактор.

За україномовний сегмент Facebook відповідає московський офіс компанії, «який неодноразово займався політичною підтримкою Путіна і так званих сепаратистів», наголошується на сайті.

Port Europe засмучені й тим, що польський офіс Facebook також не реагує на діяльність російських тролів, які за допомогою масових скарг блокують профілі проукраїнських активістів. Постраждалі адміни мають намір звертатися до польських журналістів і неурядових організацій, аби здійснити тиск на адміністрацію Facebook, щоб вона припинила дії, які перетворюють цей портал на знаряддя російської пропаганди.

Сторінка запису на безкоштовний е-курс білоруської мови для українців була визнана такою, що не відповідає стандартам Facebook.

11 червня MediaSapiens повідомляла про створення безкоштовного е-курсу білоруської мови для українців. Це було знаком подяки за підтримку значною частиною білоруського суспільства Майдану й АТО ***(Facebook блокує профілі за білоруську мову на прохання російських тролів // Media Sapiens (http://osvita.mediasapiens.ua/web/social/facebook_blokue_profili_za_bilorusku_movu_na_prokhannya_rosiyskikh_troliv). – 2015. – 17.06).***

Зарубіжні спецслужби і технології «соціального контролю»

В России записывают разговоры всех граждан, рассказал основатель соцсети «ВКонтакте» П. Дуров в интервью изданию The Kernel, сообщает BG со ссылкой на Medialeaks.

П. Дуров объясняет такую прослушку граждан тем, что «страной управляет человек из разведки». «Он понимает, что хорошо иметь что-нибудь на каждого, на всякий случай. Информация – это сила, особенно в XXI в. Чем больше информации, тем больше власти. Если кто-то раскроет дела правительства, как Э. Сноуден раскрыл АНБ, медиа все опубликует – и в обществе будут против этого», – цитирует П. Дурова издание.

Следят за гражданами не только в России: известно, что правительство США ответственно за прослушки по всему миру, говорит П. Дуров, ссылаясь

на документы Э. Сноудена. По его словам, Э. Сноуден даже рассматривал его предложение работать во «ВКонтакте», но отказался из соображений безопасности ***(Павел Дуров: В России прослушивают всех // InternetUA (http://internetua.com/pavel-durov--v-rossii-proslushivauat-vseh). – 2015. – 9.06).***

***

Популярні українські дописувачі Facebook оголосили, що мають наміри подати на соцмережу до якогось з українських судів. Про це на прес-конференції в Києві повідомили п'ятеро відомих у соцмережі українців, серед яких депутат Верховної Ради Б. Береза (понад 120 тис. читачів), журналіст Ю. Бутусов (135 тис.) і літератор А. Бондар (20 тис.), пише ВВС Україна.

Мета – не так отримати матеріальне відшкодування від репутаційних втрат, як надати справі розголосу й привернути увагу самого Facebook і міжнародних ЗМІ до проблеми «кремлівських тролів». «Справа в принципі, – пояснив завдання судового позову А. Бондар, якого навесні забанили за вірш про "Чё там у хохлов". Facebook завдає нам репутаційної шкоди, так само ми можемо і мусимо завдати йому цих втрат. Бо коли така велика соціальна мережа є знаряддям цензури, зокрема російської, це – скандал. Ну ось ми і скандалимо».

У прес-службі Facebook, куди звернулася ВВС Україна, не стали коментувати ідею із судом.

А. Гук, партнер юридичної фірми «Анте», каже, що шанси на розгляд справи в Україні є. Свій позов блогери планують обґрунтувати, спираючись на український закон про міжнародне приватне право. «Якщо ви споживаєте послугу без комерційної мети, і якщо ви є громадянином України і послугу вам надає іноземний елемент, у цьому випадку Facebook, то ви маєте право свої споживацькі права захищати в українському суді, – пояснює юрист. – Можливо, це буде наше легендарне українське ноу-хау: Печерський районний суд, який може скасувати все, аж до рішення ООН, нарешті стане на захисті наших прав. Печерський суд – це образно. Куди саме подавати скаргу, блогери ще не вирішили».

Формальна підстава для скарги – завдання шкоди діловій репутації. Правник пояснює, що кожен з позивачів веде активну діяльність онлайн, має тисячі підписувачів, і коли його відлучають від соцмережі навіть на кілька днів, його ділова репутація зазнає втрат. «Основна мета – мати процес, який приверне увагу до цього питання, і нема різниці, де його робити», – розповідає А. Гук.

Паралельно блогери планують скаржитися в обидва офіси Facebook і навіть готують петицію до Державного департаменту США, підкріплюючи її свідченнями потерпілих.

Нагадаємо, з упередженим ставленням у соцмережі українці стикнулися з розвитком російської агресії в Україні, зокрема під бан підтрапляють проукраїнські пости та сторінки. Через це українці попросили засновника Facebook М. Цукерберга створити українську адміністрацію в мережі.

Прохання відкрити український офіс у тому числі перепостив і Президент України П. Порошенко ***(Українські блогери готують позов на Facebook // Інформаційна агенція «Вголос» (http://vgolos.com.ua/news/ukrainski_blogery_gotuyut_pozov_na_facebook_182607.html). – 2015. – 8.06).***

***

Инструменты шифрования социальных сетей не позволяют ФБР отслеживать преступников. Об этом заявил заместитель директора ФБР М. Стейнбах.

По мнению М. Стейнбаха, Конгресс США должен принять новое законодательство, которое обязывало бы соцсети передавать пользовательские данные правоохранительным органам так же, как это делают телекоммуникационные компании.

Заместитель директора ФБР заявил, что Конгресс должен использовать закон о помощи телекоммуникационных компаний правоохранительным органам (Communications Assistance for Law Enforcement Act) для создания аналогичного закона, регулирующего деятельность социальных сетей и интернет-провайдеров.

Напомним, в сентябре прошлого года SecurityLab сообщал о заявлении главы ФБР Д. Коуми, в котором он высказал опасение, что реализованные в мобильных устройствах Apple и Google новые системы защиты и шифрования данных способны поставить многих пользователей «вне закона».

Представитель Республиканской партии У. Хард заявил, что принятие предложенных М. Стейнбахом изменений в закон о помощи телекоммуникационных компаний правоохранительным органам могут серьезно ослабить защиту частной жизни и персональных данных ***(ФБР стремится обязать социальные сети предоставлять спецслужбам персональные данные // InternetUA (http://internetua.com/fbr-stremitsya-obyazat-socialnie-seti-predostavlyat-specslujbam-personalnie-dannie). – 2015. – 7.06).***

***

На Android-устройствах вышло новое приложение FireTweet, которое обеспечит пользователей доступом к Twitter в тех регионах, где сеть микроблогов заблокирована государством. Сервис микроблогов, к примеру, неоднократно запрещали в Турции и Египте. Также он недоступен в Китае и Иране.

Дистрибутив программы (в виде APK-файла) можно загрузить только с официального сайта: firetweet.io. В Google Play она недоступна. Fire Tweet предоставляет все привычные функции Twitter, причем бесплатно и без показа рекламы. Вход можно выполнить при помощи уже существующего аккаунта или зарегистрировать новый.

Весь HTTP-трафик, говорят разработчики Twitter-клиента, пропускается через распределенную сеть прямых прокси-серверов (промежуточных звеньев). Таким образом, принцип работы FireTweet схож с известным анонимайзером Tor, только мобильное приложение куда проще для настройки и использования.

FireTweet создала группа энтузиастов под названием Lantern, ранее разработавшая программу LimeWire для обхода блокировок с ПК. В основе Android-приложения лежит p2p-сеть, которая соединяет пользователей из регионов, где доступ к Twitter запрещен, с пользователями из других стран – там, где блокировки сняты. По словам представителей Lantern, «позднее в этом году» они планируют выпустить iOS-версию FireTweet ***(Android-приложение поможет обойти блокировку Twitter // InternetUA (http://internetua.com/Android-prilojenie-pomojet-oboiti-blokirovku-Twitter). – 2015. – 10.06).***

***

Таджикские интернет-провайдеры по распоряжению властей страны разблокировали доступ к социальным сетям, новостным ресурсам и информагентствам.

«Мы получили распоряжение восстановить прямой доступ к Facebook, другим соцсетям и всем основным сайтам, которые блокировались по устному распоряжению Службы связи», – сказал агентству на условиях анонимности руководитель одного из провайдеров.

В компаниях полагают, что решение было принято властями из-за проведения в Таджикистане конференции по итогам Международного 10-летия действий «Вода для жизни». На мероприятие (9–11 июня) прибыли 1,5 тыс. представителей 99 стран мира, в том числе Генсекретарь ООН Пан Ги Мун.

Соцсети и интернет-издания были заблокированы в Таджикистане согласно распоряжению Службы связи при правительстве Республики с 29 мая. В частности, были недоступны Facebook, «Одноклассники», «ВКонтакте», YouTube. Кроме того, стали недоступными сайты таджикской службы радио «Свобода» и информагентства ASIA-Plus.

По мнению экспертов, решение правительства было принято после видеобращения теперь уже бывшего командира таджикского ОМОН полковника Г. Халимова, которое было распространено по всем соцсетям в конце мая. В нем Г. Халимов на русском языке объяснил свое решение присоединиться к «Исламскому государству» (ИГ) недовольством теми порядками, которые существуют в МВД Таджикистана, в том числе запретом на совершение ежедневных пятикратных намазов. Кроме того, полковник высказал свое негативное отношение к российско-таджикским и российско-американским отношениям.

