СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(19.10–1.11)

2015 № 19

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(19.10–1.11)
№ 19

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

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

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Соцсети: основные тренды 2015 года

Hyser приводит последние данные о состоянии и ключевых трендах социальных сетей в этом году. Какие соцсети вошли в наш список? (http://hyser.com.ua/tehnology/socseti-osnonvye-trendy-2015-goda-29972).

Facebook, Twitter и LinkedIn – впереди всех

Опрос почти 4000 маркетологов по всему миру выявил, какие социальные сети они используют для привлечения клиентов. 93 % респондентов применяют Facebook, 79 % от общего числа опрошенных также используют Twitter, а 71 % – LinkedIn.

Pinterest набирает обороты

Этот сервис долгое время считался «женским», однако статистика наглядно показала, что Pinterest – это не только дизайн, еда и женская мода. Его популярность среди мужчин также быстро растет, предлагая много контента, казалось бы даже на самые неожиданные темы. Так, за последний год на 96 % возросло количество пинов, посвященных мужской моде, и на 118 % – посвященных автомобилям и мотоциклам.

Facebook – главная платформа для видео

М. Цукерберг заявил, что вся новостная лента Facebook будет состоять преимущественно из видео уже в ближайшие пять лет. Похоже, ждать осталось совсем недолго: 50 % пользователей Facebook просматривают в ленте как минимум один видеоролик в день. В III квартале 2014 г. эта социальная сеть насчитала 1 млрд просмотров, но эта цифра возросла до 4 млрд за I квартал 2015 г.!

Популярые мессенджеры

Из 10 самых популярных приложений для смартфонов шесть предназначены для отправки сообщений. Они становятся основой повседневного общения, особенно среди молодых пользователей. А вся десятка выглядит так:

1. Facebook
2. Whatsapp
3. Facebook messenger
4. Instagram
5. Line
6. Viber
7. Kakaotalk
8. Clash of Clans
9. Wechat
10. Twitter

Соцсети все более привлекают к себе аудиторию, будучи оперативным источником новостей, познавательного и развлекательного контента ***(Соцсети: основные тренды 2015 года // Hyser (http://hyser.com.ua/tehnology/socseti-osnonvye-trendy-2015-goda-29972). – 2015. – 19.10).***

***

Facebook не хочет, чтобы пользователи уходили из социальной сети. Потому она старательно копирует функции других сервисов и добавляет все новый контент, вроде видео и новостных статей, пишет TechCrunch.

Чем больше времени пользователь проводит в Facebook, тем быстрее она приближается к выполнению своей миссии, озвученной М. Цукербергом – «сделать мир более открытым и усилить связи между людьми». Также социальная сеть зарабатывает больше денег, показывая рекламу. Вот несколько способов, которыми Facebook все больше ассимилирует Интернет и старается всеми силами удерживать пользователей на страницах социальной сети.

Специальная подача видео

Facebook хочет стать видеосервисом, не превращаясь при этом в YouTube, где пользователи сами выбирают, что смотреть. Вместо этого Facebook показывает видео прямо из ленты, при этом о существовании некоторых видео пользователи могли и не предполагать.

Предложенные видео

Впрочем, если пользователь хочет смотреть что-то определенное, Facebook теперь сможет порекомендовать связанные видео, чтобы люди не прекращали процесс просмотра. В мобильном приложении достаточно пролистать страницу, когда первое видео закончилось.

Видео открепляется от ленты новостей

Facebook не хочет, чтобы пользователи заскучали и закрыли видео, не досмотрев его до конца. Потому теперь можно открепить видео от ленты и перетащить его в сторону. После этого можно будет продолжить листать ленту, а видео будет продолжать воспроизводиться сбоку.

Мгновенные статьи

Facebook предзагружает статьи для отображения в ленте мобильного приложения, за счет этого они отображаются практически мгновенно. Таким образом, компания снижает для себя риск того, что, прочитав одну статью, пользователь покинет соцсеть и продолжите чтение уже на сайте издания.

Мгновенная реклама

Та же технология используется и для рекламы. Благодаря предзагрузке в мобильном приложении Facebook можно видеть рекламу без ущерба для скорости загрузки. Компания полагает, что это повышает шансы того, что пользователь кликнет на объявление и принесет Facebook пару долларов.

Функция добавления ссылок

Если нужно что-то написать и добавить к своему сообщению ссылку на какой-либо сайт, то теперь не придется покидать страницу Facebook отправляться в поисковую систему. Теперь строка поиска по ключевым словам есть в мобильном приложении.

Актуальные новостные тренды

Читать газеты теперь не обязательно, так как в Facebook теперь также есть новостные рубрики политики, науки, спорта, развлечений.

Кнопка «Купить» в Facebook

Теперь чтобы что-то приобрести, не обязательно покидать социальную сеть. Кнопка «Купить» позволит совершать платежи прямо из новостной ленты, заполняя данные кредитной карты в форме Facebook.

Лента покупок Facebook

Во время шопинга в Facebook можно не просматривать всю новостную ленту. Можно перейти к просмотру ленты покупок и не отвлекаться от выбора интересующего товара. Само собой, это избавляет от необходимости покидать Facebook.

Поиск товаров и услуг

Своим «Поиском продуктов» Facebook бросает вызов таким компаниям как Google и Amazon. Как и лента новостей, результаты поиска во многом будут зависеть от предпочтений пользователя и его друзей.

Секция покупок на страницах Facebook

Facebook хочет, чтобы ее страницы могли заменить сайт для маленького бизнеса, который практически не имеет другой возможности продвигаться в Интернете. Потому социальная сеть добавила разделы «Магазин» и «Услуги». Теперь небольшие компании могут зарабатывать в Facebook не только лайки, но и деньги.

Функция «В этот день»

Хотите немного поностальгировать? Функция «В этот день» позволяет вам вспомнить важные события, которые произошли в этот день в прошлом и были опубликованы на Facebook. Функция была скопирована из приложения TimeHop.

Новые возможности встроенного графического редактора Facebook

Теперь можно рисовать что-либо поверх фотографий, размещенных в Facebook, как в приложении Snapchat.

Заметки Facebook

Facebook отполировала ранее неудобный раздел «Заметки», сделав его похожим на приложение Medium. С помощью этого раздела пользователь может кратко обновлять статус или создавать большие тексты.

Сервис Facebook Live

Чтобы конкурировать с приложениями Periscope и Meerkat, Facebook запустила собственный сервис потокового видео Live. Но чтобы сервис не был перегружен скучными трансляциями, пока доступ к нему имеют лишь знаменитости.

Группы For Sale («На продажу»)

Функция групп For Sale похожа на Craigslist или другую доску объявлений. Только в данном случае люди имеют возможность торговать с другими пользователями Facebook.

Видеозвонки в Facebook Messenger

Если пользователи уже обмениваются сообщениями через Facebook Messenger, почему бы не использовать также функционал видеовызовов? С новой функцией видеозвонков Facebook Messenger замыкает экосистему Facebook. Теперь социальная сеть может транслировать рекламу буквально везде.

Виртуальный ассистент Facebook M

Виртуальный ассистент Facebook M работает через Messenger и является гибридом искусственного интеллекта вроде Siri или Google Now с сервисом живой помощи. Можно использовать ассистента вместо того, чтобы искать что-то с помощью Google.

Платежи в Messenger

Теперь возможно проводить платежи прямо из Facebook Messenger. Это избавляет от необходимости пользоваться другими платежными сервисами.

Поиск GIF изображений в Messenger

Чтобы удержать пользователей от использования Google или приложения Giphy, Facebook встроила в Messenger собственную поисковую систему для изображений GIF. Кроме того, так компания пытается доказать, что Messenger – больше чем просто приложение для обмена сообщениями ***(20 картинок о том, как Facebook поглощает интернет // iGate (http://igate.com.ua/news/10806-20-kartinok-o-tom-kak-facebook-pogloshhaet-internet). – 2015. – 20.10).***

***

Последняя версия Skype для Windows и Mac, а также веб-версия программы теперь позволяют создавать уникальную ссылку, по которой ваши друзья могут подключиться к вашей видеоконференции. При этом подключиться можно с веб-версии или со смартфона, даже не имея аккаунта в Skype. Эта полезная функция перекочевала в программу из Skype for Business (бывшая Lync).

Возможность генерировать ссылку на конференцию в настоящее время доступна только жителям США и Великобритании, но разработчики собираются очень быстро, всего за пару недель, распространить ее по всему миру. Также в ближайшее время конференции можно будет начинать на iPhone, iPad и Android. По поводу Skype для Windows Mobile – ни слова.

Сообщается, что функцию можно опробовать и в других странах – например, в Канаде. Чтобы начать конференцию, нужно нажать знак «плюса» над списком контактов и скопировать соответствующую ссылку из окна. При этом каждая ссылка уникальна для каждого пользователя ***(Для участия в видеоконференции по Skype теперь не нужна регистрация // iGate (http://igate.com.ua/lenta/10807-dlya-uchastiya-v-videokonferentsii-po-skype-teper-ne-nuzhna-registratsiya). – 2015. – 20.10).***

***

Новое исследование Piper Jaffray может возобновить разговоры об упадке Facebook, по крайней мере в его молодой аудитории. Опрос, проведенный среди подростков в США, показал, что самой любимой социальной сетью среди них является Instagram. Так ответила треть всех опрошенных.

На втором месте идет Twitter, который играет главную роль для 20 % подростков. Затем идет Snapchat с 19 %, и лишь после него – Facebook. Всего 15 % респондентов сказали, что это их самый любимый социальный сайт, причем эта цифра снижается все последние годы.

Конечно, это не означает, что остальные 85 % не пользуются Facebook. У подавляющего большинства из них есть на нем аккаунт, и многие им

пользуются. Однако руководство и акционеров Facebook не может не беспокоить тот факт, что в США уже каждые два подростка из трех откровенно предпочитают Facebook другие соцсети.

Говоря о других социальных сетях, 3 % опрошенных предпочитают Tumblr и по 1 % – Google+ и Pinterest. 8 % входят в категорию «другое», и также интересно, что ответ «не пользуюсь никакими соцсетями» не дал никто. Другими словами, абсолютно все американские подростки «сидят» на том или ином социальном сайте.

В этом исследовании есть как минимум один позитивный момент для Facebook: ей принадлежит Instagram, поэтому с финансовой стороны все пока относительно неплохо.

Впервые вопрос об актуальности Facebook среди молодой аудитории возник в 2013 г., когда руководство Facebook само сообщило инвесторам о небольшом снижении подростковой аудитории. Корневая аудитория сайта становится все старше.

Ряд исследований показывают, что подростки начинают меньше пользоваться Facebook отчасти из-за присутствия там взрослых, в основном их родителей. В этой ситуации «бегство» в Instagram и Snapchat становится для них способом создания некой новой среды, свободной от влияния взрослых ***(Facebook уступает уже трем социальным сетям по популярности среди американских подростков // InternetUA (http://internetua.com/Facebook-ustupaet-uje-trem-socialnim-setyam-po-populyarnosti-sredi-amerikanskih-podrostkov). – 2015. – 20.10).***

***

Социальная сеть Twitter объявила о запуске новой функции – возможности создавать опросы. В ближайшие дни она станет доступна пользователям приложений Twitter на всех платформах – iOs, Android и десктопной версии Twitter.com. До сегодняшнего дня узнать мнение пользователей в Twitter можно было несколькими способами: задать подписчикам вопрос и отслеживать их ответы, попросить их проголосовать, сделав ретвит или добавив твит в избранное, или же подсчитывать хэштеги, обозначающие варианты ответа на вопрос.

Теперь выяснить мнение подписчиков в Twitter по тому или иному вопросу станет еще проще. Новая функция позволяет любому пользователю в несколько кликов создать опрос, состоящий из двух вариантов ответов. Голосование будет происходить в течение 24 часов. После его завершения все принявшие участие в опросе пользователи получат уведомление об этом и смогут узнать итоговые результаты. Пользователи Twitter могут участвовать в любых вопросах без каких-либо ограничений. Во всех случаях голосование будет анонимным ***(Twitter введет опросы // Marketing Media Review (http://mmr.ua/show/twitter_vvedet_oprosy). – 2015. – 21.10).***

***

Facebook запустила новый формат публикаций СМИ «мгновенные статьи» для всех пользователей iOS-устройств. Компания также объявила о

запуске бета-версии этого функционала для устройств Android. По словам директора по продуктам Facebook К. Кокса, теперь через «мгновенные статьи» в социальной сети ежедневно будут размещаться тысячи публикаций СМИ. Об этом пишет searchengines.ru

Facebook также снова расширила число партнёров, принимающих участие в этой программе. Теперь к ним присоединились Vox Media, Slate, The Huffington Post и The Daily Mail. Интерес издателей вызван значительным трафиком, который Facebook направляет к их сайтам.

По словам К. Кокса, «мгновенные статьи» загружаются в 10 раз быстрее, чем обычные. Кроме того, ими чаще делятся пользователи. Те публикации, которые получают больше всего перепостов, обычно ранжируются в новостной ленте выше.

Среди изданий, которые согласились поддерживать новый формат, значатся: Billboard, Billy Penn, The Blaze, Bleacher Report, Breitbart, Brit + Co, Business Insider, Bustle, CBS News, CBS Sports, CNET, Complex, Country Living, Cracked, Daily Dot, E! News, Elite Daily, Entertainment Weekly, Gannett, Good Housekeeping, Fox Sports, Harper's Bazaar, Hollywood Life, Hollywood Reporter, IJ Review, Little Things, Mashable, Mental Floss, mindbodygreen, MLB, MoviePilot, NBA, NY Post, The Onion, Opposing Views, People,Pop Sugar, Rare, Refinery 29, Rolling Stone, Seventeen, TIME, Uproxx, US Magazine, USA Today, Variety, The Verge и The Weather Channel.

«Мгновенные статьи» помечаются в новостной ленте иконкой в виде молнии. Увидеть такие публикации можно, подписавшись на указанные выше издания, или же если статьей поделился кто-то из друзей пользователя. Помимо ускоренной загрузки, «мгновенные статьи» также могут включать различные визуальные элементы, такие как 3D-карты и панорамные фотоснимки, которые можно рассмотреть, наклоняя смартфон.

Напомним, что Facebook начала публикацию статей и видеороликов ведущих изданий посредством новой функции «мгновенные статьи» в мае этого года. Запуск нового функционала был призван ускорить загрузку мобильных страниц публикаций СМИ. Партнёрами по запуску выступили девять медиаиздателей: The New York Times, National Geographic, BuzzFeed, NBC, The Atlantic, The Guardian, BBC News, Spiegel и Bild. На момент запуска «мгновенные статьи» были доступны только ограниченному числу пользователей приложения Facebook для iPhone.

В сентябре Facebook дала доступ к функционалу «мгновенных статей» ещё 21 партнёру, в числе которых известные онлайн-издания и медиакомпании. Социальная сеть также начала показывать оптимизированные под мобильные устройства материалы большему количеству пользователей.

Кроме того, в этом месяце Google запустил конкурирующий проект Accelerated Mobile Pages, призванный улучшить мобильный интернет. Основу проекта составляет принципиально новый формат открытого типа AMP HTML. Благодаря ему, разработчики теперь могут с лёгкостью создавать облегчённые версии стандартных веб-страниц. Представители поисковой системы обещают, что со временем технология будет развиваться и начнёт применяться и в других сервисах Google – к примеру, в Google Новостях ***(Facebook запустил***

«мгновенные статьи» для всех пользователей iOS // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45059/118/lang,ru/?period=1). – 2015. – 21.10).

