

**СОЦІАЛЬНІ МЕРЕЖІ  
ЯК ЧИННИК  
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

*Огляд інтернет-ресурсів  
(12–24.05)*

**2015 № 10**

# **Соціальні мережі як чинник інформаційної безпеки**

**Інформаційно-аналітичний бюлетень**  
**Додаток до журналу «Україна: події, факти, коментарі»**  
Огляд інтернет-ресурсів  
(12–24.05)  
№ 10

## **Засновники:**

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

## **Відповідальний редактор**

Л. Чуприна, канд. наук із соц. комунікацій

## **Упорядник**

Т. Касаткіна

Заснований у 2011 році  
Виходить двічі на місяць

© Національна бібліотека України  
імені В. І. Вернадського, 2015

Київ 2015

## ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ.....	4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА .....	13
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ .....	19
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ .....	36
Інформаційно-психологічний вплив мережевого спілкування на особистість .....	36
Маніпулятивні технології .....	39
Зарубіжні спецслужби і технології «соціального контролю».....	46
Проблема захисту даних. DDOS та вірусні атаки .....	50

## РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Facebook запустила обещанный просмотр статей целиком, не покидая сайт. Сервис под названием Instant Articles стал доступен 13 мая, пока публикации тестируют The New York Times, BuzzFeed, National Geographic и ещё несколько изданий в приложении для iPhone. Об этом пишет goem.ru.

Instant Articles даёт анализировать статистику, а также совмещается с инструментами comScore, Omniture и Google Analytics. Реклама может появляться внутри Instant Articles. Если её продают сами издания, то они забирают всю выручку, если Facebook, то соцсеть забирает свои обычные 30 %.

Главное преимущество Instant Articles – экономия времени. Facebook также обещает делать разбор шрифтов, форматирование и прочие данные с сайта, чтобы каждая статья выглядела максимально похоже на сайт издания. Что касается медиафайлов, то Facebook предлагает вставлять картинки (их можно увеличивать по клику), видео, фоновое аудио и карты. К каждому посту можно будет прикрепить профиль автора.

Ранее компания тестировала технологию через читалку Paper, которая не снискала большого успеха, однако помогла компании разобраться, что именно нужно сделать в Instant Articles. Paper, тем не менее, пока закрывать не будут.

Менеджер по продукту в Paper М. Рекхау, который также стоит за Instant Articles, рассказал TechCrunch, что оптимизация ленты – главное направление в Facebook в последние несколько лет. Сначала были оптимизированы фотографии и видео, теперь дошла очередь и до статей. Скорость загрузки и удобство для пользователей – главные особенности, которые подчёркивают в Facebook, однако ясно, что таким образом компания методично затыкает дыры, из которых пользователи уходят из приложения на сторонние ресурсы (*Facebook начал публиковать материалы ведущих изданий через функцию «Мгновенные статьи» // МедиаБизнес (<http://www.mediabusiness.com.ua/content/view/43368/118/lang,ru/>). – 2015. – 13.05).*

\*\*\*

Pinterest объявила о запуске Платформы для разработчиков (Developers Platform) – API для создания и интеграции приложений.

По словам представителя Pinterest, это первый раз, когда соцсеть открывает доступ к API для разработки приложений. Для начала будет запущена бета-версия программы, где разработчики из США смогут зарегистрироваться для доступа к API.

Платформа позволит разработчикам использовать более 50 млрд проектов, мест и продуктов Pinterest для создания и развития приложений.

Мы ожидаем увидеть целый ряд приложений, которые преобразуют отрасли образования, транспорта или планирования отдыха. Представьте себе

приложение для заказа ингредиентов по рецепту из пина или бронирования поездки на основе пинов.

Несмотря на то что Платформа для разработчиков доступна пока только в Соединенных Штатах Америки, маркетологам и специалистам других стран в области интернет-рекламы все же стоит обратить на это внимание. Ведь, запуская API для разработчиков, Pinterest открывает новые горизонты для бизнеса (*Pinterest запустил платформу для разработчиков приложений // ProstoWeb* ([http://www.prostoweb.com.ua/internet\\_marketing/sotsialnye\\_seti/novosti/pinterest\\_zapustil\\_platformu\\_dlya\\_razrabotchikov\\_prilozheniy](http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/pinterest_zapustil_platformu_dlya_razrabotchikov_prilozheniy)). – 2015. – 14.05).

\*\*\*

TweetDeck внедрил подтверждение отправки твитов. Обновление призвано помочь специалистам социальных медиа избежать случайной публикации твитов из неправильных аккаунтов. Например, публикация личной информации в брендовом аккаунте может вызвать неловкость и стоить карьеры.

Функция доступна всем пользователям TweetDeck в Интернете, Chrome, Windows и последнем приложении Mac. Для ее активации следует нажать на вкладку «Аккаунты», выбрать профиль аккаунта и активировать «Шаг подтверждения». С этого момента любой твит, который пользователь отправляет из TweetDeck, не будет опубликован до тех пор, пока пользователь не кликнет на проверочное окно «Готов к твиту?»

Обновление поможет людям, ведущим несколько аккаунтов, а также тем, кто хочет перед отправкой проверить орфографические и грамматические ошибки.

Twitter обязала пользователей TweetDeck с 31 марта 2015 г. переключиться на авторизацию в платформе через учётную запись в Twitter (*TweetDeck внедрил подтверждение отправки твитов // ProstoWeb* ([http://www.prostoweb.com.ua/internet\\_marketing/sotsialnye\\_seti/novosti/tweetdeck\\_vnedril\\_podtverzhdzenie\\_otpravki\\_tvitov](http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/tweetdeck_vnedril_podtverzhdzenie_otpravki_tvitov)). – 2015. – 13.05).

\*\*\*

Число тех, кто получил возможность пользоваться Интернетом благодаря инициативе Facebook, в настоящее время достигло миллиарда. Об этом сообщил на своей странице в соцсети гендиректор Facebook М. Цукерберг.

Бесплатный доступ предоставляется к таким сервисам, как Wikipedia и Facebook, а также к различным ресурсам с информацией о здравоохранении и возможностях трудоустройства через специальное приложение. Реализация данной инициативы стала возможной благодаря партнерству социальной сети с местными операторами TNM и Airtel Malawi.

«Предоставлять людям бесплатный доступ в сеть – правильная вещь. Мы продолжим подключать все больше жителей и стран и не остановимся до тех

пор, пока каждый человек в мире не сможет подключиться к Интернету», – написал М. Цукерберг.

Также он представил в инфографике последнюю статистику по проекту. Internet.org в настоящее время запущен в 10 государствах: Гватемале, Колумбии, Гане, Замбии, Малави, Танзании, Кении, Индии, Бангладеш, Индонезии и на Филиппинах. Число людей, впервые воспользовавшихся Интернетом благодаря этой инициативе, оценивается в более чем 9 млн, а количество сервисов, доступных бесплатно, превысило сотню.

Кроме этого, основатель крупнейшей соцсети представил проектное изображение модели беспилотника Aquila, который в будущем должен раздавать Интернет с неба, и несколько его характеристик. Планируется, что такой летательный аппарат сможет покрывать сетью территорию площадью 40–80 кв. км. Размах его крыла составит 42 м, а высота полета – 18–27 км.

В августе 2013 г. М. Цукерберг запустил фонд Internet.org, в который входят также Ericsson, Nokia, Samsung, Opera Software, Qualcomm и ряд других компаний. Его основной целью является предоставление бесплатного доступа к Интернету для 5 млрд человек по всему миру (в основном, речь идет о населении бедных африканских стран). В рамках проекта Facebook при помощи партнеров планирует увеличить эффективность передачи электронных данных и снизить стоимость подключения в 100 раз.

Похожую инициативу развивает и Google. Интернет-компания намерена потратить более миллиарда долларов на развитие атмосферных спутников и других беспилотных летательных аппаратов, которые позволят подключить к Интернету удаленные регионы мира (*Facebook обеспечил бесплатным интернетом миллиард человек // InternetUA (<http://internetua.com/Facebook-obespecsil-besplatnim-internetom-milliard-cselovek>). – 2015. – 15.05*).

\*\*\*

Мессенджеры заменяют соцсети

Основатель социальной сети «ВКонтакте» П. Дуров сообщил об очередных успехах своего нового проекта, защищенного мессенджера Telegram, а компания BitTorrent, создавшая одноименную технологию обмена данными, выпустила свой безопасный мессенджер Vleer. «Газета.Ru» попыталась разобраться в феномене интернет-мессенджеров, которые стали одной из самых успешных телекоммуникационных технологий последних лет.

Самый знаменитый российский интернет-предприниматель П. Дуров в интервью изданию TechCrunch заявил, что месячная аудитория сервиса Telegram составила 62 млн, а количество ежедневно отправляемых через Telegram сообщений достигло 2 млрд.

По мнению самого П. Дурова, это отличные показатели, ранее сервису потребовалось девять месяцев, чтобы увеличить свою аудиторию на 15 млн (с марта по декабрь 2014 г.). За последние же пять месяцев рост пользовательской базы составил 12 млн.

Отметим, что другие сервисы мгновенных сообщений показывают еще более впечатляющий рост. Так, WhatsApp, купленный компанией Facebook весной 2014 г. за 19 млрд, нарастил за минувший год абонентскую базу с 450 млн до фантастических 800 млн.

Количество активных пользователей Viber за три последних месяца 2014 г. увеличилось на 15 % и к февралю 2015 г. достигло 236 млн человек. Всего же в Viber зарегистрировано 516 млн пользователей.

Удивительно здесь то, что во время взрывного роста социальных сетей многие эксперты прочили скорую смерть сервисам мгновенных сообщений. Аргументация была такова: все пользователи со временем перейдут на внутренние мессенджеры социальных сетей.

Не секрет, что мессенджеры существовали задолго до социальных сетей. Например, ICQ, или «аська», дожившая до наших дней и довольно успешно развивающаяся в настоящее время под крылом Mail.Ru Group, появилась в конце 1996 г., а разработка открытого протокола Jabber (сейчас – XMPP), на котором работает WhatsApp, началась еще в 1998 г. Однако с развитием социальных сетей об ICQ на время подзабыли. На Jabber работало много клиентов, но по-настоящему популярным стал только появившийся в 2009 г. WhatsApp.

Своим ренессансом сервисы мгновенных сообщений обязаны в первую очередь появлению смартфонов и широкополосного мобильного доступа в Интернет. Можно сказать, что выход первого iPhone стал вехой начала новой эры мессенджеров.

Если старые приложения идеально подходили под условия работы на десктопах в условиях медленного доступа в Интернет, то новые мессенджеры так же органично вписались в размеры экранов смартфонов, идеально подошли под тач-интерфейсы и расширили функции стандартных SMS. Кроме того, мобильный Интернет и сенсорные экраны сделали Интернет доступным и понятным более широкой аудитории, и мессенджеры получили еще больше новых пользователей.

При этом сами социальные сети, как ни странно, оказались в роли догоняющих и были вынуждены прибегнуть к практике приобретений успешных новых проектов, чтобы не потерять свой рынок.

Здесь сыграл свою роль и психологический аспект. Психика человека устроена так, что нам гораздо проще ассоциировать одно наименование с каким-то одним простым и понятным продуктом или услугой. Facebook – лента друзей, Twitter – статусы, а Вася Петров – сантехник. Сантехник-стоматолог не вызывает понимания и доверия, хотя он может быть хорошим и сантехником, и виртуозным стоматологом. Именно поэтому М. Цукерберг не стал сливать WhatsApp с интерфейсом Facebook, и даже мессенджер Facebook получил отдельный домен messenger.com, хотя он вряд ли станет лидером на этом рынке.

Еще одной немаловажной причиной четкого разделения мессенджеров и социальных сетей в сознании аудитории является кардинальное отличие поведения пользователя в этих двух средах.

Социальные сети изменили поведение аудитории Интернета на 180 градусов. Если пользователи «до социальных сетей» быстро усваивали урок, что в сети необходимо оставлять как можно меньше данных о себе, по возможности соблюдать полную анонимность, то «пользователям социальных сетей» прививается публичное поведение и привычка все выставлять напоказ.

Успешный современный человек – это отчасти и успешный блогер: посетил интересное место – чекин и селфи, встретил знаменитость – статус, взял в руки новинку в магазине – быстрый firstlook в сеть, примерил туфли из новой коллекции – фотосессия. Функция гео-позиционирования отслеживает перемещения и отмечает фешенебельные клубы и европейские города на карте автоматически. Да, такое поведение может вызывать иронические комментарии и насмешки, но оно же и привлекает всеобщее внимание и становится инструментом самопрезентации.

При этом каждому необходим свой приватный уголок. Если социальная сеть – это все напоказ, то мессенджер – это «место», где можно быть самим собой, поделиться чем-то секретным или интимным. Более того, у пользователей возникает потребность надежной защиты этой области своей жизни, которую нельзя доверить социальным сетям, пропагандирующим совсем другую модель поведения. Общий информационный фон последних двух лет – откровения Э. Сноудена о слежке спецслужб в Интернете, интимные фото знаменитостей, попавшие в сеть, – сформировали запрос не просто на приватное, но даже на сверхприватное общение. Отсюда и успех Telegram, и появление других защищенных мессенджеров.

Так, 13 мая компания BitTorrent, создавшая и поддерживающая знаменитый одноименный протокол обмена данными BitTorrent, представила свой защищенный мессенджер Bleep для Windows, Mac OS X и всех основных мобильных платформ.

Bleep предназначен для обмена сообщениями и фотографиями и совершения голосовых звонков в зашифрованном виде. Особенность Bleep – работа в пиринговой сети, то есть без центрального сервера (на котором хранится переписка) и поддержка end-to-end-шифрования между абонентами. Пользователи Bleep могут зарегистрироваться при помощи адреса электронной почты, номера мобильного телефона либо общаться полностью анонимно.

Также разработчики добавили функцию Whisper для обеспечения защиты переписки на самих устройствах. При включении режима Whisper время «жизни» сообщений составляет 25 секунд, затем они безвозвратно удаляются.

С ростом производительности смартфонов, дальнейшим проникновением быстрого мобильного Интернета и развитием инфраструктуры сами мессенджеры продолжают усложняться и обрывать новыми функциями: от банальных наклеек и мобильных игр, которые, кстати, приносят им хороший доход, до рекомендательных сервисов на основе гео-информации и



семантического анализа разговоров и мобильных платежей через сообщения. Зачастую мессенджеры, например «публич чаты» Viber, начинают выполнять функцию каналов массовой коммуникации. Для традиционных СМИ эти каналы приобретают такое же важное значение, как и социальные сети. Брендам публичные аккаунты позволяют установить тесную коммуникацию со своей ядровой аудиторией.

Таким образом, мессенджеры становятся следующим «большим интернет-трендом». И хотя они вряд ли смогут полностью заменить «стену» социальной сети, часть пользовательского внимания и времени, проводимого в Интернете, они на себя перетянут.

Глава представительства Viber в России Е. Рощупкин уверен, что будущее за частными сетями и личным общением: «Люди все меньше и меньше заинтересованы в том, чтобы рассказывать о себе широкой аудитории, а ищут более личное и персональное общение. Мы видим рост популярности приложений, предлагающий возможности общения один-на-один. И нам кажется, что будущее именно за личным общением в небольших группах и коллективах».

Мессенджеры уже сейчас начинают интегрировать сторонние сервисы для того, чтобы в будущем пользователи могли обмениваться информацией о своих предпочтениях и интересах, делиться информацией о заказе билетов, поездках на такси прямо через личные сообщения или общение в группах благодаря открытому API.

«Сервисы мгновенных сообщений могут стать для пользователя социальной платформой с множеством функций. Например, не выходя из приложения, можно играть, читать новости, а не только общаться и звонить друзьям. Те же «публич чаты» за полгода суммарно уже набрали более 3 млн подписчиков. Свои чаты открыли такие издания, как Rolling Stone, Hello, TimeOut. Большой популярностью пользуется чат резидентов Comedy Club», – говорит Е. Рощупкин (*Мессенджеры заменяют соцсети // InternetUA (<http://internetua.com/messendjери-zamenyauat-socseti>). – 2015. – 15.05*).

\*\*\*

Новый стриминговый музыкальный сервис Apple, который, скорее всего, получит название Apple Music, будет включать в себя социальную сеть для исполнителей. Об этом сообщает lenta.ru со ссылкой на портал 9to5Mac.

Музыканты смогут создавать в соцсети профили и публиковать в них, например, фрагменты треков, фотографии, видеоклипы или анонсы концертов, а также делиться контентом своих коллег. В свою очередь слушатели, используя аккаунт на iTunes, получат возможность комментировать публикаций звезд, ставить «лайки». При этом они не смогут создавать свои страницы в соцсети по аналогии с исполнителями.

Согласно информации портала, ключевой функцией социальной сети станет Artists Activity («Активность исполнителей»), которую можно будет по

желанию отключить в настройках. Соцсеть будет доступна для версий Apple Music на iOS, Android и Mac.

Сам музыкальный сервис будет интегрирован в обновленное приложение музыки для iOS 8.4 и основан на стриминговом приложении Beats Music, доработанным под экосистему Apple. Владельцы библиотеки на облачном хранилище Beats Music также смогут перенаправить ее в Apple Music.

Apple планирует запустить свой новый сервис уже к концу июня, а его анонс произойдет 8 июня на конференции компании для разработчиков Worldwide Developers Conference (WWDC). Ожидается, что Apple Music будет платным, однако при запуске выйдет бесплатная пробная версия (**СМИ сообщили о планах Apple запустить соцсеть для музыкантов // МедиаБизнесе** (<http://www.mediabusiness.com.ua/content/view/43389/118/lang,ru/>). – 2015. – 14.05).

\*\*\*

Facebook подтвердил в разговорах с несколькими разработчиками свое желание запустить игры в мессенджере. На сегодняшний день неясно, как будут работать эти игры и когда появится первая игра, пишет Marketing Media Review (<http://mmr.ua/news/id/v-facebook-messenger-pojavjatsja-igry-44383/>).

«В настоящее время мы считаем, что платформа мессенджера лучше всего подходит для приложений, сфокусированных на создании контента и курировании контентом, – сказал представитель Facebook Mashable. – Но одна из причин, по которой мы предоставили доступ к платформе для всех разработчиков, чтобы посмотреть, что люди создают. Потом мы поймем, что еще будет уместным».

Messenger, который насчитывает 600+ млн пользователей, за последние шесть месяцев добавил новые функции, начиная от обслуживания покупателей и платежей между двумя физическими лицами и заканчивая видео чатом. Он также открыл платформу для сторонних разработчиков, чтобы стимулировать вовлечение и рост пользователей.

Игры для мессенджера очень целесообразны. Благодаря им пользователи проведут в приложении больше времени (**В Facebook Messenger появятся игры // Marketing Media Review** (<http://mmr.ua/news/id/v-facebook-messenger-pojavjatsja-igry-44383/>). – 2015. – 19.05).

\*\*\*

Twitter начал запуск обновлённой страницы поиска для всех авторизованных пользователей десктопной версии сервиса. Внедрение нового функционала, который проходил тестирование с апреля, уже начато. Об этом пишет searchengines.ru.

«Мы запускаем новый поисковый интерфейс для пользователей веб-версии Twitter. Мы и дальше продолжим улучшение этого функционала, чтобы

ещё больше облегчить пользователям поиск того, что они ищут в Twitter», – прокомментировал запуск пресс-секретарь компании.

Среди основных нововведений – поисковые фильтры (люди, фотографии, видео), которые ранее находились с левой стороны поискового интерфейса, были перемещены наверх страницы. Теперь фильтры размещены под горизонтальным баннером, включающим поисковый запрос.

Заголовок More options даёт возможность задать более точные критерии поиска и искать новости; твиты от читаемых пользователей; твиты от людей, которые находятся поблизости, и другие.

Из меню More options пользователи также могут сохранить поиски; встроить их путём доступа к виджетам и начать расширенный поиск.

Ранее пользователи могли выбирать между популярными и всеми твитами, релевантными поисковому запросу. Теперь заголовок «Все» (All) переименован в Live, акцентируя внимание на том, что публикации в Twitter осуществляются в режиме реального времени.