Власти Таджикистана неоднократно блокировали доступ к информационным ресурсам и различным сайтам, что, по мнению СМИ, связано с тем, что в последнее время оппозиционно настроенные политики активизировали свою деятельность в Интернете, подвергая резкой критике

президента Таджикистана Э. Рахмона. Однако в октябре 2014 г. при очередном восстановлении доступа к соцсетям глава правительственной Службы связи Б. Зухуров заявлял, что доступ к сайтам мог быть закрыт в связи с техническими проблемами, а не действиями властей ***(В Таджикистане из-за приезда Генсека ООН восстановили доступ к соцсетям // InternetUA (http://internetua.com/v-tadjikistane-iz-za-priezda-genseka-oon-vosstanovili-dostup-k-socsetyam). – 2015. – 9.06).***

***

Народный депутат фракции партии «Блок Петра Порошенко» И. Винник, в соавторстве с другими парламентариями, подготовил и внес в Верховную Раду законопроект «О внесении изменений в некоторые законодательные акты Украины по совершенствованию информационного режима проведения антитеррористической операции» (регистр. № 2050).

«Мы уточняем действующие статьи Уголовного кодекса, которые предусматривают ответственность должностных лиц и граждан Украины за любые призывы к терроризму или любым террористическим действиям. Мы усиливаем ответственность за такие действия, отдельно выписываем ответственность должностных лиц за публичные призывы к терроризму. Это будет наказываться более тяжелой ответственностью», – сообщил И. Винник, передает «Солидарность».

Законопроект также предлагает внести изменения в закон о борьбе с терроризмом. «В Украине много людей пользуется социальными сетями и сознательно или бессознательно подвергают опасности наши военные формирования, когда информируют общество о местонахождении военных частей, военной техники и т. п. Учитывая, что эта информация по содержанию является тайной и не может быть обнародована, она через социальные сети получает широкую огласку. Понятно, что такая информация используется нашим врагом. Поэтому в законе о борьбе с терроризмом мы предлагаем установить ответственность граждан, которые опрометчиво или сознательно выкладывают в социальные сети важную информацию, содержащую государственную тайну и подвергающую опасности украинских военных», – сказал народный депутат ***(У Порошенко предлагают наказывать украинцев, которые взболтнули лишнего в соцсетях // From-ua (http://from-ua.com/news/349780-u-poroshenko-predlagayut-nakazivat-ukraincev-kotorie-vzboltnuli-lishnego-v-socsetyah.html). – 2015. – 10.06).***

***

Бельгійська комісія із захисту недоторканності приватного життя подала до суду на компанію Facebook на підставі втручання. Про це повідомляє EUobserver.

«Відстеження соцмережею поведінки як її членів, так і людей, що не зареєстровані у Facebook, порушує бельгійське та європейське законодавство»,

– заявили представники комісії. У свою чергу голова комісії В. Дебекеларе наголосив: «Поведінка Facebook є неприйнятою».

Це перший випадок, коли національний гарант захисту персональних даних у Європі подає до суду проти Facebook через те, що компанія порушує Закон «Про персональні дані».

Підставою для справи стало дослідження комісії, згідно з яким Facebook відстежує поведінку користувачів на інших веб-сайтах за замовчуванням, поки вони не відмовляться від цього, замість того щоб робити це тільки після отримання відповідного дозволу.

Також з'ясувалося, що компанія відстежує поведінку людей, які навіть не зареєстровані на сайті соцмережі, що є порушенням правил ЄС.

У травні комісія представила свої висновки й рекомендації Facebook, чиє європейське представництво зареєстровано в Ірландії. Голова комісії В. Дебекеларе: «Вони відповіли, що не приймають бельгійське законодавство або компетенцію Бельгійської комісії із захисту недоторканності приватного життя і що це непорозуміння».

Натомість представник Facebook зауважив, що «впевнений, що немає ніяких підстав» для порушення такої справи ***(Бельгія подала до суду на Facebook через втручання у приватне життя // Media Sapiens (http://osvita.mediasapiens.ua/media_law/law/belgiya_podala_do_sudu_na_facebook_cherez_vtruchannya_u_privatne_zhittya). – 2015. – 15.06).***

***

У Венесуелі людей можуть позбавляти свободи через коментарі у Twitter або фотографії в Instagram

Вільна преса Венесуели витіснена на веб-сайти чи в малотиражні видання, а журналістів можуть звільняти з роботи через коментарі на тему політики. Про надзвичайні утиски свободи слова з боку режиму Н. Мадуро в інтерв'ю MediaSapiens розповіли політологи з Венесуели Л. Альберто і Х. Рафасчіері.

Нині венесуельці використовують Facebook, YouTube і Twitter, щоб дізнатися про події, які не з'являються в офіційній пресі, наприклад інформацію про масові заворушення, політичні репресії та промови опозиційних політиків. Це сталося через збільшення цензури та самоцензури в традиційних засобах масової інформації.

Це стало очевидним під час національних протестів у 2014 р., коли більшість жителів Венесуели і світу були поінформовані про нинішню кризу громадською журналістикою. Такі ж значні телевізійні мережі, як CNN, висвітлювали події, використовуючи надійні фотографії й матеріали, які були опубліковані в Twitter або Facebook.

Крім того, у поточному венесуельському політичному контексті, де збільшення цензури в традиційних засобах масової інформації є правилом, стає обов'язковим використання нових методів для донесення інформації до

громадськості. Особливо використовуючи такі інформаційні й комунікаційні технології, як Інтернет і смартфони.

…Придушення свободи слова є одним з основних напрямів політики, спрямованої на збереження влади.

Видається, що дії влади, яка намагається блокувати міжнародні засоби масової інформації, корелюють з великим списком обмежень прав журналістів і свободи слова у Венесуелі. Починаючи із заохочення самоцензури, закінчуючи закриттям газет, журналів і телеканалів, – аж до обмежень, накладених на друковані ЗМІ у зв'язку з імпортуванням паперу…

Міжнародна преса зазнає тих самих труднощів, що й венесуельські ЗМІ, коли вона повідомляє про події, що тут відбуваються. Так, журналіста Ф. дель Рінкона був миттєво звільнено із CNN через тиск, який чинив уряд на його телевізійну станцію. І багато міжнародних репортерів, таких як Ф. Коммісарі, були заарештовані за «неправильне» висвітлення наших громадських протестів.

Усі ці дії є складовою частиною загальної політики цензури, яка орієнтована режимом чавесистів на придушення вільних думок та інформації. У Венесуелі є газети, які припинили свою діяльність через дефіцит паперу й типографської фарби. У такий спосіб уряд контролює незалежні засоби масової інформації, не застосовуючи сили безпосередньо. Але можна побачити, що якщо ці ЗМІ не бажають пристосуватися до бажань режиму, то вони потрапляють під жорсткі юридичні санкції й насильство.

Інтернет-ЗМІ також не змогли уникнути репресивної політики уряду. Уряд Н. Мадуро контролює Інтернет, обмежуючи доступ до певних сайтів, які пропонують інформацію про іншу ціну валюти й політичні протести.

У Венесуелі частіше виникають труднощі, коли потрібно купити комплектуючі частини для комп'ютера та пристрої, що необхідні для доступу до Інтернету, такі як модеми й маршрутизатори. Крім того, у дні, коли опозиція організовує свої заходи, уряд перекриває доступ до Інтернету або чинить перешкоди для з'єднання із соціальними мережами Twitter або Facebook.

Щодо ведення блогів у Венесуелі, то деякі люди, які ведуть власні блоги або ж є дуже активними в мікроблогінгу в соціальних мережах, були ув'язнені або покарані іншим чином за свої політичні коментарі в кіберпросторі.

…У сьогоднішній Венесуелі є нормальною практикою позбавляти людей свободи через їхні коментарі на Twitter або фотографії в Instagram. Декілька венесуельців були притягнуті до судової відповідальності лише за те, що вони розмістили фотографії великих черг людей, що чекали під супермаркетами можливості купити туалетний папір або борошно.

…Партія влади у Венесуелі намагається контролювати Інтернет, застосовуючи для цього різноманітні методи. Вони проводять репресивні заходи проти онлайн-спільноти, які полягають у блокуванні деяких сайтів та в уповільненні навігаційної швидкості серверів.

Останнім часом PSUV (Partido Socialista Unido de Venezuela, Об'єднана соціалістична партія Венесуели. – Прим. ред.) ініціювала підготовку закону, який визначатиме перелік обмежень для користувачів при отриманні доступу

до віртуального світу. Це збільшить і розширить цензуру. Утім, досі репресії проти Інтернету у Венесуелі не досягли того рівня, який спостерігається в Китаї, на Кубі або в Північній Кореї.

…Ми не можемо сказати, що режим впаде цього року, ми не можемо сказати, що це може статися в наступному році… Але ми можемо стверджувати одне: оскільки наша країна, як і раніше, продовжує перебувати в економічній і політичній кризі, чинний президент та весь його режим будуть стикатися зі сценаріями політичної нестабільності ***(Каспрук В. У Венесуелі людей можуть позбавляти свободи через коментарі у Twitter або фотографії в Instagram // Media Sapiens (http://osvita.mediasapiens.ua/media_law/world_journalists/u_venesueli_lyudey_mozhut_pozbavlyati_svobodi_cherez_komentari_utwitter_abo_fotografii_v_instagram). – 2015. – 13.06).***

***

У Криму порушили кримінальну справу проти користувача соцмережі «ВКонтакте» за поширення в мережі матеріалів на кшталт нацистських. Про це повідомила прес-служба відомства, пише Корреспондент.net (http://ua.korrespondent.net/ukraine/3528830-u-krymu-sudytymut-korystuvacha-vkontakte-za-natsyzm).