***

Instagram представил приложение для создания зацикленных видео. Новое приложение Boomerang позволяет создавать зацикленные видео длинной в 1 секунду. Видео проигрываются вперед и назад, создавая смешные эффекты. Интерфейс приложения очень прост: у пользователя только две кнопки, одна для снимка, другая для выбора между двумя камерами.

Созданным видео можно поделиться в Facebook и Instagram, а также в других сетях ***(Instagram представил приложение для создания зацикленных видео // Marketing Media Review (http://mmr.ua/show/instagram_predstavil_prilozhenie_dlya_sozdaniya_zatsiklennyh_video). – 2015. – 22.10).***

***

Компанія Facebook оголосила про розширення можливостей пошуку із соціальної мережі, тепер він буде охоплювати більше 2 трлн публікацій.

Про це повідомили в прес-службі фірми, передає Еспресо.TV.

Завдяки новим можливостям, починаючи з 23 жовтня, пошук буде проводитися не тільки по вподобаним сторінкам і профілям друзів, але і по всім нотаткам, опублікованим у соціальній мережі.

«Ми змінили пошукову систему Facebook так, що тепер користувачі зможуть дізнатися, що весь світ думає про теми, які їх цікавлять, не обмежуючись думками лише їхніх друзів та членів родини», – ідеться в повідомленні.

Новий тип пошуку доступний лише для користувачів зі США ***(Facebook розширив пошук до 2 трлн публікацій // Espreso.tv (http://espreso.tv/news/2015/10/23/facebook_rozshyryv_poshuk_do_2_trln_publikaciy). – 2015. – 23.10).***

***

Facebook обновила свое приложение для iOS, исправив проблему с быстрым разрядом аккумулятора мобильных устройств, на которых оно запущено. Об этом в своем аккаунте в соцсети сообщил главный инженер компании А. Грант.

«Мы получили несколько сообщений о проблемах с батареей при использовании приложения Facebook для iOS и занялись поисками источника неисправности. Мы исправили несколько моментов и добавили пару улучшений – они будут доступны в последней версии», – пояснил он.

А. Грант уточнил, что проблемы касались работы центрального процессора, управления аудиосессией при воспроизведении видео (этот процесс выполнялся и после просмотра видео или прослушивания музыки), а также истории посещенных мест. Он принес извинения за доставленные неудобства и пообещал продолжить работу над энергоэффективностью

мобильного приложения ***(Facebook исправил проблему быстрой разрядки iPhone своим приложением // InternetUA (http://internetua.com/Facebook-ispravil-problemu-bistroi-razryadki-iPhone-svoim-prilojeniem). – 2015. – 23.10).***

***

Бум на патриотические соцсети в Украине продолжается. Встречайте севис микроблогов BoxY, который очень напоминает старый-добрый Twitter. С той лишь разницей, что помимо стандартных прелестей в нем также можно размещаться музыку с SoundCloud и видео с YouTube и Vimeo – администрация не хочет, чтобы на сайте нарушали авторские права. В сервисе также есть игры, а размер сообщений ограничен 750 символами, пишет AIN.UA (http://ain.ua/2015/10/25/611624).

«BoxY – это социальная сеть, которая позволяет каждому человеку создать свой микроблог, общаться с друзьями, делиться впечатлениями, заниматься саморазвитием и многое другое. Наш сайт был разработан в первую очередь для украинцев», – говорится в описании проекта.

Изначально авторы хотели назвать сеть «Ласточка» в честь птицы, которая «символизирует весну, добро, счастье и возрождения». Однако на финальной стадии разработки решили изменить имя проекта на BoxY (от английского слова ящик). «Потому что наш сайт является ящиком, где будут храниться сообщения, воспоминания, переживания, радость и другие яркие моменты из жизни наших пользователей», – пишут создатели.

В BoxY можно зарегистрироваться через другие популярные соцсети, в частности Facebook и Twitter. Пользователь может настраивать дизайн интерфейса под себя, менять обложку и аватар профиля. Примечательно, что в сервисе есть жизнь. Как и в Twitter, здесь есть тренды, рекомендации и другие возможности. Пользователей можно фоловить, делать репосты их записей и оставлять комментарии.

Сайт адаптирован под различные устройства и доступен на украинском и русском языках. Русский авторы проекта решили добавить, чтобы избежать спекуляций на языковую тему. «Каждый человек имеет право свободно общаться на том языке, на котором ему хочется. В то же время знать родной язык, как и историю, крайне необходимо, потому что “позабывшие прошлое – не имеют будущего”», – говорится в описании проекта.

Основатели отмечают, что на сегодняшний день у проекта нет спонсора, и команда не получает доходов. Зарабатывать планируют на размещении рекламы, также готовы принимать пожертвования от небезразличных пользователей.

Напомним, ранее в уанете появился еще один украинский аналог Twitter – Zozu.org. Посты в нем также были ограничены 140 символами, но назывались они «зозульками». Впрочем, на сегодняшний день сайт не работает, а домен не занят ***(В уанете появилась очередная украинская соцсеть BoxY – сервис микроблогов с музыкой и видео // AIN.UA (http://ain.ua/2015/10/25/611624). – 2015. – 25.10).***

***

Facebook расширила возможности уведомлений

Команда разработчиков Facebook рассказала о новой функциональности, которая начала внедряться в мобильный клиент социальной сети. В мобильном приложении Facebook существенно расширена вкладка уведомлений.

Вкладка настраиваемая и может включать дни рождения друзей и другие даты и события, результаты спортивных состязаний и напоминания о ТВ-шоу на основе страниц, залайканных пользователем, фильмы в кинотеатрах поблизости, а также другую информацию. Во многом принцип похож на работу сервиса Google Now.

Новая опция начала постепенно внедряться в приложение Facebook под Android и iOS для пользователей из США ***(Facebook расширил возможности уведомлений // Ultramir.net (http://ultramir.net/techno/28140-facebook-rasshiril-vozmozhnosti-uvedomleniy.html). – 2015. – 28.10).***

***

Останній квартальний звіт про доходи Twitter показав, які проблеми платформа відчуває у сфері додавання нових користувачів. Наприкінці вересня загальна аудиторія соціальної мережі становила 307 млн активних учасників, що всього лише на 3 млн більше, ніж три місяці тому – збільшення на 2 %.

Кількість користувачів у США – найпривабливіша аудиторія для рекламодавців – залишилася такою ж і становила 66 млн із початку року.

Поки Twitter залишається популярним серед знаменитостей і ЗМІ, однак соціальна мережа не змогла отримати масову підтримку на ринку, яка, наприклад, зробила компанію Facebook такою всюдисущою ***(В Twitter'і вже другий квартал поспіль не з'являються нові користувачі // Bublbe.com (http://bublbe.com/ua/ekonomika-i-biznes/10569-v-twitter-i-vzhe-druhyi-kvartal-pospil-ne-z-iavliaiutsia-novi-korystuvachi). – 2015. – 28.10).***

***

Facebook запустила новую опцию «Запрос на сообщение» в Messenger. Об этом написал глава бизнеса по обмену сообщениями Д. Маркус на своей странице в соцсети.

Теперь пользователи Messenger смогут связаться и начать общение с любым человеком, который не входит в их сеть контактов в социальной сети. Для этого не нужно знать его номер телефона, достаточно лишь имени.

Ранее сообщения от пользователей, которые не входят в круг друзей пользователя, отправлялись в папку «Другое», доступную только в веб-версии Facebook. Теперь папка «Другое» будет удалена, а каждое сообщение от стороннего контакта станет запросом на общение без добавления в список друзей.

«Запрос на сообщение» можно будет отклонять без прочтения. При этом его отправитель не узнает, был он прочитан или нет ***(В Facebook Messenger теперь можно общаться с незнакомыми людьми // IGate (http://igate.com.ua/lenta/11032-v-facebook-messenger-teper-mozhno-obshhatsya-s-neznakomymi-lyudmi). – 2015. – 30.10).***

***

Как выглядит украинская аудитория Instagram

В связи с тем, что с осени этого года украинские компании могут размещать рекламу в соцсети Instagram, рекламный реселлер Admixer опубликовал подробную инфографику о том где живет, что любит и на каком языке говорит украинский пользователь Instagram.

Согласно данным исследования, общее количество зарегистрированных пользователей Instagram в Украине составляет 830 тыс. В географическом плане лидирующие позиции занимают Днепропетровская, Львовская, Одесская и Харьковская области, а также Киев.

Ядро аудитории формируют женщины 25–34 лет, интересующиеся покупками и модой, технологиями, собственными хобби и многим другим. Молодые семьи с маленькими детьми – самая массовая группа украинских пользователей по критерию семейного положения.

Подавляющее большинство пользователей из Украины интересуются тематикой бизнеса и индустрии. Второе место отошло развлечениям, тройку лидеров замыкают покупки и мода. Среди прочих интересов пользователей: хобби и увлечения, семья, еда и напитки и пр. Чаще всего украинцы публикуют фотографии в Instagram с устройств Apple.

Зарабатывать в Instagram могут не только компании, но и самые обычные пользователи ***(Как выглядит украинская аудитория Instagram – статистика от Admixer // Блог Imena.UA (http://www.imena.ua/blog/ua-instagram-infograph/). – 2015. – 29.10).***

***

За последние полгода после сделки с Google органический десктопный поисковый трафик Twitter возрос на 20 %, сообщается в отчете SimilarWeb. По оценкам аналитиков компании, эта цифра равна дополнительным 35 млн переходов в месяц. Google начал индексировать твиты в режиме реального времени в мае 2015 г.

Интересно, что Google индексировал всего 3 % всех публичных твитов. Однако даже такой небольшой объем индексации был достаточен для значимого увеличения поискового трафика. По данным SimilarWeb, максимальный прирост поискового трафика наблюдался в период с июня по июль 2015 г. За это время трафик возрос на 15 %, что равно примерно 25 млн переходов. Кроме того, увеличилось число людей, которые остаются в Twitter после перехода из Google.

Отметим, что несмотря на рост поискового трафика, сделка с Google не привела к увеличению числа новых пользователей Twitter ***(Отображение твитов в результатах поиска Google помогло Twitter увеличить посещаемость // IGate (http://igate.com.ua/lenta/11028-otobrazhenie-tvitov-v-rezultatah-poiska-google-pomoglo-twitter-uvelichit-poseshhaemost). – 2015. – 29.10).***

***

Carplanet.com.ua – так назвали нову соціальну мережу, створену в Україні для автомобілістів

Українські автомобільні фани отримали новий майданчик для віртуального спілкування. Соціальна мережа carplanet.com.ua надає місце не тільки для форуму і обміну новинами, але і для декількох корисних сервісів – продажі автомобілів, пошуку запчастин, допомоги мандрівникам. У живому спілкуванні онлайн власники машин різних марок зможуть спільно розв'язувати свої технічні проблеми, ділитися досвідом діагностики й ремонту, фотографіями цікавих місць, відвіданих за участю свого улюбленого залізного друга.

Також Carplanet напевно допоможе об'єднатися і стати більш згуртованими членам клубів різних марок, що проживають у відокремлених один від одного регіонах нашої такої немаленької країни.

Але звичайно ж головною, центровою на Carplanet буде сторінка «П'єдестал», де кожен зможе представити свій автомобіль на суд публіки, щоб отримати свою порцію захоплених лайків і здорової, предметної критики. Частина сторінок сайту доступна користувачам без реєстрації. Якщо судити за анкетами постійних відвідувачів, Carplanet уже почав формувати навколо себе співтовариство українських громадян, що володіють автомобілями самих різних брендів. В абсолютній більшості це – молодь, що обіцяє carplanet.com.ua велике і світле майбутнє.

На сьогодні портал уже наповнюється інформацією – новинами, повідомленнями, оголошеннями про продаж – одним словом, автомобілями ***(Нова соціальна мережа для автофанів з'явилася в Україні // АВТОпалац (http://autopalace.com.ua/news/podiji/nova-sotsialna-merezha-dlya-avtofaniv-z-yavylasya-v-ukrajini/). – 2015. – 21.10).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Активисты провели 19 октября Twitter-шторм с хештегом #CrimeaIsUkraine, чтобы напомнить об украинском Крыме. Об этом информирует VIDIA со ссылкой на Facebook-страницу акции.

Как отмечается в сообщении, онлайн-акция связана с тем, что французские и британские издательства недавно опубликовали учебные пособия с Крымом в составе России, рассказали организаторы. Такой атлас мира выпустило французское издательство Larousse, а британское Oxford University Press подготовило учебник, где полуостров обозначен как российский.

«Похоже, они забыли о том, что в марте 2014 г. Крым был незаконно аннексирован Россией путем нелегитимного "референдума", который состоялся

благодаря российским сапогам на украинской земле. Так же Франция и Великобритания забыли об их обязанности защищать украинскую территориальную целостность в соответствии с Будапештскимо меморандумом 1994 г.», – говорится в сообщении.

Организаторы призывали, используя хештег #CrimeaIsUkraine, напомнить «этим прежде надежным издательствам о резолюции ООН 68/262, в которой Великобритания и Франция вместе с сотней других стран четко заявляют, что Крым – это Украина».

Добавим, что Посольство Украины в Великобритании после инцидента призвало издательство Oxford University Press исправить ошибку в своем учебнике. А официальный представитель МИД Франции Р. Надаль, комментируя выпуск издательством Larousse некорректного атласа, заявил, что Франция не признает незаконной аннексию Крыма, говорится в сообщении ***(Активисты провели акцию твиттер-шторма, напомнив миру, что Крым – это Украина // «ОстроВ» (http://www.ostro.org/general/world/news/483765/). – 2015. – 19.10).***

***

Радник голови Дніпропетровської облдержадміністрації Д. Дубілет на своїй сторінці в соцмережі Facebook запустив опитування, для визначення п'яти адміністративних послуг, які стануть електронними і будуть доступними на сайті https://igov.org.ua/.

Такий підхід для Дніпропетровщини – не новий. Півроку тому на подібному голосуванні визначили, які адмінпослуги першими перейдуть у мережу Інтернет. Це реєстрація авто в МРЕВ, отримання закордонного паспорта і довідки про доходи, реєстрація місця проживання та даних ПП або юридичної особи. На сьогодні всі ці послуги доступні на сайті iGov.

Мешканці Дніпропетровщини вже користуються 51 електронною послугою. Ще 40 перейдуть в онлайн найближчим часом ***(Які ще послуги перейдуть в он-лайн – вирішать мешканці Дніпропетровщини // Дніпропетровська ОДА (http://www.adm.dp.ua/OBLADM/obldp.nsf/document.xsp?id=EAC98A52EC0E2E9AC2257EE3002FB40B). – 2015. – 19.10).***

***

Більшість згадок українських олігархів у соцмережах має характер репостів матеріалів онлайн-ЗМІ.

У період з 1 липня 2014 по 31 червня 2015 р. найчастіше в соціальних мережах згадувалися такі акціонери найбільших вітчизняних ФПГ як П. Порошенко (більше 820 тис. згадувань), І. Коломойський (більше 302 тис.), Д. Фірташ (більше 95 тис.), С. Тарута (майже 47 тис.) і В. Пінчук (майже 32 тис.). Про такі результати дослідження, проведеного в цей період за допомогою YouScan в Facebook, Twitter, VKontakte, Odnoklassniki, LiveJournal, Google Plus, Instagram, а також на інших соціально-медійних майданчиках, пише керуючий партнер TLFRD М. Стародубська у свіжому номері MMR.