Когда появляются новые твиты, релевантные поисковому запросу, пользователи получают уведомление и могут нажать на ссылку для загрузки новых результатов поиска.

По умолчанию в результатах поиска отображаются популярные твиты, а также релевантные аккаунты и фото.

В отличие от изначального эксперимента, в этой версии Twitter добавил модуль «Похожие поиски» (Related searches). Он расположен на левосторонней панели над «Близкие по духу» (Who to follow) и разделом «Актуальные темы» (Trending topics) *(Twitter запускает новый поисковый интерфейс в десктопной версии сервиса // МедиаБизнес (<http://www.mediabusiness.com.ua/content/view/43432/118/lang,ru/>). – 2015. – 19.05).*

\*\*\*

Facebook обновила приложения своего мессенджера для Android, iOS, теперь они поддерживают видеосвязь во всех странах мира за редкими исключениями. По словам вице-президента Facebook Д. Маркуса, видеосвязь недоступна в ОАЭ из-за блокировки операторами, а также в Египте, Саудовской Аравии и Бахрейне из-за низкого качества передачи данных.

Чтобы инициировать видеозвонок, нужно перейти на страницу чата с определенным контактом и нажать на кнопку видеокамеры. Звонок будет возможен только в том случае, если человек доступен в сети и поделился с вами номером своего телефона, то есть дал согласие на общение не только в переписке.

Видеосвязь в мессенджере Facebook появилась в конце апреля, но была доступна жителям лишь 18 стран *(Видеосвязь через Facebook Messenger теперь доступна по всему миру // InternetUA (<http://internetua.com/videosvyaz-cserez-Facebook-Messenger-teper-dostupna-po-vsemu-miru>). – 2015. – 20.05).*

\*\*\*

Протести щодо проекту Internet.org з надання безкоштовного доступу до ряду сервісів у мережі поширюються світом. Про це повідомляє ВВС.

Загалом 67 правозахисних організацій у сфері цифрових технологій, включаючи рух за свободу в Уганді (Freedom Uganda), організацію Usuarios Digitales в Еквадорі та індонезійську ICT Watch, написали лист засновникові Facebook М. Цукербергу, висловивши свої побоювання щодо ініціативи Internet.org.

Вони наголосили, що проект загрожує свободі вираження поглядів, приватності та принципів мережевого нейтралітету.

Facebook продовжує відстоювати свою позицію.

«Ми переконані, що все більше і більше людей, отримуючи доступ до Інтернету, побачать його переваги і захочуть використовувати ще більше сервісів», – відповів прес-секретар компанії на питання ВВС.

«І ми настільки в це віримо, що працюємо з операторами, пропонуючи людям основні сервіси безкоштовно. Переконані, що нові користувачі швидко захочуть вийти за рамки основних і почнуть платити за нові можливості», – додав він.

Раніше М. Цукерберг зазначав, що інтернет-нейтральність не суперечить наданню інтернет-доступу тим, хто його потребує (*Протести щодо проекту Цукерберга Internet.org зростають // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/protesti\_schodo\_proektu\_tsukerberga\_internetorg\_zrostayut/). – 2015. – 21.05).*

\*\*\*

23 мая на мероприятии Dribbble Meetup ведущий дизайнер «ВКонтакте» П. Шумаков анонсировал приложение соцсети для обработки фотографий. В настоящее время проект носит кодовое название ProjectX.

По словам П. Шумакова, на сегодня устройство ленты «ВКонтакте» не позволяет пользователям сфокусироваться на обновлениях от друзей из-за большого количества записей от сообществ. Новое приложение должно решить эту проблему.

В сервисе будет реализована полная синхронизация со «ВКонтакте», цветокоррекция изображений и обмен фильтрами: пользователи смогут самостоятельно создавать фильтры и делиться ими с друзьями.

При этом представитель «ВКонтакте» отметил, что соцсеть не задумывается о конкуренции с Instagram, поскольку обладает собственной широкой аудиторией. Фотоприложение будет решать проблемы с пропуском обновлений от друзей (*Зачем «ВКонтакте» разрабатывает отдельное приложение для фотографий // InternetUA (http://internetua.com/zacsem-vkontakte--razrabativaet-otdelnoe-prilojenie-dlya-fotografii). – 2015. – 24.05).*

\*\*\*

Google начала показывать твиты в реальном времени

Google и Twitter сообщили в своих официальных блогах, что заключили сделку. Компании договорились, что записи из сервиса микроблогов будут более заметно представлены в выдаче поисковика. Причем индексация будет происходить в реальном времени.

Пока что обновленная выдача доступна лишь на мобильных устройствах, однако в будущем Google обещает реализовать нововведение и в десктопных браузерах. При вводе запроса в верхней части страницы отображается «карусель» из релевантных твитов, в том числе с изображениями. Пролитывать твиты можно горизонтальными свайпами.

Блок с твитами не всегда оказывается в верхней части страницы, Google может отображать его и в середине, уже после других ссылок, или не отображать вовсе. Как отмечает блог Search Engine Land, по каким именно запросам в выдаче оказываются твиты, в Google сообщить отказались. Вероятно, поисковик ориентируется на активно используемые в данный момент в сервисе микроблогов хэштеги, тренды Twitter или темы, популярные в новостях.

В Twitter рассказали изданию, что никаких денег напрямую от Google за клики по твитам не получают. Зато сервис микроблогов получает трафик и потенциальных новых пользователей. Если на мобильном устройстве установлено приложение Twitter, ссылки на твиты из поиска могут открываться прямо в нем.

В настоящее время функция запущена лишь для англоязычных пользователей в США. В будущем обещана поддержка других языков, география тоже наверняка расширится (*Google начал показывать твиты в реальном времени // InternetUA (<http://internetua.com/Google-nacsal-pokazivat-tviti-v-realnom-vremeni>). – 2015. – 20.05*).

## **СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА**

У четвер, 14 травня, увечері за місцевим часом чергову онлайн-сесію запитань та відповідей Facebook розпочали саме із запитання, яке поставили українці.

Як інформує VIDIA, модератор зустрічі повідомив, що найпопулярнішим запитанням, яке набрало 45 тис. лайків, було саме про Україну і поставив його користувач з Ізраїля на ім'я Григорій.

Користувач поскаржився на несправедливість при блокуванні сторінок і дописів з боку Facebook, пояснюючи це тим, що український сегмент курирує російський менеджмент.

Зі слів очільника компанії Fесеbook, він особисто переглянув, про що йдеться перед тим, як надати відповідь. М. Цукерберг прокоментував, що дійсно було кілька дописів, які вони вирішили видалити за порушення правил, що забороняють використання «мови ненависті» проти іншої національності.

«На жаль, є кілька дописів, які порушили це правило. Люди поскаржились, і ми, переглянувши ці дописи, визначили, що деякі з цих дописів містили образливу лексику щодо деяких росіян, і ми їх зняли», – пояснив М. Цукерберг.

Він також запевнив, що у Росії не існує адміністрації Facebook, яка б модерувала український сегмент мережі.

«Звучали також запитання, чи дописи, зроблені українцями, модеруються росіянами в час, коли між Україною та Росією триває конфлікт. Це не відповідає дійсності – у нас немає такого російського офісу. Тому кожен, хто думає, що модерація відбувається з російського офіса антиукраїнськими модераторами, помиляється», – запевнив М. Цукерберг.

Він пояснив, що модерацію здійснюють працівники представництва компанії у Дубліні, які володіють мовою, якою зроблено допис. Проте додав, що в системі існувала помилка, через яку авторам окремих дописів помилково повідомили не ту причину – наявність оголеності в зображеннях замість лексики ненависті. За цю помилку Facebook вибачився, повідомив М. Цукерберг.

Після цього М. Цукерберг відповів і на запитання Президента України П. Порошенка щодо можливості відкриття представництва Facebook в Україні. Він сказав, що з часом таку можливість можуть розглянути, але пояснив, що доцільність лежить у площині розвитку компанії, зокрема розробки програмного забезпечення.

Запитання П. Порошенка демонстрували на екрані, та П. Цукерберг був помітно радий увазі Президента України (*Цукерберг відповів українцям коли буде офіс Facebook у Києві // Інформаційна агенція «Вголос» ([http://vgolos.com.ua/news/tsukerberg\\_vidpoviv\\_ukraintsyam\\_koly\\_bude\\_ofis\\_facebook\\_u\\_kyievi\\_180412.html](http://vgolos.com.ua/news/tsukerberg_vidpoviv_ukraintsyam_koly_bude_ofis_facebook_u_kyievi_180412.html)). – 2015. – 15.05).*

\*\*\*

18 травня відзначається 71-а річниця з дня депортації кримськотатарського народу, пише Корреспондент.net (<http://ua.korrespondent.net/ukraine/3516297-ukraintsi-vlashtuvaly-Twitter-shtorm-na-pidtrymku-krymskykh-tatar>).

18 травня в день 71-річчя депортації кримських татар користувачів соцмереж закликають приєднатися до Twitter-шторму.

Ініціаторами акції виступили ГО Центр UA, Крим SOS, Громадський рух «Чесно», пише Телекритика.

«З моменту анексії півострова права кримськотатарського населення зазнали жорстоких гонінь. Істотних обмежень зазнали й права на свободу слова

– 1 квітня майже всі незалежні, кримськотатарські ЗМІ були закриті», – повідомляють організатори.

За їхніми словами, щоб долучитися до акції, треба використовувати свій акаунт у Twitter, щоб написати повідомлення, яке складається з тексту повідомлення й хештега (#SaveCrimeanTatars, #QirimSurgunu) *(Українці влаштували Twitter-шторм на підтримку кримських татар // Кореспондент.net (http://ua.korrespondent.net/ukraine/3516297-ukraintsi-vlashtuvaly-Twitter-shtorm-na-pidtrymku-krymskykh-tatar). – 2015. – 18.05).*

\*\*\*

Международный фонд защиты природы запустил социальную кампанию в Twitter. Организация использовала эмодзи-символы, чтобы рассказать историю о вымирающих видах и призвать пользователей жертвовать средства с помощью социальной сети, пишет Marketing Media Review (<http://mmr.ua/news/id/wwf-prizval-sdelat-pozhertvovaniya-s-pomoschju-smajlikov-44291/>).

Идея кампании возникла после того, как в организации обнаружили, что 17 героев в эмодзи алфавите представляют вымирающие виды животных.

Кампания призывает отправить твит с эмодзи, представляющим вымирающее животное, чтобы другие пользователи сделали ретвит и таким образом стали участниками кампании. С помощью специальной технологии сервиса WWF подсчитает количество твитов с эмодзи в месяц и превратит их в пожертвования (0,10 евро за твит).

В конце месяца пользователи получают отчет о количестве использованных эмодзи с ссылкой, куда они могут внести пожертвования. Они могут пожертвовать всю сумму, или ее часть или вообще не делать пожертвований.

Кампания, разработанная Wieden+Kennedy, запущена ко дню вымирающих животных, который отмечается 15 мая *(WWF призвал сделать пожертвования с помощью смайликов // Marketing Media Review (http://mmr.ua/news/id/wwf-prizval-sdelat-pozhertvovaniya-s-pomoschju-smajlikov-44291/). – 2015. – 12.05).*

\*\*\*

Работники пресс-службы прокуратуры Донецкой области создали официальный аккаунт в соцсети Twitter. Об этом говорится в сообщении ведомства, пишут «Новости Донбасса» (<http://novosti.dn.ua/details/250742/>)

«Теперь Вы можете следить за нашими новостями в Twitter. Здесь мы будем регулярно делиться с вами оперативной информацией и новостями. А также анонсировать наши мероприятия», – говорится в сообщении *(У пресс-службы прокуратуры Донецкой области появился официальный Twitter // Новости Донбасса (http://novosti.dn.ua/details/250742/). – 2015. – 12.05).*

\*\*\*

Для борьбы с кремлевской пропагандой в ряды «Информационных войск Украины» уже записались более 40 тыс. добровольцев.

Как передает Цензор.НЕТ, об этом в эфире «5 канала» сообщила заместитель министра информационной политики Украины Т. Попова.

«Набор в ряды “Информационных войск” продолжается... Где-то две-три недели назад там было уже более 40 тыс. добровольцев», – сказала она.

Со слов Т. Поповой, «Информационные войска» на различных интернет-сайтах дают миллионные распространения той информации, которую дает Министерство информполитики.

«Сейчас наши “раззомбирующие” ролики имеют более миллиона просмотров, потому что добровольцы работают на разных форумах и в разных пабликах», – добавила заместитель министра информационной политики.

Отметим, в конце февраля 2015 г. в Украине начался набор в «Информационные войска».

«За год нам удалось создать мощную боевую армию, которая мужественно защищает нас на территории Донбасса. А сейчас пора дать отпор русским оккупантам и на информационном фронте. Каждый украинец с доступом к Интернету может сделать свой вклад в информационную борьбу», – говорится на портале «Информационные войска Украины» (*Мининформполитики: в «Информационных войсках Украины» уже более 40 тысяч добровольцев // Цензор.НЕТ ([http://censor.net.ua/news/335853/mininformpolitiki\\_v\\_informatsionnyh\\_voyiskah\\_ukrainy\\_uje\\_bolee\\_40\\_tysyach\\_dobrovoltsev](http://censor.net.ua/news/335853/mininformpolitiki_v_informatsionnyh_voyiskah_ukrainy_uje_bolee_40_tysyach_dobrovoltsev)). – 2015. – 12.05).*

\*\*\*

Кировоградские чиновники и депутаты, которые идут в ногу со временем, уже давно зарегистрировались в популярных социальных сетях. Интернет-сайт Кавун решил проанализировать, что сегодня волнует известных людей города.

Начнем с губернатора Кировоградщины С. Кузьменко. Официальной страницы главы области на Facebook найти не удалось. Однако активной в Интернете является заместитель председателя ОГА В. Атаманчук. Чиновница регулярно обновляет фотографии, пишет преимущественно о работе или делится своими мыслями. Постоянно выставляет информацию о различных совещаниях с ее участием.

Главная тема, которую обсуждает в Интернете заместитель мэра С. Васильченко – свои рабочие значительные достижения и достижения Кировоградской власти. В рабочее или в нерабочее время – чиновник почти всегда онлайн. Активно отписывает комментарии (как он говорит – общается с людьми), критику совершенно не воспринимает и всегда огрызается. Личными фотографиями С. Васильченко делится крайне редко, исключительно по работе. Публикует на своей странице интересные для него материалы на медицинскую тематику (например, о вакцинации), или же обнародует ответы на его



депутатские запросы. Зачастую пишет различную информацию об областном онкодиспансер, где когда-то работал главным врачом.

Еще один народный депутат К. Ярынич тоже ярый фейсбукивец. Как и все, он делится фотографиями, выставляет даже СЕЛФИ с операционной онкодиспансера, которые впоследствии удаляют (*Кировоградские депутаты и чиновники онлайн // Городской портал Кировограда (http://kr.ua/news/news/2130/). – 2015. – 13.05).*

\*\*\*

Київська міська державна адміністрація створила офіційну сторінку в соціальній мережі Facebook

Одним з ефективних способів налагодження конструктивного, плідного діалогу та зворотного зв'язку влади з громадськістю є використання соціальних мереж, зокрема Facebook, – переконаний керівник апарату Київської міської державної адміністрації В. Бондаренко.

«Для оперативного і достовірного інформування громадськості про діяльність міської влади та налагодження конструктивного діалогу з мешканцями міста ми створили сторінку КМДА у мережі Facebook. Відтепер усі користувачі, вподобавши сторінку, зможуть отримувати новини, анонси подій та іншу інформацію про події у місті. Сподіваюся, сторінка буде цікавою та корисною для киян, які частіше використовують соціальні мережі, ніж офіційні сайти», – сказав В. Бондаренко.

Він наголосив, що новостворена сторінка Київської міської державної адміністрації – єдина офіційна в мережі Facebook, до функціонування інших сторінок, які ведуться від імені міської держадміністрації, у КМДА не мають ніякого стосунку. Адміністратором справжньої сторінки є управління інформаційного забезпечення та доступу до публічної інформації апарату КМДА.

В управлінні зазначають, що відповіді адміністратора сторінки користувачам в особистих повідомленнях на запитання чи пропозиції є винятково консультативними і не можуть використовуватися як офіційна відповідь установи, у тому числі для представників засобів масової інформації.

Для отримання офіційної відповіді, зокрема публічної інформації, необхідно звертатися в установленому порядку (детальніше – у розділі «Контакти» на офіційному інтернет-порталі КМДА).

Сторінка у Facebook: <https://www.facebook.com/712429695547137>  
(*Київська міська державна адміністрація створила офіційну сторінку в соціальній мережі Facebook // Київська міська державна адміністрація (http://kievcity.gov.ua/news/23930.html). – 2015. – 13.05).*

\*\*\*

Президент США Б. Обама завів особисту сторінку в соціальній мережі Twitter. Twitter поставив навпроти імені Б. Обама блакитний значок підтвердження особи, зарезервований для відомих людей, пише

Корреспондент.net (<http://ua.korrespondent.net/world/3516620-obama-zaviv-osobystyi-akkaunt-v-Twitter>).

«Привіт, Twitter! Це Барак. Правда! Шість років на посту, і, нарешті, мені дали мій власний акаунт», – написав Б. Обама.

Білий дім на своїй сторінці ретвітнув повідомлення Б. Обама.

Акаунт Б. Обама розміщено за адресою: POTUS (President Of The United States – «Президент США»).

Крім того, існує акаунт за адресою: BarackObama, на який підписано майже 60 млн осіб. Його ведуть співробітники адміністрації президента (**Обама завів особистий акаунт в Twitter // Корреспондент.net** (<http://ua.korrespondent.net/world/3516620-obama-zaviv-osobystyi-akkaunt-v-Twitter>). – 2015. – 19.05).

\*\*\*

Кримськотатарський телеканал АТР, який з 1 квітня не виходить в ефір через відмову Роскомнагляду в перереєстрації, відкрив офіційний YouTube-канал. Про це канал повідомив на своїй сторінці у Facebook, пише telekritika.ua.

«Щоб фільми, які були зроблені нами за минулий місяць, були доступні кожному, ми відкрили офіційний канал на YouTube. Тут наші свіжі роботи :) У майбутньому ми постараємося викласти сюди весь наш архів, який повинен бути надбанням всього народу. Підписуйтеся і поширюйте :)), – ідеться в повідомленні кримськотатарського каналу.

Нагадаємо, як повідомила «Телекритиці» заступник генерального директора АТР з інформаційної політики Л. Буджурова, із травня відновила роботу інформаційна редакція АТР. Нові сюжети планувалося публікувати на сайті каналу.

Після припинення мовлення команда готувала документальні проекти – зокрема про кримських татар – дітей війни та перших репатріантів. Зараз на YouTube-каналі опубліковано 12 відеоробіт.

«По крихтах ми збирали спогади тих, хто відкрив шлях на Батьківщину, хто закладав фундамент перших будинків, кого намагалися виселити повторно ... Але всі вони подолали ці випробування. Бо кожен з них, як і кожен з нас має право на Батьківщину», – анонсує документальні ролики канал.

Нагадаємо, 1 квітня припинив роботу не лише телеканал АТР, а й інші ЗМІ кримськотатарського медіа-холдингу АТР, до якого входить ще дитячий телеканал Lale («Ляле»), радіостанції Meydan («Мейдан») і «Лідер».

19 березня «глава» окупаційної влади Криму С. Аксьонов заявив, що «у напіввійськовий час» робота таких телеканалів як кримськотатарський канал АТР недопустима.

Водночас керівництво кримськотатарського телеканалу АТР повідомляло, що мовник готовий позбавитись свого інформаційно-політичного контенту, якщо це дасть змогу перереєструватись за російським законодавством.

1 квітня Президент України П. Порошенко доручив Міністерству інформаційної політики створити умови для роботи кримськотатарського каналу АТР в Україні.

Тим часом керівництво холдингу АТР заявляє, що не полишає надій перереєструватися за російським законодавством і продовжити мовлення в Криму.