Прокуратура встановила, що користувач є прихильником ідеології нацизму. Він розміщував тексти, аудіо, відео та фото, що спрямовані на розпалювання національної ненависті і ворожнечі.

«Згідно з експертним висновком, ці матеріали містять ознаки приниження людської гідності групи осіб за ознакою національності, а також виправдання ворожих, насильницьких дій по відношенню до неї», – зазначено в повідомленні.

Прокуратура взяла під контроль перебіг і результати попереднього розслідування ***(У Криму судитимуть користувача Вконтакте за нацизм // Корреспондент.net (http://ua.korrespondent.net/ukraine/3528830-u-krymu-sudytymut-korystuvacha-vkontakte-za-natsyzm). – 2015. – 17.06).***

Проблема захисту даних. DDOS та вірусні атаки

Украина вошла в топ-15 стран с наибольшим количеством DDoS-атак. Такие данные получила компания Kaspersky Lab в ходе анализа внутренней статистической информации за первые три месяца этого года.

Количество DDoS-атак с использованием ботнетов в Украине увеличилось по сравнению с предыдущим аналогичным периодом и составило 122. Всего в I квартале 2015 г. киберпреступники совершили более 23 тыс. DDoS-атак с применением ботсети на ресурсы, расположенные в 76 странах. При этом мишенями зачастую были серверы на территориях России, Китая,

США и Канады. В первой десятке жертв также оказались ресурсы из разных стран Европы и Азиатско-Тихоокеанского региона. В I квартале ботнеты атаковали больше 12 тыс. жертв по всему миру.

Самая длительная DDoS-атака, зафиксированная в I квартале этого года, продолжалась 140 часов (около шести дней), а наибольшее количество атак, которые пришлось вынести одному ресурсу, составляла 21, то есть примерно по две атаки в неделю. Для сравнения: в прошлом квартале было зарегистрировано максимум 16 атак на один ресурс.

Что касается командных серверов, с которых велось управление этими атаками, чаще всего они располагались в США, Китае и Великобритании. Аналитики Kaspersky Lab объясняют лидирующие позиции Китая и США в обоих рейтингах тем, что хостинг в этих странах относительно дешевый и большинство дата-центров расположены именно в них ***(Украина – в топ-15 стран с наибольшим количеством DDoS-атак // InternetUA (http://internetua.com/ukraina---v-top-15-stran-s-naibolshim-kolicsestvom-DDoS-atak). – 2015. – 9.06).***

***

Исследователь компании Check Point Н. Колесова обнаружила новое вымогательское ПО Troldash, которое предлагает жертве связаться со злоумышленниками при помощи электронной почты. Об этом сообщается на сайте BBC. На момент написания новости страница блога Check Point с подробным описанием Troldash была недоступной.

В то время как большинство киберпреступников стараются скрыть свою личность, создатели Troldash используют электронные сообщения для того, чтобы потребовать выкуп за дешифрование данных и указать метод оплаты.

Новое вымогательское ПО распространяется при помощи спама. Сразу после того, как вредоносный файл загружен в систему, запускается процесс шифрования, а затем жертва видит сообщение с инструкциями по проведению оплаты.

Представившись именем одной из жертв, Н. Колесова связалась со злоумышленниками с помощью электронной почты. В ответ на свое сообщение эксперт получила требование перевести на счет киберпреступников 250 евро. Подозревая, что злоумышленники настроили автоматическое создание ответов, специалист попросила прислать ей более подробные инструкции по оплате. После этого Н. Колесовой было отправлено электронное письмо на русском языке, в котором вымогатели требовали суму в 12 000 р. Эксперт продолжила «торговаться» со злоумышленниками и, в конце концов, договорилась о выплате только 7000 р. ***(Вымогательское ПО предлагает связаться со злоумышленниками посредством электронной почты // InternetUA (http://internetua.com/vimogatelskoe-po-predlagaet-svyazatsya-so-zloumishlennikami-posredstvom-elektronnoi-pocsti). – 2015. – 6.06).***

***

В Facebook замечена очередная вирусная эпидемия. Многие украинские пользователи жалуются, что их друзья в социальной сети уже пострадали от неизвестного вируса.

Как отметил О. Сыч, руководитель антивирусной лаборатории Zillya!, вирус применяет стандартную схему. От имени пострадавшего в ленте появляется якобы ссылка на видео с неприметным описанием типа «323412341234». На preview видеоролика размещено, как правило, что-то пикантное (например, фото полуобнаженной девушки). По уже испытанной технологии, злоумышленники отмечают в сообщении всех друзей из списка пострадавшего (пользователь [имя] вместе с…). Таким образом, этот пост отображается и в их ленте тоже.

Кликнув на видео, пользователь переводится на другой сайт, где ему сообщают, что он не может посмотреть видео, потому что не установлен некий кодек. Сайт предлагает загрузить и установить необходимый кодек. Собственно, именно кодек и является вирусом.

Справедливости ради надо сказать, что Facebook отреагировал оперативно и в настоящее время пытается заблокировать попытки перехода по этим ссылкам. Но не факт, что вирус не поменяет через некоторое время модель атаки.

Всегда необходимо помнить, что учетную запись вашего друга могут взломать. Поэтому надо взять за правило никогда не переходить по ссылкам, которые ведут на странный и неизвестный домен. Всегда лучше уточнить, что вам прислали и действительно ли это прислал ваш друг.

В любом случае, опасны только ссылки, ведущие на внешние веб-ресурсы. Если же их не нажимать, то страница социальной сети угрозы не представляет ***(В Facebook замечена очередная вирусная эпидемия // InternetUA (http://internetua.com/v-Facebook-zamecsena-ocserednaya-virusnaya-epidemiya). – 2015. – 7.06).***

***

В результате проведения глобального исследования компания Microsoft выяснила, что 99,6 % интернет-пользователей готовы продавать информацию о себе за деньги.

Исследование Microsoft под названием The Consumer Data Value Exchange базировалось на данных, предоставленных цифровым ассистентом Cortana (аналог Siri), который анализирует электронную почту, историю поиска и прочую пользовательскую информацию.

В ходе исследования компания Microsoft выяснила:

– 54 % пользователей ожидают, что бренды знают и понимают их, поэтому выстраивают коммуникацию, исходя из их (клиентов) ценностей и предпочтений;

– 55 % пользователей уверены, что данные об их действиях в Интернете собираются без разрешения;

– 83 % опрошенных ожидают, что компании будут спрашивать у них разрешение на использование их личных данных.

Пользователи готовы предоставить информацию о себе брендам:

– 99,6 % – за деньги;

– 89,3 % – за скидки и бонусы;

– 65,2 % – за баллы на покупки товаров и услуг.

Что готовы отдавать пользователи?

– Историю поиска – 79 %;

– Журнал посещения сайтов – 65 %;

– Историю покупок – 19 %.

Какую личную информацию готовы предоставить пользователи:

– Личная история – 70 %;

– Возраст – 75 %;

– Пол – 73 %.

В ходе проведенного ранее исследования также выяснилось, что 60 % интернет-пользователей положительно относятся к таргетированной рекламе. Но при этом 62 % признались, что не хотели бы, чтобы торговцы отслеживали их местоположение ***(99 % пользователей готовы продавать информацию о себе в Интернете // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2015/06/05/9-per-cent-of-internet-users-are-ready-to-sell-personal-information.html). – 2015. – 5.06).***

***

ИБ-исследователи «Доктор Веб» проанализировали и добавили в вирусные базы новый троян, предназначенный для обеспечения доступа к SMTP-серверам для массовой рассылки рекламных почтовых сообщений. Вредоносная программа, которую эксперты «Доктор Веб» назвали Trojan.Proxy.27552, отличается несколькими конструктивными особенностями, которые проявляются уже на этапе установки вредоноса в инфицированной системе.

В процессе инсталляции Trojan.Proxy.27552 пытается создать свои копии в системной папке C:\Windows\System32 с именами csrss.exe, svchost.exe и rundll32.exe, даже несмотря на то, что в указанной директории располагается оригинальный файл csrss.exe. В случае, если у вредоноса окажутся достаточные системные полномочия (троян запущен от имени учетной записи администратора и для него включены привилегии отладчика), он пытается завершить в памяти процесс csrss.exe по его полному пути. Завершение процесса незамедлительно выводит из строя Windows с демонстрацией «синего экрана смерти».

После запуска Trojan.Proxy.27552 проверяет наличие подключения к Интернету путем установки соединения с серверами smtp.gmail.com:25 и plus.smtp.mail.yahoo.com:25. При возникновении проблем с доступом к сети троян завершает свою работу. В том случае, если соединение с Интернетом присутствует, вредоносная программа пытается получить с удаленных узлов

актуальный список IP-адресов, управляющих серверов. Затем списки сравниваются, из них удаляются локальные сетевые адреса – троян формирует окончательный перечень управляющих серверов и записывает полученные данные в системный реестр Windows.