За її даними, найчастіше українські олігархи згадувалися у Twitter, LiveJournal і Facebook. Нейтральні згадки становлять від 36 % у В. Пінчука до 51 % у В. Нусенкіса. Негативні – від 22 % у К. Жеваго до 39 % у В. Новинського. Нарешті, позитивні – від 17 % у В. Нусенкіса до 37 % у В. Антонова.

Більшість згадок українських олігархів у соцмережах має характер репоста матеріалів онлайн-ЗМІ. Найвища частка авторських постів у дослідженому періоді була зафіксована по Д. Фірташу (28 %), С. Таруті (24,5 %), Р. Ахметову (23,9 %) і І. Коломойському (21,1 %). А ось по О. Мкртчану та В. Антонову (по 1,1 %) такий контент практично відсутній ***(У Вадима Новинського найогидніша репутація серед українських олігархів в соціальних мережах // Espreso.tv (http://espreso.tv/news/2015/10/23/u_vadyma_novynskogo_samaya_otvratytelnaya_reputacyya_sredy_ukraynskykh_olygarkhov_v_socyalnykh_setyakh). – 2015. – 23.10).***

***

Министерство иностранных дел Финляндии использует возможности Facebook для борьбы с наплывом мигрантов, сообщает Yle.

Ведомство развернуло кампанию в социальной сети, информирующую об ужесточенных правилах предоставления убежища в Финляндии. Цель кампании – сократить число приезжающих в Финляндию просителей убежища.

По информации МИДа, охват кампании уже достиг порядка 100 тыс. человек.

Как сообщили в парламентской фракции «Истинных финнов», объявления написаны на арабском языке, целевой аудиторией являются молодые люди, планирующие поездку для получения убежища.

Глава фракции С. Терхо убежден, что правдивая информация о шансах получить убежище в Финляндии отвечает интересам как потенциальных беженцев, так и государства. «Зачем тратить 10 тыс. евро на поездку, если депортация обратно почти гарантирована», – заявил он ***(В Финляндии борются с мигрантами с помощью Facebook // InternetUA (http://internetua.com/v-finlyandii-boruatsya-s-migrantami-s-pomosxua-Facebook). – 2015. – 25.10).***

***

Google создал сервис для беженцев, который позволяет им быстро узнать главную информацию о стране, в которую они бежали.

Поисковый гигант презентовал сайт Crisis Info Hub, где мигранты имеют легкий доступ к важной информации о жилье, медицинских учреждениях и транспортных маршрутах, пишет Engadget, информирует news.eizvestia.com (http://news.eizvestia.com/news_technology/full/536-google-anonsiroval-servis-dlya-bezhencev).

Воспользоваться услугой мигранты могут через смартфон.

Помимо нового сервиса, корпорация ищет добровольцев для улучшения работы Google переводчика (Translate), который очень полезен для беженцев в

другой стране. «Если вы говорите на немецком или арабском и готовы протянуть руку помощи, обращайтесь на страницу Translate Community корпорации Google», – отметили в издании ***(Google анонсировал сервис для беженцев // Экономические известия (http://news.eizvestia.com/news_technology/full/536-google-anonsiroval-servis-dlya-bezhencev). – 2015. – 27.10).***

***

На странице «Типичная Макеевка» в социальной сети провели опрос среди жителей ДНР о том, довольны ли они жизнью: 54,2 % респондентов проголосовали за ответ «Я только за Донбасс в составе Украины. Иначе никак».

13,9 % проголосовавших отметили, что ожидали большего и за полтора года (с оккупационными властями – НБН) мнение начинает меняться.

В то же время 10,4 % жителей ответили, что изменили мнение о ДНР и категорически против такой жизни.

Стоит отметить, 18 % все еще верят в «республику» и считают, что «сейчас туго, но надо немножко подождать». Еще 3,5 % ответивших считают, что в ДНР «все прекрасно, все лучше, чем хотелось».

Как сообщал НБН, недовольство жизнью в ДНР также растет среди боевиков. Наемники недовольны невыплатами зарплаты и запретом открывать огонь ***(На паблике ДНР в соцсети более 54 % проголосовали за Донбасс в составе Украины // Независимое Бюро Новостей (http://nbnews.com.ua/ru/news/164375/). – 2015. – 26.10).***

***

«Соціальні мережі – найефективніший механізм взаємодії», – Єлизавета Масляк

Про секрети успішної волонтерської діяльності, поразки і перемоги, про героїчні будні волонтерів «Київ 1» поспілкувався з волонтеркою і чудовою, світлою людиною Є. Масляк.

Так, на запитання про найбільш дієвий механізм діяльності волонтерів, Є. Масляк відповіла таким чином: «Волонтерів, які регулярно пишуть у соціальних мережах про потреби поранених, моніторять журналісти. ЗМІ самі обирають, про які випадки варто написати. Соціальні мережі – це найбільш ефективний механізм взаємодії.

При цьому не варто забувати про комунікацію як з волонтерами, так із людьми з різних регіонів, які хочуть допомогти. На жаль, на телебаченні про поранених говорять усе менше, але коли звертаєшся з проханням розповісти про бійців, яким потрібні кошти для лікування, погоджуються з задоволенням. Зрозумійте, усі зайняті своїми справами, у всіх своє життя, проблеми і радощі. І це нормально. Що подає телебачення – те люди й сприймають. Деколи буває затишшя, коли в ЗМІ немає повідомлень про поранених, тоді люди думають, що поранених і немає. А насправді практично кожних два тижні привозять дуже багато нових хлопців на лікування.

Я вважаю, що на ТБ варто створити окремі рубрики, не просто розповідати історії поранених, а вирішувати, як “закрити” ті чи інші проблеми,

як можна отримати вичерпну інформацію і т. д. Систематизувати всі дані, потреби і проблеми АТО, адже точково допомагати уже недостатньо. Не забуваймо іще про один аспект: є багато військових, які ніколи не зізнаються, що їм щось потрібно. От з такими "проблемними" людьми потрібно працювати дуже обережно, залучати психологів» ***(«Соціальні мережі – найефективніший механізм взаємодії», – Єлизавета Масляк // Київ 1 (http://kyiv1.org/news/socialni-meregi-najefektivnishij-mehanizm-vzaemo-043415/). – 2015. – 21.10).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Новое исследование Socialbakers выявило, что только 3 % постов – рекламные в ленте Facebook. Хотя в это сложно поверить, беря во внимание прошлогодний доход от рекламы сети в 11,5 млрд дол. Исследование не учитывало мобильную рекламу и рекламные посты, размещенные справа. По данным Socialbakers, 24–29 % ленты составляет контент страниц, принадлежащих компаниям, знаменитостям, публичным личностям и организациям. Чем меньше страниц лайкнет пользователь, тем больше спонсируемых постов он увидит. Около 10 % постов являются спонсируемыми (но 97 % контента, который пользователь видит в своей ленте, органический). В 2013 г. Socialbakers обнаружили, что страницы брендов получали больше взаимодействий (лайков, шейров и комментариев), но теперь пользователи в три раза активней взаимодействуют с контентом страниц медиа компаний и издателей. Компания также заметила, что если второй пост в ленте не является постом страницы, то возможно, он был платным (46 %). Далее в ленте почти каждый пятый пост является постом страницы ***(Пользователи активней взаимодействуют со страницами медиа, чем брендов // Marketing Media Review (http://mmr.ua/show/polyzovateli_aktivney_vzaimodeystvuyut_so_stranitsami_media__chem_brendov_). – 2015. – 20.10).***

***

Ряд лондонських банків вводить нову систему, згідно з якою для підтвердження особи клієнти повинні робити селфі.

Про це повідомляє Еспресо.TV із посиланням на Daily Mail.

Розробник з Нью-Йорка створив програмне забезпечення Percieve, яке використовує біометричні дані для виявлення випадків шахрайства.

Програма аналізує отримане зображення, щоб переконатися в особистості клієнта. Як додаткову перевірку вона також порівнює отриманий знімок з фотографіями з таких соціальних мереж, як Facebook, Twitter і LinkedIn. Після закінчення перевірки система або схвалює платіж, або видає повідомлення про спробу шахрайства.

Повідомляється, що кілька великих банків Лондона збираються почати використовувати бета-версію існуючої програми, однак жоден з них поки не

заявив про це публічно. Рішення перейти на нову систему пов'язано з тим, що за останній рік було зафіксовано близько 5 млн випадків онлайн-шахрайства.

Раніше компанія Mastercard заявляла про те, що планує запустити технологію Selfie Pay, яка порівнює тільки що зроблене Селфі з уже існуючими збереженими знімками ***(Лондонські банки хочуть підтверджувати особистість клієнтів за допомогою селфі // Espreso.tv (http://espreso.tv/news/2015/10/20/londonski_banky_khochut_pidtverdzhuvaty_osobystist_kliyentiv_za_dopomogoyu_selfi). – 2015. – 20.10).***

***

Согласно новому исследованию eMarketer, Facebook названа самой эффективной социальной сетью руководителями отрасли. Топы 29 компаний назвали три крупнейшие социальные платформы – Facebook, LinkedIn и Twitter и три новых – Instagram, Pinterest и Snapchat среди серии категорий, таких как креативные возможности, рекламный таргетинг, измерения и ROI. Респонденты отметили Facebook топ платформой в рамках возможностей для таргетинга и измерения эффективности ROI. Однако сеть еще не обошла YouTube по эффективности видеорекламы. Оба канала получили отметку B+. Instagram получил высшую отметку за креативность, вовлечение и формирование осведомленности о бренде, и низкие оценки за измерения, ROI и стимул к действию. А Pinterest получил высокие оценки в большинстве категорий, кроме возможностей для измерений и рекламного таргетинга ***(Facebook назван самой эффективной рекламной платформой // Marketing Media Review (http://mmr.ua/show/facebook_nazvan_samoy_effektivnoy_reklamnoy_platformoy). – 2015. – 21.10).***

***

YouTube представил платный сервис без рекламы YouTube Red. Новая версия доступна за 9,99 дол. в месяц для ПК и Android, и за 12,99 дол. – для iOS. Со временем, канал планирует запустить эксклюзивный контент на YouTube Red, который нельзя будет посмотреть на традиционном сайте. Это будут новые шоу с популярными звездами YouTube, включая PewDiePie, Joey Graceffa, Toby Turner и MatPat. Подписка будет доступной с 28 октября вместе с бесплатной 30-дневной версией. Канал решился на платный контент ввиду конкуренции в лице сервиса потокового видео Netflix, у которого 69 млн платных подписчиков благодаря популярным оригинальным сериалам, и в лице Facebook, которая активно продвигает видео в ленте. Канал поделится с создателями видео своим доходом, исходя из количества «времени просмотра». То есть создатели длинных видео могут заработать больше. Сервис будет запущен в США, а затем и на других рынках в течение года ***(YouTube представил платный сервис без рекламы «YouTube Red» // Marketing Media Review (http://mmr.ua/show/youtube_predstavil_platnyy_servis_bez_reklamy_youtube_red). – 2015. – 22.10).***

***

«ВКонтакте» запускает тестирование нового сервиса, который позволит пользователям отправлять личные сообщения сообществам, а администраторам – ответ от имени их групп. Об этом рассказал руководитель отдела B2B-маркетинга компании А. Усманов на конференции RIW 2015 в Москве.

По мнению представителей компании, новый сервис сделает более эффективной коммуникацию между клиентами и брендами. Те организации, которые начнут использовать функцию, получат преимущество над своими конкурентами и получат лояльность клиентов, считают во «ВКонтакте». В компании также ожидают, что сервис будет востребован среди органов государственной власти и представителей шоу-бизнеса.

Пока идет закрытое тестирование нововведения. Некоторые отобранные группы и публичные страницы уже начали знакомство с функцией, например, Tele2, Yota, Adidas и ASOS. Сейчас ей уже можно пользоваться в приложениях для iOS и Android, а также в мобильной и полной версиях сайта. В компании обещают скоро запустить обновление для Windows Phone.

В личных сообщениях между пользователем и сообществом доступен обмен изображениями, документами, аудиозаписями, видео и геолокацией, как и в обычных диалогах. Сообщения пользователей смогут увидеть создатели и администраторы сообществ, модераторам они будут недоступны.

Точную дату запуска функции для всех сообществ пока не объявили. Она начнет работать после тестирования на разных сегментах рынка ***(«ВКонтакте» тестирует сервис личных сообщений для сообществ // IGate (http://igate.com.ua/lenta/10857-vkontakte-testiruet-servis-lichnyh-soobshhenij-dlya-soobshhestv). – 2015. – 22.10).***

***

Социальная сеть «Одноклассники» запускает новый инструмент для размещения нативной видеорекламы. Об этом рассказал представитель социальной сети С. Боярский на конференции Russian Interactive Week 2015, пишет searchengines.ru

Нативное видео очень схоже с запущенными недавно в «Одноклассниках» промопостами – размещается в обычной ленте пользователя через myTarget. Основным отличием является наличие специализированной статистики, позволяющей рекламодателю видеть, какую именно часть видео просмотрел пользователь, как часто ставил ролик на пузу, использовался ли при просмотре полноэкранный режим и т. д.

В настоящее время для формата тестируется автозапуск видео. Официальный релиз с результатами теста ожидается в ноябре.

«“Одноклассники” стали первой соцсетью, которая запустила нативный формат видеорекламы. Протестировать формат можно уже сейчас из рекламного кабинета myTarget. Видеоролик можно таргетировать на нужную аудиторию. Если креатив будет хорошим, то видео станет виральным», – комментирует запуск пресс-секретарь социальной сети А. Жбанова.

Напомним, «Одноклассники» запустили функционал продвигаемых промопостов в новостных лентах пользователей в сентябре 2015 г. Для рекламного поста можно устанавливать нужный таргетинг, в котором доступны

256 параметров, включая возраст, пол, интересы, локацию, доход, а оформлен он может быть в разных, привычных для пользователей сети форматах: в виде заметки с прикрепленным опросом, музыкальной дорожкой, фотографией или галереей снимков ***(Одноклассники запускают нативную видеорекламу // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45069/118/lang,ru/). – 2015. – 22.10).***

***

Twitter представит первую рекламу для функции Moments.

Функция, которая дебютировала две недели назад в качестве инструмента для отслеживания событий в реальном времени, получила первого рекламодателя. Twitter даст рекламодателям канал в «Моментах» на 24 часа, где они смогут курировать твиты, видео и другой контент. И первым рекламным «Моментом» на этих выходных станет фильм «Крид». Продвигаемые «Моменты» отлично вписываются в тренд нативной рекламы, ведь они создают продвигаемый контент, который не выглядит как прямая реклама. «Продвигаемые “Моменты” выглядят так же, как и обычные “Моменты”, кроме того факта, что их создают бренды, а не простые пользователи», – рассказал М. Дерелла, вице-президент Twitter по доходам в Северной Америке ***(Twitter представит первую рекламу для функции Moments // Marketing Media Review (http://mmr.ua/show/twitter_predstavit_pervuyu_reklamu_dlya_funktsii_moments). – 2015. – 24.10).***

***

Twitter запустил инструмент социального мониторинга и аналитики для брендов – Brand Hub. Новый функционал позволит компаниям в одном месте получать статистику по трендам доли рекламного воздействия (share of voice) и узнавать, что люди говорят об их брендах в Twitter. Об этом пишет searchengines.ru

Многие крупные бренды уже используют различные сторонние инструменты аналитики социальных медиа, чтобы определить долю рекламного воздействия, настроение аудитории и другие социальные сигналы. Brand Hub в Twitter – это расширение существующего набора аналитических инструментов для рекламодателей. Ведущее место в новом функционале занимает метрика TrueVoice.