23 квітня так званий «прем'єр-міністр» С. Аксьонов підписав указ про створення «Общественной крымскотатарской телерадиокомпани» (ОКТРК), на яку планується виділити більше 177 млн р. (близько 79 млн грн) з федерального бюджету. 27 квітня стало відомо, що новий провладний кримськотатарський телеканал у Криму називатиметься «Міллет», радіо – «Ветан» *(Телеканал АТР відкрив офіційний YouTube-канал з документалістикою // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43440/118/lang,ru/). – 2015. – 19.05).*

## БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Facebook предложила рекламодателям розміщати рекламу мобільних приложений в виде карусели, пише Marketing Media Review (<http://mmr.ua/news/id/facebook-zapustil-reklamu-ustanovki-prilozhenij-v-vide-karuseli-44285/>).

Новый формат будет поддерживать пять изображений и ссылок, которые будут прокручиваться по горизонтали. Этот формат будет доступен как для рекламы установки приложений, так и для вовлекающих объявлений. По данным Facebook, ссылка в немобильной карусели приводит к снижению стоимости конверсии на 30–50 %, а также на 20–30 % – по сравнению с рекламой, состоящей из одного изображения.

Формат карусели должен стать хитом у рекламодателей и их целевых аудиторий. Карусель мобільних объявлений будет доступна для ссылочных объявлений в API, Power Editor и Ad Create Tool. Mobile Install и Engagement Ads доступны только в API.

В прошлом году Facebook запустила формат карусели для достижения брендовыми рекламодателями нескольких целей в одном рекламном пространстве. Формат позволяет рекламодателям выделить различные атрибуты, выгоды или даже продукты в одном месте.

Нововведение даст рекламодателям возможность направлять пользователей на конкретные страницы приложений, где они смогут приобрести виртуальные товары или получить дополнительную информацию *(Facebook запустил рекламу установки приложений в виде карусели //*

\*\*\*

Основные тактики для увеличения трафика из соцсетей

Социальные сети в настоящее время очень популярны. Именно поэтому их используют для привлечения трафика. Однако сделать все это далеко не так просто, как может показаться на первый взгляд. Но при правильном подходе можно получить максимальный трафик. Существует 11 специальных тактик, которые помогут это сделать.

Существует мнение, что сервис Twitter был создан исключительно для того, чтобы пользователи менялись друг с другом мыслями, объем которых не будет превышать 140 знаков. Однако в действительности можно повысить частоту кликов примерно на 108 %, если добавить в твит ссылку на статью с изображением.

Необходимо стараться делать перерывы между публикациями. Это увеличит трафик из соцсетей. Нельзя перегружать новостную ленту подписчиков. Когда новости постоянно, буквально каждую минуту мелькают в ленте, они очень скоро могут просто надоесть. Желательно подходить к публикации контента очень взвешенно и тщательно. Главное подобрать оптимальное сочетание частоты и качества. Для разных сетей данный показатель является разным. Например, в Twitter нужно добавлять новость не чаще чем один раз в час, в VK надо делать один пост за три часа, а в Facebook в день от одного до четырех постов.

Нужно делиться с пользователями только лишь самым лучшим контентом. Вне зависимости от того, в какой социальной сети идет продвижение, публикации не самого качественного контента могут нивелировать рейтинг. Надо постараться научить подписчиков ожидать исключительно ценный и увлекательный материал. Это очень важно для увеличения трафика.

Надо следовать такому правилу, как 80/20. Эта пропорция является оптимальной для постинга. То есть порядка пятой части новостей с собственного ресурса нужно публиковать в социальных сетях вместе с 80 % с остальных познавательных источников. Не нужно допускать перебора сообщений о собственном сайте, потому что это выглядит слишком навязчиво и очень похоже на наглую саморекламу.

Лучше всего размещать ссылки в верхней части сообщения. Во время публикации новости в социальной сети каждый раз надо вставлять ссылку в начале. Этот вариант увеличивает многократно вероятность клика.

В Facebook лучше не писать без изображений. Читатели данного ресурса любят картинки и не очень хорошо воспринимают информацию без фото. Согласно статистике можно понять, что обновленный статус с изображением обеспечивает намного большее количество комментариев и лайков. Надо также добавлять к изображению призыв к действию, потому что он повышает

кликабельность примерно на 14 % (*Основные тактики для увеличения трафика из соцсетей // Новости ИТ (<http://www.novostiit.net/osnovnyie-taktiki-dlya-velicheniya-trafika-iz-sotssetey-00021027>). – 2015. – 12.05*).

\*\*\*

Facebook обновила инструментарий нативной рекламы в Audience Network, добавив новые шаблоны, менеджер объявлений и возможность горизонтальной прокрутки.

Платформа по размещению рекламы в мобильных приложениях Audience Network была запущена Facebook в октябре 2014 г. Одна из уникальных рекламных опций, предлагаемых этим сервисом, – API для нативной рекламы как для iOS, так и Android-устройств. Теперь компания усилила этот функционал.

Новые шаблоны позволят клиентам платформы кастомизировать в объявлении всё, начиная от высоты и ширины и заканчивая цветом заголовка и кнопок. Это позволит издателям быстро и легко изменить нативные объявления, чтобы привести их в соответствие с внешним видом и «духом» приложений.

Сохранять и доставлять объявления поможет новая функция Native Ads Manager. Менеджер объявлений будет предзагружать 10 объявлений и доставлять их, исходя из прогнозируемого дохода.

Кроме того, в Audience Network теперь будет поддерживаться горизонтальная прокрутка объявлений. Эта опция будет доступна и в шаблонах, и в менеджере нативных объявлений, и поможет рекламодателям максимизировать количество объявлений в рамках заданного пространства приложений.

Более подробная информация о нововведениях в Audience Network доступна в официальном блоге Facebook для разработчиков.

Напомним, что в прошлом месяце компания добавила видеофункционал в рекламу десктопных приложений. Нововведение призвано увеличить число установок игровых десктоп-приложений, разработанных для социальной сети (*Facebook расширил инструментарий нативной рекламы в Audience Network // ProstoWeb ([http://www.prostoweb.com.ua/internet\\_marketing/sotsialnye\\_seti/novosti/facebook\\_rasshiril\\_instrumentariy\\_nativnoy\\_reklamy\\_v\\_audience\\_network](http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_rasshiril_instrumentariy_nativnoy_reklamy_v_audience_network)). – 2015. – 14.05*).

\*\*\*

Компания Pinterest совместно с маркетинговой консалтинговой фирмой MillwardBrown провела исследование, опросив 2001 активных и неактивных пользователей Pinterest по электронной почте между 20 февраля и 7 марта, пишет Marketing Media Review (<http://mmr.ua/news/id/52-polzovatelej-pinterest-pokupajut-blagodarja-servisu-44324/>).

Около 24 % респондентов назвали себя неактивными пользователями – это те, кто не пользовался сервисом в течение шести месяцев. Опрос остальных 1500 активных пользователей позволил выявить целый ряд интересных маркетинговых фактов:

Примерно 52 % респондентов сообщили, что веб-ресурс помогает им найти товары, которые они хотят купить.

Более 60 % опрошенных отнесли себя к «мамам Миллениума».

Чуть менее 50 % участников опроса отметили, что Pinterest рекомендует к покупке релевантные товары.

30 % респондентов заявили, что они совершили покупку в Интернете благодаря сервису Pinterest.

32 % приобрели товары офлайн после просмотра контента Pinterest.

Почти 80 % активных пользователей ответили, что контент Pinterest о еде и рецептах помог им решить, что купить.

60 % респондентов совершили покупку благодаря контенту по домашнему декору.

Около 25 % активных пользователей Pinterest не совершали никаких действий: не покупали и не посещали сайт бренда, ритейлера или медиа.

«Целью исследования было достижение глубокого понимания того, что делают наши пользователи и как они используют платформу», – прокомментировала глава Pinterest по маркетинговым коммуникациям Е. Смит.

Социальный сервис Pinterest активно работает над вовлечением пользователей мужского пола, но данное исследование в очередной раз показало, что на сайте по-прежнему преобладают пользователи женского пола. Так, «Мамы Миллениума» лидируют почти во всех категориях, в которых Pinterest помог им принять решение о покупке: мода, домашний декор, питание и рецепты, здоровье, фитнес, волосы и красота. «Папы Миллениума» берут реванш в решениях о покупке в категориях здравоохранения и фитнеса.

Результаты опроса подтверждают, что Pinterest успешно развивает рекламное направление бизнеса. Ожидается, что сервис Pinterest последует по стопам Facebook и Twitter и добавит на страницы ресурса кнопку «купить» (52 % пользователей Pinterest покупают благодаря сервису // *Marketing Media Review* (<http://mmr.ua/news/id/52-polzovatelej-pinterest-pokupajut-blagodarja-servisu-44324/>). – 2015. – 14.05).

\*\*\*

Общая вовлеченность ведущих мировых брендов в Facebook за последний год возросла на 43,5 %, сообщила аналитическая компания Simply Measured в своем Facebook 2015 Industry Report, который основывается на данных о 100 крупнейших компаниях по версии Interbrand. И это несмотря на то, что бренды делали на 5 % меньше постов в последние три месяца по сравнению с аналогичным периодом 2014 г., пишет Marketing Media Review (<http://mmr.ua/news/id/vovlechennost-brendov-v-facebook-za-poslednij-god-vyroslana-435-44339>).

Компании уменьшили количество постов на 12 %, начиная с IV квартала 2014 г., и общий уровень вовлеченности снизился за 0,11 %. По мнению авторов исследования, это связано с тем, что компании сосредоточились на качестве постов, а не зоне охвата.

А вот вовлеченность на пост возросла примерно на 53 % за год (в исследовании учитывались как платные, так и бесплатные публикации).

Исследование 11 522 постов 96 компаний из рейтинга Interbrand 100 показало, что ссылки и фотографии производят наибольшую вовлеченность, хотя видео, конечно, тоже значимый фактор.

По сравнению с IV кварталом 2014 г. вовлеченность видео в Facebook увеличилась на 8 %. Этот рост во многом объясняется тем, что количество расшариваний брендовых видео увеличилось на 43 %. Похожая ситуация с фотографиями, вовлеченность которых возросла на 6 % за счет 53-процентного увеличения числа расшариваний.

Бренды чувствуют эту тенденцию и реагируют на нее, размещая все больше видео. Хотя делают они это достаточно сдержанно. Рост публикаций видео среди 100 крупнейших брендов по версии Interbrand составил всего 2 %.

Но это относится не ко всем брендам. Например, Adidas разместил 13 видео за I квартал 2015 г. (в IV квартале 2014 г. их было всего семь), чем заработал на 1,487 % больше комментариев, на 9,398 % больше лайков и на 9,041 % больше расшариваний. Видео бренда с наибольшей вовлеченностью на данный момент получило более 17 млн просмотров, почти 600 тыс. лайков и 26 тыс. расшариваний.

И еще несколько интересных фактов:

Вовлеченность статусов упала на 72 % в I квартале 2015 г., так как бренды стали размещать на 40 % меньше таких обновлений.

Количество лайков на страницах снизилось на 3 %, что, вероятно, является последствием мартовского удаления неактивных аккаунтов из Facebook (*Вовлеченность брендов в Facebook за последний год выросла на 43,5 % // Marketing Media Review (<http://mmr.ua/news/id/vovlechennost-brendov-v-facebook-za-poslednij-god-vyrosla-na-435-44339/>). – 2015. – 14.05*).

\*\*\*

Twitter обновила дизайн продвигаемых твитов, убрав желтый бейдж. Это было сделано для того, чтобы сделать их максимально похожими на обычные твиты.

Фиолетовый бейдж в политических продвигаемых твитах удаляться не будет, а желтые бейджи будут означать продвигаемые тренды и аккаунты.

Теперь дизайн продвигаемых твитов максимально согласован с другими социальными сетями, включая Pinterest, LinkedIn и Facebook (*Twitter изменил дизайн продвигаемых твитов // ProstoWeb ([http://www.prostoweb.com.ua/internet\\_marketing/sotsialnye\\_seti/novosti/twitter\\_izmenil\\_dizayn\\_prodvigaemyh\\_tvitov](http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_izmenil_dizayn_prodvigaemyh_tvitov)). – 2015. – 15.05*).

\*\*\*

Twitter поделилась статистикой потребления видео в рамках социальной сети, пишет searchengines.ru.

Данные компании основаны на исследованиях, проведённых по 14 странам мира, в ходе которых было опрошено более 1 тыс. пользователей Twitter. При этом выборки респондентов были составлены таким образом, чтобы отразить демографический профиль каждой страны. В основу отчёта компании легли данные по США, отражающие общую ситуацию.

Как показали результаты исследования, видеоролики в Twitter просматривает большинство пользователей сервиса (82 %), при этом бóльшая часть просмотров осуществляется с мобильных устройств.

«90 % просмотров видео в Twitter происходит с мобильных устройств. Кроме того, пользователи сервиса микроблогов в 1,9 раза более склонны загрузить видео онлайн, чем средний интернет-пользователь в США», – заявил представитель компании М. Тейлор.

По данным опроса, пользователи предпочитают смотреть следующие виды видеоконтента:

новости – 64 %;

видео из прямых трансляций спортивных мероприятий – 54 %;

фрагменты телешоу – 50 %;

видео знаменитостей – 45 %;

видео других пользователей – 40 %;

видео брендов – 37 %.

70 % респондентов ответили, что они преимущественно или по большей части смотрят те видеоролики, которые появляются в хронике. Только 11 % опрошенных пользователей используют поиск в Twitter, чтобы найти конкретные видео.

Возможно, эта ситуация изменится после того, как Twitter внедрит улучшенный поисковый интерфейс, который в настоящее время проходит тестирование.

По данным компании, нативное видео в Twitter вызывает бóльшую вовлечённость, чем сторонние видео, которыми делятся пользователи сервиса. Этот показатель включает в 2,5 раза больше комментариев; в 2,8 раза больше ретвитов и в 1,9 раза больше занесений в «Избранное».

«Наши рекламодатели также видят, что продвигаемое видео в Twitter демонстрирует высокие показатели вовлечённости», – отметил представитель компании.

Напомним, что недавнее исследование от Interactive Advertising Bureau выявило, что 68 % маркетологов и руководителей агентств ожидают увеличения рекламных бюджетов на онлайн-видео в течение следующего года (*90 % просмотров видео в Twitter происходит с мобильных устройств // МедиаБизнес* (<http://www.mediabusiness.com.ua/content/view/43422/118/lang,ru/>). – 2015. – 18.05).



\*\*\*

Net Set – социальная сеть для покупок

Net-a-Porter, крупнейший онлайн-ритейлер, решил запустить собственный социальный проект. Основная идея – возможность покупок, с последующей демонстрацией приобретенных товаров многочисленным друзьям и подписчикам.

Net Set ориентирована на мобильные устройства. Именно мобильная аудитория, по мнению разработчиков, обязана в большей степени оценить возможность рекомендовать товары друг другу, делиться мнениями о покупках, показывать фотографии и, конечно же, приобретать что-либо через сеть.

Плюсом проекта станет и обратная связь – именно об этом говорится в пресс-релизе. Выгоду получают не только пользователи, выбирающие продукцию более чем 300 брендов, но и владельцы, которые смогут пообщаться со своими «почитателями», узнать мнение о продукции, взять на вооружение дельные советы.

«Мы уверены, что Net Set ждет невероятный успех – для того есть все предпосылки», – заявила Н. Массене, основатель сайта. – У нас имеется определенная база людей. На наш сайт, Net-a-Porter, ежедневно заходят 300 тыс. человек. Они же и станут нашими первыми пользователями. В крупнейших социальных сетях на нашу страницу в общей сложности подписано около 4 млн людей. Они тоже заинтересуются Net Set».

Как именно через социальную сеть можно будет покупать товары, пока что не уточняется, как не уточняется, в каких странах она будет доступной (*Net Set – социальная сеть для покупок // ProstoWeb ([http://www.prostoweb.com.ua/internet\\_marketing/sotsialnye\\_seti/novosti/net\\_set\\_sotsialnaya\\_set\\_dlya\\_pokupok](http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/net_set_sotsialnaya_set_dlya_pokupok)). – 2015. – 18.05*).

\*\*\*

Социальный сервис веб-закладок Pinterest сообщил о внедрении ряда новых рекламных опций, среди которых анимационный продвигаемый пин или Cinematic Pins, пишет Marketing Media Review (<http://mmr.ua/news/id/pinterest-zapustil-animacionnye-reklamnye-piny-44404/>).

Представители компании считают, что пины с внедрением анимации будут привлекать больше качественного вовлечения, не раздражая пользователей, а значит это отличная альтернатива навязчивому формату видеорекламы.

Тестирование новой опции происходило с привлечением широкого круга аудитории, опираясь на полученные отзывы и были созданы Cinematic Pins. Анимационные пины активируются при скроллинге страницы и становятся неподвижны при прекращении прокрутки. При клике на изображение пользователь ознакомится с полной версией анимационного трека.

Представители социального сервиса также сообщили о планируемом запуске новой формы специфического таргетинга по интересам пользователей

и внедрении ценовой модели, основывающейся на показатели вовлеченности (*Pinterest запустил анимационные рекламные пины // Marketing Media Review (http://mmr.ua/news/id/pinterest-zapustil-animacionnye-reklamnye-piny-44404/).* – 2015. – 20.05).

\*\*\*

Facebook видит возможности для брендов общаться с потребителями через WhatsApp

Выступая на глобальной конференции по технологиям, медиа и телекому, организованной J. P. Morgan, CFO Facebook, Д. Вехнер отметил, что социальная сеть в настоящее время экспериментирует с Messenger, чтобы позволить брендам контактировать с потребителями, пишет Marketing Media Review (<http://mmr.ua/news/id/facebook-vidit-vozmozhnosti-dlja-brendov-obschatsja-s-potrebiteljami-cherez-whatsapp-44403/>).

Компании тестируют мессенджер в качестве сервиса для обслуживания клиентов, возможности для пользователей обращаться напрямую к брендам и совершать онлайн-заказы.

Д. Вехнер также отметил, что видит возможности в добавление такой услуги и для WhatsApp.

Тем не менее, бренды уже начали экспериментировать с платформой. Clarks ранее в этом году запустил кампанию, которая призывала пользователей добавить новый мобильный номер к WhatsApp после просмотра тизерных видео в социальных медиа. В результате кампании бренд получил уникальные фото, видео и сообщения с номеров.

Facebook также фокусируется на том, чтобы стать синонимом слову «мобильное видео» и работать с брендами над тем, как они могут создавать контент для сайтов.

Вице-президент по маркетинговым решениям К. Эверстен отметила, что брендам необходимо начать думать о том, как создавать именно мобильные видео и более короткий контент для сайтов социальных медиа.

Она отметила, что 47 % ценности мобильных видео создаются в первые три секунды и 74 % в последние 10 секунд.

«Мы видим, что компании начинают задумываться над развитием креатива специально для мобильных видео. Поэтому более короткий формат видео – это возможность, над которой они работают. Кроме того, видео можно потреблять в зависимости от времени дня и окружения с выключенным звуком и брендам необходимо понять, как создавать видео, которые могут доносить сообщение и без звука» (*Facebook видит возможности для брендов общаться с потребителями через WhatsApp // Marketing Media Review (http://mmr.ua/news/id/facebook-vidit-vozmozhnosti-dlja-brendov-obschatsja-s-potrebiteljami-cherez-whatsapp-44403/).* – 2015. – 20.05).

\*\*\*

Восемь советов, как продавать через социальные сети

Если вы работаете с социальными сетями и бываете на встречах у клиента, наверняка в топе наиболее задаваемых вопросов есть «Как быстро мы начнем продавать?», «Как вы планируете продавать мой товар?» и т. д. Компания Seomarket ответила на ключевые вопросы по этой теме, пишет Marketing Media Review (<http://mmr.ua/news/id/8-sovetov-kak-prodavat-cherez-socialnye-seti-44412/>).

Что и в каких социальных сетях можно продать?

SMM, или маркетинг в социальных сетях в настоящее время у всех на слуху. Все понимают, что продвигать компанию в социальных сетях нужно. Но вот как правильно это делать? А, точнее, как продавать товары в соцсетях? Попробуем ответить на самые распространенные вопросы в этом ключе.

Начнем с краткой статистики. Специалисты из GfK Ukraine проанализировали, что, где и как часто украинцы покупают в Интернете. Оказалось, что в прошлом году более 39 % интернет-покупателей заказывали товары и услуги через социальные сети. Для сравнения, в 2013 г. этот показатель равнялся 12 %.