Вредонос регулярно обновляет список управляющих серверов, отслеживает состояние ветви реестра, отвечающей за его автозапуск, а также реализует функции backconnect-proxy сервера. Связь с управляющими серверами организована таким образом, что они фактически заставляют инфицированную ОС поддерживать активное соединение заданный период времени ***(Новый троян-спамер выводит из строя Windows // InternetUA (http://internetua.com/novii-troyan-spamer-vivodit-iz-stroya-Windows). – 2015. – 5.06).***

***

Компания Check Point Software Technologies представляет третий ежегодный отчет Secutiry Report-2015, характеризующий основные киберугрозы, которым подвергаются организации во всем мире.

Security Report-2015 дает представление о масштабах проникновения и степени сложности новых угроз в корпоративном сегменте. Мобильность, облака, виртуализация и другие новейшие технологии изменили принципы ведения бизнеса. Компании используют эти инструменты для увеличения производительности, часто забывая о том, какие последствия могут возникнуть из-за недостаточного внимания к вопросам безопасности. Исследование Check Point Security Report-2015 выявило повсеместное распространение и дальнейший рост киберугроз на основе информации, собранной в 2014 г. Отчет базируется на интегрированном детальном анализе более чем 300 тыс. часов сетевого трафика, собранного с более чем 16 тыс. шлюзов системы Threat Prevention и 1 млн смартфонов.

2014 г. ознаменовался небывалыми темпами роста вредоносного ПО. Согласно отчету, каждый час организацию в среднем атакуют 106 неизвестных вредоносных программ. Это в 48 раз больше, чем 2,2 случая загрузки вредоносного ПО в час, зафиксированные в 2013 г. Неизвестное вредоносное ПО будет и дальше наносить вред организациям. Но более значительной угрозой является так называемое ПО «нулевого дня» – злоумышленники разрабатывают его с нуля, используя те уязвимости в программном обеспечении, о которых производители еще не подозревают.

Кроме того, киберпреступники продолжают использовать ботов, чтобы расширить свои сети и ускорить распространение вредоносных программ. В 2014 г. 83 % исследованных организаций были заражены ботами, которые имели возможность постоянно обмениваться данными с командными серверами (C&C).

Мобильные устройства являются слабым звеном в системе безопасности, предоставляя мошенникам наиболее легкий доступ к ценным корпоративным данным. Исследование Check Point выявило, что в организациях, где

используется более чем 2 тыс. мобильных устройств, существует вероятность 50 %, что, как минимум, шесть из них инфицировано или выбрано киберпреступниками как цель атаки.

Семьдесят два процента опрошенных ИТ-специалистов согласны с тем, что главная и самая сложная задача в мобильной безопасности – это обеспечить сохранность корпоративной информации. Шестдесят семь процентов указали, что их второй проблемой является управление персональными устройствами сотрудников, на которых хранится как их личная, так и бизнес-информация. Организациям требуется осознать, что корпоративные данные находятся в зоне риска – это критически важно для принятия надлежащих мер по обеспечению безопасности мобильных устройств.

Корпорации сегодня широко используют различные приложения, чтобы организовать и упорядочить бизнес-процессы. Однако эти приложения зачастую становятся уязвимыми местами в системе безопасности. Например, программы для обмена файлами несут в себе очевидные риски. Развитие «теневой ИТ-индустрии» – приложений, которые не поддерживаются и не финансируются централизованными ИТ-отделами – приводит к еще большему росту угроз.

Согласно исследованию, 96 % опрошенных организаций в 2014 г. использовали как минимум одно приложение с высоким уровнем риска – это на 10 пунктов больше, чем годом ранее. Исследователи Check Point также обнаружили, что каждый час происходят 12,7 событий, связанных с приложениями высокого риска. Это предоставляет киберпреступникам множество возможностей для проникновения в корпоративную сеть.

Киберпреступники не являются единственной угрозой для безопасности корпоративных данных. Действия внутри сети могут так же легко приводить к потере данных, как и хакерское проникновение извне. Check Point обнаружил, что 81 % проанализированных компаний пострадали от инцидентов утечки данных, это на 41 % выше, чем в 2013 г. Утечки информации могут происходить по разным причинам, но наиболее частыми являются действия сотрудников. Большинство компаний фокусируют свою стратегию безопасности на защите данных от хакеров, однако не менее важно защищать данные от внутренних утечек.

«Сегодняшние киберпреступники – искусные и беспощадные: они охотятся за уязвимостями сети, пытаясь взломать системы безопасности. Чтобы защититься от атак, организации должны изучить природу недавно обнаруженных уязвимостей и понять то, насколько их сети им подвержены, – говорит В. Дягилев, глава представительства Check Point Software Technologies в России и СНГ. – Только вооружившись сочетанием знаний и мощных программных решений по безопасности, организации в состоянии защититься от постоянно эволюционирующих угроз. Они должны превратить безопасность в движущую силу своего развития, сделав ее ключевым компонентом бизнеса. Это откроет им доступ к инновациям и позволит повысить производительность всех корпоративных систем» ***(Каждый час организацию атакуют 106***

неизвестных вредоносных программ // ITnews (http://itnews.com.ua/news/77169-kazhdyj-chas-organizatsiyu-atakuyut-106-neizvestnykh-vredonosnykh-programm). – 2015. – 5.06).

***

Власти США признали факт внешнего проникновения в компьютерную сеть Службы управления персоналом США (U.S. Office of Personnel Management, OPM), которая хранит информацию о бывших и нынешних госслужащих. Скомпрометированы персональные данные примерно 4 млн человек.

По имеющейся информации, проникновение случилось в декабре 2014 г. Государственные ИТ-специалисты осознали происходящее в апреле 2015 г. В настоящее время идёт инспекция сети, очистка компьютеров, оценка ущерба и аудит. К расследованию подключилось ФБР. Что характерно, это уже вторая успешная атака на Службу управления персоналом США.

Четыре миллиона сотрудников, пострадавшие от кражи конфиденциальных данных, будут уведомлены о случившимся с 8 по 17 июня. Им предложат помощь по отслеживанию платежей с банковской карты и противодействию использованию личных данных третьими лицами (identity theft).

«Мы очень серьёзно относимся к ответственности по безопасности хранения информации в наших системах, – чётко заявила директор OPM К. Арчулета, – и в сотрудничестве с партнёрами из других агентств, наша опытная команда постоянно определяет возможности для ещё большей защиты данных, которые нам доверены».

Газета The Washington Post пишет со ссылкой на анонимных информаторов, что источником атаки является Китай.

После взлома OPM в июле 2014 г. чиновники тоже обвиняли китайцев ***(Крупная атака на госслужбу США: враг получил 4 МЛН ID // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2015/06/05/opm-to-notify-employees-of-cybersecurity-incident.html). – 2015. – 5.06).***

***

Обнаружен новый вирус троян – malumPoS, который ворует платежные данные из POS-терминалов отелей и торговых точек. Вредоносная программа внедряется сразу в оперативную память PoS-системы. В основном такие атаки поражают терминалы, работающие на платформе Oracle Micros.

В настоящее время эта платформа очень широко используется в розничной торговле, пищевой промышленности и гостиничной индустрии по всему миру. Большая часть компаний-пользователей платформы сосредоточены в США.

По словам экспертов службы онлайн-безопасности Trend Micro, новый вариант трояна malumPoS является конфигурабельным, поэтому не исключено,

что в его функционал со временем добавятся новые возможности. К примеру, злоумышленник может модифицировать или добавить новый процесс, а также изменить список целевых систем.

После заражения системы, MalumPoS маскируется под драйвер видеокарты NVIDIA (NVIDIA Display Driver). Несмотря на то что обычно компоненты NVIDIA не играют значительной роли в PoS-системах, их привычность для большинства пользователей пает возможность трояну выглядеть совершенно безобидно.

Помимо Oracle Micros, целевыми системами MalumPoS являются Oracle Forms, Shift4 и платформы, доступ к которым осуществляется через браузер Internet Explorer. Троян чаще всего ориентируется на данные кредитных карт Visa, MasterCard, American Express, Discover и Diners Club ***(Вирус троян атакует POS-терминалы в гостиницах и магазинах // InternetUA (http://internetua.com/virus-troyan-atakuet-POS-terminali-v-gostinicah-i-magazinah). – 2015. – 9.06).***

***

В течение нескольких последних лет основатель австралийской IT-компании Security Dimension П. Хаяти разрабатывает систему Smart Honeypot. С ее помощью эксперт намерен использовать системы потенциальных жертв хакеров как ловушки для злоумышленников.

Во время тестирования своей системы П. Хаяти разместил в различных географических регионах (Америка, Европа, Азия и Океания) тринадцать таких ловушек, замаскировав их под серверы Amazon Web Services и Google Cloud. Результаты проведенного таким образом исследования оказались довольно неожиданными.

«Все хосты были идентичными и имитировали типичный сервер, – пояснил П. Хаяти во время конференции Hack in the Box. – Их IP-адреса во время эксперимента не публиковались в открытом доступе. Однако даже в этом случае злоумышленникам понадобилось в среднем 10 мин для того, чтобы найти их и предпринять попытку нападения».

Интересно, что возможности хакеров были изначально ограничены, поскольку соединение можно было установить исключительно по SSH. В конечном итоге исследователь выяснил, что подавляющее большинство атак осуществляют боты, прибегающие к методу перебора. Некоторые из них использовали одну единственную комбинацию логина и пароля на всех серверах-ловушках и больше не проявляли активности, однако большинство проверяло возможность авторизации при помощи учетных данных из различных утечек. Наиболее часто используемыми логинами оказались root и admin.