TrueVoice

Метрика TrueVoice запущена только в Brand Hub и показывает рекламодателям, какую долю занимают их бренды в обсуждениях в рамках сервиса микроблогов. Эта метрика измеряет показы органических твитов, позволяя увидеть, как рекламные кампании в социальной сети и других каналах влияют на органические упоминания о брендах в Twitter.

«Мы определяем TrueVoice вашего бренда, анализируя твиты о нём и твиты о конкурентах. Затем мы определяем, какой процент от этих показов приходится на ваш бренд. По мере того как потребители видят рекламу вашего

бренда и конкурентов на телевидении, в социальных и медийных каналах, они отправляют твиты, которые затем подсчитываются в режиме реального времени через TrueVoice™», – комментирует запуск представитель компании.

Метрика по умолчанию анализирует твиты за семь дней. Этот диапазон может быть расширен до 28 дней.

Доля рекламного воздействия конкурентов

На панели управления в Brand Hub бренды могут видеть свою долю органических и рекламных показов, а также долю показов, полученных конкурентами.

Здесь также можно просмотреть изменения в TrueVoice и показах бренда в течение недели, а также диаграммы трендов, которые отображают долю обсуждений конкретного бренда в сравнении со средней долей конкурентов за неделю.

Статистика по аудитории, которая говорит о бренде

Вкладка Audience в Brand Hub показывает как обобщённые данные о людях, публикующих твиты о бренде – пол, местоположение, род занятий, уровень дохода и другие, так и список ведущих инфлюенсеров (агентов влияния) бренда.

Панель Conversation Details отображает наиболее популярные фразы, используемые в твитах о бренде.

В настоящее время аналитический функционал Brand Hub доступен лишь некоторым крупным и средним рекламодателям в англоговорящих странах ***(Twitter представил Brand Hub – инструмент социального мониторинга и аналитики для брендов // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45102/118/lang,ru/). – 2015. – 27.10).***

***

С 15 сентября все пользователи «ВКонтакте» получили доступ к новому сервису сети – «Товарам». Если ранее виртуальной магазинной витриной служили альбомы сообществ, то теперь возможно создание полноценных карточек товаров. Как же эффективно использовать все преимущества сервиса для розничной интернет-торговли – в материале специалистов SMM-отдела компании Seomarket, пишет AIN.UA (http://ain.ua/2015/10/30/612540?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed %3A+ainua+ %28AIN.UA %29).

Для кого?

«Мы создаем новую платформу, при помощи которой малые и средние магазины смогут получить доступ к многомиллионной аудитории “ВКонтакте”, а тесная социальная интеграция позволит вывести интернет-магазины на новый уровень за счет синергетического эффекта», – комментирует операционный директор «ВКонтакте» А. Рогозов.

Онлайн-магазин на базе социальной сети подходит для продажи любых товаров. Некоторые пользователи наполняют раздел услугами: предлагают путевки, перевозки, дизайн, разработку имиджа и пр. По многочисленным просьбам, разработчики «ВКонтакте» даже создали отдельную категорию

«Услуги». Но, как показывает практика, большинство предложений из сферы услуг не имеют фиксированных цен и рассчитываются индивидуально для каждого клиента. Поэтому в данном случае онлайн-витрина товаров является неэффективной, а предложения с условными ценами скорее вызовут раздражение у потенциальных покупателей, чем стимулируют покупку.

Сейчас «ВКонтакте» классифицирует магазины по 12 категориям. Больше всего в сети представлено магазинов с одеждой, товарами для досуга и подарками.

Стоит обратить внимание, что сервис создан для сообществ, основная цель которых – продажи через социальные сети. Развлекательным и информационным сообществам запрещено сдавать другим магазинам раздел «Товары» в аренду, размещать в нем рекламу или цены на рекламу. Единственное исключение – продажа товаров с символикой сообщества.

Преимущества сервиса «Товары»

Бесплатно. Вы ничего не теряете, если попробуете применить функционал в своем сообществе. К тому же, раздел «Товары» всегда можно отключить.

Полноценная товарная витрина. Преимущества интернет-магазина в рамках социальной сети с многомиллионной аудиторией. Фотографии, описание характеристик, условия доставки и контакты продавца создаются под каждый товар.

Галерея. Загрузка нескольких изображений в одну карточку товара. Сейчас доступны одна основная и четыре дополнительные картинки.

Поиск и фильтры. В распоряжении пользователей удобный поиск по товарам или по подборкам, а также сортировка товаров по цене и дате добавления.

Основная подборка. Сервис предлагает выбрать основную подборку товаров магазина. Это очень удобная функция для продажи определенных позиций. Три последних товара основной подборки будут всегда отображаться на главной странице.

Публикация товаров на стене магазина, других ваших сообществ и рассылка товара друзьям с помощью кнопки «Поделиться». Здесь главное – не переусердствовать, так как массовую рассылку товаров «ВКонтакте» расценивает как спам.

Удобная коммуникация между продавцом и покупателем. Заказчик, прямо из карточки товара может связаться с продавцом, которому вместе с сообщением от покупателя приходит ссылка на товар.

Новые фаны. Бесплатные новые подписчики придут к вам через поиск по топ-сообществам.

Недостатки функционала «Товаров»

Время. Вам потребуется много времени на заполнение раздела. Лучше выделите для этого помощника, который постоянно будет загружать товары, следить за обновлениями цен и ассортимента. Или же воспользуйтесь платными программами автозагрузки и синхронизации. Например, VK-sync за одну карточку товара просит 1,07 грн.

Сервис «Товары» не работает в мобильной версии. Как скоро доработают этот функционал – неизвестно.

Отсутствие превью подборок. При публикации на стене сообщества ссылок на подборки магазина, превью не подгружается, как это было с альбомами. Вам придется отдельно добавлять к посту картинку, чтобы привлечь внимание аудитории.

Как попасть в топ и для чего это нужно?

Чтобы стимулировать пользователей активировать раздел, администрация сети запустила топ сообществ-магазинов, в который можно попасть бесплатно. Продавцам важно находиться в топе. Это увеличивает видимость магазина среди целевой аудитории и приводит новых фанов.

Для попадания в топ магазинов необходимо выполнить несколько условий:

Оставить заявку на добавление в топ.

Активно вести сообщество: публиковать посты, загружать товары, работать с обратной связью.

Качественно оформить раздел «Товары»: создавать подборки, полностью заполнять карточки товаров, использовать качественные изображения.

Если все сделано правильно, вас должны включить в топ. Но учтите, что большое количество загруженных товаров не гарантирует первых позиций в рейтинге, так как у пользователей топ магазинов отображается по-разному.

Как пользоваться «Товарами ВКонтакте»?

Если после прочтения этой статьи, вы решитесь перевести сообщество в магазин, воспользуйтесь этими рекомендациями.

Активация раздела

«Товары» доступны как группам, так и публичным страницам. Включается сервис в меню «Управление сообществом» во вкладке «Информация» в пункте «Товары».

Заполнение и модерация

Если финансовые возможности не позволяют оплатить программу автозагрузки товаров, придется все делать вручную. Заполнение одной карточки занимает в среднем 3–5 минут.

Соцсеть пока не устанавливала лимит на количество товаров для одного магазина. Поэтому загружайте столько карточек товаров, сколько захотите.

Лайфхаки по заполнению раздела:

Создавайте товары непосредственно в подборках, а не в общем разделе. В этом случае, поле «Подборка» в карточке товара выставляется автоматически.

Заполняйте поля «Название» и «Описание» товаров внимательно. Эти данные учитываются при поиске.

Используйте автозамены для оптимизации работы. Например, в программе Punto Switcher можно запрограммировать сочетание клавиш на вставку определенного текста. Вы сэкономите время на наборе текста, который дублируется в нескольких карточках товаров.

Обратите внимание в карточке товара на поле «Категория». Перечень категорий «ВКонтакте» еще не совершенен, но постоянно обновляется. Выбирайте максимально подходящий вариант. Это важно, потому что соцсеть

вскоре запустит единый каталог категорий товаров. В него попадут абсолютно все товары, которые будут классифицироваться согласно этому перечню.

Добавляйте качественные изображения. «ВКонтакте» рекомендует размер 400*700. Обратите внимание, что миниатюра товара будет стандартной квадратной формы.

Оформляйте подборки красиво. Хорошая картинка не только заинтересует покупателя, но и повысит шансы магазина попасть в список ТОП-сообществ.

Контролируйте наличие ассортимента. «ВКонтакте» добавил в карточку товара пункт «Товар недоступен». Используйте ее, если товара нет в наличии.

Реагируйте на обратную связь от пользователей быстро. Все ответы и комментарии по товарам отображаются во вкладках «Ответы» и Комментарии» на личной странице администратора магазина.

Продвигайте товары. Напишите небольшой текст о продукте, добавьте завлекающую картинку или видео, прикрепите ссылку на товар и опубликуйте. Такой пост лучше смотрится в новостной ленте и не воспринимается как навязчивая реклама.

Сервис «Товары ВКонтакте» – эффективный инструмент, который стоит использовать для торговли через социальные сети или повышения продаж на вашем сайте ***(Что такое «Товары ВКонтакте» и как с ними работать? // AIN.UA (http://ain.ua/2015/10/30/612540?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed %3A+ainua+ %28AIN.UA %29). – 2015. – 30.10).***

***

Убытки соцсети для бизнеса LinkedIn возросли в девять раз

Социальная сеть LinkedIn, предназначенная для поиска и установления деловых контактов, сообщила о квартальных итогах, которые оказались существенно выше прогнозов Уолл-стрит. Убытки компании возросли более чем в девять раз.

За трехмесячный отчетный период, завершившийся 30 сентября 2015 г., LinkedIn зафиксировала убыток на уровне 40,5 млн дол., или 31 цента в расчете на одну акцию, против денежных потерь в размере 4,3 млн дол., или 3 центов на акцию, годом ранее.

Если не учитывать некоторые разовые расходы, то соцсеть завершила квартал со скорректированной прибылью в 78 центов, что на 32 цента больше, чем ожидали опрошенные Thomson Reuters аналитики. Они также прогнозировали менее крупную выручку по сравнению с реальной – 755,8 против 779,6 млн дол. соответственно. В годовом исчислении выручка поднялась на 37 %.

В III квартале 2015 г. на продаже премиум-аккаунтов LinkedIn заработала 138 млн дол., увеличив результат аналогичного временного отрезка прошлого года на 21 %. Рекламный бизнес, за который отвечает подразделение Marketing Solutions, показал 28-процентный прирост выручки – до 140 млн дол. Сервис платных объявлений работодателей и соискателей вакансий принес компании доход в 502 млн дол., что на 46 % больше показателя годичной давности

(Убытки соцсети для бизнеса LinkedIn выросли в 9 раз // InternetUA (http://internetua.com/ubitki-socseti-dlya-biznesa-LinkedIn-virosli-v-9-raz). – 2015. – 1.11).

***

Facebook запускает новый рекламный блок «Слайд-шоу» (Slideshow), предназначенный для развивающихся рынков с медленным или ненадёжным интернет-соединением. Об этом пишет searchengines.ru

Новый формат представляет собой «заменитель видео» и пригодится как крупным брендам, так и предприятиям малого бизнеса. С его помощью они смогут создать более динамичные и вовлекающие видеообъявления в условиях 2G-соединения. Например, в Индии.

Идея состоит в том, что бренд создаёт две кампании: одну с обычным видео и вторую со слайд-шоу. Facebook будет определять скорость интернет-соединения пользователей и показывать им объявления соответствующего формата.

«Слайд-шоу облегчает рекламодателям процесс создания видеообъявлений из обычных изображений. Для этого достаточно загрузить от трёх до семи изображений – это могут быть как фрагменты из уже готового видео, фотосессии или же стоковые картинки из нашей библиотеки – и выбрать продолжительность слайд-шоу, от 5 до 15 секунд.

Новый формат сокращает затраты времени и ресурсов на подготовку видео, а меньший размер файла позволяет повысить привлекательность объявлений на базовых устройствах или же в условиях медленного интернет-соединения. В начале тестирования мы выявили, что размер файлов 15-секундных слайд-шоу может быть в пять раз меньше, чем у видеороликов той же длительности. Слайд-шоу демонстрируются в беззвучном режиме, предоставляя рекламодателям новый способ поведать свою историю людям во всём мире», – сообщается в официальном блоге компании.

В ближайшие недели новый формат будет доступен в Power Editor и Ads Manager. В будущем он также может появиться в Instagram.

Во время презентации представитель Facebook заявил, что более половины дохода компании поступает из рынков за пределами США.

Напомним, что к 2020 г. компания хочет обеспечить Интернетом всех землян. В сентябре основатель и генеральный директор Facebook М. Цукерберг призвал мировых лидеров и инноваторов внести всеобщий доступ к Интернету в число приоритетных задач.

В июне этого года социальная сеть запустила Facebook Lite – облегчённую версию своего приложения для Android, разработанную специально для развивающихся рынков. Продукт предназначен для пользователей медленных смартфонов и мобильных сетей. При этом он не является частью проекта Internet.org ***(Facebook представил новый формат рекламы для рынков с медленным интернет-соединением // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45150/118/lang,ru/). – 2015. – 30.10).***

***

Facebook запустит собственную доску объявлений

Сервис Local Market станет торговой площадкой, где каждый участник сможет выставить на продажу или приобрести товары различных категорий: технику, мебель, автомобили, одежду, книги и детские товары. Полный перечень на сегодняшний день неизвестен. Приложение еще не представлено официально, но у некоторых пользователей иконка этого сервиса на короткое время появлялась в мобильной версии Facebook, сообщает Tech Crunch.

Каждый лот будет стандартно сопровождаться комментарием, информацией о стоимости, а также фотографией или видео. Искать необходимые товары можно будет по ключевым словам. Возможность разместить объявление на Local Market появлялось у некоторых пользователей, когда они писали посты в группах Facebook, занимающихся продажей товаров «из рук в руки». В дальнейшем новый сервис будет автоматически собирать информацию с торговых площадок в конкретном регионе.

Впрочем, пока что ни у кого из посетителей Local Market сервис не работал дольше двух часов. В Facebook не стали отрицать, что компания проводит тестирование ранее не анонсированного сервиса, однако от комментариев на данную тему отказались. Ранее представители корпорации заявляли, что всего в социальной сети сейчас зарегистрированы десятки миллионов различных групп и торговые площадки являются одним из самых популярных направлений ***(Facebook запустит собственную доску объявлений // InternetUA (http://internetua.com/Facebook-zapustit-sobstvennuua-dosku-ob-yavlenii). – 2015. – 1.11).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Привязанность современного поколения к смартфонам не может не сказаться на их поведении и усваивании информации. Американские ученые считают, что негативнее всего тяга к постоянной переписке сказывается на молодых девушках и их успеваемости в школе. Они проявляют признаки, присущие игроманам: не могут урезать время за перепиской, обзаводятся бессонницей и врут, скрывая привычку.

В ходе исследования были опрошены 403 школьника. Оказалось, что парни и девушки увлечены виртуальной перепиской примерно одинаково, но больший эффект она оказывает на девочек. На успеваемость парней, которые и так не отличаются хорошими оценками в школе, «текстинг» практически не влияет.