Товары, которые украинцы чаще всего покупают в Интернете – это одежда, аксессуары, подарки, обувь, косметика и парфюмерия. Не трудно сделать выводы и понять, что, преимущественно, покупателями социальных сетей является прекрасная половина человечества.

Эта информация наталкивает на мысли, что идти в социальные сети стоит и о том, что они продают. Но как это правильно сделать?

Что нужно делать для того, чтобы товары продавались через социальные сети?

Для того, чтобы у вас были продажи через социальные сети, необходимо выдержать такие основные условия:

- аудитория вашей компании совпадает с аудиторией социальной сети;
- отсутствуют барьеры для покупки вашего товара через соцсеть (в виде дополнительных регистраций, не оперативной обработки запросов и т. д.);
- вы инвестировали в ваше сообщество: наполнили его информацией, контентом, наработали аудиторию и вышли на средний/высокий уровень вовлечения;
- вы достигли высокого уровня доверия (путем качественной работы с обратной связью);
- вы понимаете, что для того, чтобы продавать в Интернете, необходимо время (минимум три месяца).

Если вы готовы поставить уверенные плюсики напротив каждого пункта – поздравляем! Вы на правильном пути, и вот теперь мы поделимся с вами некоторыми хитростями, которые помогут вам эффективно продавать ваш товар.

1. Указывать актуальную цену товара

Зачем строить лишний барьер на пути к покупке? Вы боитесь отпугнуть покупателей ценой, хотите, чтобы у них сначала родилось желание купить и только потом выдавать цену? Будьте уверены – те, кому будет неприятно

цена вашего товара – уйдут от вас после того, как узнают ее из личного сообщения. Так зачем тратить на них лишнее время?

## 2. Максимально упростить процедуру заказа

Если вы представляете интернет-магазин, позаботьтесь о том, чтобы ваш товар можно было приобрести максимально простым путем – без перехода на сайт, регистраций и кучи других ненужных процедур. Очень часто именно они являются причиной отказа от покупки. Покупка сразу под постом, или в личные сообщения – простой и понятный клиенту путь, который повышает шансы на то, что товар будет приобретен.

## 3. Постоянно обновлять ассортимент, предоставить пользователю большой выбор

Почему женщины (которые чаще всего покупают в Интернете) так любят шоппинг? Потому что им нравится часами ходить по магазинам, выбирать и осознавать, что одна из этих вещей рано или поздно станет их собственностью. То же и в соцсетях – предоставьте клиентам выбор. Дайте им возможность побродить по альбомам, посмотреть, проанализировать и купить. Кроме того, большой ассортимент ведет к удовлетворению потребностей большего числа клиентов.

Также следите за актуальностью товара. Создайте альбом «Есть в наличии». Часто причиной отказа от покупок является долгое время ожидания товара либо вообще его отсутствие (при том, что в альбоме/на сайте он есть).

## 4. Следить за трендами и обыгрывать их

Ни для кого уже не секрет, что именно на трендах можно заработать быстро и много. Следите за тем, о чем люди говорят в Интернете, что происходит вокруг, что им интересно – и применяйте это к вашему товару. Трендовые вещи всегда более популярны, чем стандартный ассортимент

## 5. Постоянно обновлять информацию сообщества

Покажите своим клиентам, что у вас хороший поток, товары обновляются – людям нравится то, что вы продаете и то, что вы делаете. Но не переусердствуйте, чтобы вас не забанили в новостной ленте. Какая главная цель таких действий? Вы постоянно мелькаете в поле зрения потенциального покупателя, и когда у пользователя возникает потребность в вашем товаре, угадайте, кого он вспоминает первого? Да, вы правильно догадались.

## 6. Оперативно реагировать на комментарии

Оперативная реакция равно более высокая вероятность совершения покупки. Пока вы долго будете отвечать на вопросы от пользователей – они могут купить продукцию у ваших конкурентов.

## 7. Комьюнити менеджмент

Комьюнити менеджмент – практически самая важная составляющая в работе с вашим сообществом. С его помощью вы формируете доверительные отношения с пользователями, которые могут конвертироваться в ваших клиентов. Что для этого нужно? Давать публичные ответы на негатив, ни в коем случае не удалять его и, если необходимо, публично признать свои ошибки. Также старайтесь собирать фидбек от ваших довольных клиентов.

Это повысит лояльность аудитории, которая в будущем сможет рекомендовать ваш магазин друзьям. Главное – чтобы отзывы были правдивыми и настоящими. Фейковые отзывы будут работать против вас.

#### 8. Рекламу давать на интересные предложения, скидки

Если вы планируете давать рекламу, всегда говорите о ваших скидках, интересных предложениях. Реклама работает эффективнее, и вы получите больше, больше продаж (*8 советов, как продавать через социальные сети // Marketing Media Review (http://mmr.ua/news/id/8-sovetov-kak-prodavat-cherez-socialnye-seti-44412/). – 2015. – 21.05).*

\*\*\*

#### Как отследить конверсии через социальные сети?

Если вы ведете комплексные маркетинговые компании, которые состоят из нескольких инструментов продвижения, отследить конверсии через социальные сети не всегда просто. Бывает так, что социальные сети являются одной из причин, которые ведут к продажам, сообщают специалисты Seomarket. Такие конверсии называются ассоциированными, пишет Marketing Media Review (<http://mmr.ua/news/id/kak-otsledit-konversii-cherez-socialnye-seti-44421/>).

Есть несколько вариантов, как можно отследить конверсии через соцсети, в том числе ассоциированные:

#### Кнопки Call-to-Action на Facebook

Самый простой способ отследить конверсию из социальной сети. Можно промаркировать ссылку и с помощью Google Analytics отслеживать переходы и конверсии. Надеемся, остальные социальные сети в ближайшем будущем также придумают подобную навигацию.

#### Промокоды

Промокод – неплохой способ посчитать конверсии из социальных сетей и привлечь заинтересованную аудиторию в сообщество.

#### Как это работает?

Вариантов, как воплотить эту идею – множество. Один из них – генератор уникальных промокодов для участников сообщества. К примеру, введите в ваш контент-план рубрику, которая будет выходить, допустим, по четвергам «50 промокодов для покупки определенной категории товара» и анонсируйте ее. Не забудьте, что скидки доступны только для участников сообщества. Со временем пользователи привыкнут к тому, что каждый четверг вы выдаете участникам сообщества уникальные коды, который дают право на скидку при покупке товара определенной категории. Таким образом, и волки сыты, и овцы целы. Вы создаете реальную мотивацию для того, чтобы люди присоединялись к вам, и, одновременно с этим, можете отслеживать конверсии из социальных сетей.

#### Приложения

Во многих социальных сетях есть возможность добавления приложений. Они бывают самые разные и в этом их прелесть.

- Как можно использовать приложения, если мы говорим о продажах в социальных сетях?
- Скидки, бонусы за совершение каких-то действий (ответы на вопросы – сбор статистических данных)
- Скидки, бонусы за победу в брендированных играх (отстраиваем знание бренда)
- Скидки, бонусы за вирусное распространение какой-либо информации из приложения (охват)
- Скидки, бонусы за вступления в сообщества компании в других соцсетях, которые фиксирует приложение
- Скидки, бонусы за активность в сообществе (которые фиксирует приложение)

В общем, вариантов – масса. Стоит добавить, что так называемая «геймификация» (т. е. всевозможные игровые активности с помощью приложений в том числе) не только приносит измеряемые результаты (количество участников, конверсии, повышение вовлечения и т. д.), но и довольно интересна для аудитории социальных сетей.

#### Программы лояльности

Вариантов программ лояльности, как и приложений, существует масса. Суть таких программ – награждать бонусами тех клиентов/участников сообщества/подписчиков, которые находятся с вами уже долгое время. Один из вариантов – разработать приложение, которое будет фиксировать (после того, как участник в нем регистрируется), сколько времени пользователь является участником группы. Самым преданным – дарить скидки.

Эти советы помогут вам понять, как лучше продавать в социальных сетях. Есть вопросы по этой теме или о чём-либо связанным с SMM – оставляйте их в комментариях (*Как отследить конверсии через социальные сети? // Marketing Media Review (<http://mmr.ua/news/id/kak-otsledit-konversii-cherez-socialnye-seti-44421/>). – 2015. – 21.05*).

\*\*\*

Кампании Twitter на основе целей стали доступны для всех рекламодателей в мире.

Программа предусматривает шесть доступных целей: вовлеченность в твит, клики или конверсии, установка приложения или вовлеченность, подписчики, просмотры видео.

Бета-версия кампаний на основе целей доступна предприятиям малого и среднего бизнеса, а также рекламным API партнерам. Новинка призвана помочь им сосредоточиться на конкретных целях: например, увеличении количества подписчиков, кликов или установок приложения. Рекламодатели, использующие функцию, будут платить только за тот вид вовлеченности, который они выбрали. Например, если рекламодатель работает над привлечением кликов на сайт, все ретвиты или занесения в избранное будут бесплатны.

Использование таких кампаний повышает эффективность рекламы в Twitter и приводит к лучшим результатам при меньших затратах.

В августе прошлого года Twitter усовершенствовал свои рекламные продукты, давая некоторым рекламодателям возможность платить только за выбранный вид вовлеченности (*Реклама Twitter на основе целей стала доступна всем рекламодателям // Состав.ру (<http://sostav.ua/publication/reklama-twitter-na-osnove-tselej-stala-dostupna-vsem-reklamodatelyam-66863.html>). – 2015. – 21.05*).

\*\*\*

Пользователи YouTube получают возможность покупать товары, кликнув по ссылке в рекламном ролике, сообщает газета The Financial Times, пишет Media Review (<http://mmr.ua/news/id/youtube-pozvolit-pokupat-tovary-po-ssylke-v-reklame-44442>).

Рекламодатели смогут размещать ссылку на конкретные товары, совмещая продвижение бренда с предложением, нацеленным на конкретного потребителя.

«Потребители пользуются YouTube, чтобы развлечься и получить информацию. Очень много запросов на тему “как пользоваться” тем или иным продуктом. Пользователь по-настоящему заинтересован, что, с точки зрения рекламодателя – идеальный момент, чтобы донести до него информацию», – заявил вице-президент Google (*YouTube позволит покупать товары по ссылке в рекламе // Marketing Media Review (<http://mmr.ua/news/id/youtube-pozvolit-pokupat-tovary-po-ssylke-v-reklame-44442>). – 2015. – 22.05*).

\*\*\*

Компания Scale Model, специализирующаяся на моделировании сообществ в социальных сетях для маркетинговых нужд, предлагает рекламодателям в Twitter опыт самого точного таргетинга, который они когда-либо получали, пишет Marketing Media Review (<http://mmr.ua/news/id/brendam-stal-dostupen-novyj-targeting-v-tvittere-44429/>).

Сервис способен выделять сообщества в микроблоговой соцсети по принципу интересов, отслеживать, каким контентом делятся их участники и, в конечном счете, предоставлять маркетологам данные для таргетинга.

Инструментарий Twitter Ads уже позволяет строить кампании на основе ключевых фраз, географии, пола, местоположения пользователей и т. д. Однако Scale Model делает акцент на высоком качестве анализа ключевиков, контента и хештегов в каждом конкретном сообществе.

Особенность сервиса в том, что он умеет определять, когда группы людей по интересам, например, «Технологические стартапы» образуются из нескольких подгрупп, в данном случае, это могут быть журналисты, предприниматели, выпускники профильных ВУЗов и т. п. Scale Model понимает, как они взаимодействуют друг с другом, и умеет вычленять

специфические интересы каждой. Таким образом, технология может позволить брендам коммуницировать с наиболее точно выделенной аудиторией.

В настоящее время сервис предлагает рекламодателям шесть публичных моделей Twitter-сообществ, на аудиторию которых они могут таргетировать с помощью интеграции Scale Model и Twitter Advertising API: 2016 Elections, «Любители животных», «Изменение климата», «Путешествия», «ТВ-культура» и «Политика США». Каждая из этих групп распадается на меньшие подгруппы, например, «Политика США» включает «Медиа», «Прогрессивных» и «Консервативных», в то время как «Любители животных» содержат в себе одновременно аудитории заводчиков собак и кошек.

Представители компании поясняют, что время моделирования зависит от сложности и размера сообщества (*Брендам стал доступен новый таргетинг в Твиттере // Marketing Media Review (<http://mmr.ua/news/id/brendam-stal-dostupen-novuj-targeting-v-tvittere-44429/>). – 2015. – 21.05*).

\*\*\*

Facebook добавила кнопку «Позвонить сейчас» в локальные объявления

При нажатии на кнопку «Позвонить сейчас» телефон автоматически набирает номер рекламодателя, чтобы пользователь мог узнать интересующую его информацию или сделать предварительный заказ.

В настоящее время кнопка «Позвонить сейчас» доступна только в США. Остается надеяться, что если она докажет свою эффективность там, то со временем появится и в арсенале рекламодателей других стран.

Новая кнопка дополняет кнопку «Проложить маршрут», которая была частично запущена в локальных объявлениях в прошлом октябре (*Facebook добавил кнопку «Позвонить сейчас» в локальные объявления // ProstoWeb ([http://www.prostoweb.com.ua/internet\\_marketing/sotsialnye\\_seti/novosti/facebook\\_dobavil\\_knopku\\_pozvonit\\_seychas\\_v\\_lokalnye\\_obyavleniya](http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_dobavil_knopku_pozvonit_seychas_v_lokalnye_obyavleniya)). – 2015. – 21.05*).

\*\*\*

Настройка и оптимизация рекламных кампаний во «ВКонтакте»

Высокая популярность социальных сетей среди пользователей Интернета легко объясняется тем, что площадки предоставляют неограниченные возможности для общения, поиска знакомых и интересной информации. По данным TNS, среднестатистический пользователь Интернета около четверти от всего времени в сети проводит в социальных сетях. Такой факт не может остаться незамеченным маркетологами и специалистами по рекламе: сегодня более 75 % рекламодателей используют социальные сети в качестве рекламного канала.

Если говорить про отрасли, то это, прежде всего, e-commerce – 17 %, развлечения – 12 %, финансовые услуги – 11 %, красота и здоровье – 9 %, телеком – 8 %, на прочие отрасли приходится около 44 %.

Неудивительно, что с ростом внимания к социальным сетям развиваются рекламные возможности площадки. В социальных сетях, в частности во



«ВКонтакте», используя тонкие настройки, можно четко определить целевую аудиторию и таргетировать на нее рекламные объявления. Причем работать с пользователями социальных сетей вы можете на каждом этапе воронки продаж:

- Формирование спроса. Можно использовать настройки таргетирования по тематическим интересам, гео, пол, возраст и т. д.
- Увеличение продаж. В данном случае можно работать с аудиторией, которая уже была у вас на сайте, используя ремаркетинг.
- Повторная коммуникация с клиентами. Чтобы напомнить о себе пользователям, совершившим покупку на вашем сайте, можно загрузить базу контактов на площадку и таргетировать на них рекламные сообщения.

Важно помнить, что на каждом этапе воронки конкуренция увеличивается, и нужно быть готовым к борьбе за каждого пользователя, идущего по воронке продаж. А теперь несколько советов, которые помогут не только довести пользователя до конверсии, но и позволят эффективно управлять рекламными кампаниями и последующей оптимизацией для снижения CPA.

#### Шаг 1: Сегментируем целевую аудиторию

При создании любой рекламной кампании необходимо делать сегментацию целевой аудитории. Основными параметрами сегментации являются пол, возраст и гео. При этом главным вопросом остается, как правильно сгруппировать аудиторию без потери трафика и эффективности рекламных кампаний.

##### По возрасту

Учитывая специфику социальной сети «ВКонтакте», лучше делить аудиторию на возрастные группы по 5–8 лет. При данном сегментировании количество трафика и CPC находятся в оптимальных пропорциях. Деление аудитории по возрасту, например, по 1–2 года, может привести к высоким ценам за клик и малому трафику.

##### По полу

Разделение по кампаниям на мужчин и женщин в первую очередь зависит от рекламируемого товара. Если речь идет сугубо о женских товарах/услугах, то мужчин можно смело исключать и не тратить на них время и рекламный бюджет. Но в наше время всё больше становится областей, где женщины проявляют покупательскую активность, например, автобизнес или бытовая техника. В данном случае сегментация обязательна.

##### По гео

Есть несколько особенностей и для гео-настроек. Например, если вы используете таргетинг на всю страну, то крупные города лучше выносить в отдельные кампании. Плюс «ВКонтакте» позволяет таргетировать объявления на конкретные районы, улицы и станции метро, что в отдельных случаях значительно повышает эффективность рекламных кампаний. Например, такой таргетинг хорошо работает, если вы рекламируете кафе или пункт выдачи вашего интернет-магазина.

##### По интересам и поведенческому таргетингу

Помимо сегментации по социально-демографическим признакам пробуйте разные настройки по интересам и по поведенческому таргетингу, опираясь на тематику и околотематику рекламируемой продукции. Также не забывайте выделять кампании с настройками на мобильный трафик (смартфоны и планшеты).

Важно помнить, что все вышеперечисленные сегментации необходимо комбинировать между собой и находить оптимальный вариант для вас. На начальном этапе не рекомендуется использовать деление по соц-дему без использования интересов, потому как ещё не известна ваша целевая аудитория и есть большой риск неэффективного расхода бюджета.

Помните, чем больше целей вы преследуете, тем детальнее нужно разбивать аудиторию. При создании нескольких кампаний с настройками на широкую аудиторию полученный трафик будет сложно анализировать, и, как следствие, в дальнейшем такие кампании практически невозможно оптимизировать.

Для удобства структурирования большого количества рекламных объявлений во «ВКонтакте» вы можете создавать в одной рекламной кампании объявления с индивидуальными настройками.

#### Шаг 2: Устанавливаем код ремаркетинга

Во «ВКонтакте», как и в других социальных сетях, есть возможность таргетирования на пользователей, которые посещали вашу страницу, – ремаркетинг. Такой инструмент позволяет увеличить CTR в три раза и повысить конверсию до 2,5 раз, при этом CPO уменьшается в 2–3 раза.

При этом важно помнить, что код ремаркетинга для «ВКонтакте» должен быть индивидуальным для каждой страницы сайта. Недостаточно установить только один код на главную страницу, коды необходимо устанавливать на каждый раздел сайта, не говоря уже о тех, кто добавил товар в корзину и тех, кто совершил заказ. Это даёт возможность для разнообразных комбинаций таргетинга и создания релевантных креативов под каждую из них.

Предположим, у вас интернет-магазин продуктов, где появился новый йогурт. Установив коды на каждую категорию товаров, вы сможете настроить рекламную кампанию данного йогурта следующим образом: показывать её всем пользователям, которые посещали страничку молочной продукции, или тем, кто просто совершал у вас покупку. Дополнительно можно попробовать таргетинг на аудиторию посетителей, которые добавляли товары (любые) в корзину, но ещё не сделали заказ.

Теперь, когда вы сегментировали аудиторию, подготовительный этап можно считать завершённым. При этом важно помнить, если у вас получилось большое количество рекламных кампаний, то лучше воспользоваться системами автоматизации, поскольку на ручное управление и оптимизацию рекламных кампаний в таком случае будет уходить очень много времени. К счастью, на рынке много решений по автоматизации кампаний, и вы можете выбрать оптимальную систему, которая будет учитывать особенности бизнеса (например, Plarin, Adtrack, Control).

### Шаг 3: Запускаем кампании и собираем статистику

Настал момент, когда вы запустились, пошел трафик, стала накапливаться статистика. И сразу возникают вопросы: когда можно начинать оптимизировать рекламные кампании и какой рекламный бюджет выделить на тестирование? Универсального ответа нет, все зависит от отрасли, бюджета и объема рекламной кампании. В любом случае, если вы начинаете с нуля, то будьте готовы выделить до 30 % бюджета на тестирование и сбор статистики.

Отдельно нужно учитывать, что трафик на площадке «ВКонтакте» в течение суток распределяется неравномерно, а ускоренно (показ объявлений с максимальной обоснованной частотой). Равномерности можно добиться только при нахождении оптимальной ставки. Если ставка окажется завышенной, то бюджет растрагится моментально, а если заниженной – трафик будет низким. Для выбора оптимальной ставки после запуска рекламной кампании уделите мониторингу 20–30 минут.