Отчет об экспериментах, проведенных П. Хаяти, доступен на официальном веб-сайте Hack in the Box ***(Исследователь проанализировал атаки на поддельные серверы Amazon и Google // InternetUA***

(http://internetua.com/issledovatel-proanaliziroval-ataki-na-poddelnie-serveri-Amazon-i-Google). – 2015. – 7.06).

***

Начальники управления информационной безопасности в компаниях Met Office, Economist Group и аэропорту Хитроу, Лондон, предупреждают, что бизнес-компаниям в первую очередь необходимо создавать стратегии реагирования и способы смягчения последствий от кибератак. В противном случае их могут ожидать портящие репутацию кибернападения, как это случилось с Sony.

Начальник управления информационной безопасности в аэропорту Хитроу М. Джонс отметил, что кибератака на Sony в 2014 г. была осуществлена злоумышленниками, которые с помощью своих компрометирующих кампаний на крупные предприятия пытаются показать свое превосходство. М. Джонс уверен, что целью атаки на Sony являлось не похищение персональных данных, а порча реноме компании. По мнению эксперта, хакеры, спонсируемые Северной Кореей, пытались «наказать» Sony за фильм о вымышленном покушении на Ким Чен Ына.

Директор по информационной безопасности в Economist Group В. Гави полностью поддерживает своего коллегу и считает, что нападение на Sony является предупреждением для компаний, которые при отсутствии своевременной модернизации систем безопасности могут попасть в число будущих жертв преступников.

Начальник управления информационной безопасности в Met Office Д. Кидд заметил, что за последние 18–24 месяцев злоумышленники все чаще обращаются к более изощренным способам совершения кибератак. Предприятия должны заняться моделированием потенциальных угроз и разработать методы смягчения возможных последствий ***(Компаниям стоит подготовиться к компрометирующим репутацию кибератакам // InternetUA (http://internetua.com/kompaniyam-stoit-podgotovitsya-k-komprometiruuasxim-reputaciua-kiberatakam). – 2015. – 7.06).***

***

ИБ-исследователи помешали мошеннической кампании, во время которой злоумышленники использовали Skype как ботнет для рассылки вредоносного рекламного ПО. Первым неладное заподозрил старший научный сотрудник фирмы PhishMe Р. Токазовски после того, как его коллега получил несколько звонков по Skype от неизвестного пользователя.

Имя звонившего состояло из строчки, в которой говорилось, что пользователь получил новое видеосообщение и его можно просмотреть на сайте www.viewror.com. Нажав на домен, жертве предлагается загрузить и установить исполняемый файл videoplayer.exe., который, по словам злоумышленников, является видеопроигрователем Media Player Classic, с помощью которого можно просмотреть полученное сообщение.

При открытии вредоносный файл запрашивает права администратора и сразу после разрешения начинает устанавливать и запускать в системе рекламу. Р. Токазовски также отметил, что каждый раз, когда пользователи устанавливают вредонос, злоумышленники получают неплохие деньги ***(Злоумышленники использовали Skype в качестве ботнета // InternetUA (http://internetua.com/zloumishlenniki-ispolzovali-Skype-v-kacsestve-botneta). – 2015. – 7.06).***

***

Аналитики компании Verisign, которая занимается вопросами безопасности на просторах сети, зафиксировали существенный рост количества хакерских атак.

По итогам I квартала этого года количество DDoS-атак во всем мире превысило показатели, которые фиксировались на протяжении всего 2014 г. Рост по сравнению с предыдущим кварталом составил 7 %.

Кроме того, частота хакерских атак на компьютерные сети как государственного, так и финансового сектора заметно возросла. В IV квартале прошлого года доля таких DDoS-атак от их общего количества составляла 15 % против 18 за текущий отчетный период.

При этом треть всех нападений по-прежнему приходится на IT и SaaS-сервисы.

Среди ключевых факторов, спровоцировавших рост количества инцидентов, специалисты Verisign называют доступность различных инструментов для DDoS-атак, процветание подпольного бизнеса по сдаче ботнетов в аренду и громкие политические события мирового значения ***(Активное распространие DDoS-атак по всему миру связано с подпольной арендой ботнетов // InternetUA (http://internetua.com/aktivnoe-rasprostranie-DDoS-atak-po-vsemu-miru-svyazano-s-podpolnoi-arendoi-botnetov). – 2015. – 7.06).***

***

Как защитить телефон и компьютер от хакеров при подключении к Wi-Fi

Проблема информационной безопасности в мире становится все более актуальной из-за стремительного роста пользовательских данных. Оглядываясь на 2014 г., эксперты отмечают тревожное количество киберпреступлений, которые совершались регулярно. Нашумевшие хакерские атаки затронули многие известные бренды, банки, СМИ и социальные сети.

Среди наиболее заметных взломов на российском рынке утечка 4,7 млн учетных записей пользователей Mail.ru, а также взлом российского сайта знакомств Topface. По данным «Индекса Критичности Утечек данных» (Breach Level Index), за первую половину 2014 г. в мире было зафиксировано 559 случаев кражи данных, в результате которых было похищено 175 млн учетных записей пользователей.

«Несмотря на апокалиптические заголовки в прессе, освещающей эти инциденты, больше всего настораживает то, что большинство людей все равно не воспринимают кибербезопасность как серьезную проблему. Но на самом деле этот вопрос серьезнее, чем кажется на первый взгляд, ведь от утечек данных страдают не только крупные компании, но и простые обыватели, которые могут стать жертвой хакерской атаки в своей повседневной жизни», – отметил эксперт по безопасности, вице-президент компании Gemalto Д. Харт.

Одной из наиболее острых проблем становится безопасность публичных сетей Wi-Fi. Сегодня хакеры легко могут получить доступ к персональной информации, подключившись к публичной бесплатной Wi-Fi сети, имея оборудование стоимостью около 4000 р. и ноутбук. «Мы провели эксперимент, вол время которого воспользовались устройством, замаскированным под официальную Wi-Fi точку кафе, в результате чего посетители заведения, сами об этом не догадываясь, подключались к нашей сети. Даже такое простое оборудование дает возможность успешно перехватывать подключения и фактически обманывать телефоны и компьютеры, порой даже с возможностью понизить уровень защиты их “безопасного соединения с Интернетом”, чтобы получить доступ к критически важным данным. Так можно взломать электронную почту, банковские аккаунты или отслеживать перемещения людей», – рассказал Д. Харт. Этот эксперимент еще раз подтвердил, что публичные сети отличный способ для хакеров получить доступ к данным пользователей.

Руководитель группы консультантов по безопасности Check Point Software Technologies А. Разумов привел другой пример: «Еще несколько лет назад появилось приложение Face Niff, которое позволяло входить в социальную сеть “ВКонтакте” и другие аналогичные сайты под чужой учетной записью. Для этого необходимо было подключиться к Wi-Fi точке, например, в кафе и перехватить cookie. Это давало возможность войти на сайт под именем другого пользователя, посмотреть его историю, от его имени разослать сообщения. Разумеется, наличие специального оборудования делает задачу еще более простой и незаметной для пользователя».

К сожалению, полностью обезопаситься при использовании публичных Wi-Fi-сетей очень сложно. «В арсенале хакеров множество средств для взлома, начиная от перехвата трафика и заканчивая организацией фальшивого Wi-Fi-спота. Поэтому при работе в публичных открытых Wi-Fi-сетях рекомендуется ограничиться чтением новостей и просмотром новых фотографий своих друзей, поскольку более критичная информация может быть перехвачена», – отметил генеральный директор компании Zecurion А. Раевский.

Тем не менее, существует несколько мер, с помощью которых вы можете не дать хакерам получить вашу персональную информацию. «Во-первых, выключите общий доступ. Находясь дома, пользователи могут делиться файлами, картинками и даже удаленно подключаться к своей сети. Но при использовании публичной сети лучше отключить эти сервисы, так как кто-

нибудь может получить к ним доступ, причем не обязательно хакеры – в зависимости от настроек, многие данные могут не иметь никакой защиты вовсе.

Обычно по беспроводной сети через веб-соединения HTTP происходит обмен незашифрованными данными, и люди с нужными навыками и плохими намерениями могут очень легко получить к ним доступ. Это не так серьезно, если речь идет о вашем поисковом запросе на каком-нибудь развлекательном портале, но гораздо серьезнее, если это пароль от вашей электронной почты. Использование протокола HTTPS (для посещения веб-сайтов) или включение SSL (Secure Sockets Layer – уровень защищенных сокетов) при использовании онлайн-приложений вроде почтовой программы шифрует данные, которые передаются между персональным компьютером и веб-узлом, таким образом скрывая их от злоумышленников, – посоветовал Д. Харт. – Во-вторых, регулярно устанавливайте предлагаемые обновления браузера. Разработчики программного обеспечения всегда стараются мыслить на шаг вперед киберзлоумышленников и постоянно обновляют и добавляют новые защитные механизмы программ, поэтому, если вы хотите сохранить свои данные, не поленитесь потратить 5 мин на обновление не только своего браузера, но и другого программного обеспечения».