Ученым удалось выяснить и различия в подходе к переписке у разных полов: девушки переписываются для общения с друзьями и поддержки отношений, а парни – для передачи какой-то базовой информации. Всего ученые насчитали, что подростки отправляют около 167 сообщений в день. При этом большинство опрошенных чаще используют смартфоны для переписки и реже для звонков ***(Тягу подростков к переписке сравнили с увлечением азартными играми // InternetUA (http://internetua.com/tyagu-podrostkov-k-perepiske-sravnili-s-uvlecseniem-azartnimi-igrami). – 2015. – 19.10).***

***

Социальные сети помогают учить иностранный язык. К примеру, специалисты указывают на значимость такого инструмента, как «карта диалектов».

Это работает следующим образом: когда вы размещаете твит, благодаря GPS вашего телефона у вас есть возможность указать, где именно вы отправляете послание. Лингвисты использовали карту с геотегами твитов, изучив, где и какие формы языка кто использует.

Иногда их исследования подтверждают то, что мы уже и так все знаем: различные диалекты английского, как правило, отличаются в произношении. «Однако люди также склонны писать их по-разному в Twitter. Иногда это учит нас чему-то новому», – уверены лингвисты.

Общение в Интернете – это также бесценная языковая практика. Люди, которые много общаются онлайн с другими, получают намного больше возможностей для практики письма, чем мы когда-либо наши предки в доцифровую эпоху. Прежде чем это стало нормальным для использования электронной почты и ведения аккаунтов в социальных сетях, большинство людей прекращали писать после того, как они закончили школу. Действительно, многим не доводилось сочинять ничего дольше, чем список покупок или поздравительную открытку ***(Социальные сети помогают учить иностранный язык // ZdravoE (http://zdravoe.com/101/p16872/index.html). – 2015. – 21.10).***

***

Американский офтальмолог и предприниматель С. Потаразу объяснил, насколько опасными могут быть социальные сети для подростков и детей, пишет «Обозреватель» (http://tech.obozrevatel.com/news/41890-deti-brodyat-v-podvorotnyah-facebook-i-instagram-amerikanets-napugal-opasnostyu-sotssetej.htm).

«Вы знаете, где сейчас находятся ваши дети? Еще 10 лет назад ответ “да, они дома” очень порадовал бы вас. Родители чувствуют себя комфортно, когда знают, что их дети в безопасности», – пишет врач в своей колонке для CNN, сообщает «Новое время».

Однако это больше не соответствует действительности. Сегодня у детей есть смартфоны и планшеты, благодаря которым они могут зависать в темных переулках, даже не выходя из дома, продолжает автор. Недавнее исследование американского аналитического центра Pew Research Center выявило, что 92 %

подростков ежедневно бывают онлайн, и еще 24 % ответили, что они находятся онлайн «постоянно».

«Если вы думаете, что они сидят в Facebook, и вы можете проследить за их активностью, то подумайте ещё раз», – отмечает колумнист. Согласно опросу среди американских подростков, только 15 % детей назвали Facebook своей любимой сетью, 33 % выбрали Instagram, 20 % отдали предпочтение Twitter и еще 19 – Snapchat, приложению, которое позволяет публиковать фото включительно с собственными снимками в обнаженном виде, исчезающие сразу после просмотра.

Появление социальных технологий может нести определенную ответственность за тревоги и депрессии, которые наблюдаются среди молодежи. Facebook, Twitter, Snapchat и Instagram – все они классные, пока ситуация не выходит из-под контроля.

В ходе социологического исследования 2014 National College Health Assessment, в рамках которого были опрошены 80 тыс. студентов американских колледжей, 54 % респондентов сообщили, что в течение последних 12 месяцев они испытывали подавляющее чувство беспокойства, а 32,6 % сказали, что «чувствовали себя настолько подавленными, что трудно было работать». Исследование показывает, что 6,4 % студентов «преднамеренно наносили себе разного рода увечья – порезы, ожоги, удары и пр.», 8,1 % всерьёз задумывались о суициде и ещё 1,3 % – предпринимали соответствующие попытки.

«Это ужасающая статистика, но нам некого винить, кроме самих себя», – пишет С. Потаразу.

Совместно с экспертами в области развития ребенка агентство CNN изучало привычки в социальных медиа более 200 восьмиклассников. Согласно этому исследованию, некоторые 13-летние подростки проверяют ленту новостей своих аккаунтов в социальных медиа около сотни раз на день.

Сегодня дети растут в мире, в котором ждут немедленного отклика, удовлетворения и уведомления. У мозга нет времени на развитие; они должны адаптироваться к изменениям в одно мгновение, что порождает тревогу. Трудности взросления ещё никогда не были столь публичными.

Социальные технологии предоставляют платформу, где можно вести распутный образ жизни. Представьте себе стресс последних классов средней школы – конкуренция за популярность, давление, связанное с желанием вписаться в общество, оценочный характер социальной деятельности – и всё это в ускоренных темпах.

«Мы стараемся защитить наших детей, чтобы они не блуждали сами в потемках, но выясняется, что именно этим они и занимаются, только онлайн», – заключает автор ***(Дети бродят в подворотнях Facebook и Instagram: американец напугал опасностями соцсетей // «Обозреватель» (http://tech.obozrevatel.com/news/41890-deti-brodyat-v-podvorotnyah-facebook-i-instagram-amerikanets-napugal-opasnostyu-sotssetej.htm). – 2015. – 22.10).***

***

Новое программное обеспечение заставит кибер-хулиганов подумать дважды.

В 2013 г. тогдашняя 13-летняя школьница Т. Прабху из пригорода Чикаго пришла домой из школы и прочитала новость о 11-летней девочке, которая покончила жизнь самоубийством, спрыгнув с водонапорной башни. В течение нескольких месяцев до этого девочка неоднократно подвергалась издевательствам через Интернет. «Меня это потрясло, я была очень расстроена и сердита, – говорит Т. Прабху, которой сегодня уже 15. – Я знала, что должна что-то предпринять, чтобы такое больше никогда не повторилось».

Так Т. Прабху придумала кибер-защиту от кибер-издевательств. Она изобрела программное обеспечение под названием ReThink, которое сканирует социальные сети для выявления сообщений оскорбительного характера и даёт написавшему возможность подумать – на самом ли деле он хочет оставить такое сообщение. Программа, которую могут установить родители на домашних компьютерах или учителя на школьных компьютерах, использует проверку контекстуально связанных слов, чтобы помечать сообщения с таким содержанием.

Для Т. Прабху программа связана с личным опытом. Раньше она тоже подвергалась оскорблениям через Интернет, получая неприятные сообщения по поводу одежды, которую носила.

Кибер-запугивание является действительно серьёзной проблемой. Исследования показывают, что 43 % детей подвергались кибер-травле. Около 70 % студентов сообщили, что часто встречаются с онлайн-издевательствами. Жертвы таких притеснений в девять раз чаще думают о самоубийстве как выходе из положения.

ReThink работает по схеме – мозг подростка как «автомобиль без тормозов», говорит Т. Прабху. «Хорошо известно, что подростки делают импульсивные, необдуманные поступки».

Действительно, префронтальная кора – область мозга, ответственная за самоконтроль и принятие решений – в полной мере развивается только к 25 годам. Это, вероятно, один из основных факторов, который стоит за безответственными и рискованными поступками подростков – будь-то отправка сообщений, вождение без прав, драки или даже просто пренебрежение домашним заданием.

Т. Прабху получила много сообщений от людей, которые не понаслышке знакомы с последствиями кибер-притиснений – от родителей, чьи дети совершили самоубийство после неоднократных случаев кибер-издевательств, полицейских, которые имеют дело с расследованиями таких дел, школьных администраций, которые борются с этим явлением. И конечно от самих жертв.

Чтобы проверить, как это работает, можно скачать приложение для iPhone. Если выложить в Facebook «Я ненавижу тебя», то ReThink в всплывающем окошке предложит «Давайте заменим эти слова, чтобы сделать их позитивными». Если попробовать написать «Ты жирная», то появится «Не говорите вещи, о которых можете позже пожалеть!». ReThink также очень чувствителен к мату.

Хотя ReThink явно не идеальный инструмент для борьбы с кибер-жестокостью, но он предлагает подросткам второй шанс, которым они склонны воспользоваться. По данным исследования, подростки меняли своё мнение о

публикации оскорбительного сообщения в 93 % случаев ***(Новое программное обеспечение заставит киберхулиганов подумать дважды // InternetUA (http://internetua.com/novoe-programmnoe-obespecsenie-zastavit-kiberhuliganov-podumat-dvajdi). – 2015. – 24.10).***

***

Почему Facebook или Twitter теряют популярность?

Последние статистические данные четко указывают что «классические» социальные сети, как Facebook или Twitter из месяца в месяц теряют свою популярность. Набирают ее в свою очередь сервисы, такие как Instagram и Snapchat (которые уже имеют, соответственно, 400 и 100 млн активных пользователей). По данным исследователей из Университета Мичигана, эту тенденцию можно очень просто объяснить.

Исследования ученых показывают, что пользователи получают гораздо больше удовольствия от Snapchat, чем с Facebook. Тщательный анализ позволил также прийти к выводу, почему это так. Оказывается, что сайты, на которых общение происходит в виде передачи фотографий, больше похожи на встречи лицом к лицу, и именно они являются наиболее популярными социальными взаимодействиями людей.

Исследование строилось на случайных вопросах типа: «какие эмоции вы испытываете сейчас?» и «какое очень приятное было твое последнее взаимодействие?». Из ответов следует, что коммуникации при помощи изображений доставляют больше радости, чем основанные исключительно на тексте, потому что это более естественно. Фото лучше выражает эмоции, чем даже «живые» сообщения ***(Почему Facebook или Twitter теряют популярность? // Новости IT (http://interteam.com.ua/pochemu-facebook-ili-twitter-teryayut-populyarnost/). – 2015. – 27.10).***

***

Социальные сети способны многое рассказать о здоровье человека

Исследование, проведенное в Университете Пенсильвании, показало: люди часто делятся в соцсетях важной информацией о состоянии своего здоровья. Иногда ее легко заметить. Например, если человек сообщает, что забыл принять таблетку. А в некоторых случаях все не столь очевидно (допустим, когда пользователь размещает на своей странице много фотографий вредной пищи), пишет The Hindustan Times.

Изменения в сложности используемых слов могут свидетельствовать о когнитивных нарушениях. Уменьшение количества слов в сообщениях и небольшое количество друзей позволяют сделать предположение о депрессии.

Еще в соцсетях бывает информация об образе жизни человека, к примеру, его диете и уровне физической активности. Кроме того, на своей странице пользователь может рассказывать о том, соблюдает ли он назначения медиков, и о новых заболеваниях.

Также ученые обнаружили: люди с определенным диагнозом гораздо чаще использовали в социальных сетях термины, которые имели отношение к заболеванию, по сравнению с теми, у кого не было такого диагноза. Так,

словосочетание «боль в животе» на своей странице в Facebook употреблял 21 % пользователей с диагнозом «боли в области живота» и только 8 % людей без этого диагноза ***(Социальные сети способны многое рассказать о здоровье человека // Healthy Living (http://healthyliving.com.ua/zdorove-2/novosti/4740-sotsial-nye-seti-sposobny-mnogoe-rasskazat-o-zdorov-e-cheloveka). – 2015. – 30.10).***

Маніпулятивні технології

Наверняка многие из пользователей «ВКонтакте» когда-нибудь задумывались над тем, что будет, если социальной сети не станет. Главная проблема заключается в том, что у многих юзеров в аккаунтах хранится масса личной информации, друзья, переписки. Так вот 24–25 октября пользователи «ВКонтакте» были охвачены паникой, когда появилось известие, что социальная сеть закрывается, а персональные данные юзеров станут достоянием общественности.

Панику спровоцировал один из пользователей «ВКонтакте», который на своей стене разместил пост, поделившись с друзьями, что в ближайшее время социальная сеть будет закрыта. Чтобы уберечь свои персональные данные от просмотра другими пользователями, по словам информатора, было необходимо разместить его сообщение каждому юзеру на своей стене.

«С понедельника программы ВКонтакте не будет Её полностью удаляют!((Нам сидеть ВКонтакте осталось совсем чуть-чуть! Так, вот, чтобы все твои переписки, и картинки, и фотки не разошлись по всему инету кинь себе на стенку вот это!» – говорится в тексте данного сообщения.

Сообщение очень быстро распространилось по соцсети. Начались массовые публикации по соцсетям с хештегами #ВернитеДурова #вк_живи #ВкНеСтанет. Чтобы прекратить панику, администрации «ВКонтакте» даже пришлось выступить с официальным заявлением о том, что сайт закрываться не собирались, а по факту распространения неправдивой информации техподдержка провела собственное расследование. Выяснилось, что эта акция являлась всего лишь попыткой раскрутить один из аккаунтов недобросовестного пользователя.

Несмотря на все уверения руководства, перспектива скорого закрытия соцсети испугала большинство пользователей, которые используют «ВКонтакте» не только для работы, но и для хранения важных для себя данных. Инцидент заставляет задуматься о роли социальных сетей в нашей жизни. Отметим, что это не единичный случай, подобная ситуация имела место в «ВКонтакте» всего пару месяцев назад ***(Пользователей «ВКонтакте» напугали новостью о закрытии соцсети // InternetUA (http://internetua.com/polzovatelei--vkontakte--napugali-novostua-o-zakritii-socseti). – 2015. – 26.10).***

***

Партию «Нова Держава», по спискам которой в Николаевский горсовет баллотируются активисты КПУ и одиозные «регионалы», активно пиарят в сепаратистских пабликах в социальной сети «ВКонтакте».

Об этом говорится в письме постоянного читателя, пришедшем на редакционную почту «Эгалите».

«Стал свидетелем безпредела, что творится в социальных сетях. В ряде сепаратистских групп “ВКонтакте” активно распространяется видео-ролик, агитирующий голосовать за бывшую коммунистическую партию, а сейчас партия “Новая Держава” на местных выборах. Причем, в ролике часто встречаются фотографии таких местных сепаратистов как Е. Бондаренко и другие, также кадры с триколором», – говорится в письме.

Так, агитационный ролик николаевской организации партии «Нова Держава» размещен в группах «25 ОКТЯБРЯ – ВЫБОРЫ НА ОККУПИРОВАНОЙ УКРАИНЕ», «Группа поддержки Александра Захарченко», «Николаев | Армия Народного Освобождения» и многих других.

При этом ролик сопровождается текстом: «Давайте поддержим те немногие политические силы, которые остались бороться за свободу людей от фашистского гнета киевских властей на Украине. Голосуй за «НОВУЮ ДЕРЖАВУ», голосуй за свой город без фашизма!» ***(Николаевскую партию «Нова Держава» активно пиарят в сепаратистских пабликах // Эгалите (http://egalite.com.ua/news/13509). – 2015. – 20.10).***

***

19 октября в соцсетях стала появляться «важная информация» о том, что во время выборов на избирательных участках будут присутствовать военкомы, которые на месте сверят списки призывников и прямо перед голосованием вручат повестки на прохождение медицинской комиссии, пишет 0564.ua (http://www.0564.ua/news/999912)

Данный пост был размещен в интернет-сообществе «Это Кривой Рог, детка».

Человек, который прислал новость в сообщество – «Андрей Билецкий» якобы узнал эту «важную информацию» от своего дяди, работающего в военкомате.

Отметим, что сам автор поста создал свою страничку за сутки до получения «важной информации».

В комментариях к данному посту большинство криворожан стали высмеивать автора, называя сообщение «вбросом» и «фэйком».