Часто во «ВКонтакте» наблюдается ситуация, когда внутри одной кампании весь трафик на себя перетягивает объявления с лучшим CTR, а остальным просто не достаётся трафика. В такой ситуации можно остановить на некоторое время «лидеров» и дать возможность объявлениям, запоздавшим на старте проявить себя.

### Шаг 4: Оптимизируем рекламные кампании

Пользуясь Google Analytics и Яндекс.Метрикой, вы сможете отслеживать, как качественные показатели (процент отказов, глубина просмотра и время на сайте), так и количество конверсий с каждого из объявлений. Разберёмся на примере туроператора:

- аудитория возрастом от 18–24 имеют большой процент отказов (от 70 %);
- несколько заказов принесла аудитория женщин возрастом 45+;
- аудитория «Путешеств\_25–32» имеет дорогой клик и средние качественные показатели.

Смело отключаем кампании с возрастом 18–24 лет, аудиторию «жен\_45+» дополнительно сегментируем по возрастам: 45–54, 55–64 и 64+, а в аудитории с большой стоимостью клика смотрим на каждое из объявлений. Объявление с лучшим CTR имеет меньшую стоимость клика, поэтому его оставляем, а другие рекламные сообщения останавливаем. В противном случае, они будут конкурировать с нашими же объявлениями. На этом первый этап оптимизации можно завершить. Даём время покрутиться объявлениям, собрать больше конверсий и переходим ко второму этапу оптимизации.

На втором этапе можно работать с креативом, при этом не забывайте про последующую сегментацию. Пользователи социальных сетей в среднем за несколько секунд принимают решение кликнуть на объявление или нет. Поэтому ваш креатив должен быть максимально понятным, красивым и зазывающим. Смотрите на самые кликабельные сообщения, пробуйте делать цветные рамки, тестировать рисованные креативы или, например,

анимированные изображения (.gif), а также экспериментировать с форматами площадки «ВКонтакте».

Когда вы определились с лучшими креативами и разбили вашу целевую аудиторию на нужные сегменты, можно переходить на третий этап оптимизации – снижение CPC и CPA. Удобнее всего это делать с помощью автоматизированных систем, задав процентное соотношение CPC от рекомендуемой ставки. Кроме того, системы позволяют настроить расписание показов в течение дня. Если же вручную, то постепенно снижайте CPC (примерно по 50 коп.) на объявлениях с хорошим CTR.

Следуя этим советам, вы можете значительно повысить эффективность ваших рекламных кампаний в социальных сетях и добиться нужного результата (*Настройка и оптимизация рекламных кампаний во «ВКонтакте» // ProstoWeb*

([http://www.prostoweb.com.ua/internet\\_marketing/sotsialnye\\_seti/stati/nastroyka\\_i\\_optimizatsiya\\_reklamnyh\\_kampaniy\\_vo\\_vkontakte](http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/stati/nastroyka_i_optimizatsiya_reklamnyh_kampaniy_vo_vkontakte)). – 2015. – 22.05).

## **СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ**

### **Інформаційно-психологічний вплив мережевого спілкування на особистість**

Насколько опасна зависимость от смартфонов и как от нее избавиться

В Мельбурне несколько лет назад произошел любопытный случай. Засмотревшаяся в свой смартфон туристка упала с пристани и провела в воде почти полчаса, пока не подоспели спасатели. В документации они указали, что даже находясь в воде, женщина не расставалась со своим гаджетом.

Этот случай иллюстрирует крайнюю степень привязанности или зависимости от мобильных устройств, потому такие происшествия на самом деле не так уж и часты. Тем не менее сложно отрицать тот факт, что мы так или иначе зависим от разного рода девайсов. Иногда мы уделяем им слишком много времени, отодвигая в сторону бытовые заботы, работу, обучение и просто полноценный отдых. Практически каждому случалось в ответственные моменты, требующие концентрации внимания, отвлекаться на свой гаджет.

Писатель М. Оглес полагает, что мы на скорую руку адаптировавшись к мобильным устройствам, еще не в полной мере осознали все потенциальные последствия их использования. Он приводит интересный пример с автомобилями. Так, со времени создания авто, датированным 1886 г., до 1968 г. для водителей не были предусмотрены ремни безопасности. Было бы неразумным полагать, что и производители авто, и водители не знали о

потенциальных рисках вождения машины, особенно на высоких скоростях. Еще в начале XX в., когда авто были запущены в массовое производство, об этих рисках все отлично знали. Тем не менее на их осмысление и поиск способов предотвращения ушло более 80 лет.

Конечно, можно заявить, что сравнивать авто со смартфонами не корректно. И это отчасти верно. Пользуясь смартфонами мы лишь в исключительных случаях подвергаем риску свои жизни и жизни других людей. Тем не менее не стоит забывать о том, что широкое распространение гаджетов наблюдается лишь последние 10 лет. И каждый год разработчики развивают функциональность своих устройств, из-за чего пользователи все больше времени уделяют своим девайсам. Чем же это чревато в будущем?

На самом деле в настоящее время проводится много исследований, посвященных влиянию новых технологий (в том числе и смартфонов) и Интернета. Если отбросить фейковые заказные исследования, то в основном результаты исследований достаточно пессимистичны по отношению к результатам зависимости человека от новых технологий. Рассмотрим несколько таких исследований, а также приведем простые правила, которые позволят ограничить негативное влияние гаджетов на нашу жизнь.

#### Исследования

##### Техноференс

Техноференс – это термин, описывающий негативное воздействие технологий на романтические отношения между людьми. Чаще всего этот термин используют по отношению к смартфонам. В прошлом году эксперты провели исследование на влияние таких невинных с первого взгляда вещей, как просмотр во время разговора смсок или быстрые движения по экрану для проверки уведомлений, на эмоциональный фон партнеров. Оказалось, что существует определенная взаимосвязь между этими мелочами и депрессивными состояниями, конфликтами и прочими негативными психическими проявлениями.

##### Техношея

Второе любопытное и не менее грозное в выводах исследование свидетельствует о появлении нового заболевания у гаджетоманов – техношеи. Это аналог туннельного синдрома, но связанный с чрезмерной нагрузкой на спинные и шейные мышцы при постоянных наклонах головы для взгляда на смартфон. По заключению экспертов, данное заболевание в запущенных случаях может приводить к необходимости хирургического вмешательства. Стоит также вновь напомнить, что широкое распространение смартфоны получили меньше десяти лет назад. То ли еще будет.

##### PUMP

PUMP – это аббревиатура от Problematic Usage of Mobile Phones и по совместительству шкала негативного воздействия мобильных устройств на поведение пользователей. По последним заключениям, есть определенное сходство зависимости от гаджетов с зависимостью от различных наркотических

веществ. На данном этапе соответствующего диагноза нет, но специалисты обсуждают возможность его введения.

#### Решение проблемы

К сожалению, универсального способа устранения проблемы зависимости нет. Все обусловлено конкретными обстоятельствами, ведь стоит разделять людей, часть работы которых состоит в регулярном мониторинге информации с помощью разных гаджетов и простых юзеров, которые привыкли к своему устройству настолько, что для них оно является неотъемлемой частью жизни, хотя реальной пользы приносит куда меньше чем вреда.

#### Ограничить вмешательство смартфона в нашу жизнь

Ограничить можно отключив звуковые и визуальные оповещения. Допускается оставить только главные – SMS и звонки. Все остальные подождут. Если же вам требуется регулярно просматривать email ограничьтесь оповещением обычной иконкой. Тем не менее, даже если вы будете соблюдать это правило, рано или поздно вам захочется просто «пощелкать» смартфон от безделья. Чтобы избавиться от этой дурной привычки, или по крайней мере ограничить ее воздействие на свою жизнь, следуйте следующему правилу.

#### Выделить для гаджета свое место

Именно так. От скуки и ввиду того что ваш смартфон обычно всегда под рукой, вы сами того не осознавая, частенько проверяете его и бессмысленно серфите в ущерб своему времени. Прискорбно, но оно у вас не бесконечно. И можно найти занятия куда полезнее и интереснее для вас, чем пустое и бессмысленное использование вашего гаджета. А для того чтобы ограничить непродуктивное времяпровождение за девайсами, просто отведите им отдельное место. Пусть это будет отдельная полка или стол, а на работе – папка, сумка или рюкзак. Главное, чтобы гаджет не находился под рукой и не перетягивал на себя ваше внимание.

Данные правила вряд ли помогут вам без осознания того, зачем собственно вы собираетесь ограничить использование смартфона. Это обязательное условие, благодаря которому вы не только сможете свести к минимуму негативное воздействие гаджетов, но и расставить приоритеты в жизни. А она не настолько длинная, чтобы с этим затягивать (***Насколько опасна зависимость от смартфонов и как от нее избавиться // InternetUA (<http://internetua.com/naskolko-opasna-zavisimost-ot-smartfonov-i-kak-ot-nee-izbavitsya>). – 2015. – 12.05).***

\*\*\*

Отправка текстовых сообщений и вождение одновременно, возможно, наиболее опасная комбинация действий – и этот факт часто подтверждается статистикой.

#### Селфи за рулем

Несмотря на то что 1,3 млн автомобильных аварий в год случаются из-за использования сотового телефона, водители увеличили свое присутствие в

социальных сетях и СМИ в то время как они находятся за рулем, в соответствии с CBSNews.com.

Недавний опрос от компании AT&T показал, что 38 % водителей пользуются социальными медиа в то время как находятся на сиденье водителя.

С предписанными законами в 39 государствах, запрещающих использование сотовых телефонов, отправку sms-сообщений, двигаясь, должно было уменьшиться число отвлекающихся водителей, но использование социальных медиа за рулем укрепилось.

Смс за рулем

61 % из 2000 опрошенных американцев заявили, что они читали и/или отправляли текстовые сообщения в то время как были за рулем, в это же время еще 17 % признали, что они снимают селфи во время вождения.

«Большинство респондентов заявили, что они делают эти вещи по привычке – и утверждают, что они могут делать это одновременно безопасно», в соответствии со статьей.

AT&T также обнаружили, что 33 % людей могут общаться по электронной почте во время вождения, 28 % осуществляют навигацию в сети и 12 % захватили видео.

Опрос был проведен в рамках кампании AT&T It Can Wait, которая направлена на то, чтобы выделить опасности, отвлекающие от вождения (*Самая большая проблема на дорогах – социальные сети // Newsland (<http://newsland.com/news/detail/id/1548398/>). – 2015. – 23.05*).

## Маніпулятивні технології

Недавно Facebook заблокировала сообщение журналиста С. Пархоменко о самолете малазийских авиалиний Boeing-777, сбитом в небе над Донбассом летом прошлого года. Впоследствии компания извинилась, признав, что блокировка произошла по ошибке. Однако, по мнению блогера А. Носика, данный инцидент является очередным эпизодом кибервойны, развязанной прокремлевскими ботами против «неугодных» учетных записей в соцсети.

Как пояснил А. Носик, для блокировки используется довольно простая технология. Боты направляют в адрес конфликтной комиссии (Abuse Team) тысячи жалоб на определенную учетную запись, которая якобы нарушает пользовательское соглашение. Таким образом, англоязычный модератор делает вывод, что учетная запись действительно нарушает пользовательское соглашение и блокирует ее. Если пользователь начинает публично протестовать против блокировки (как в случае с С. Пархоменко), компания так же публично извиняется и проводит разблокировку. Возможен и другой вариант. Если «нарушитель» конфиденциально связывается с администрацией Facebook, разблокировка аккаунта происходит «по-тихому». Что любопытно, если «нарушитель» вообще не предпринимает никаких действий, его учетная

запись со временем разблокируется сама по себе, но сообщение останется по-прежнему недоступным.

Технология, используемая ботами, была отработана еще несколько лет назад на LiveJournal, после чего русскоязычное руководство площадки приняло контрмеры. Однако с Facebook дело обстоит несколько иначе. По словам А. Носика, в службе поддержки соцсети нет сотрудников «правильно понимающих российскую ситуацию». Кроме того, Россия не является приоритетной страной для Facebook, поэтому качество модерации в ее русскоязычном сегменте намного ниже (**Блогер рассказал, как прокремлевские боты блокируют неудобные аккаунты в Facebook // InternetUA** (<http://internetua.com/blogger-rasskazal--kak-prokremlevskie-boti-blokiruuat-neugodnie-akkaunti-v-Facebook>). – 2015. – 13.05).

\*\*\*

Администраторы социальной сети Facebook, курирующие украинский сегмент ресурса, воюют с детьми и своим произволом блокируют фотографию, способную раскрыть глаза на роль России в событиях на Востоке Украины.

Так, сообщает [ukraina.1440minut.info](http://ukraina.1440minut.info) со ссылкой на [Joinfo.ua](http://Joinfo.ua), администраторы социальной сети начали блокировать фотографию малышки из Кировограда, которая получила медаль «За мужество и отвагу» вместо погибшего отца, который воевал на Донбассе. Вручение награды детям героев состоялось накануне Дня победы в мемориальном комплексе «Крепостные валы», где была открыта аллея участникам солдатам АТО. Всего на Аллею славы занесли имена 117 воинов.

После того как отчет о мероприятии был опубликован на городской сайте, по социальным сетям «расползлось» душераздирающее фото белокурой малышки с огромными синими глазами, которая держит орден убитого российскими боевиками отца.

Однако некоторое время спустя обнаружилось, что фотография таинственным образом исчезает со страниц перепостивших ее, а Facebook рассылает предупреждения о блокировке данного контента.

«Проблема сидит в Ольгино, откуда приходит соответствующее количество жалоб. Простым нажатием кнопки “мне не нравится это фото”. Поскольку массив жалоб просто нереально большой, фото или его автор банятся по простому количеству жалоб», – пишут пользователи (**Фото девочки из Кировограда блокирует Facebook из-за медали отца // Весь Кировоград** ([http://www.kirovograd.net/shortly/2015/5/12/foto\\_devochki\\_iz\\_kirovograda\\_blokiruet\\_facebook\\_izza\\_medali\\_otca.htm](http://www.kirovograd.net/shortly/2015/5/12/foto_devochki_iz_kirovograda_blokiruet_facebook_izza_medali_otca.htm)). – 2015. – 12.05).

\*\*\*

Как украинцам ответить на действия кремлевских ботов?

Так как за последнюю неделю значительно возросла активность прокремлевских ботов в Facebook (на проблему даже обратил внимание П. Порошенко), напрашивается следующий вопрос: считаете ли вы правильной



интернет-борьбу в формате «Глаз за глаз», когда в ответ на блокировки ольгинскими ботами пользователи начнут блокировать страницы видных (и невидных) деятелей Нефтяной Державы?

Сам механизм неплохо описал в своем материале «Как кремлеботы нагнули Фейсбук» блогер А. Носик. Как становится ясно из текста, даже открытие украинского представительства Facebook не поможет справиться с блокировками по количеству жалоб.

На странице любого Д. Медведева и МИДа РФ можно найти посты, которые написаны в нарушение украинского законодательства.

Достаточно создать ресурс, это может быть даже просто Twitter-аккаунт (просто в качестве примера), где, скажем, раз в сутки будет публиковаться ссылка на блокируемый пост с объяснением причины. Чтобы все было законно, а не как у Ольгинских ботов.

Схема работы следующая:

1. Неравнодушные пользователи жалуются на запись.
2. Набирается определенное количество жалоб (около 200 уже будет достаточно).
3. Запись удаляется или страница блокируется полностью.

Для вопрошающих «А чем мы будем лучше их?» ответ: тем же, чем наши воины отличаются от кадыровских наемников. Тем, что делаем это сознательно и не за деньги.

Как минимум, это добавит головной боли ведущим страницы деятелей северного соседа.

Как максимум – приведет к пересмотру Facebook правил публикации постов и блокировки аккаунтов (*Как украинцам ответить на действия кремлевских ботов? // UAINFO (<http://uainfo.org/blognews/1431503231-kak-ukrainsam-otvetit-na-deystviya-kremlevskih-botov-.html>). – 2015. – 13.05).*

\*\*\*

У мережі Інтернет поширюється відеофрагмент, змонтований у стилі ТСН Тиждень, у якому акторка вдає журналістку телеканалу «1+1» та ломаною українською розповідає про голод, що панує у Росії. Про це пише 1plus1.ua.

Відео під назвою «Через українські санкції у Росії почався голод» було розміщено на одному з антиукраїнських ресурсів на сайті відеохостингу YouTube.

«Таких продуктів, як молоко, сало та хліб вже давно немає на прилавках, залишилися тільки рибні відходи, ними вони і “куштуються”», – старанно грає роль дівчина.

«Ми переглянули цей ролик з журналістами ТСН Тижня та дуже посміялися. Мабуть, наші новини дійсно популярні у Москві», – прокоментував випусковий редактор ТСН Тижня Р. Опаленик.

Телеканал 1+1 вже не вперше стикається з подібними спробами дискредитації зі сторони Кремля, тож вбачає у цьому відео лише чергове

невдале намагання скомпрометувати канал *(Кремлівські боти знімають псевдо-сюжети від імені ТСН // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43427/118/lang,ru/). – 2015. – 19.05).*

\*\*\*

Група українських Facebook-користувачів звернулася до служби підтримки соцмережі з проханням видалити расистський контент на сторінці російського пропагандистського телеканалу «Звезда».

У пості, який користувачі вимагали видалити, Білий дім, резиденцію президента США, назвали расистським висловом – nigga house.

Ініціатором звернення виступив О. Ворошило.

На заклик О. Ворошила відгукнулися кілька десятків українських користувачів, однак усі вони отримали однакову відповідь від Facebook – контент не порушує правила соціальної мережі *(Facebook вважає расистські висловлювання щодо Обами нормальними, головне аби росіян не ображали // UkrainianWatcher (http://watcher.com.ua/2015/05/21/facebook-vvazhae-rasistski-vyslovlyuvannya-schodo-obamy-normalnymi-holovne-aby-rosiyan-ne-obrazhaly/). – 2015. – 21.05).*

\*\*\*

Операція «Блокада». Чому українців «мочат» в Facebook?

Скандал с блокировкой профилей известных украинцев в крупнейшей социальной сети мира – Facebook – набирает обороты. В течение последних недель читатели Facebook не могли видеть сообщений А. Бондаря, А. Ройтбурда или В. Кипиани, пишет «Обозреватель» *(http://obozrevatel.com/politics/74356-operatsiya-blokada--pochemu-izvestnyih-ukraintsev-mochat-v-facebook.htm).*

7 мая руководитель компании М. Цукерберг во время открытого интернет-чата заявил, что в блокировании аккаунтов украинцев нет политического подтекста. Как пояснил М. Цукерберг, временный запрет публикаций не производится в России, поскольку – вопреки распространенному в Украине мнению – российского офиса не существует. После начала боевых действий на Востоке Украины должность ответственного за украинский-российские вопросы занимает Т. Кристенсен – руководитель подразделения Facebook в Северной Европе.

По словам М. Цукерберга, украинцев блокировали из офиса в Дублине, где есть специальная команда сотрудников, которые владеют многими языками и решают такого рода проблемы. М. Цукерберг также заверил, что лично проверил часть сообщений пользователей, которые были заблокированы, и полностью согласен с действиями своих сотрудников. В то же время руководитель Facebook признал определенные недостатки системы автоматической блокировки учетных записей.

Впрочем, и за последнюю неделю временные отключения украинцев от Facebook не прекратились. DW разбиралась в причинах этого явления.

Слово – не воробей

Ежедневно в социальной сети Facebook блокируется от 500 до тысячи аккаунтов украинских пользователей, рассказал в интервью DW киевский интернет-эксперт, основатель сайта Watcher М. Саваневский. По его словам, это началось с конца февраля – начале марта этого года. «С этого времени ежедневно поступали сообщения о блокировке или удаления аккаунтов известных политиков, депутатов, журналистов. Это набирало обороты и достигло максимума в конце апреля – начале мая», – сказал М. Саваневский.

Среди тех, чьи профили в сети заблокировали, публицист и писатель А. Бондарь, художник А. Ройтбурд, журналист А. Капустин, историк и публицист В. Кипиани, политик Б. Береза.