Использование защитных программ, где это возможно, также снизит риски взлома компьютера или смартфона, подключенного к Wi-Fi. «Отключите автоматическое подключение Wi-Fi. Современные компьютеры и устройства автоматически подключаются к Wi-Fi-сетям, если находят их в зоне видимости. Таким образом, можно стать жертвой взломщиков, даже не пользуясь Интернетом», – добавил А. Раевский. Но наиболее эффективным способом защиты устройств при подключении к общественной сети Wi-Fi является использование VPN (Virtual Private Network) ***(Как защитить телефон и компьютер от хакеров при подключении к Wi-Fi // InternetUA (http://internetua.com/kak-zasxitit-telefon-i-kompuater-ot-hakerov-pri-podkluacsenii-k-Wi-Fi). – 2015. – 9.06).***

***

Засилье мобильных устройств провоцирует рост хакерских атак в корпоративном секторе.

Аналитическая компания CheckPoint фиксирует рост случаев утечек корпоративных данных. Злоумышленники в Интернете все активнее атакуют крупные корпорации.

По сравнению с 2013 г. на сегодня существенно возросло количество DDoS, DoS и атак с применением техники переполнения буфера. Жертвами хакерских действий всё чаще становятся крупные компании.

Восемьдесят шесть процентов организаций обращались к инфицированным сайтам, 63 % пытались загрузить файлы с вредоносным содержимым и в 83 % случаев корпоративные сети были заражены ботами, устанавливающими соединение со своими C&C-серверам каждую минуту.

Девяносто один процент организаций стали больше использовать персональные мобильные устройства при работе с корпоративной информацией. В 44 % организаций, при этом, этот процесс никак не регламентируется.

За минувший год более 500 тыс. Android- и 400 тыс. iOS-устройств, имеющих отношение к корпоративному сектору, в более чем 100 странах были заражены вредоносным программным обеспечением.

Эксперты обнаружили свыше 20 вариантов троянов удалённого доступа для мобильных платформ из 18 различных семейств.

Девяносто шесть процентов компаний работают с потенциально опасными приложениями – в 92 % компаний были обнаружены инструменты для удаленного администрирования ***(Засилье мобильных устройств провоцирует рост хакерских атак в корпоративном секторе // InternetUA (http://internetua.com/zasile-mobilnih-ustroistv-provociruet-rost-hakerskih-atak-v-korporativnom-sektore). – 2015. – 10.06).***

***

10 июня был взломан сайт Объединенного штаба Литовской армии, в результате чего на нем была размещена ложная информация. Об этом сообщает издание Delfi, передает Европейская правда.

Так, на сайте появилась информация о том, что якобы цель учений «Удар меча», которые проходят в странах Балтии и Польше – подготовка к аннексии Калининградской области.

В настоящее время эта информация удалена.

«Аналитики Национального центра кибербезопасности расследуют факт взлома», – сказала пресс-секретарь Минобороны Литвы В. Цемините.

В учениях «Удар меча-2015» (1–19 июня) в Эстонии, Латвии, Литве и Польше задействованы около 6 тыс. военнослужащих из 13 стран-членов НАТО и Финляндии.

Учения организуют сухопутные силы США в Европе.

Напомним, ранее сообщалось, что активисты национал-большевистской «Другой России» ворвались на территорию военной базы в Латвии, где проходят учения НАТО, и установили там флаг в цветах «георгиевской ленты» ***(Хакеры взломали сайт армии Литвы и заявили о подготовке аннексии Калининграда // GlavPost.Com (http://glavpost.com/post/11jun2015/WorldPolitics/42751-hakery-vzlomali-sayt-armii-litvy-i-zayavili-o-podgotovke-anneksii-kaliningrada.html). – 2015. – 11.06).***

***

Международная антивирусная компания Eset провела опрос с целью выяснить опасность социальных сетей для компаний. По словам 80 % экспертов в сфере информационных технологий, злоумышленники могут получить доступ к корпоративным данным через соцсети.

Тридцать шесть процентов ИТ-специалистов говорят, что сети их компаний могут быть взломаны через аккаунты сотрудников, использующих социальные медиа на работе, поскольку зачастую вопросы безопасности работы в соцсетях в корпоративной среде игнорируются.

У 12 % компаний уже был опыт столкновения с заражением вредоносным ПО через Facebook и другие подобные сервисы. 56 % опрошенных профессионалов в области ИТ признали, что принятые в компании правила использования этих порталов не используются.

«Социальные сети часто остаются без внимания в корпоративной стратегии безопасности, поскольку не воспринимаются как угроза. Это ошибочный подход – хакеры постоянно ищут новые способы получить доступ к данным компаний, а соцсети представляют собой открытую дверь», – отметил специалист по безопасности Eset М. Джеймс ***(Соцсети опасны для бизнеса // InternetUA (http://internetua.com/socseti-opasni-dlya-biznesa). – 2015. – 11.06).***

***

Эксперты по кибербезопасности из фирмы FireEye, проанализировавшие апрельскую атаку на французский телеканал TV5Monde от имени «Исламского государства», обнаружили её связь с малоизвестной группировкой российских хакеров. Об этом сообщает BuzzFeed News.

По данным фирмы FireEye, инфраструктура, через которую осуществлялась атака на TV5Monde в апреле, схожа с той, которую обычно используют хакеры из российской группировки APT28.

Здесь есть общие показатели. Сайт «Киберхалифата», где появилась информация по атаке на TV5Monde, размещался на том же блоке IP-адресов, что и другая часть инфраструктуры APT28, и использовал тот же сервер и доменный регистратор, что и APT28 в прошлом.

Группировка APT28 известна и под другими названиями: Pawn Storm, Tsar Team, Sedit и Fancy Bear. FireEye наблюдала за ней продолжительное время: по словам представителей фирмы, APT28 отличается от других хакеров тем, что проводит взломы не ради финансовой выгоды, а для сбора полезной государству информации.

В отчёте от 27 октября 2014 г. FireEye заявила, что скорее всего APT28 финансируется российским правительством. Это специалисты определили по косвенным признакам: атакам на сайты госорганов Грузии, Венгрии и Польши, журналистов, пишущих о Кавказе, а также на НАТО и ОБСЕ. Кроме того, во вредосном коде нашли использование русского языка, а время его сборки примерно соответствовало часовым поясам Москвы и Санкт-Петербурга.

Во вторник 9 июня французская газета L’Express рассказала о причастности российских хакеров со ссылкой на источники, близкие к расследованию атаки на телеканал. Следователи отказались от версии, что за произошедшим стоит «Исламское государство», и перешли к изучению группировки APT28. Газета также отметила ухудшение отношений между Францией и Россией в последнее время.

Нападание хакеров на TV5Monde произошло в ночь с 8 на 9 апреля. Тогда злоумышленникам удалось приостановить вещание телеканала на 18 часов. Премьер-министр Франции М. Вальс назвал это «неприемлемой атакой на свободу слова и самовыражения».

В Facebook TV5Monde взломщики разместили сообщение от имени якобы связанной с «Исламским государством» группировки «Киберхалифат» и опубликовали документы, якобы принадлежащие родственникам французских военнослужащих, участвующих в операции против исламистов в Сирии и Ираке. Хакеры также взломали Google+ телеканала, разместили там изображения с надписью Je SuIS IS (игра слов, примерно переводящаяся как «Я – "Исламское государство"»).

Как выяснилось позднее, незадолго до атаки в эфире TV5Monde показали сюжет с репортёром, на фоне которого висел листок с распечатанными паролями от Twitter и Instagram телеканала ***(Российских хакеров обвинили в атаке на французский канал от имени «Исламского государства» // InternetUA (http://internetua.com/rossiiskih-hakerov-obvinili-v-atake-na-francuzskii-kanal-ot-imeni--islamskogo-gosudarstva). – 2015. – 10.06).***

***

Файлы PowerPoint начали использоваться в фишинговых атаках

Исследователи из Fidelis Cybersecurity проанализировали зафиксированные в 2014 г. инциденты безопасности, во время которых эксплуатировалась уязвимость в Windows (CVE-2014-4114). По словам специалистов, при помощи файлов PowerPoint с внедренным вредоносным кодом злоумышленники довольно эффективно обходят антивирусную защиту своих жертв. Для успешной атаки достаточно, чтобы пользователь целевой системы открыл документ в формате слайдшоу.

В Fidelis Cybersecurity также напоминают, что в июне – октябре прошлого года брешь в Windows фигурировала только в атаках группировки Sandworm Team. Однако в настоящее время информация об уязвимости стала доступна широкой общественности, и соответствующие эксплоиты начали использоваться во время фишинговых кампаний. В большинстве случаев потенциальные жертвы получают электронные письма со вложенными файлами в расширении .PPS.

Напомним, что указанная брешь позволяет удаленное выполнение кода и затрагивает операционные системы Windows Vista, Windows Server 2008, Windows 7, Windows 8, Windows 8.1, Windows Server 2012, а также Windows RT 8.1 ***(Файлы PowerPoint начали использоваться в фишинговых атаках // InternetUA (http://internetua.com/faili-PowerPoint-nacsali-ispolzovatsya-v-fishingovih-atakah). – 2015. – 13.06).***

***

Интернет вещей открывает дорогу хакерам-убийцам

Компьютерные вирусы всегда были только компьютерными – хакеры могли навредить компьютерам и оборудованию, но не другим людям. Многие продвинутые пользователи не раз с улыбкой объясняли менее продвинутым, что от компьютерного вируса нельзя заразиться самому. Похоже, что в эпоху Интернета вещей это навсегда изменится, и киберугрозы примут совершенно новый и зловещий оборот.