Как сообщили 0564 в Дзежинско-Долгинцевском военкомате, данную информацию распространяют для того, чтобы как можно меньше молодых людей пришли на избирательные участки в день выборов ***(В Кривом Роге через «вбросы» в соцсети пытаются отпугнуть молодёжь от участия в выборах // 0564.ua – Сайт города Кривого Рога (http://www.0564.ua/news/999912). – 2015. – 20.10).***

***

За неделю до местных выборов в Украине резко возросло число людей, желающих нарушить закон ради денег. Появились даже многочисленные интернет-сообщества в соцсетях, где предлагают купить и продать голоса! «Чтобы получить деньги, продавец своего голоса должен предъявить фото бюллетеня с “правильной” галочкой на мобильном телефоне. За это платим от 300 грн», – гласит «инструкция» в одной из групп. Желающим достаточно оставить сообщение со знаком «+» (в знак согласия продать свой голос. – Авт.) на ленте группы – и с продавцом свяжутся покупатели. Лишь за последнюю неделю в подобных группах появились десятки заявок на куплю-продажу голосов, в том числе – даже на оптовые. Среди продавцов и покупателей есть жители Киева, Днепропетровска, Житомира, Запорожья, Северодонецка. «Сегодня» под видом покупателя связалась с одним из участников группы. «Да, я продаю свой голос за 500 грн. Все равно за кого. Готова поискать других желающих продать голоса», – рассказала нам жительница Днепропетровска Ирина С, пишет «Сегодня» (http://www.segodnya.ua/politics/society/ukraincy-torguyut-golosami-portyat-byulleteni-i-agitiruyut-v-dni-tishiny-659500.html).

В МВД уже готовятся к борьбе с нарушениями на этих выборах. «О существовании подобных интернет-сообществ мы знаем. Обратим на них внимание, потому как все его участники – потенциальные нарушители закона (по новым законам, скупщикам и продавцам голосов грозит штраф от 170 до 5100 грн, или даже до семи лет тюрьмы. – Авт.). Строгость наказания зависит от количества скупленных или проданных голосов. Но одной фиксации предложения мало: нужно изъять фото с телефона и провести экспертизу», – рассказал спикер МВД А. Шевченко ***(Серов И. Украинцы торгуют голосами, портят бюллетени и агитируют в дни тишины // Сегодня (http://www.segodnya.ua/politics/society/ukraincy-torguyut-golosami-portyat-byulleteni-i-agitiruyut-v-dni-tishiny-659500.html). – 2015. – 20.10).***

***

Прокуратура Гамбурга розслідує справу щодо менеджерів соціальної мережі Facebook через закиди про розпалювання ворожнечі. Як повідомив речник прокуратури, провадження відкрито за заявою, яка надійшла 5 жовтня, пише Reuters 20 жовтня.

«Зараз ми перебуваємо на етапі перевірки викладених у заяві фактів», – наголосив представник прокуратури Гамбурга. Оцінки викладеним у заяві даним він не надав.

Раніше видання Der Spiegel повідомило, що до прокуратури звернувся адвокат Ч. Джун. У тексті його заяви, яка є у розпорядженні Reuters, обвинувачення щодо розпалювання ворожнечі стосуються трьох високопосадовців у національному та міжнародному офісах Facebook.

Їм закидається, що відповідні пости не видаляються з мережі навіть після прямої вказівки на них. «Facebook намагається поводитись так, ніби нічого не можна зробити», – сказав в інтерв’ю агенції адвокат. «Водночас інші випадки показують, що Facebook доволі легко видаляє пости, якщо він цього хоче», – додав юрист, який займається питаннями комп’ютерного права.

Як відомо, минулого місяця засновник Facebook М. Цукерберг пообіцяв канцлерці Німеччини А. Меркель, що він потурбується про заходи проти закликів до розпалювання ворожнечі. «Я думаю, ми повинні працювати над цим», – наголосив він. Коли А. Меркель перепитала, чи хоче він покращити ситуацію, М. Цукерберг відповів ствердно ***(Прокуратура Гамбурга перевіряє скаргу на менеджерів Facebook щодо розпалювання ворожнечі // MediaSapiens (http://osvita.mediasapiens.ua/media_law/law/prokuratura_gamburga_pereviryae_skargu_na_menedzheriv_facebook_schodo_rozpalyuvannya_vorozhnechi/). – 2015. – 20.10).***

***

На Донбасі сепаратисти дошкуляють українським бійцям пропагандистським SMS-спамом і зіпсованими банкнотами.

Про це повідомляє медіа-центр Міноборони України.

Як зазначається, на мобільні телефони українських воїнів, особливо тих, які нещодавно прибули до зони АТО, надходять SMS-повідомлення, зміст яких, здебільшого, спрямований на вихваляння «республік» і приниження України. Для подібної спам-розсилки використовуються номери українських операторів мобільного зв'язку. Водночас жоден з операторів мобільного зв'язку навіть і не здогадується, що його номери використовуються ворогом для ідеологічних диверсій.

У Міноборони стверджують: це робота кремлівських кураторів.

Зі слів фахівців, ця технологія не нова і працює таким чином: за допомогою спеціального обладнання та програмного забезпечення бойовики «ламають» мережу ретрансляційних вишок операторів стільникового зв'язку, підключаються до неї та загалом можуть слухати телефонні розмови та читати повідомлення абонентів. Згодом, коли в зоні покриття з'являються номери, які раніше не реєструвались у цьому районі, програма-робот автоматично надсилає на телефон цього абонента SMS-повідомлення пропагандистського змісту.

Крім того, як зазначається, вірусне поширення пропаганди «русского мира» здійснюється й через українські гроші. Наприклад, у магазині бійцю АТО намагались відрахувати решту банкнотою із штампом з гаслами «новоросії» та інтернет-адресою пропагандистського ресурсу бойовиків ***(Бойовики розсилають українським бійцям SMS, у яких вихваляють псевдореспубліки // Західна інформаційна корпорація (http://zik.com.ua/ua/news/2015/10/19/boyovyky_rozsylayut_ukrainskym_biytsyam_sms_u_yakyh_vyhvalyayut_psevdorespubliky_634419). – 2015. – 19.10).***

***

На сторінці української мережі «Друзі» з'явилася інформація зі звинуваченням власника мережі в діяльності на користь Росії. Наводимо текст повідомленя мовою оригіналу (http://zamkova.info/tehnologii/18610-ukrainsku-socialnu-merezhu-druzi-vykryly-u-diialnosti-na-koryst-rosii.html).

«Добридень дорогі користувачі соціальної мережі druzi.org.ua. Мене звуть Микита і Я є захисником українського web, так само я є тим хто зламав сайт druzi.org.ua!

Усім нам відомо що йде війна між Україною та Росією, але я фізично не можу захищати батьківщину і я вирішив захищати її як можу оскільки Україна це моя батьківщина!

У той момент доки наші герої віддають життя за батьківщину хтось набиває собі на цьому кишені, саме така ситуація і сталася з власником сайту druzi.org.ua.

Сайт druzi.org.ua спонсорувала Росія, власник сайту прикидаючись патріотом набивав собі на цьому кишені, а Росія отримувала інформацію про українських жителів.

Я виходив на власника сайту з фактами про його сепаратизм і зраду батьківщини, але він мене сміливо посилав на* зі своєї російської яндекс пошти.

Я виконав свій борг перед батьківщиною, Я захистив нас від чергової російської афери, будьте обережні з появою нових Українських соціальних мереж оскільки будь-яка з них може виявитися зовсім не Українською.

Є і хороші новини, я так само перевірив і інші Українські соціальні мережі, такі як weua.info, ц.укр, evaax.com і зробив про них свою оцінку:

weua.info: Власник дійсно Українець, перша версія сайту була невдала подивимось що покаже друга версія сайту.

ц.укр: Сайт знаходиться на Російській cms і дизайн його нічим не відрізняється від сайту “ВКонтакте”, власник сайту на зв’язок не виходить тому є вірогідність що доля цього сайту буде така ж як і сайт druzi.org.ua.

evaax.com: Власники сайту є Українцями і сайт обіцяють дуже цікавий, але за фактом три рази переносять відкриття сайту» ***(Українську соціальну мережу «Друзі» викрили у діяльності на користь Росії // Замкова гора (http://zamkova.info/tehnologii/18610-ukrainsku-socialnu-merezhu-druzi-vykryly-u-diialnosti-na-koryst-rosii.html). – 2015. – 21.10).***

***

Сайт WikiLeaks, специализирующийся на публикации попавших в его распоряжение «закрытых» правительственных материалов, начал выкладывать переписку главы ЦРУ США Д. Бреннана.

Почта, относящаяся к разведывательной деятельности, хранилась в одном из личных ящиков Д. Бреннана. Этот аккаунт не находился в ведении системы правительственного обмена корреспонденцией, сообщает «фрАза» (http://fraza.ua/news/22.10.15/233224/wikileaks_opublikoval_pervye_dannye_iz_vzlomannoj_pochty_glavy_tsru.html).

В частности, опубликована 47-страничная анкета Д. Бреннана, заполненная им перед тем, как он занял пост директора ЦРУ. Форма этой анкеты, SF86, предусматривает ответы на вопросы о биографических данных, местах учебы и работы, о допущенных правонарушениях, об употреблении запрещенных веществ, наличии алкогольной зависимости и тому подобное.

Также приведена аналитическая записка по ситуации в Иране и его политике, а также рекомендации по взаимодействию с властями этой страны.

Кроме того, опубликованы материалы, темой которых является применение пыток во время допросов подозреваемых в террористической деятельности после теракта 11 сентября 2001 г. в Нью-Йорке.

Упоминание о имеющемся у Д. Бреннана личном email-аккаунте появилось 18 октября. Редакция The New York Post опубликовала интервью с хакером, который заявил, что ему удалось взломать принадлежащую главе ЦРУ учетную запись на портале AOL и получить доступ к хранившимся в ней документам.

WikiLeaks позиционирует себя как некоммерческий проект и утверждает, что его цель – анализ документов, ставших доступными вследствие утечки информации. Портал официально открыт в 2007 г. С WikiLeaks связана одна из крупнейших информационных утечек в истории США – в 2010 г. на сайте был опубликован целый ряд военных и дипломатических документов о секретной деятельности Вашингтона.

В США все государственные чиновники обязаны переписываться при помощи специальной правительственной электронной системы. Она имеет дополнительную защиту и автоматически сохраняет всю историю переписки ***(WiKiLeaks опубликовал первые данные из взломанной почты главы ЦРУ // «фрАза» (http://fraza.ua/news/22.10.15/233224/wikileaks_opublikoval_pervye_dannye_iz_vzlomannoj_pochty_glavy_tsru.html). – 2015. – 22.10).***

***

Співробітниками Служби безпеки України був виявлений фейковий веб-ресурс – копія порталу СБУ «Реєстр дозволів для переміщення осіб в районі проведення АТО».

Про це повідомила прес-служба СБУ, новину передає «Преса України».

«Підроблений портал знаходиться за адресою 0s.ovzha.xxxxxxxxxxx.erenta.ru. Посилання на нього активно поширюється у російських соцмережах і позиціонується як перевірена можливість отримання дозволу для перетину лінії зіткнення. Доменне ім’я зареєстроване однією з російських компаній, відображення порталу в мережі також забезпечується з російських ресурсів», – ідеться в повідомленні.

За оперативною інформацією відомства, до створення фейкового ресурсу доклали руки спецслужби РФ та їхні фахівці.

СБУ закликала українських громадян пильнувати при заповненні подібних форм із персональною інформацією на інтернет-ресурсах і користуватися виключно офіційним сайтом urp.ssu.gov.ua ***(Спецслужби РФ створили фейковий веб-ресурс видачі перепусток в зону АТО // «Пресса Украины» (http://uapress.info/uk/news/show/102530). – 2015. – 29.10).***

Насколько закрыт Интернет в закрытых странах

В последние несколько лет в мире все чаще поднимается вопрос об устранении любых границ и цензуры в Интернете. Во многих авторитарных странах разворот в сторону Запада часто идет рука об руку с проникновением Интернета. Одним из подобных примеров может служить Куба. «Газета.Ru» выяснила, насколько закрыт Интернет в закрытых странах.

Правительства авторитарных стран давно осознали необходимость ограничения доступа своих граждан в Интернет и введения интернет-цензуры для упрочнения собственной власти. Так, Китай начал разработку проекта «Золотой щит», известного как «великий китайский фаервол», еще в 1998 г. и ввел его в эксплуатацию через пять лет. Китайскому правительству понадобилось наладить длительную работу с американскими IT-компаниями, такими как IBM и Cisco, чтобы суметь решить задачу фильтрации контента и, по сути, частичной информационной изоляции населения.

Тем не менее Интернет в КНР чрезвычайно развит, и страна располагает полноценными аналогами большинства интернет-сервисов – поисковиков, социальных сетей, мессенджеров и магазинов мобильных приложений. Китайский рынок важен и для развития американских IT-компаний, поэтому им приходится идти на адаптацию своих сервисов и устройств под требования китайского законодательства, в том числе и внедрять средства блокировки нежелательного контента и наблюдения, хотя в публичных заявлениях это отрицается. Однако до конца 2014 г. «Золотой щит» регулярно подвергался DDoS-атакам, а на территории Гонконга и Тайваня граждане часто имеют неограниченный доступ в глобальную сеть.

Совсем иная ситуация складывается в так называемых закрытых странах, таких как Северная Корея, Ирак, Сирия и Куба, которые не располагают возможностью по созданию полноценных замен основным интернет-сервисам.

Для их населения ограничение доступа в Интернет, особенно для молодой и активной его части, является чувствительным проявлением цифрового неравенства.

На Кубе Интернет с момента информирования о нем населения в 1990-х годах практически не развивался в связи с отсутствием финансирования телекоммуникаций и запрета на поставку телекоммуникационного оборудования в связи с торговым эмбарго. В настоящее время из-за неразвитости инфраструктуры Куба не использует на полную мощность даже проложенные по территории острова телефонные линии и оптико-волоконный кабель, соединяющий Кубу с Венесуэлой. В 2012 г. проникновение интернет-доступа на Кубе достигло 25,6 % населения. В основном это дорогой и медленный доступ через спутниковые телефоны, которые оплачивают родственники за границей. В среднем интернет-доступ в стране стоит 2 дол. в час при уровне месячного дохода 20 дол.

Тем не менее ситуация меняется. Прокладка оптико-волоконного кабеля в Венесуэлу была профинансирована Пекином, а к визиту папы римского Франциска компания Huawei установила Wi-Fi-хот-споты для работы прессы,

сообщает The Verge. Правительство США частично сняло торговое эмбарго в части телекоммуникационного оборудования и направило руководству Кубы предложение о прокладке подводного интернет-кабеля из Майами. Кубинские власти планируют обеспечить 60 % населения мобильным Интернетом и половину – доступом на дому к 2020 г.

Однако если раньше цензура Интернета на Кубе основывалась на том, что на острове практически не было Интернета, то на сегодняшний день перед кубинскими властями эта проблема встала в полный рост.

Поскольку первым поставщиком интернет-технологий на Кубу стали китайские компании, есть основания полагать, что вместе с ними на Остров свободы придут и технологии «Золотого щита», которые дадут возможность обеспечивать цензурирование интернет-контента.

Куда более развит Интернет в еще одной закрытой стране – Северной Корее. Основные города и организации страны объединены в национальную сеть оптико-волокнными линиями с пропускной способностью до 2,5 Гбит/с. Иностранцы даже могут выходить в глобальную сеть при помощи 3G после соответствующей проверки. Однако в конце 2014 г. правительство Северной Кореи объявило о блокировке Wi-Fi-спотов в иностранных посольствах, поскольку они транслировали нецензурированный доступ на близлежащие здания.