«Конкретных причин блокировки в Facebook мне не объяснили, просто сказали, что нарушил правила, посоветовав читать их», – сообщил в комментарии DW публицист А. Бондарь. Его аккаунт блокировали дважды: за публикацию шуточное стихотворение со словами «че там у хохлов», а также за сообщение в поддержку заблокированного в Facebook блогера Е. Гендина.

Страница А. Ройтбурда, как рассказал художник, заблокировали после критики о деятельности одного из украинских чиновников. «Что там является языком ненависти? – возмущается художник. – То, что я сравнил названия населенных пунктов с какими нелестными этнонимами, вроде Хацапетовки и Жидачева? Это ни в коем случае не является попыткой опорочить кого-то, а лишь констатация фонетической схожести». Причины такой придирчивости, говорит А. Ройтбурд, – механическая система контроля в Facebook.

Спецслужбы в соцсетях

В украинском сегменте Интернета многочисленные примеры блокировки украинцев в Facebook объясняют атакой «русских ботов». В частности, А. Бондарь считает, что отправляя жалобы на публикации популярных в социальных сетях людей и добиваясь блокировки аккаунтов, украинцам пытаются закрыть рот.

С другой стороны, отмечает М. Саваневский, можно привести немало примеров, когда администраторы социальной сети отказываются реагировать на жалобы на публикации сепаратистов с призывами убивать украинцев. «Российским спецслужбам и компаниям, которые им помогают, удалось найти дыры в системе оповещения о нарушении правил социальной сети. Сегодня они могут заблокировать любой аккаунт», – добавил М. Саваневский.

Не исключает спланированной атаки на украинский сегмент Facebook и профессор Европейской школы менеджмента и технологий С. Гайкен. «Это похоже на русскую информационную операцию. Следует заметить, что интернет-блокады часто испытывают политические партии. На 100 процентов таких же случаев в истории не припомню, но похожую ситуацию можно было наблюдать ранее в Сирии и Иране», – сообщил в комментарии DW С. Гайкен.

Между тем среди украинских блоггеров распространяется еще одна версия блокировки аккаунтов – вроде бы это делает украинское же Министерство информационной политики. «Но я не думаю, что оно со своей цензурой и структуре на это способно», – считает А. Ройтбурд.

Ответственность за жизнь

«Я пользовался Facebook как почтовым ящиком – там моя информация, контакты, работа, – продолжает А. Ройтбурд. – И если это все уничтожат, уничтожат мою интеллектуальную собственность». Сейчас художник ждет разблокировки аккаунта. Для пострадавших от правил Facebook в Киеве создали сервис по оказанию помощи. «В основном мы консультируем людей. Свои обращения к администрации социальной сети посылаем только в отдельных случаях. Иногда это помогает», – рассказала одна из инициаторов, менеджер по телекоммуникациям Украинского кризисного медиа-центра О. Крячко.

Поведение Facebook М. Саваневский объясняет особенностями бизнеса, ведь это «компания, построенная на доверии пользователей». И если бы менеджеры признали возможность манипуляций с системой оповещения, это могло бы еще больше подорвать доверие к компании и ее сервиса. «Я бы даже не исключал, что это могло бы повлиять на капитализацию акций компании на рынке. Поэтому Facebook сегодня никак на это не реагирует», – подытожил эксперт.

По его мнению, администрация Facebook не осознает, какую важную роль играет эта социальная сеть в гибридной войне России против Украины. «Мы должны осознавать, что с тех семи тысяч мирных жителей и полторы тысячи военных, погибших на Донбассе, какая доля погибла по вине социальных сетей, которые вовлекают людей в войну», – отметил М. Саваневский (*Операция «Блокада». Почему украинцев «мочат» в Facebook? // Обозреватель (<http://obozrevatel.com/politics/74356-operatsiya-blokada--pochemu-izvestnyih-ukraintsev-mochat-v-facebook.htm>). – 2015. – 23.05*).

\*\*\*

Группа специалистов по современным медиа из Лондонского городского университета установила, что массовые уличные протесты и активность в социальных сетях связаны более сложным образом, чем предполагалось ранее. В некоторых случаях уличные волнения граждан можно предсказать за один день до их начала по возросшему количеству твитов и постов. В других случаях медиа-активность идет параллельно с нарастанием физического участия в акциях или опосредована арестами и побоями. В третьих между ними вообще не обнаруживается отчетливой связи. Точность прогноза зависит от страны, где происходят волнения и влияния традиционных средств массовой информации. Работа опубликована в Journal of Communication.

Исследователи изучили три кейса: движение «Возмущенных» (Indignados) в Испании (2011 г.); движение Оссуру в США (2011 г.) и «Укусную революцию» в Бразилии (2013 г.). В анализ были включены шесть

количественно выраженных переменных: число твитов, постов в Facebook, связанных с акциями протеста; официальные оценки количества протестующих на улицах и в палаточных лагерях; число зарегистрированных арестов и обращений в больницы с травмами.

Для оценки влияния одних переменных на другие использовалась «причинность по Грэнджеру» – статистический метод для установления причинно-следственной связи между двумя временными рядами. Согласно принципу Грэнджера, если паттерн второй временной последовательности, в общем и целом повторяет паттерн первой, но с определенным сдвигом во времени, то можно сказать, что он детерминирован первым рядом, и в будущем предсказать его значения, основываясь на уже известных значениях первого ряда. Таким образом, гипотетически, можно связать, например, число протестующих и предшествующее митингу количество твитов и постов в соцсетях.

В реальности оказалось, что такая связь прослеживается, но далеко не всегда и с разным набором переменных. В целом, основываясь на количестве твитов и постов, в США и Испании можно предсказать протестную активность граждан на следующий день, так как Twitter играл там ключевую роль в локальной координации и логистике протестующих. Однако эта зависимость имела и обратный характер. Так, в Испании увеличение количества постов в Facebook постепенно возрастало до митинга и значительно более резко во время физического участия в акциях протеста. В США наблюдался тот же эффект плюс связь между числом инцидентов с полицией. Чем жестче полицейские разгоняли демонстрантов, тем большее количество постов было на следующий день в соцсетях.

В то же время в Бразилии вообще не было обнаружено никаких взаимосвязей между активностью в социальных медиа и физическим присутствием на акциях протеста. Множество постов и твитов в Бразилии наблюдалось только после волнений, в случае если кто-то из протестующих был ранен или следовали массовые аресты.

Таким образом, данные нового исследования в целом противоречат устоявшемуся мнению о ведущей роли социальных медиа и Интернета в возникновении и поддержке гражданских протестов последнего времени: от «Арабской весны» и до «Уксусной революции». В зависимости от культурного и географического контекста, проникновения Интернета и влияния телерадиовещания зависимость между виртуальной и уличной протестной активностью может быть как прямая, так и обратная. Или ее может не быть вообще. Следовательно, как предиктор она может использоваться только в ограниченном числе случаев (*Facebook и Twitter оказались не виноваты в «Уксусной революции»* // *Newsland* (<http://newsland.com/news/detail/id/1547682/>). – 2015. – 21.05).

## Зарубіжні спецслужби і технології «соціального контролю»

В Крыму закрыто за «экстремизм» более 10 сайтов. Об этом на своей странице в Facebook заявила «прокурор» полуострова Н. Поклонская.

«По интернет-сайтам, на которых идет пропаганда фашизма, нацизма, проводятся определенные исследования нашими специалистами», – заявила она.

«При получении ответов, что действительно прослеживаются радикальные настроения, прокуратура инициирует блокировку подобных сайтов. На территории Республики Крым уже закрыто более 10 интернет-сайтов за экстремистские высказывания. Возбуждены уголовные дела по данному факту. Каждый, кто призывает к фашизму, будет наказан», – добавила Н. Поклонская.

При этом она напомнила, что в 2014 г. в Крыму был вынесен один приговор по факту размещения жителем полуострова «сообщений националистического толка и изображений с фашистской символикой в социальных сетях» *(Поклонская: В Крыму более 10 интернет-сайтов закрыто за «экстремистские высказывания» // Mignews.com.ua (<http://mignews.com.ua/regiony/krym/5615150.html>). – 2015. – 12.05).*

\*\*\*

За 10 місяців українські кібервійська заблокували 4 млн дол., що розміщено на 198 рахунках терористів.

Про це повідомляє хакер Є. Докунін, передає «Преса України».

«За червень – березень Українські Кібер Війська заблокували 4 мільйони доларів на 198 рахунках терористів», – розповідає хакер.

Сьогодні Є. Докунін заблокував нові рахунки прихильників ДНР і ЛНР у системах WebMoney та Яндекс.Деньги.

«Рахунки в цих системах вже заблокували. А в QIWI теж заблокують, як це було раніше. Ще чекаю відповідь від PayPal. В системі WebMoney гаманці прив'язані до рахунку WMID 155866242967, що належить RedRat», – розповідає хакер.

Таким чином, українські кібервійська завдали чергового удару по сепаратистах і терористах та зупинили фінансування тероризму в трьох системах *(Кібервійська заблокували \$4 млн терористів // InternetUA (<http://internetua.com/k-berv-iska-zablokuvali--4-mln-terrorist-v>). – 2015. – 17.05).*

\*\*\*

Роскомнадзор направил в Google, Facebook и Twitter официальные письма, в которых потребовал от них прекратить противоправные действия в России, пригрозив санкциями, пишет Marketing Media Review (<http://mmr.ua/news/id/roskomnadzor-prigrozil-sankcijami-facebook-twitter-i-google-44399/>).

Претензии социальным сетям (претензии к Google касаются сервисов YouTube, BlogSpot и Google+) направил глава ведомства А. Жаров. Он потребовал от них не нарушать российское законодательство, сообщает газета «Известия». Издание не уточняет, какие именно страницы вызвали недовольство в Роскомнадзоре.

В случае продолжения противоправных действий компаниям пригрозили штрафами и блокировкой страниц. Как объяснил официальный представитель ведомства В. Ампелонский, именно после таких писем обычно происходят определенные подвижки в общении.

Ранее письма в Google, Facebook и Google направил заместитель руководителя М. Ксензов, указавший, что компании нарушают положения российского закона о блогерах. В частности, они не предоставили запрошенные ведомством данные о суточной посещаемости ряда страниц. Первоначальный штраф за это нарушение составляет 300 тыс. р., за повторное – 500 тыс. р.

Независимый юрист А. Богатов, комментируя заявление Роскомнадзора, указал, что взыскать средства с американских компаний Facebook и Twitter будет сложно. Деньги можно будет получить лишь с агентов, которые собирают с них деньги за рекламу. Что касается Google, то она владеет в России дочерней компанией, а в данном случае может действовать правило «сын за отца не отвечает».

Представители Twitter, Google и Facebook не ответили на запросы «Известий» (*Роскомнадзор пригрозил санкциями Facebook, Twitter и Google // Marketing Media Review (<http://mmr.ua/news/id/roskomnadzor-prigrozil-sankcijami-facebook-twitter-i-google-44399/>). – 2015. – 20.05*).

\*\*\*

Основатель самой популярной в России социальной сети «ВКонтакте» П. Дуров рассказал изданию Mashable, как предпочел бежать из своей родной Москвы после того, как люди, лояльные к Кремлю, отняли у него контроль над компанией.

Он навлек на себя гнев сотрудников ФСБ, когда начали появляться страницы о политических протестах, пишет The Business Insider.

«Когда П. Дуров отказался закрыть страницу активиста А. Навального, сотрудники ФСБ пришли к его дверям с автоматами и потребовали их впустить», – утверждает издание.

«Я по-настоящему испугался, – признался П. Дуров в интервью. – Я впервые подумал: может, мне стоит подумать о будущем – о будущем моей страны и моей компании». При этом П. Дуров признался, что никогда не интересовался политикой, а то, что он не подчинился Кремлю, было продиктовано скорее опасениями, что пользователи уйдут в другую соцсеть.

«В конце 2013 г. некая московская инвестфирма, имеющая связи с Кремлем, приобрела 48 % акций “ВКонтакте” у двух из крупнейших инвесторов компании. По некоторым сведениям, эту сделку организовал глава

“Роснефти”, верный сторонник В. Путина И. Сечин, чтобы расширить контроль над этой сетью», – сказал он.

П. Дуров поведал, что именно тогда понял, что Кремль за ним «гонится», и решил уехать в Нью-Йорк. После того как ситуация успокоилась, он ненадолго вернулся в Россию, но к тому времени он почти полностью потерял контроль над соцсетью «ВКонтакте».

В феврале прошлого года он полностью отказался от административной власти и продал оставшийся пакет акций верному стороннику В. Путина И. Таврину.

Он оставался на посту гендиректора, пока в апреле не уволился из компании окончательно. «Пора было уходить, потому что к тому моменту я не имел в компании никакой власти», – пояснил П. Дуров. В 2006 г., когда П. Дуров основал «ВКонтакте», российские власти все еще терпимо относились к свободе Интернета.

В 2011 г. скептическое отношение президента В. Путина к Интернету усилилось, когда люди начали использовать Интернет для протестов против предполагаемых фальсификаций на парламентских выборах (*Павел Дуров рассказал, как путин отобрал у него соцсеть «ВКонтакте» // Daily (<http://daily.com.ua/world/20-05-2015211325>). – 2015. – 20.05*).

\*\*\*

Агентство национальной безопасности США планировало заражать смартфоны вирусной шпионской программой, перехватывая интернет-трафик онлайн-магазинов Google и Samsung, передает портал Intercept.

Сведения об операции, получившей кодовое название Irritant Horn, содержались в секретных документах, обнародованных бывшим сотрудником американских спецслужб Э. Сноуденом в сотрудничестве с телеканалом с CBS News и порталом Intercept.

Согласно плану, спецслужбы собирались с помощью системы XKEYSCORE вычленять в общем потоке интернет-трафика трафик со смартфонов, отслеживать его путь к серверам онлайн-магазинов Google и Samsung, а затем перехватывать, чтобы отправлять на мобильные устройства шпионские программы под видом полученных от Google и Samsung данных. Среди функций программ – копирование списка контактов из зараженного телефона, а также трансляция сведений о местонахождении гаджета.

Разработка плана велась в период с ноября 2011 по февраль 2012 г., в его подготовке участвовали специалисты из всех стран соглашения Five Eyes («Пять глаз»). Помимо США, в него входят Великобритания, Новая Зеландия, Канада и Австралия. Согласно информации Intercept, один из главных мотивов для подготовки Irritant Horn – опасения по поводу возможной новой «арабской весны». Неизвестно, был ли план реализован (*Спецслужбы США планировали заразить смартфоны шпионским вирусом? // Центр Інформаційної Безпеки (<http://www.bezpeka.com/ru/news/2015/05/22/irritanthorn.html>). – 2015. – 22.05*).



\*\*\*

Депутаты украинского парламента внесли ряд изменений в отечественное законодательство, благодаря которым разрешается фото- и видеофиксация действий чиновников, представителей власти, милиции и силовых структур скрытыми спецсредствами или гаджетами.

Соответствующий законопроект был принят в Верховной Раде 22 мая. Согласно этому закону, вводится институт общественного обвинения, что даёт возможность открытия уголовного производства по фактам коррупции по инициативе любого физлица или юрлица.

В этом же законе из действующего Уголовного кодекса Украины исключены статьи, запрещающие приобретение, сбыт или применение спецсредств для фиксации, получения и записи визуальной и звуковой информации, которая может служить в качестве доказательств по делу о вымогательстве, даче или получении взятки.

«Если сейчас кто-то в зале сидит с часами Apple, или с очками Google, то это – тоже вещи, которые подпадали под действующую статью», – пояснил необходимость законодательных изменений народный депутат А. Кожемякин, представлявший в парламенте новый законопроект *(Українцям разрешили ввозить и использовать Google Glass и «шпионские» видеокамеры для слежения // Блог Imena.UA (<http://www.imena.ua/blog/yes-to-google-glass/>). – 2015. – 22.05)*.

\*\*\*

У Краматорську і Слов'янську СБУ затримала двох адміністраторів соціальної мережі за сприяння терористам.

Як повідомляє прес-центр СБУ, спецслужба викрила двох громадян, які організували та адміністрували 26 груп антиукраїнської спрямованості в соціальній мережі «ВКонтакте» і намагалися втягнути молодь у протиправну інформаторську діяльність.

Місцеві жителі (21 і 23 років) під різними псевдонімами створили інтернет-спільноти, через які поширювали відео- та фотоматеріали про розташування підрозділів Збройних сил України в Слов'янському районі. Також вони оприлюднювали реквізити банківських карток та електронних гаманців для збору коштів для терористичних угруповань.

«Адміністратори сепаратистських мереж затримані. Під час обшуків у їхніх помешканнях вилучено комп'ютерну техніку з антиукраїнськими матеріалами та інші докази їхньої протиправної діяльності», – повідомляє прес-центр СБУ.

У рамках кримінального провадження за ст. 258-3 (сприяння діяльності терористичної організації) тривають слідчі дії, встановлюються зв'язки затриманих з бойовиками із «ДНР» *(СБУ затримала двох адміністраторів соцмережі за допомогою терористам // InternetUA (<http://internetua.com/sbu-zatrimala-dvoh-adm-n-strator-v-socmerez--za-dopomogu-teroristam>). – 2015. – 24.05)*.

\*\*\*

В Южной Корее вступило в законную силу решение Комиссии связи Кореи о принудительном мониторинге смартфонов, находящихся в использовании у несовершеннолетних граждан страны. Согласно этому распоряжению, телекоммуникационные компании и опекуны будут обязаны устанавливать шпионские программы на мобильные абонентские терминалы детей и подростков, не достигших возраста в 18 лет.

Как сообщает агентство Associated Press, в обязанность поставщикам услуг связи и родителям несовершеннолетних теперь вменяется проверка наличия предустановленного на приобретаемых юными гражданами страны смартфонах отслеживающего программного обеспечения. В общей сложности, разрешенными к использованию являются 15 приложений для мониторинга, включая разрабатываемую при поддержке южнокорейского правительства утилиту SmartCOP.

Первоочередной задачей подобного ПО декларируется борьба с неприемлемым для детей содержанием, таким как порнография. Помимо этого, мониторинг будет включать в себя статистику посещения интернет-ресурсов и использования приложений, а также передачу спутниковых данных о местонахождении устройства родителям ребенка.

Впрочем, есть у нового требования правительства и одна небезынтересная особенность – оно распространяется только на устройства под управлением ОС Android. Таким образом, родители, выбирающие для своих чад свободу самоопределения, имеют вполне законную возможность обойти установленные ограничения, выбрав мобильные аппараты, работающие на альтернативных платформах. Кроме того, вне обязательного мониторинга остаются и приобретенные ранее устройства. Эту проблему планируется решить рассылкой писем от имени администрации школ, в которых родителей будут уведомлять о необходимости установки шпионского ПО и на уже имеющиеся смартфоны (*Власти Южной Кореи обязали родителей устанавливать шпионское ПО на смартфоны несовершеннолетних // InternetUA (<http://internetua.com/vlasti-ujnoi-korei-obyazali-roditelei-ustanavlivat-shpionskoe-po-na-smartfoni-nesovershennoletnih>). – 2015. – 24.05).*

### **Проблема захисту даних. DDOS та вірусні атаки**

Популярный сервис анонимных мнений «Спрашивай.ру» был взломан российским хакером по прозвищу w0rm.

Злоумышленник опубликовал электронную базу с личными данными 6,72 млн пользователей сервиса «Спрашивай.ру» на одном из файлообменников. Сколько людей воспользовалось опубликованными данными, информации пока нет.

База записей с пользовательскими данными содержит информацию об электронной почте, имени пользователя, пароле и его IP-адресе. Также в записи может быть указана информация о дате рождения, ФИО, телефон и ссылки на соцсети пользователя.

В «Спрашивай.ру» подтвердили утечку: «Факт несанкционированного доступа к данным довольно большой части пользователей мы подтверждаем. Также сообщаем, что эти данные в будущем не позволят раскрыть авторов анонимных вопросов. Все реквизиты деактуализированы, а идентификаторы – изменены в 14:09 по московскому времени».