Первые тревожные звоночки уже есть. Издание Wired пишет, что специалист по безопасности Б. Риос обнаружил уязвимость в популярной модели медицинской помпы с подключением к Интернету, которая дает возможность хакерам удаленно повысить дозу медикамента вплоть до смертельного. Иными словами, хакер получает возможность убить человека.

Ранее Б. Риос находил и другие уязвимости в медицинских помпах – приборах, которые делают внутривенные инъекции лекарств. Такие системы, устанавливаемые в больницах, могут иметь выход в Интернет. Однако предыдущие уязвимости не были столь фатальными, как последняя. «Мы впервые обнаружили возможность изменения дозы», – сообщил изданию Б. Риос.

Найденная уязвимость относится как минимум к пяти моделям помп, производимых американской компанией Hospira. В мире насчитывается свыше 400 тыс. помп, произведенный этой фирмой. Среди уязвимых моделей: PCA LifeCare, PCA3 LifeCare, PCA5 LifeCare, Plum A+, а также вся линия Symbiq (свернутая в 2013 г.). Модель Plum A+ – одна из самых популярных, она разошлась тиражом в 325 тыс. экземпляров. Более того, Б. Риос предполагает, что уязвимость существует также на моделях Plum A+3, Sapphire и SapphirePlus.

Фатальная уязвимость содержится в механизме хранения библиотеки лекарств, которая записана в память помпы. В таких библиотеках прописаны верхние и нижние границы дозировок. Проблема в том, что доступ к этим библиотекам полностью открыт и не требует аутентификации, что позволяет кому угодно, подключившись к сети больницы (в том числе через Интернет), перезаписать всю библиотеку с другими дозировками, в том числе смертельными.

Более того, хакер теоретически может сменить всю прошивку на помпе, что даст возможность контролировать не только дозировки, но и всю работу устройства. Он может, помимо прочего, отключить встроенный тревожный сигнал на помпе, который должен срабатывать при потенциально опасной дозировке, и сделать так, что дисплей помпы будет подтверждать полную безопасность дозировки, показывая неверные данные. «Если обновить прошивку на главной системной плате, можно делать с помпой все, что угодно», – объясняет Б. Риос.

Зачем помпам подключение к Интернету? Это позволяет производителю удаленно обслуживать помпы и обновлять прошивку на них через Интернет. Но ровно это же могут делать и хакеры. Помпа содержит коммуникационный модуль, который подключается к Интернету по стандартному серийному

кабелю. Компрометация этого модуля и кабеля автоматически не означает компрометацию помпы – хакеру еще необходимо разобраться, как работает прошивка. Но по большому счету это лишь вопрос времени.

В самой Hospira ранее говорили, что компрометация помп невозможна в силу того, что между коммуникационным модулем и системной платой существует некое разделение. Б. Риос признает наличие физического разделения, однако в серийном кабеле существует мост, позволяющий его преодолеть. Последние исследования Б. Риоса в Hospira пока не прокомментировали.

Между тем специалист намерен наглядно продемонстрировать процесс компрометации помпы на июльской конференции по вопросам информационной безопасности SummerCon в Нью-Йорке ***(Интернет вещей открывает дорогу хакерам-убийцам // InternetUA (http://internetua.com/internet-vesxei-otkrivaet-dorogu-hakeram-ubiicam). – 2015. – 16.06).***

***

Компания «Доктор Веб» предупреждает о появлении опасной вредоносной программы, жертвами которой становятся владельцы мобильных устройств под управлением операционной системы Android. Зловред носит имя Android.BankBot.65.origin.

Основная особенность обнаруженного трояна заключается в том, что он встроен в официальное приложение для доступа к мобильному банкингу Сбербанка России. Причём программа-носитель сохраняет все свои оригинальные функции, в результате чего обнаружить подвох не так-то просто. Распространяется эта модифицированная версия клиентского приложения через один из популярных веб-порталов, посвящённых мобильным устройствам.

Сразу после установки зловред создаёт специальный конфигурационный файл и соединяется с управляющим сервером, на который отправляет такие данные, как IMEI-идентификатор зараженного устройства, наименование мобильного оператора, MAC-адрес встроенного Bluetooth-адаптера, версия ОС и пр. Кроме того, злоумышленникам может отсылаться зашифрованный список контактов пользователя.

Троян по команде от управляющего сервера способен перехватывать входящие SMS и отправлять различные сообщения на заданные телефонные номера. С помощью вредоносной программы киберпреступники могут похищать деньги с банковских счетов пользователей и осуществлять различные мошеннические схемы. К примеру, злоумышленники могут разместить специально сформированные SMS среди сообщений жертвы, например, о блокировке банковской карты с требованием позвонить в «банк» по указанному номеру, с просьбой пополнить баланс «попавшего в беду родственника» и т. п. ***(Опасный банковский троян атакует Android-пользователей // InternetUA (http://internetua.com/opasnii-bankovskii-troyan-atakuet-Android-polzovatelei). – 2015. – 15.06).***

***

ИБ-исследователи из компании Malwarebytes обнаружили новую разновидность вредоносного приложения, инфицирующего Android-устройства. Старший аналитик из Malwarebytes Н. Колье опубликовал в блоге описание вредоноса, получившего название Trojan.Dropper.RealShell.

Особый интерес исследователей вызвали механизмы, которые использовали вирусописатели для сокрытия вредоносного кода внутри APK-файлов.

По словам Н. Колье, вредонос хранит свои файлы в папках res и Assets внутри APK. В отличии от обычных дропперов, которые скрывают свое присутствие в APK, обновленная версия вредоноса использует необычную технику компиляции библиотек путем соединения нескольких файлов в один. Такой подход усложняет обнаружение вредоноса на системе и усложняет его поиск по сигнатурам.

Внутри APK файлы вредоноса выглядят как временные или ненужные файлы, и только после компиляции всего приложения можно определить, что именно из этих файлов и состоит сам дроппер.

Аналитики Malwarebytes ожидают рост количества атак с использованием обфусцированных APK взамен существующей практики принудительной установки нежелательного ПО на систему. Практика обфусцирования APK не является новой, однако методы и приемы злоумышленников становятся более сложными, что говорит о повышении интереса вирусописателей к мобильным платформам ***(Android-устройствам угрожает новый троян // InternetUA (http://internetua.com/Android-ustroistvam-ugrojaet-novii-troyan). – 2015. – 17.06).***

***

Китайские хакеры обходят защиту Tor и VPNПо данным исследователей безопасности из AlienVault, китайские хакеры нашли способ обхода защиты популярных инструментов анонимизации, использующихся, как правило, создателями и потребителями веб-контента, признанного государственными ведомствами противозаконным.

Речь идет о таких технологиях, как VPN и Tor, позволяющих скрыть истинное местонахождение системы пользователя. Оба инструмента пользуются популярностью во всем мире и особенно в Китае, где цензура осуществляется при помощи так называемого «Золотого щита».

По словам экспертов, разработавшие методы обхода хакеры использовали их для компрометации веб-сайтов, посещаемых китайскими независимыми журналистами, а также мусульманским этническим меньшинством. Более того, проэкслуатированная злоумышленниками уязвимость затрагивала также 15 довольно крупных китайских порталов, в том числе Baidu, Alibaba и RenRen (о возможных нападениях на них ничего не сообщается).

В AlienVault подчеркивают, что использование бреши позволяло похищать имена, адреса, даты рождения, номера телефонов и cookie-файлы пользователей. При этом исправления безопасности для указанной уязвимости уже были выпущены, однако не все веб-сервисы установили их вовремя.

Причастность китайского правительства к нападению, по словам экспертов, подтверждает лишь тот факт, что взлом упомянутых веб-сайтов не влечет получение финансовой выгоды ***(Китайские хакеры обходят защиту Tor и VPN // InternetUA (http://internetua.com/kitaiskie-hakeri-obhodyat-zasxitu-Tor-i-VPN). – 2015. – 16.06).***

***

Администрация Президента отмечает необходимость совершенствования защиты интернет-ресурсов из-за регулярных хакерских атак со стороны России. Об этом «Українським новинам» сказал заместитель главы Администрации Д. Шимкив.

«Угрозы в киберпространстве становятся более сложными, нужна дополнительная эвристика. Россияне пытаются атаковать нас, у них очень сильные специалисты, поэтому дополнительная защита должна строиться», – отметил он. По словам Д. Шимкива, регулярно идут попытки различных группировок как нарушить работу сайтов органов власти, так и проникнуть во внутренние сети.

Вместе с тем замглавы Администрации подчеркнул, что в Государственной службе специальной связи работает профессиональная команда, которая обеспечивает защиту.

Он также отметил, что защита новой версии сайта Президента лучше, чем у предыдущей ***(АП: хакерские атаки со стороны России усилились // InternetUA (http://internetua.com/ap--hakerskie-ataki-so-storoni-rossii-usililis). – 2015. – 14.06).***

***

Бундестаг не может справиться с вирусом в собственной компьютерной сети

Эксперты предполагают, что немецкому парламенту придется полностью заменить все компоненты информационной сети Parlakom, атакованной хакерами еще в начале мая. Размещенное в ней вирусное ПО продолжает свою работу до сих пор, отправляя данные в неизвестном направлении, сообщает IT World со ссылкой на издание Der Spiegel.