Северная Корея пошла по пути жесткой дифференциации доступа. Основной части населения доступен локальный аналог Интернета «Кванмен» с поисковиком, электронной почтой и, по разным источникам, от 1 до 5,5 тыс. разрешенных правительством сайтов. Также северокорейским пользователям доступна операционная система Red Star на базе ядра Linux.

Однако часть пользователей, имеющих правительственное разрешение, обладают полным доступом к Интернету. Таким образом, у Северной Кореи есть квалифицированные специалисты в сфере информационных технологий.

В частности, сотрудников Политехнического университета им. К. Чхэка в Пхеньяне и Университета им. К. Сена обвиняют в хакерстве, нелегальном заработке через Интернет за рубежом, а также громких атаках на Sony Pictures и южнокорейского оператора двух АЭС.

Сирия, о которой много сейчас говорится, не пошла по пути Северной Кореи. Туристический бизнес являлся важной статьей доходов этой страны, а телекоммуникации также являются весьма прибыльной отраслью, поэтому жесткая изоляция страны от Интернета чревата конфликтом интересов. Правительство Б. Асада шло по пути блокировки Facebook, YouTube, Twitter и других крупнейших интернет-сервисов.

Тем не менее с 2000 г. количество интернет-пользователей в Сирии значительно увеличилось и превысило 1 млн в 2008 г. Возросло количество смартфонов, а GSM-сеть была развернута повсеместно. В стране действуют два оператора – MNT и Syriatel. Во всех городах развиты сети интернет-клубов и кафе, где можно выйти онлайн, отсканировать и распечатать документы. Однако в сравнении с 22,5-миллионным населением страны проникновение Интернета низкое.

В начале гражданской войны в июне 2011 г. в Сирии 3G-, DSL- и dial-up-доступы были прекращены, что вызвало еще больше протестов.

При этом сторонники Б. Асада сами используют Интернет для атак на своих противников и пропаганды. Сирийское правительство спонсирует группу хакеров, известных как Сирийская электронная армия (SEA), которые при помощи фишинговых писем и троянов атакуют сайты правозащитных организаций и аккаунты в социальных сетях. Поскольку Интернет стал практически незаменимым средством коммуникации, это также дает возможность SEA нарушать коммуникацию оппозиционных сил и получать важную тактическую информацию, используемую в боях.

Телекоммуникации в соседнем с Сирией Ираке сильно пострадали во время войны в 2003 г. Но за последующие десять лет количество оптико-волокнных линий, спутниковых станций и абонентов сотовой связи 3G значительно увеличилось. В стране действует три сотовых оператора, а количество абонентов в 2012 г. достигло 27 млн человек. Число интернет-пользователей в 2012 г. достигло 2,2 млн человек, что составляет 7,1 % населения страны.

После войны Ирак радикализировался, и правительство страны ввело цензуру в Интернете и стало использовать его для наблюдения. В августе 2009 г. правозащитная организация OpenNet Initiative сообщила о том, что выявила на территории Ирака мониторинг электронных писем пользователей и сообщений в социальных сетях через местных интернет-провайдеров без соответствующего юридического контроля.

В 2012 г. публикация в Интернете видео «Невинность мусульман», снятого в США, обернулась массовыми протестами и угрозами убийства христиан в г. Мосуле на севере Ирака. Это инцидент позволил взглянуть на феномен цензуры в Интернете с другой стороны.

Интернет стал не только каналом распространения пропаганды, но и средством ведения войны между государствами. Если до недавнего времени мировое сообщество отвергало и осуждало цензуру и контроль глобальной сети, то сейчас этот взгляд изменился, и правительства ведущих стран совместно пытаются выработать понятия и принципы коллективной кибер-безопасности ***(Насколько закрыт интернет в закрытых странах // InternetUA (http://internetua.com/naskolko-zakrit-internet-v-zakritih-stranah). – 2015. – 19.10).***

***

На Донеччині Служба безпеки України припинила діяльність інформаторської мережі терористів ДНР.

Про це повідомляє Еспресо.TV із посиланням на прес-службу СБУ.

«Упродовж серпня – вересня зловмисники збирали інформацію про місця дислокації та маршрути пересування Збройних сил України», – ідеться в повідомленні.

У відомстві зазначають, що отримані дані передавалися представникам фейкових спецслужб терористичної організації та використовувалися для завдавання артилерійських ударів по позиціях українських військових.

Координатора та членів мережі затримано співробітниками контррозвідки СБУ.

«Військовою прокуратурою сил антитерористичної операції відкрито кримінальне провадження за ч. 1 ст. 258-3 (створення терористичної групи або участь у ній) ККУ. Оперативно-слідчі дії тривають», – пише прес-служба ***(СБУ «накрила» чергову інформаторську мережу терористів // Espreso.tv (http://espreso.tv/news/2015/10/19/sbu_quotnakrylaquot_chergovu_informatorsku_merezhu_terorystiv). – 2015. – 19.10).***

***

Социальная сеть Facebook будет оповещать пользователей о слежке за аккаунтами со стороны правительства. Об этом сообщил глава службы безопасности Facebook А. Стамос, передает Huffington Post.

«Мы будем информировать пользователей о том, что их аккаунты стали целью слежки со стороны агентов, работающих на государство», – заявил А. Стамос.

Вместе с тем А. Стамос не раскрыл информацию о том, как будет совершаться сбор информации о шпионаже, ссылаясь на то, что хочет оставить методы, которые будут использоваться социальной сетью, в тайне.

Он также отметил, что если пользователь получил подобное сообщение, это может свидетельствовать о том, что его мобильное устройство или компьютер были заражены вредоносной программой ***(Facebook пообещал предупреждать пользователей о слежке // Подробности (http://podrobnosti.ua/2066470-facebook-poobeschal-preduprezhdat-polzovatelej-o-slezhke.html). – 2015. – 19.10).***

***

Адміністрація популярного месенджера Viber розмістила в Росії свої сервери з персональними даними користувачів – про це повідомила представник Viber Media О. Грачова.

Перенесення серверів було здійснено на виконання законодавства РФ.

«У Росії будуть зберігатися номери телефонів і логіни користувачів. Повідомлення ми не зберігаємо, вони знаходяться на пристроях користувачів», – пояснила О. Грачова.

Згідно з російським Законом «Про персональні дані» інтернет-компанії зобов'язані зберігати на території Росії дані громадян РФ.

Щоправда, такі компанії, як Facebook, Twitter і Google проігнорували ці вимоги ***(Viber переносить частину своїх серверів в Росію // UkrainianWatcher (http://watcher.com.ua/2015/10/19/viber-perenosyt-chastynu-svoyih-serveriv-v-rosiyu/). – 2015. – 19.10).***

***

Трафик мессенджера Telegram полностью заблокирован в Иране, сообщает создатель сервиса П. Дуров в своем Twitter.

«Иранское министерство информации и связи потребовало у Telegram обеспечить их инструментами шпионажа и цензуры. Мы проигнорировали требование, они нас заблокировали», – пишет П. Дуров.

Как сообщает П. Дуров, команда разработчиков Telegram работает над созданием p2p-протокола, работающего по принципу «от пользователя к пользователю» без центрального сервера, что позволит обходить подобные блокировки ***(Дуров рассказал о блокировке Telegram в Иране // InternetUA (http://internetua.com/durov-rasskazal-o-blokirovke-Telegram-v-irane). – 2015. – 21.10).***

***

У Луганській області Служба безпеки України блокувала незаконну діяльність адміністратора антиукраїнської онлайн-спільноти.

25-річний студент, що навчався на бюджетному відділенні одного з вишів, створив групу в російській соціальній мережі. Він розповсюджував тексти та інші матеріали, спрямовані на повалення конституційного ладу України, зміну її державних кордонів, підтримку російсько-сепаратистських збройних угруповань, розпалювання національної та релігійної ворожнечі, ненависті, приниження національної честі та гідності українців, наругою над Гімном і Державним прапором України.

Відповідно до відкритого кримінального провадження за ч. 1 ст. 110 (посягання на територіальну цілісність і недоторканність України) Кримінального кодексу України тривають слідчі дії ***(На Луганщині СБУ затримала студента за інтернет-сепаратизм // InternetUA (http://internetua.com/na-luganskxin--sbu-zatrimala-studenta-za--nternet-separatizm). – 2015. – 25.10).***

***

Смольнинский районный суд Петербурга постановил прекратить деятельность группы MDK в соцсети «ВКонтакте» по требованию прокуратуры, заявившей о размещении на сайте оскорбительных материалов, пишут «Вести» (http://vesti-ukr.com/nauka-i-tehnologii/120952-sud-prikazal-zakryt-samoe-dorogoe-soobwestvo-vkontakte-mdk).

Материалы интернет-сообщества признаны запрещенными в России. Об этом ходатайствовала прокуратура города, ссылаясь на экспертные заключения по опубликованным в группе материалам, пишет РИА Новости.

Эксперты обнаружили в контенте MDK признаки дискриминации по национальной и религиозной принадлежности, а также те материалы, которые могут нанести вред психическому здоровью детей, подростков и молодежи.

По данным портала allsocial.ru MDK с показателем 6,8 млн подписчиков входит в топ-5 самых популярных пабликов «ВКонтакте» по количеству посетителей. В 2013 г. AIN.UA писал, что один рекламный пост в сообществе стоил около 20 тыс. грн, что являлось на тот момент самой дорогой записью в какой-либо группе соцсети ***(Суд приказал закрыть самое дорогое сообщество ВКонтакте MDK // «Вести» (http://vesti-ukr.com/nauka-i-tehnologii/120952-sud-prikazal-zakryt-samoe-dorogoe-soobwestvo-vkontakte-mdk). – 2015. – 27.10).***

***

Депутат Госдумы Д. Горовцов («Справедливая Россия») просит Генпрокурора Ю. Чайку проверить аккаунты украинского полка «Азов» в сети Интернет, и в частности в социальной сети «ВКонтакте», передает корреспондент ИА REGNUM.

По словам Д. Горовцова, к нему обращаются избиратели в связи с публикуемыми в Интернете материалами полка «Азов», в которых содержатся призывы к насилию и нарушению территориальной целостности Российской Федерации, демонстрируется нацистская символика.

Согласно полученной информации, руководство полка «Азов» возглавляет ряд неонацистских организаций Украины и имеет тесные связи с националистической организацией «Правый сектор», запрещенной в РФ, а члены полка придерживаются праворадикальных и неонацистских взглядов, пояснил депутат.

В этой связи парламентарий просит Ю. Чайку дать поручение провести проверку изложенной информации на предмет исполнения законодательства о противодействии экстремистской деятельности и при наличии законных оснований принять меры прокурорского реагирования ***(Депутат Госдумы просит Чайку проверить аккаунты «Азова» на экстремизм // ИА REGNUM (http://regnum.ru/news/society/2000443.html). – 2015. – 28.10).***

***

Руководство так называемой «ДНР» заявило о намерении наладить обратную связь с населением временно оккупированных территорий Донецкой области.

Об этом 28 октября заявил главарь «ДНР» А. Захарченко, анонсируя запуск своей официальной страницы в социальной сети Facebook, передает InfoResist со ссылкой на сепаратистское «Донецкое агентство новостей».

«На фоне приблизительного перемирия все большую остроту приобретают вопросы экономического восстановления и политического строительства. Более того, могу сказать, что чем меньше у нас войны – тем больше политики. И тем в большей степени оружием становится слово. Люди задают много вопросов, и на них надо отвечать», – рассказал А. Захарченко.

Но уже 29 октября утром официальная страница террориста А. Захарченко в Facebook оказалась заблокированной ***(Facebook заблокировал аккаунт террориста Захарченко сразу после его создания // GlavPost.Com (http://glavpost.com/post/29oct2015/Nets/62453-facebook-zablokiroval-akkaunt-terrorista-zaharchenko-srazu-posle-ego-sozdaniya.html). – 2015. – 29.10).***

***

Согласно исследованию экспертов из Citizen Lab, число правительственных структур, использующих шпионское ПО FinFisher, значительно возросло за последнее время. Специалисты из Citizen Lab в течение нескольких лет мониторили использование таких средств наблюдения, как FinFisher в странах с тоталитарным режимом правления. Стоит отметить,

что FinFisher является эксклюзивной шпионской программой, которая продается исключительно государственным учреждениям и правоохранительным органам.

Исследователи отслеживали физическое расположение серверов, подконтрольных немецкой структуре FinFisher GmbH, которая направлена на выслеживание операций и личностей злоумышленников. FinFisher способно удаленно управлять любым компьютером, которое ПО инфицировало, копировать файлы, перехватывать звонки в Skype, записывать каждое нажатие клавиш и пр.

FinFisher использует для работы главный сервер под названием FinSpy Master и многочисленные промежуточные серверы FinSpy Relay, которые выступают в роли C&C-серверов. Как только устройство инфицировано FinFisher, шпионская программа связывается с промежуточными серверами, которые, в свою очередь, передают информацию на главный сервер. Эксперты из Citizen Lab использовали инструмент Zmap, который помог обнаружить 135 серверов, в том числе главных и промежуточных. Как правило, главные серверы расположены у пользователей шпионского ПО, в то время как прокси-серверы могут находиться где угодно.

Самым интересным является тот факт, что именно промежуточные серверы, предназначенные для сокрытия главного сервера, помогли экспертам обнаружить расположения FinSpy Master. Если кто-то пытается подключиться к IP-адресу FinSpy Relay, ему отображается поддельная страница Google.com и Yahoo.com. Исследователи обнаружили, что, если ложная Google.com выполняет запрос «my ip address», поисковая система будет отображать реальный IP-адрес FinSpy Master.

В случае с Yahoo.com, эксперты использовали другой способ для обнаружения местоположения главного сервера. Исходный код веб-страницы уже содержал в себе данные о расположении FinSpy Master, так как Yahoo использует эти данные для отображения погоды и новостей на главной странице. Таким образом эксперты выяснили, что шпионское ПО FinFisher используется государственными структурами в 32 странах по всему миру, в том числе в Анголе, Египте, Иордании, Казахстане, Кении, Ливане, Марокко, Парагвае, Саудовской Аравии, Словении, Испании, Тайване, Турции и Венесуэле. В некоторых случаях исследователям даже удалось проследить IP-адрес конкретных государственных учреждений ***(Число использующих шпионское ПО FinFisher правительств значительно возросло // InternetUA (http://internetua.com/cislo-ispolzuuasxih-shpionskoe-po-FinFisher-pravitelstv-znacsitelno-vozroslo). – 2015. – 22.10).***

***

Американская компания Freedom House, которая ежегодно публикует доклад с обзором интернет-свободы в мире, перевела Россию из категории «частично свободных» в «несвободные» страны, сообщает РБК.

В докладе представлено 65 крупных стран, которые охватывают 88 % всех пользователей Интернета в мире. Каждой стране были присвоены баллы: 0 баллов – максимальная свобода, 100 баллов – максимальная несвобода.

Проранжировав страны по баллам, организация Freedom House разделила их на три группы: «свободные», «частично свободные» и «несвободные». В 2015 г. Россия опустилась из категории «частично свободные» в «несвободные» страны, набрав 62 балла против 60 в прошлом году.

По мнению Freedom House, свободными в Рунете являются лишь темы сатиры и обсуждения этнических меньшинств, остальные же подвержены цензуре. К ним относятся: критика власти, военные конфликты, коррупция, оппозиция, протестная мобилизация, права сексуальных меньшинств, вопросы социальной сферы и богохульства. Эксперты фонда говорят, что основной причиной отнесения России к категории «несвободных», являются законы о переносе данных и борьбе с экстремизмом ***(России присвоен статус страны с «несвободным Интернетом» // IGate (http://igate.com.ua/lenta/11057-rossii-prisvoen-status-strany-s-nesvobodnym-internetom). – 2015. – 30.10).***

***

Оккупанты начали штрафовать крымчан за посты в соцсетях.