Администрация сервиса также сообщила, что вход по старым реквизитам (логину и паролю) невозможен: система автоматически сбрасывает пароль каждый раз при вводе прежних данных, и поменять его можно только через привязанную к аккаунту почту. Однако у части пользователей в почтовом ящике используется те же самые логин пароль, что и на «Спрашивай.ру», а популярные почтовые сервисы пока не сбрасывали их реквизиты (*Хакер взломал 6.72 млн аккаунтов сервиса анонимных мнений «Спрашивай.ру» // InternetUA (http://internetua.com/haker-vzломal-6-72-mln-akkauntov-servisa-anonimnih-mnenii--sprashivai-ru). – 2015. – 12.05).*

\*\*\*

Хакери з раніше невідомого угруповання Social Hack взяли на себе відповідальність за злом російськомовного сайту Russia Today.

Про це повідомляє Еспресо.TV із посиланням на російську службу ВВС.

Головний редактор телеканалу М. Симоньян повідомила, що хакерам вдалося відредагувати деякі тексти, розміщені на сайті.

«Зломщики намагалися змінювати контент вже написаних статей. Розслідуємо, з яких IP адрес намагалися захопити сайт», – зазначила головний редактор RT.

Зокрема, після такого «редагування» замість новини з висловом Д. Пескова про мінські домовленості з'явилося рекламне повідомлення.

Контроль над сайтом вдалося відновити за дві години (*Хакери зламали сайт російських пропагандистів Russia Today // Espresso.tv (http://espresso.tv/news/2015/05/13/khakery\_zlamaly\_sayt\_rosiyskykh\_propahandyst iv\_russia\_today). – 2015. – 13.05).*

\*\*\*

Сайт з доповіддю, яку почав готувати російський опозиціонер Б. Немцов, про війну на Донбасі був підданий DDoS-атаці. Про це у Facebook повідомив член бюро федеральної політради російської партії «РПП-Парнас» І. Яшин.

«Сайт <http://t.co/qaKQSzlyFu>, на якому розміщена доповідь #ПутинВойна, піддався потужній DDoS-атаці. Вирішуємо проблему, скоро відновимо доступ», – написав російський опозиціонер. Згодом він повідомив, що DDoS-атаки на сайт продовжуються. «Але макет доповіді #ПутинВойна в pdf доступний також за посиланням:

<https://docs.google.com/file/d/0B83Lt4C02gp4b0g2a1RoWEJnZ0E>», – написав І. Яшин.

Крім того, він повідомив, що розпочато збір коштів на видання друкованої версії доповіді. «Беріть участь! Треба, щоб доповідь прочитали не тільки користувачі Інтернету, а й ті, хто звик отримувати новини з газет і ТБ», – закликав опозиціонер.

Збір коштів: Яндекс-гроші: 410013115196628, PayPal: putin.voina@yandex.ru.

Нагадаємо, що 12 травня в Москві презентували доповідь «Путін. Війна» про військовий конфлікт в Україні, яку російський опозиційний політик Б. Немцов розпочав готувати до того, як був убитий у ніч на 28 лютого в Москві.

Над текстом працювали журналісти А. Муждабаєв та О. Кашин, колишній віце-прем'єр Росії А. Кох, члени політради РПР-ПАРНАС І. Яшин і Л. Мартинюк, виконавчий директор партії О. Шоріна.

«Путін. Війна» – це 64-сторінкове дослідження, що об'єднало в собі свідчення, які демонструють втручання Москви в українську політику й присутність російських збройних сил на Сході України. Деякі факти вже були опубліковані, деякі оприлюднюються вперше. Дослідження розбите на 11 глав, які охоплюють події в Україні від подій на Майдані, коли, за версією авторів доповіді, у Кремлі був розроблений сценарій «повернення Криму», і дотепер.

У доповіді йдеться, на яких умовах російські військовослужбовці воюють на Донбасі, скільки їх вже загинуло, зокрема під містами Дебальцевому й Іловайську (Донецька область). Автори доповіді стверджують, що родичі загиблих солдат отримали по 2 млн р. і дали підписку про нерозголошення обставин смерті військових.

У документі наводяться дані про витрати російського бюджету на військову операцію на Сході України і анексію Криму. За оцінками співавтора доповіді, директора з макроекономічних досліджень ВШЕ С. Алексашенка, 10 місяців агресії на Сході України коштували російському бюджету 53 млрд р. Ще 80 млрд було витрачено на біженців, які переїхали в Росію з Донеччини та Луганщини.

Як повідомив РБК І. Яшин, наразі доповідь була надрукована мінімальним тиражем (2 тис. примірників). Окрім Москви презентації документа заплановані в регіональних центрах – Петербурзі, Ярославлі, Челябінську та інших містах. Одночасно почнеться кампанія зі збирання коштів на видання доповіді для подальшого поширення. Розмір наступного тиражу буде залежати від зібраних коштів.

Б. Немцов збирався протиставити свою доповідь офіційній версії подій. «Я придумав, що робити. Треба написати доповідь “Путін. Війна”, видати її величезним тиражем і роздавати на вулицях. Розповімо, як Путін розв'язав цю війну. Тільки так ми переможемо пропаганду», – ці слова Б. Немцова наводяться в тексті доповіді (*Сайт з доповіддю Бориса Немцова про війну на*

\*\*\*

Вице-президент WhiteHat Labs из WhiteHat Security Р. Хансен обнаружил уязвимость, которая получила название Magic Hash. Из-за ошибки в PHP при работе с хешами в некоторых ситуациях злоумышленник может подобрать пароль к учетной записи пользователя, обойти аутентификацию и другие средства обеспечения безопасности, полагающиеся на хеширование.

Проблема возникает при использовании оператора равно-равно (==) во время сравнения двух хешей. PHP использует кодировку base16, в результате получаем строку, подобную этой: «0e812389...».

Если строка начинается с «0e» и после нее следуют только цифры, PHP будет интерпретировать эту строку как число с плавающей точкой. В итоге, условие if ('0e462097431906509019562988736854' == '0') будет истиной.

По мнению эксперта, эта брешь затрагивает миллионы сайтов и может стать действительно проблемой. Если хеш пароля пользователя в базе данных начинается с «0e», злоумышленник может воспользоваться любой строкой, которая при сравнении будет интерпретирована как 0, и успешно авторизоваться в системе без знания пароля.

В качестве временного решения эксперт предлагает использовать тройное равно (===) для подобных сравнений.

Эксперт также отмечает, что подобная проблема затрагивает не только PHP. Такие языки как Perl и JavaScript также подвержены уязвимости, поскольку не требуют обязательного объявления типа переменной перед ее использованием (*Уязвимость в PHP подвергает опасности практически любой сайт // InternetUA* (<http://internetua.com/uyazvimost-v-PHP-podvergaet-opasnosti-prakticeski-luaboi-sait>). – 2015. – 13.05).

\*\*\*

По данным американской компании root9B, российские хакеры, предположительно спонсируемые Москвой, готовят новую серию атак – в этот раз на банки США, ОАЭ и Нигерии, а также на организацию, действующую под эгидой ООН.

Российская хакерская группировка APT28, которую совсем недавно обвинили в атаке на «правительственную структуру» некоего иностранного государства, планирует взлом сетей ряда банков в США, Объединенных Арабских Эмиратах и Нигерии. Об этом говорится в докладе американской компании root9B Technologies, специализирующейся на информационной безопасности.

В список целей вошли американские финансовые организации TD Bank, Bank of America и Regions Bank, а также UAE Bank (ОАЭ) и United Bank for Africa (Нигерия). Кроме того, список предполагаемых целей включает Детский

фонд ООН – международную организацию, действующую под эгидой Организации Объединенных Наций.

Заражение компьютеров хакеры планируют осуществлять путем рассылки электронных писем и вредоносными вложениями либо ссылками на веб-сайты с вредоносным кодом. Экспертам неизвестно, когда АРТ28 планирует начать операцию. По словам специалистов, в настоящее время хакеры дописывают вредоносный код, настраивают командно-контрольный сервер и регистрируют фальшивые веб-адреса, похожие на адреса официальных сайтов финансовых и других организаций, а также популярных СМИ, по которым планируется разместить вредоносный код – [b-of-america.com](http://b-of-america.com), [regionsbnk.info](http://regionsbnk.info), [techcrunch.com](http://techcrunch.com) и др.

Представители root9B отметили, что ни одна из указанных организаций не является их клиентом. «Но мы понимаем, что это наш долг – поделиться информацией», – заявил генеральный директор root9B Э. Хипкинс. В компании добавили, что это большая удача – обнаружить готовящуюся атаку (обычно выполняется анализ уже проведенных атак). Эксперты опубликовали хэш-суммы вредоносных приложений и IP-адрес командно-контрольного сервера, чтобы компании могли заблокировать их.

В докладе root9B говорится, что за последние три-пять лет российские хакеры «создали крупнейший из обнаруженных ботнетов, похитили логины и пароли к десяткам миллионов аккаунтов и украли почти 900 млн дол. из банков по всему миру». Увеличение количества кибератак на иностранные государства – это «часть агрессивной внешней политики России», считают авторы доклада.

В конце апреля 2015 г. хакерская группировка АРТ28 была обвинена в проведении атаки на «правительственную структуру» некоего иностранного государства другим американским разработчиком средств защиты – FireEye. Специалисты не стали называть, какая именно структура и какого государства стала жертвой (*«Российские хакеры» готовят атаку на банки США // InternetUA (<http://internetua.com/rossiiskie-hakeri--gotovyat-ataku-na-banki-ssha>). – 2015. – 13.05).*

\*\*\*

Специалист по информационной безопасности Б. Томас обнаружил уязвимость в популярной утилите для операционной системы Apple OS X – MacKeeper. Уязвимость позволяет злоумышленникам исполнять на компьютере жертвы произвольный код с привилегиями администратора при посещении вредоносного сайта. В качестве демонстрации Томас разместил в своем блоге в Twitter веб-ссылку, которая отправляет в OS X команду, запускающую процесс деинсталляции MacKeeper.

Уязвимость связана с функцией операционной системы, позволяющей назначать программы для обработки ссылок различного типа. Например, при нажатии на адрес электронной почты – запускать приложение Mail и т. д. Проблема в том, что проверка таких адресов программой MacKeeper выполняется некачественно.

Причем для исполнения вредоносного кода через MacKeeper ввод пользователем пароля к своей учетной записи в OS X может не потребоваться – если этот пароль был введен в MacKeeper ранее (в рамках нормальной работы приложения, для выполнения некоторых действий). Если же пароль не вводился, злоумышленник может подделать запрос на ввод пароля, поступивший якобы от лица MacKeeper.

Под угрозой могут находиться миллионы пользователей. В марте 2015 г. разработчик сообщил, что за пять лет существования приложение MacKeeper было загружено 20 млн раз. Насколько долго уязвимость присутствовала в программе, Томас не уточняет. 8 мая разработчик MacKeeper выпустил обновление 4.3.1, в котором «дыра» была устранена.

Основные функции MacKeeper: удаление ненужных файлов (включая журналы, кэш, дубликаты и т. д.), защита от вредоносных веб-сайтов (посредством движка Avira), оптимизация производительности, шредер и шифрование файлов. Продукт был разработан украинской компанией ZeoBIT. В 2013 г. права на него были проданы немецкой фирме Kromtech Alliance (*Популярная утилита для Mac служит «дверью» для вирусов // InternetUA (<http://internetua.com/populyarnaya-utilita-dlya-Mac-slujit--dverua--dlya-virusov>). – 2015. – 13.05).*

\*\*\*

Уязвимость в программном механизме «ВКонтакте» позволяет хакерам получать прямые ссылки на изображения, отправленные в личных сообщениях, а также хранящиеся в личных и групповых фотоальбомах. Обнаружил ошибку программист из Казани К. Хисматуллин, написавший о ней в своем блоге.

«Я создал эксплойт, который bruteforce-методом получает идентификаторы фотографий, загруженных в определенный период, а затем с помощью этой уязвимости получил возможность узнать прямые ссылки на изображения», – отметил К. Хисматуллин. Он также подчеркнул, что раздобыть прямую ссылку можно для любого хранящегося изображения, независимо от настроек конфиденциальности.

По словам К. Хисматуллина, для того чтобы получить ссылки на все загруженные в течение последнего года фотографии, требуется около двух часов работы. Программист отметил, что администрация «ВКонтакте» уже знает о наличии уязвимости (*Программист нашел ошибку в работе «ВКонтакте» // InternetUA ([http://internetua.com/programmist-nashel-oshibku-v-rabote--vkontakte](http://internetua.com/programmist-nashel-oshibku-v-rabote-vkontakte)). – 2015. – 14.05).*

\*\*\*

Информация о состоянии здоровья людей во всех странах мира приобрела особую ценность, и хакеры начали настоящую охоту за ней. За последние несколько лет в сети появилось множество сервисов, мониторящих здоровье клиентов при помощи различных гаджетов, и за последние два года 90 % из них были взломаны.

Статистика, предоставленная информационным агентством Bloomberg и порталом Slash Gear, относится пока только к США, но эксперты утверждают, что аналогичная картина происходит и ко всему миру. Рост количества атак против сервисов по охране здоровья наносит существенный вред, который можно измерить в денежном эквиваленте – по меньшей мере 6 млрд дол. в год. Фактически, это означает, что сфера здравоохранения с недавних пор интересует хакеров и тех, на кого они работают, даже больше, чем сфера финансов.

По словам экспертов, более половины из всех совершенных атак носили криминальный характер, и вся полученная в результате совершения виртуального нападения информация могла быть использована в корыстных целях. Ярким примером может являться взлом страховой компании Anthem, произошедший в феврале текущего года. В результате успешно проведенной атаки хакерам удалось завладеть личной информацией о миллионах клиентов данной организации. Данные этих людей, включая и такие важные, как номера кредитных карт, были скомпрометированы.

Информация подобного рода может быть использована для самых разных целей. К примеру, личность одного человека может быть «украдена», что в последнее время стало настоящей проблемой в США. Данные другого человека могут быть использованы для получения кредита на крупную сумму.

Компании, работающие в сфере здравоохранения, начали работы по улучшению своих систем защиты информации, но пока неизвестно, насколько активно ведется их усовершенствование. Пока же, считают эксперты, более половины организаций не смогут отбить любую хакерскую атаку, которая может готовиться против них (*Хакеры активно угрожают сервисам охраны здоровья // InternetUA (<http://internetua.com/hakeri-aktivno-ugrojauat-servisam-ohrani-zdorovya>). – 2015. – 15.05*).

\*\*\*

IT-специалист Д. Доненфелд обнаружил в драйвере ozwrap ядра Linux пять уязвимостей.

Четыре из обнаруженных брешей позволяют злоумышленнику спровоцировать зацикливание или отказ в обслуживании ядра Linux, отправив оформленные определенным образом пакеты (packet-of-death).

Первая и вторая уязвимости могут эксплуатироваться благодаря выходу за границы буфера, третья – из-за условий при делении на ноль. Четвертая брешь вызывает бесконечное зацикливание, а пятая возникает из-за возможности чтения из области, которая находится за пределами выделенного буфера. Эксперты создали прототипы эксплоитов для того, чтобы показать, как эксплуатируются уязвимости.

Специалисты считают, что уязвимости не слишком опасны, поскольку драйвер ozwrap используется в очень редких случаях. Кроме того, для эксплуатации брешей злоумышленникам необходимо будет отправить пакеты на канальном уровне в рамках единственного сегмента LAN-сети.



Драйвер `ozwraп` необходим для работы USB-контроллера в режиме, когда взаимодействие с устройствами периферии осуществляется посредством Wi-Fi вместо физического подключения. Подобный метод работы контроллера предполагает преобразование USB-команд в протокол второго уровня сетевой модели и передачу их в форме пакетов типа `0x892e` (*В ядре Linux обнаружены 5 уязвимостей // InternetUA (<http://internetua.com/v-yadre-Linux-obnarujeni-5-uyazvimostei>). – 2015. – 14.05).*

\*\*\*

Эксперты из Incapsula обнаружили массивный ботнет из скомпрометированных домашних маршрутизаторов SOHO, используемый для осуществления DDoS-атак. За последние несколько месяцев десятки клиентов компании стали жертвами тысяч инфицированных маршрутизаторов, осуществляющих атаки HTTP-флуд на уровне приложений.

По данным исследователей, скомпрометированные устройства заражены трояном Spike и Linux-ботом MrBlack, о котором впервые сообщила компания «Доктор Веб» в мае прошлого года. Поначалу эксперты Incapsula предположили, что для взлома маршрутизаторов злоумышленники использовали уязвимости в аппаратном обеспечении. Однако позже выяснилось, что устройства можно легко скомпрометировать по протоколам HTTP и SSH через порты по умолчанию. При этом интерфейс защищен учетными данными по умолчанию (`admin/admin`).

Как сообщили исследователи, большинство взломанных маршрутизаторов являются устройствами на базе ARM производства Ubiquiti Networks. В общей сложности в инфицированных роутерах было обнаружено 13 тыс. образцов вредоносного ПО – в среднем на каждый зараженный маршрутизатор пришлось по четыре варианта Spike. Кроме того, эксперты выявили такие угрозы как BillGates, Dofloo и Mayday.

В течение 121 дня эксперты зафиксировали вредоносный трафик, исходящий с 40 тыс. IP-адресов 1,6 тыс. провайдеров по всему миру, а также IP-адреса подконтрольных злоумышленникам C&C-серверов. Зараженные устройства расположены по всему миру, однако свыше 85 % из них находятся в Бразилии и Таиланде.

По данным Incapsula, скомпрометированные маршрутизаторы использовались несколькими группировками, в том числе активистами из Anonymous. Не исключено также, что ботнет использовали хакеры из Lizard Squad (*Обнаружен крупный ботнет из домашних маршрутизаторов // InternetUA (<http://internetua.com/obnarujen-krupnii-botnet-iz-domashnih-marshrutizatorov>). – 2015. – 14.05).*

\*\*\*

Компания Microsoft совместно с ИБ-компанией FireEye пресекла деятельность китайской группировки APT 17, использовавшей блог Microsoft TechNet для маскировки хакерских операций. Группировка, предположительно

спонсируемая китайским правительством, хорошо известна своими атаками на госорганизации США, предприятия оборонной промышленности, а также юридические и информационно-технологические компании.

TechNet – интернет-ресурс с высоким трафиком, содержащий техническую информацию о продукции Microsoft, новости и предстоящие события для профессионалов в сфере информационных технологий. На портале также есть форум, на котором пользователи могут оставлять комментарии и задавать вопросы.

Участники АРТ 17 размещали комментарии на TechNet и создавали профильные страницы, содержащие закодированные IP-адреса C&C-сервера, которые направляли вариант бэкдора BLACKCOFFEE на C&C-сервер злоумышленников. В результате деятельности киберпреступников система безопасности TechNet скомпрометирована не была, однако такая тактика может успешно сработать на других интернет-площадках и форумах, отметили специалисты.

Большинство хакерских групп предпочитают компрометировать без труда манипулируемые сайты, что ведет к довольно быстрому обнаружению их деятельности и местоположения. Тактика, применяемая АРТ 17, более искусна, но далеко не нова. К примеру, известны случаи, когда несколько зомби-сетей использовали профили в Twitter в качестве канала связи. По словам экспертов, ранее АРТ 17 уже эксплуатировала популярные поисковые системы, в том числе Google и Bing, для маскировки своей активности и расположения серверов.

Как прогнозирует сотрудница FireEye Л. Галанте, в недалеком будущем подобное кодирование и обфускация станут довольно популярной тактикой среди хакерских группировок по всему миру (*Китайские хакеры использовали сайт Microsoft TechNet для осуществления атак // Центр информационной безопасности* (<http://www.bezpeka.com/ru/news/2015/05/15/hackers-used-Microsoft-TechNet.html>). – 2015. – 15.05).

\*\*\*

Калифорнийский хакер С. Камкар изобрел 3D-инструмент, способный взломать кодовый замок за 30 секунд. Все материалы, в том числе планы, трехмерные модели и коды специалист опубликовал в открытом доступе.

Несколько недель назад С. Камкар сообщил о производственном дефекте в кодовых замках Master Lock, позволяющем раскрыть комбинацию путем изучения взаимодействия кодового диска с замком. Этот процесс довольно коварен и требует применения некоторого программного обеспечения, поэтому С. Камкар решил его механизировать при помощи своего нового изобретения под названием Combo Breaker.