IT-специалисты немецкого парламента смогли обнаружить вторжение, однако справиться с ним до этого момента не удалось. Как утверждают анонимные источники из правительства, уже всерьез рассматривается вариант с полной заменой IT-инфраструктуры ведомства: как программного обеспечения, так и компьютеров.

Как отмечает Der Spiegel со ссылкой на «осведомленных людей», за хакерской атакой могут стоять российские спецслужбы, в частности СВР

(Бундестаг не может справиться с вирусом в собственной компьютерной сети // InternetUA (http://internetua.com/bundestag-ne-mojet-spravitsya-s-virusom-v-sobstvennoi-kompuaternoi-seti). – 2015. – 12.06).

***

Специалисты из Университета Индианы и Технологического института Джорджии опубликовали отчет о ряде 0-day уязвимостей в Apple iOS и OS X. Используя найденные дырки, исследователи сумели получить информацию, хранящуюся в Keychain, взломали «песочницу» и достали конфиденциальные данные из приложений Evernote, Facebook и не только.

Основой всему послужила атака XARA (Cross-App Resource Access), суть которой заключается в том, что крупные приложения могут предоставлять малвари доступ к информации других, легитимных приложений.

Анализ 1612 самых популярных приложений для Mac и 200 для приложений iOS выявил, что 88,6 % используют уязвимые для XARA-атак ресурсы системы. Одна из обнаруженных исследователями проблем касается Keychain. Эта функция присутствует в iOS 7.0.3 и OS X 10.9 Mavericks и выше. Она предназначена для хранения аутентификационных данных, токенов, ключей, данных о банковских картах, информации о сетях Wi-Fi и т. д.

По сути, каждому приложению принадлежит свой, небольшой кусочек Keychain, доступ к которому, должен быть только у этого приложения. Но исследователи выяснили, что можно создать зловреда, который мимикрирует под атрибуты обычного приложения, обманув Keychain.

Исследователи протестировали свою атаку на Keychain на Apple’s Internet Accounts и Google Chrome на OS X 10.10. Им удалось извлечь аутентификационные токены для аккаунтов iCloud и Facebook. Согласно отчету, Apple заблокировала возможность такой атаки на iCloud в 10.10.4, но это не остановит хакеров, которые могут просто удалить из Keychain запись.

Чтобы защитить приложения от влияния из вне, всему софту присваиваются идентификаторы Bundle ID (BID), которые определяют, что может делать то или иное приложение вне своего контейнера, и какие данные ему доступны. Данные идентификаторы должны быть уникальны для каждого приложения, и Apple проверяет на дубликаты все, что добавляют в App Store.

Однако Apple не справляется с проверкой подпрограмм в приложениях. Подпрограммы могут использовать тот же BID, что и другое легитимное приложение. Получается, что оба приложения работают в одной «песочнице» и имеют доступ к данным друг друга.

Также была обнаружена уязвимость в протоколе WebSocket, интегрированном в HTML5. Этим протоколом пользуется WebView в браузере, когда делает запрос к другому приложению в системе, через конкретный TCP-порт. Никакой аутентификации здесь просто нет, так что вредоносное приложение без проблем может получить доступ к контенту и прослушать этот порт.

Все вышеупомянутое относилось только к OS X, но еще одна уязвимость затрагивает, в том числе, и iOS. Как известно, приложения в обеих ОС могут делить друг с другом задачи, используя URL-схемы. В этом случае, как и в случае с WebSocket, атакующий может создать вредоносное приложение, которое будет использовать такую же URL-схему, что и другое, нормальное приложение.

Скажем, в системе появилось два приложения, и оба заявляют, что умеют открывать ссылки. Android в таких случаях спрашивает у пользователя, каким именно приложением ему воспользоваться. Устройства Apple не спрашивают ничего и не имеют никаких механизмов авторизации на такой случай. OS X просто выберет приложение, которое успело отозваться первым. iOS, напротив, отдаст предпочтение приложению, которое ответило последним. В результате малварь снова может «дублировать» функциональность легального приложения, отсылая данные куда захочет и делая, что пожелает.

Примечательно, что для проведения испытаний, авторы отчета написали собственное приложение для кражи логинов и паролей, и Apple пропустила его как в App Store, так и Mac App Store. Также исследователи утверждают, что сообщили обо всех найденных 0-day в Apple еще в октябре 2014 г., однако за прошедшие полгода в Купертино так и не занялись устранением перечисленных дырок. Устав ждать, исследователи обнародовали данные ***(В IOS и OS X обнаружен ряд 0-day уязвимостей // Центр Інформаційної Безпеки (http://www.bezpeka.com/ru/news/2015/06/19/IOS-OS-X-0-day.html). – 2015. – 19.06).***

***

Bloomberg раскрыло некоторые подробности международной кампании по борьбе с банковским вирусом Shylock. По данным издания, подобная операция проводится в Европе впервые, а как руководители выступают ИБ-эксперты правоохранительных органов Великобритании, поскольку именно там произошло наибольшее число нападений.

Впервые Shylock был выявлен еще в 2011 г. исследователями компании Trusteer, отметившими необычайную устойчивость вредоноса к обнаружению антивирусным ПО. Для повышения эффективности атак, создатели вируса использовали не только технологии шифрования, но и различные методы обфускации исходного кода.

Кроме того, Shylock оснащен функционалом, позволяющим противостоять удалению, а также восстанавливать себя после перезагрузки системы. Дополнительной преградой для борьбы с вредоносом является то, что все случаи инфекции произошли с помощью предварительно скомпрометированных злоумышленниками легитимных веб-сайтов.

Интересно также, что содействие в расследовании оказывают «Лаборатория Касперского», Microsoft и Европол. На сегодняшний день совместные усилия этих организаций позволили практически полностью демонтировать созданный Shylock ботнет. Вместе с тем эксперты отмечают, что

злоумышленники предпримут попытку восстановить работоспособность своей сети и говорить об успехе операции пока рано ***(В Европе провели международную операцию по борьбе с банковским трояном Shylock // Центр Інформаційної Безпеки (http://www.bezpeka.com/ru/news/2015/06/19/anti-Shylock.html). – 2015. – 19.06).***

***

Сомнительный инструмент для шпионажа под названием E-Detective, который использует более сотни правительственных спецслужб и правоохранительных ведомств содержит серьезные уязвимости, эксплуатация которых дает возможность злоумышленникам выполнить произвольный код и получить доступ к важной информации.

Бреши в программном обеспечении были обнаружены студентом университета Кингс-колледж (King's College London) М. аль-Бассамом.

Инструмент, разработчиком которого является тайваньская компания Decision Group, позволяет осуществлять наблюдение за пользователями компьютерных и мобильных сетей и перехватывать данные, в том числе логины и пароли на различных сервисах, таких как Google Gmail, Twitter, Facebook и даже банковских веб-сайтах.

По словам М. аль-Бассама, скрипт common/download.php в корневом каталоге позволяет неавторизованному пользователю прочитать произвольные файлы на системе, в том числе базу учетных данных и перехваченную информацию. Эксплуатация второй бреши позволяет удаленно выполнить код и изменить системные файлы. Демонстрационный пример (proof-of-concept) обнаруженных уязвимостей специалист опубликовал на портале GitHub ***(Используемый спецслужбами инструмент для шпионажа содержит серьезные уязвимости // Центр Інформаційної Безпеки (http://www.bezpeka.com/ru/news/2015/06/19/flawed-spy-tool.html). – 2015. – 19.06).***

***

В Интернете обнаружили вирус, который скрывается в размещённых на легитимных веб-сайтах изображениях. Вредонос распространяется через сайты с пиратскими генераторами лицензионных ключей.

Новый вид угрозы получил название Stegoloader, его обнаружили специалисты по безопасности из Dell SecureWorks. Вирус использует технологии цифровой стеганографии для сокрытия вредоносного кода от антивирусных инструментов.

Отличительные характеристики новой вирусной программы включают возникновение существенных затруднений во время анализа кода, а также заметно сниженную вероятность обнаружения.

В настоящее время чаще всего вирус можно «подхватить» через веб-сайты с пиратским программным обеспечением, на которых злоумышленники публикуют инфицированные генераторы лицензионных ключей.

Будучи активированным на пользовательской системе, вирус дополнительно загружает основной компонент – PNG-изображение, размещённое на легитимном портале и скрывающее вредоносный код ***(Появился интернет-вирус, зашифрованный в картинках на проверенных сайтах // Блог Imena.UA (http://www.imena.ua/blog/stegoloader). – 2015. – 17.06).***

***

Корейская Samsung объявила о выпуске обновления, которое закрывает обнаруженную ранее уязвимость во всех смартфонах на Android. Об этом сообщается в официальном блоге компании Samsung Tomorrow.

Обновление должно прийти в автоматическом режиме на все устройства, которые имеют встроенную систему защиты ядра ПО Knox. Кроме того, компания уже работает над обновлением системы для смартфонов, на которые Knox не установлен.

Ранее обнаруженная уязвимость затрагивала приложение клавиатуры, которое интегрировано в систему. Впервые эта клавиатура была установлена на Galaxy S3, который вышел в 2012 г. С того момента все смартфоны компании, работающие на Android, были подвержены этой уязвимости. По оценкам исследователей, она затронула более 600 млн смартфонов ***(Samsung выпускает обновление, закрывающее уязвимость во всех смартфонах // InternetUA (http://internetua.com/Samsung-vipuskaet-obnovlenie--zakrivauasxee-uyazvimost-vo-vseh-smartfonah). – 2015. – 22.06).***