Инструмент оснащен шаговым двигателем для вращения диска замка, сервоприводом и аппаратно-вычислительной платформой Arduino. Как отметил С. Камкар, для определения комбинации замка устройству потребуется 5

минут, но если известна первая цифра – весь процесс займет не более 30 секунд.

Combo Breaker – далеко не первая разработка С. Камкара. Он является автором первого червя, эксплуатировавшего XSS-уязвимость для распространения. За ночь червь Samy инфицировал более миллиона учетных записей на популярном сайте Myspace.com., администрация которого была вынуждена прекратить его работу до тех пор, пока уязвимость не была устранена (*Хакер создал инструмент, способный взломать кодовый замок за 30 секунд // InternetUA (<http://internetua.com/haker-sozdat-instrument-sposobnii-vzlozat-kodovii-zamok-za-30-sekund>). – 2015. – 18.05*).

\*\*\*

Эксперты, занимающиеся разработкой решений для киберзащиты компании Malwarebytes, выявили, что потенциально нежелательная программа (potentially unwanted programs, PUP) WinYahoo способна изменить настройки безопасности в Google Chrome, оставшись необнаруженной обозревателем.

Потенциально нежелательные программы не настолько опасны для пользователя, как другие виды вредоносного ПО, однако в некоторых случаях они могут подвергать ПК риску быть зараженным.

Так, PUP-программа WinYahoo, несмотря на название и тот факт, что она устанавливает поисковый движок Yahoo! в качестве используемого по умолчанию, не имеет к компании Yahoo! никакого отношения.

Как и большинство потенциально нежелательных программ, WinYahoo включена в пакет установки других приложений. Специалисты компании Malwarebytes рассмотрели WinYahoo на примере Adobe Photoshop Album Starter Edition, в состав пакета установки которой входит потенциально нежелательная программа.

Adobe Photoshop Album Starter Edition является устаревшим ПО для редактирования и обмена фотографиями, а его поддержка была прекращена компанией Adobe много лет назад. Тем не менее, последнюю версию (3.2) Adobe Photoshop Album Starter Edition можно бесплатно скачать с различных сайтов. ПО не может быть зарегистрировано, хотя есть возможность запустить его определенное количество раз.

Скачав Adobe Photoshop Album Starter Edition, пользователь, скорее всего, установит вместе с графическим редактором и средствами для обмена фотографиями и потенциально нежелательное ПО WinYahoo. В случае, если мастер установки не может обнаружить виртуальную машину на компьютере пользователя, ему будет предложено установить Yahoo! в качестве поисковой системы по умолчанию и домашней страницы на всех совместимых браузерах (Chrome, Firefox, Internet Explorer) (*Потенциально нежелательное ПО WinYahoo изменяет настройки безопасности в Chrome // InternetUA (<http://internetua.com/potencialno-nejelatelnoe-po-WinYahoo-izmenyaet-nastroiki-bezopasnosti-v-Chrome>). – 2015. – 16.05*).

\*\*\*

Неизвестные злоумышленники взломали базу данных шпионского приложения для смартфонов mSpy. Об этом рассказал исследователь в области безопасности Б. Кребс в своем блоге. Украдена персональная информация более чем 400 тыс. пользователей сервиса.

Взломщики получили доступ к сведениям об учетных записях и паролях пользователей продуктов Apple, платежной информации по 145 тыс. транзакций. Большой фрагмент с данными, полученными с этих серверов, выложен в даркнете. В архиве находится большое количество адресов электронной почты, текстовых сообщений, платежей и чеков, геолокационных данных и другой приватной информации пользователей.

«Были украдены тысячи электронных писем подписчиков mSpy со всего мира, которые платили от 8,33 до 799 дол. в зависимости от рассылки, которую они получали», – написал Б. Кребс.

В общей сложности архив содержит несколько сотен гигабайт информации, снятой с мобильных телефонов жертв, в том числе около 4 млн событий, зарегистрированных программным обеспечением.

Приложение mSpy совместимо с устройствами на iOS, Android и Windows Phone. После установки на мобильный гаджет (в случае с iPhone и iPad они должны быть джейлбрейкнуты), приложение начинает в скрытом режиме вести лог активности и записывать все sms-сообщения, звонки, события календаря и заметки. При этом появляется возможность в любой момент получить доступ к конфиденциальной информации человека, даже если она была удалена из телефона. mSpy позволяет читать переписку в почте, WhatsApp, Viber, iMessage и Skype, записывать телефонные разговоры и звуки с микрофона, отслеживать GPS-координаты устройства и отображать маршрут на карте в режиме реального времени (*Хакеры взломали приложение-шпион mSpy и выложили в открытый доступ данные 400 000 пользователей // InternetUA (<http://internetua.com/hakeri-vzломali-prilojenie-shpion-mSpy-i-vilojili-v-otkritii-dostup-dannie-400-000-polzovatelei>). – 2015. – 16.05).*

\*\*\*

ESET, международная антивирусная компания, предупреждает об увеличении роста активности мобильного трояна российского происхождения, известного под именем Android/Spy.Banker.F. Первые образцы данного трояна были обнаружены ещё в конце 2013 г. Уже в середине 2014 г. авторы вредоносной программы начали активно развивать свою разработку, запуская в эксплуатацию её новые варианты. Главная цель Android/Spy.Banker.F – различные системы онлайн-банкинга. Что касается версии трояна, исследованной специалистами ESET, она демонстрирует стабильный рост числа обнаружений с начала 2014 г. Пик обнаружений пришёлся на начало нынешнего года. На нынешнюю модификацию вредоносного ПО приходится до 68 % всех выявленных образцов семейства.

До 98 % заражений приходится на пользователей России, ещё 0,76 % и 0,21 % – на Украину и Беларусь соответственно. Отсюда следует очевидный вывод, что Android/Spy.Banker.F предназначен в первую очередь для русскоговорящей аудитории.

Само заражение происходит, когда пользователь Android посещает один из инфицированных сайтов (среди которых встречались колумбийские и чилийские). После этого на планшет или смартфон загружается APK-файл под названием Anketa, а в главном меню появляется значок «Установка». После запуска приложения оно запрашивает разрешения администратора, мотивируя это необходимостью шифрования данных – оно поддерживается в версиях Android 3.0 и выше. Благодаря полученным правам администратора, установленный троян препятствует своему удалению из системы.

После установки Android/Spy.Banker.F передаёт на удалённый сервер номер смартфона, его IMEI, страну проживания, версию операционной системы и многое другое. Также вредоносная программа позволяет злоумышленникам получить логины и пароли от онлайн-банкинга, удалённо управлять заражённым устройством и даже устанавливать другое вредоносное ПО.

Когда пользователь открывает Google Play, троян выводит на экран форму для ввода данных банковской карты. Невнимательный пользователь вполне может перепутать окно с легитимным запросом или ввести аутентификационные данные, чтобы избавиться от всплывающих окон.

Специалисты из ESET рекомендуют соблюдать осторожность при установке мобильных приложений, найденных за пределами Google Play, игнорировать сайты, предлагающие загрузить APK-файлы, и не переходить по подозрительным ссылкам, полученным в SMS или онлайн-мессенджерах (*Мобильный троян атакует устройства пользователей // InternetUA (<http://internetua.com/mobilnii-troyan-atakuet-ustroistva-polzovatelei>). – 2015. – 16.05*).

\*\*\*

Российские хакеры успешно атакуют электронную почту украинских военных, контрразведки, пограничной службы и МВД. РФ использует фишинговые атаки на электронные адреса правительства Украины.

Как информирует Цензор.НЕТ со ссылкой на ZN.UA, об этом пишет Newsweek.

Правительство России, скорее всего, разрабатывает еще более опасный вирус.

«Это вряд ли делают обычные хакеры. Уровень сложности (компьютерных вирусов. – Прим. ред.) является очень высоким. И они (вирусы. – Прим. ред.) хорошо написаны и очень скрытны», – говорит управляющий директор оборонной компании Великобритании BAE Systems Д. Гарфилд.

С 2012 г. российским компьютерным вирусом Snake были заражены десятки компьютеров в правительстве Украины и не менее 10 украинских посольств.

«Сейчас Россия имеет не только информационное превосходство в Украине, но и эффективно контролирует украинские электронные системы», – сообщает Financial Times со ссылкой на аналитиков в разведывательной сфере.

Когда Россия аннексировала Крым, она получила доступ к оперативному центру национальной телефонной компании на полуострове.

И если РФ захочет «выключить» телекоммуникации в Украине, то это будет не сложно.

«Украина не сможет ничего сделать, чтобы помешать этому», – говорит генеральный директор компании в сфере кибербезопасности TAIA Global Д. Карр.

Кибератаки российских хакеров увеличиваются во время активных боевых действий.

В настоящее время Украине необходимо перестроить свои телекоммуникационные системы без использования российских технологий **(РФ ведет против Украины широкомасштабную кибервойну, – Newsweek // Цензор.НЕТ**

**([http://censor.net.ua/news/336529/rf\\_vedet\\_protiv\\_ukrainy\\_shirokomasshtabnuyu\\_kibervoyinu\\_newsweek](http://censor.net.ua/news/336529/rf_vedet_protiv_ukrainy_shirokomasshtabnuyu_kibervoyinu_newsweek)). – 2015. – 18.05).**

\*\*\*

Федеральный резервный банк Сент-Луїса, який входить у структуру Федеральної резервної системи США, що виконує в країні функції центрбанку, піддався атаці хакерів. Кіберзлочинці змогли перенаправити людей, які користувалися деякими інтернет-ресурсами банку, на сайти, які перебували під контролем хакерів.

Про це повідомляє ТАРС із посиланням на газету New York Times.

Як повідомили її журналістам представники фінансового інституту, кіберзлочинцям вдалося протягом деякого часу перенаправляти користувачів, які працювали з окремими інтернет-ресурсами банку, на спеціально створені хакерами сторінки. Атака була проведена у квітні, на сьогодні невідомо, хто стоїть за нею.

Як зазначається, особи, які впровадились у комп'ютерні системи банку, напевно, мають серйозну підготовку. Вони могли отримати цінну інформацію, у тому числі адреси електронної пошти й паролі співробітників фінінститута. Надалі ці відомості можуть бути використані для нових більш витончених атак на інші сайти, які становлять велику важливість.

«Даному проникненню передувала ціла серія хакерських атак на урядові системи, які були здійснені в минулі місяці. Вони торкнулися в тому числі Білого дому, державного департаменту і навіть особистої поштової скриньки президента», – констатує видання.

У понеділок на офіційному сайті Федерального резервного банку Сент-Луїса було опубліковано заяву, у якій людям, які користувались інтернет-ресурсами фінансового інституту, було рекомендовано змінити паролі **(Хакери атакували один з Федеральних резервних банків США, – New York Times //**

*Західна інформаційна корпорація*  
([http://zik.com.ua/ua/news/2015/05/20/hakery\\_atakuvaly\\_odyn\\_z\\_federalnyh\\_rezer\\_vnyh\\_bankiv\\_ssha\\_\\_new\\_york\\_times\\_591258](http://zik.com.ua/ua/news/2015/05/20/hakery_atakuvaly_odyn_z_federalnyh_rezer_vnyh_bankiv_ssha__new_york_times_591258)). – 2015. – 20.05).

\*\*\*

Студенты университета Карнеги-Меллона, США, представили методику автоматического распознавания уязвимых сайтов в Интернете.

Для работы студенты приспособили ряд техник сбора данных и машинного обучения. В ходе испытаний систему проверили на выборке из 444 519 сайтов, содержащих 4 916 203 страницы. Обнаруженные подозрительные сайты часто подвергались взлому в течение последнего года.

Система ведёт постоянный анализ заражённых сайтов, автоматически извлекает характерные признаки и обеспечивает поиск таких же признаков на других ресурсах.

Новая технология позволяет определить с высокой степенью вероятности, с каких сайтов начнётся распространение вредоносных программ в будущем.

Разработка имеет реальную практическую ценность. Например, Google и другие компании тратят много сил на поиск вредоносных сайтов, которые направляют пользователя на опасные ресурсы.

Если реализовать предложенную технологию, подобные вредоносные сайты можно будет обнаруживать ещё до того как их заразили и предупреждать веб-мастеров (*Система автоматического поиска уязвимых сайтов предупредит об опасности заражения // Блог Imena.UA* (<http://www.imena.ua/blog/system-for-bug-web-search/>). – 2015. – 19.05).

\*\*\*

Согласно отчету по безопасности компании Akamai Technologies, в I квартале 2015 г. был установлен рекорд по количеству совершенных DDoS-атак. Число DDoS-атак в первой четверти 2015 г. увеличилось практически в два раза по сравнению с I кварталом 2014 г. Злоумышленники в начале нынешнего года прибегали к DDoS-атакам на 35 % чаще, чем в последнем квартале 2014 г.

Директор по информационной безопасности Akamai Э. Кобрин сообщил, что мощность типичных DDoS-атак в I квартале 2015 г. не превышала 10 Гбит/с, а их продолжительность составляла более чем 24 часа. Эксперты также обнаружили восемь «мега-атак», которые превысили 10 Гбит/с. По словам Э. Кобрина, злоумышленники начали тестирование методов DDoS-атак на IPv6.

Больше всего в I квартале 2015 г. от DDoS-атак пострадал игровой сектор, на который пришлось более 35 % от всех совершенных DDoS-атак. Популярной целью злоумышленников стал протокол SSDP, на долю которого пришлось более 20 % от всех векторов атак. На 22,22 % увеличилось число DDoS-атак на уровне приложений (уровень 7) и на 36,74 % возросло количество атак на уровне инфраструктуры (уровень 3 и 4) (*В первом квартале 2015 года был*

***установлен рекорд по количеству совершенных DDoS-атак // InternetUA (<http://internetua.com/v-pervom-kvartale-2015-goda-bil-ustanovlen-rekord-po-kolicestvu-sovershennih-DDoS-atak>). – 2015. – 21.05).***

\*\*\*

Команда исследователей разработала систему, которая позволит лучше защитить пароли от хакеров. Теперь даже если секретные коды попадут в руки к мошенникам, они не смогут ими воспользоваться.

Ранее все пароли проходили процесс шифрования сразу после попадания в базы данных различных организаций. Специальный алгоритм превращал числовой пароль в хаотичную схему (хэш). Такая система хранения была довольно надежной, прежде чем хакеры не научились конвертировать случайные символы обратно в пароли.

Специальные программы позволяют злоумышленникам обрабатывать большие объемы данных, что ставит под угрозу аккаунты пользователей.

Система ErsatzPasswords добавляет новый уровень защиты – создание поддельного пароля. Перед шифрованием и сохранением в базе, к паролю применяют функцию, генерируемую аппаратным модулем безопасности. Она изменяет пароль таким образом, что даже если хакеры смогут взломать базу и расшифровать хэши, без доступа к модулю безопасности, украденный поддельный пароль будет абсолютно бесполезным (***Поддельные пароли – лучшая защита от хакеров // InternetUA (<http://internetua.com/poddelnie-paroli---lucsshaya-zasxita-ot-hakerov>). – 2015. – 24.05).***

\*\*\*

Эксперты сообщили о новом способе распространения вирусов – они могут быть в рекламной рассылке, которая приходит на электронную почту. Мало того, что пользователей заваливают спамом, но и еще крепят к ним макровирусы – программы, написанные на макроязыках, встроенных в текстовые и графические редакторы, электронные таблицы.

Поэтому письма от неизвестного адресата, также как и подтверждение якобы о проводимом платеже, извещения о штрафе, денежном переводе, электронные билеты не открывать, советуют эксперты. Киберпреступники маскируют свои подделки под официальные письмо с указанием полных контактных данных, логотипов, легитимных ссылок компаний и банков.

Все вредоносные письма содержали вложения с расширением .doc или .xls, при открытии которого запускался скрипт VBA. Этот скрипт загружал и устанавливал в систему другие вредоносные программы, например банковского троянца Cridex, поясняют эксперты.

Еще специалисты по захлапанию вашего почтового ящика в этом году начали заводить целые домены, с которых рассылают спам различного содержания. И они даже заводят домены по теме, но не всегда. Например, в письмах с доменов .work предлагают услуги по ремонту, строительству. Реклама образовательного характера, дистанционного обучения сыпется с



доменов .science, .pink, .red, .black, присылают в рекламу азиатских сайтов знакомств (*Компьютерные вирусы стали крепить к рекламной рассылке // InternetUA (http://internetua.com/kompuaternie-virusi-stali-krepit-k-reklamnoi-rassilke)*). – 2015. – 21.05).

\*\*\*

Microsoft Threat Intelligence Center совместно с компанией FireEye, специализирующейся на защите данных, пресек деятельность хакерской группировки АРТ17, предположительно, спонсируемой китайским правительством.

Известная атаками на предприятия оборонной промышленности, юридические организации, правительственные структуры, технологические компании и компании по добыче полезных ископаемых, АРТ17 использовала сайт TechNet для управления своим командно-контрольным сервером (С&С), пишет PC World.

TechNet – интернет-ресурс Microsoft с высоким трафиком. Он содержит техническую документацию для продуктов корпорации и крупный форум, на котором пользователи могут задавать технические вопросы и получать ответы от специалистов.

Участники группировки АРТ17 – известной также как DeputyDog – создали несколько аккаунтов и оставляли в обсуждениях комментарии с закодированными IP-адресами.

ПК, зараженные трояном Blackcoffee, использовали кодированные записи на сайте Microsoft TechNet, чтобы узнать свежие IP-адреса командных серверов и наладить с ними контакт для получения команд или передачи похищенной из зараженной системы информации.

По словам специалистов FireEye, использование стороннего сайта как канала связи с командным сервером затруднило поиск истинного расположения командно-контрольных серверов и позволило инфраструктуре таких серверов оставаться работоспособной длительное время.

Добавим, что это не первая атака предположительно китайских хакеров, с которой Microsoft столкнулась за последнее время. В январе 2015 г. злоумышленники взломали почтовый сервис Microsoft Outlook. Атака длилась около суток и носила характер «человек посередине» (man in the middle) – когда хакер незаметно вклинивается в линию связи между исходным и конечным пунктом и получает возможность перехватывать данные. Согласно предположению специалистов GreatFire, атака была проведена Китайской администрацией интернет-пространства (Cyberspace Administration of China), отвечающей за интернет-цензуру в государстве (*Сайт Microsoft хакеры использовали для управления трояном // InternetUA (http://internetua.com/sait-Microsoft-hakeri-ispolzovali-dlya-upravleniya-troyanom)*). – 2015. – 21.05).

\*\*\*

Десятки тысяч сайтов, серверов и прочих сервисов глобальной сети под защитой протокола HTTPS оказались уязвимы перед новой атакой, которая позволяет читать и менять проходящие через зашифрованное соединение данные. Из первого миллиона сайтов уязвимость может быть на 8,4 %, среди почтовых серверов с адресами IPv4 это значение ещё выше. Источником угрозы является уязвимость в протоколе TLS, который используется сайтами для установки зашифрованного соединения с пользователями.

Атака под названием Logjam может быть проведена против серверов, использующих алгоритм обмена ключами Диффи-Хеллмана. Он позволяет даже при работе в общедоступном канале создать секретный ключ для установления связи. Уязвимость стала результатом ограничений правительства США на экспорт программного обеспечения, которые были введены в 90-е годы. Их цель состояла в том, чтобы не предоставлять самые передовые системы безопасности другим государствам, не усложняя работу своим спецслужбам.

Злоумышленники с возможностью мониторинга трафика между пользователем и сервером с данным алгоритмом могут внедрять код, который заставляет использовать слабое 512-битное шифрование. То же самое происходит в другой недавней уязвимости под именем FREAK.

Пока защиту от атак Logjam предоставляет только обновлённый браузер Internet Explorer. Исследователи ведут работы с создателями браузеров Chrome, Firefox и Safari, чтобы использовался как минимум 1024-битный ключ ***(Сайты с соединением HTTPS уязвимы перед атакой Logjam // InternetUA (<http://internetua.com/saiti-s-soedineniem-HTTPS-uyazvimi-pered-atakoi-Logjam>). – 2015. – 21.05).***