Верховный суд оккупированного Крыма оштрафовал жителя Бахчисарая на 9 тыс. р. за якобы пропаганду и оправдание нацизма. Об этом сообщили сегодня в пресс-службе прокуратуры Крыма, пишет «Главком» (http://glavcom.ua/news/336648.html).

По информации пресс-службы, 18-летний бахчисараец признан виновным в совершении преступлений, предусмотренных ч. 1 ст. 282 (возбуждение ненависти либо вражды, а равно унижение человеческого достоинства) ч. 1 ст. 354.1 УК РФ (реабилитация нацизма) УК РФ.

Согласно материалам прокуратуры, бахчисараец разместил на своей странице в социальной сети «ВКонтакте» текстовые, аудио- и видеозаписи, которые якобы содержат признаки пропаганды и оправдания нацизма, одобрения преступлений нацистов и их русских пособников ***(Оккупанты начали штрафовать крымчан за посты в соцсетях // Главком (http://glavcom.ua/news/336648.html). – 2015. – 30.10).***

***

Общение в социальных сетях хотят сделать наказуемым. Закон об авторском праве может стать инструментом цензуры.

Под видом борьбы с видео-пиратством через парламент пытаются протянуть закон, который сделает общение в социальных сетях уголовным преступлением.

Законопроект об авторском праве возможно установит полный контроль над интернет-контентом, передает Хроника.инфо со ссылкой на сайт ТСН.

Законопроект на скорую руку подготовило Минэкономики.

Он подразумевает процедуру безусловного блокирования контента по одной электронной жалобе ***(Общение в социальных сетях хотят сделать наказуемым // Хроника.инфо (http://hronika.info/videonovosti/96597-obschenie-v-socialnyh-setyah-hotyat-sdelat-nakazuemym-video.html). – 2015. – 1.11).***

Проблема захисту даних. DDOS та вірусні атаки

Исследователи обнаружили уязвимость в алгоритме Диффи-Хеллмана, широко используемого в шифровании данных по всему миру. По словам экспертов, представивших результаты своих трудов на конференции ACM Conference on Computer and Communications Security, брешь позволила АНБ США расшифровывать большинство HTTPS, SSH и VPN-соединений.

Брешь заключается в предусмотренном протоколом способе обмена ключами. В алгоритме применяется ограниченный набор простых чисел, которые часто повторно используются. Для того чтобы взломать хотя бы одно число в 1024-битном ключе, понадобится в течение года пытаться расшифровать его с помощью суперкомпьютера. Такой процесс обойдется злоумышленникам в сотни миллионов долларов.

Исследователи считают, что АНБ США успешно проэксплуатировала эту уязвимость, что позволило агентству расшифровать как минимум 66 % всех зашифрованных VPN и четверть SSH-серверов во всем мире. Расшифровав второе 1024-битное число, АНБ смогла перехватывать данные с примерно 20 % крупнейших HTTPS-серверов. Агентству не составляет труда осуществлять настолько дорогостоящие операции, поскольку, как следует из документов Э. Сноудена, финансирование одного лишь криптоаналитического отдела АНБ составляет 11 млрд дол. в год.

Примерно 92 % крупнейших HTTPS-доменов в мире используют два основных числа в реализации алгоритма Диффи-Хеллмана. Исследователи опасаются, что АНБ может в любой момент взломать используемое ресурсами шифрование и получить доступ ко всему трафику, проходящему через эти серверы ***(Один из наиболее надежных алгоритмов шифрования оказался подвержен уязвимости // InternetUA (http://internetua.com/odin-iz-naibolee-nadejnih-algoritmov-shifrovaniya-okazalsya-podverjen-uyazvimosti). – 2015. – 19.10).***

***

Несмотря на обещания С. Цзиньпина, как сообщают частные аналитики, хакеры Китая осуществили по крайней мере семь атак на американские компании с момента визита председателя КНР в США, который состоялся в прошлом месяце.

При этом, согласно The Washington Post, представитель Кибер-команды США отметил, что пока «слишком рано» оценивать, изменил ли Китай свое поведение.

На протяжении трех недель по завершению визита С. Цзиньпина – включая день его отъезда, 26 сентября – хакеры, которые имеют отношение к правительству Китая, попытались получить доступ к сетям технических и фармацевтических компаний. Об этом заявил в своем отчете, опубликованном в понедельник, 19 октября, Д. Алперович, соучредитель и главный технический директор компании CrowdStrike.

По его словам, хакерские атаки продолжаются и в настоящее время, иногда по несколько раз в день, что не похоже на обычные действия хакеров-разведчиков, на которых не распространяется обещание С. Цзиньпина ***(Китайские хакеры продолжают атаковать американские фирмы // Эксперт (http://www.expert.ua/novosti/0/731-kitajskie-hakeri-prodolzhayut-atakovat-amerikanskie-firmi). – 2015. – 19.10).***

***

Специалисты компании Malwarebytes обнаружили весьма интересный образчик вредоносного ПО. Малварь, получившая имя eFast Browser, стремится подменить собой весь браузер жертвы вообще, вместо того, чтобы заражать существующий.

На первый взгляд eFast Browser, это обычный представитель adware, способный на уже привычные пакости: на экране то и дело всплывают рекламные баннеры, нежелательная реклама появляется на страницах сайтов, пользователя всеми правдами и неправдами пытаются заставить перейти на вредоносный ресурс. И, конечно, малварь следит за каждым шагом жертвы, чтобы продать нелегальным рекламщикам побольше ценных данных о пользователе, дабы те могли показывать ему еще больше рекламы.

Следующими о проблеме рассказали ИБ-специалисты компании Malwarebytes, и они заметили интересную вещь. eFast Browser не пытается взломать браузер пользователя, он пытается заменить его. По данным исследователей, вредонос удаляет с зараженной машины Chrome, занимает его место и подменяет рекламными ссылками все, что только сможет. При этом иконка браузера и его дизайн выглядят в точности, как настоящий Chrome. Это и не удивительно, ведь малварь базируется на open source движке Chromium, так что подделка весьма качественная. Судя по всему, браузер сделан компанией Clara Labs, известной похожими браузерами BoBrowser, Tortuga и Unico.

Swift отмечает, что со стороны авторов малвари, это вполне разумный ход. Chrome в последнее время закручивает гайки все туже, в частности, не позволяет устанавливать сторонние расширения, поступившие не из официального магазина Google. В схожем направлении движутся браузеры Mozilla Firefox и Microsoft Edge. В такой ситуации полностью заменить браузер проще, нежели ломать настоящий.

По данным PCrisk, eFast распространяется преимущественно в комплекте с различным бесплатным софтом с подозрительных веб-сайтов. Случайно подцепить эту заразу весьма затруднительно, а удалить, к счастью, легко – как любую другую программу ***(Вредонос подменяет собой весь браузер сразу // InternetUA (http://internetua.com/vredonos-podmenyaet-soboi-ves-brauzer-srazu). – 2015. – 20.10).***

***

Хакеры Исламского государства предпринимают попытки взлома сетей американских энергетических компаний. Об этом сообщили представители

ФБР во время конференции GridSecCon, на которой присутствовали представители энергопредприятий.

Следователи не сообщили ни подробностей об инцидентах, ни обнародовали доказательства конкретных атак, однако уточнили, что все попытки оказались безуспешными. Отмечается, что в настоящее время террористы не применяют сложные инструменты, которые предназначены для взлома компьютерных систем и вызова отказа в работе.

«Твердые намерения, но, к счастью, скромные возможности. Мы опасаемся, что они (хакеры. – Ред.) купят новые техники», – цитирует издание CNNMoney слова руководителя отдела по борьбе с кибер-преступностью ФБР Д. Ригги.

В ведомстве опасаются, что Исламское государство или его сторонники приобретут на черном рынке вредоносное ПО, которое затем будет использоваться для инфицирования компьютеров и уничтожения электроники. При этом, атаки на энергетические компании могут существенным образом повлиять на энергоснабжение страны.

По словам Д. Ригги, американские спецслужбы проводят тщательный мониторинг компьютерных сетей и оперативно делятся полученной информацией с правоохранительными органами ***(Исламские хакеры безуспешно атакуют американский энергосектор // InternetUA (http://internetua.com/islamskie-hakeri-bezuspeshno-atakuuat-amerikanskii-energosektor). – 2015. – 20.10).***

***

Сервис анализа кода SourceDNA обнаружил в App Store множество «проблемных» приложений, размещенных в китайском разделе магазина. По словам специалистов, приложения использовались для сбора персональных данных, причем делалось это без ведома пользователей. Все собранные данные переправлялись на сервера китайской компании Youmi. SourceDNA выявил в App Store 256 приложений, использующих одинаковый SDK. Все они были доступны в магазине в течение нескольких месяцев. За это время общее количество скачиваний превысило отметку в 1 млн.

Среди данных, которые были собраны с помощью приложений, были списки установленных программ, идентификаторы мобильных устройств и адреса электронной почты.

Компания Apple отреагировала на ситуацию практически моментально – все приложения были удалены из App Store. Это было сделано в связи с тем, что использование подобных SDK противоречит соглашениям о безопасности и конфиденциальности. Чтобы не допустить повторения этой ситуации в будущем, корпорация усилит меры защиты и проверки приложений ***(В китайском App Store обнаружили 256 вредоносных приложений // IGate (http://iqate.com.ua/lenta/10808-v-kitajskom-app-store-obnaruzhili-256-vredonosnyh-prilozhenij). – 2015. – 20.10).***

***

Інженер Е. Батлер розробив додаток для браузера Firefox, який дає змогу отримати доступ до персональної інформації користувачів соціальних мереж, і виклав програму для вільного завантаження на своєму сайті. Про це пише Watcher.

Додаток Firesheep використовує дірки у безпеці Wi-Fi мереж – оскільки мережі з відсутністю шифрування (без паролю) є доволі вразливими та відкритими для доступу зловмисників.

Firesheep робить це все автоматично – шляхом підміни cookie-файлів, тому той, хто його встановить, може, наприклад, легко читати особисту переписку інших людей, які використали нешифроване Wi-Fi підключення для відвідування соціальних мереж.

Усього за одну добу додаток завантажили понад 100 тис. разів.

Як пише видання, зважаючи на широкий функціонал Firesheep, отримувати конфіденційні дані можна з багатьох сайтів, таких як Amazon, Google, Flickr, Facebook. Twitter, Tumblr, WordPress, та багато ін. Видання не виключає, що Firesheep уже дає змогу отримувати конфіденційні дані з популярної в Україні соцмережі «ВКонтакте».

Тому Watcher радить використовувати лише мережі Wi-Fi з шифруванням даних.

Разом з тим інтернет-ентузіасти вирішили не чекати і випустили додаток, який може блокувати будь-які спроби Firesheep зайти у ваші акаунти.

Як писав MediaSapiens, спецслужби США, використовуючи розробки вчених з Університетського коледжу Лондона, зацікавилися можливістю відслідковувати переміщення людини в сусідньому приміщенні за допомогою Wi-Fi ***(Додаток Firesheep дає змогу вкрасти ваші дані у випадку під'єднання до відкритого Wi-Fi // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/dodatok_firesheep_dae_zmogu_vkrasti_vashi_dani_u_vipadku_pidednannya_do_vidkritogo_wifi/). – 2015. – 20.10).***

***

ИБ-исследователь из Pen Test Partners К. Манро провел очень интересный эксперимент, во время которого ему удалось взломать «умные» чайники по всему Лондону, продемонстрировав таким образом слабую защиту безопасности точек доступа Wi-Fi. В исследовании К. Манро использовал iKettle – серию смарт-чайников, работу которых можно контролировать дистанционно с помощью мобильных устройств.

Эксперт заявляет, что с помощью социальной инженерии, направленной антенны и некоторого сетевого оборудования злоумышленники могут завладеть паролем от точки доступа Wi-Fi жертвы. Самое интересное, что пользователи могут управлять «умным» чайником через учетную запись в Twitter, используя обращение @wifikettle. Поэтому хакерам не составит большого труда найти в сети владельцев iKettle.

В случае, если iKettle не сконфигурирован, злоумышленники могут воспользоваться базой данных специального сайта wigle.net, который собирает информацию о всех беспроводных точках доступа по всему миру. Очень часто

на ресурсе можно найти координаты GPS, SSID, MAC-адрес и тип шифрования точки доступа.

«Если смарт-чайник не сконфигурирован, хакерам очень просто узнать место проживания жертвы и взломать ее устройство. Злоумышленники могут настроить вредоносную сеть с тем же SSID, только с более сильным сигналом, к которому iKettle подключится перед получением пакета дизассоциации, что и приведет к неполадкам с беспроводной сетью. Удаленный хакер может использовать направленную антенну, перехватить соединение iKettle, отправить две команды и получить доступ к ключу беспроводной сети в виде простого текста», – отметил К. Манро.

К. Манро также добавил, что с помощью социальных сетей можно обнаружить пользователей сконфигурированных чайников, раскрыть WPA-PSK, что позволяет скомпрометировать маршрутизатор и осуществить различные типы атак, в том числе перенаправление DNS-запросов ***(Взлом «умных» чайников может стать причиной похищения персональных данных // InternetUA (http://internetua.com/vzlom--umnih--csainikov-mojet-stat-pricsinoi-pohisxeniya-personalnih-dannih). – 2015. – 21.10).***

***

Как выяснил инженер компании Microsoft Д. Майерс, популярный менеджер паролей 1Password хранит данные пользователей в открытом виде, не подвергая их шифрованию. Проблема связана с функцией синхронизации 1PasswordAnywhere, позволяющей пользоваться сервисом на любом устройстве. 1PasswordAnywhere использует для хранения данных формат AgileKeychain, представляющий собой архив из незашифрованных JavaScript-файлов.

Формат .agilekeychain представляет собой директорию, в которой, в том числе, находится файл 1password.html. Открыв его в обычном веб-браузере, пользователь должен будет ввести пароль, после чего keychain разблокируется, предоставив доступ к информации. Проблема состоит в отсутствии шифрования метаданных – все данные пользователя хранятся в открытом виде в файле 1Password.agilekeychain/data/default/contents.js.

Как выяснилось, разработчики специально спроектировали 1Password таким образом, чтобы метаданные хранились в незашифрованном виде. Благодаря этому удается якобы повысить производительность программы, уменьшив необходимое для шифрования данных время. Разработчики не видят в этом никакой проблемы и не собираются выпускать исправление для 1Password.

Единственным способом защитить данные пользователя является переход на формат OPVault. Разработчики 1Password сменили формат хранения данных еще в 2012 г., но как формат по умолчанию программа до сих пор рекомендует использовать Agile Keychain ***(Популярный менеджер паролей 1Password хранит данные в открытом виде // InternetUA (http://internetua.com/populyarnii-menedjer-parolei-1Password-hranit-dannie-v-otkritom-vide). – 2015. – 20.10).***

***

Бывший работник Facebook Н. Фэлтон в течение 10 лет самостоятельно собирал всю личную информацию о себе, сообщает Wired.

С помощью заметок на своем сотовом телефоне Н. Фэлтон документировал основные события и моменты в жизни, включая передвижения, электронные письма, прослушанную музыку и даже появление седых волос на голове. Вся информация затем структурировалась в виде ежегодных отчетов. В 2012 г. энтузиаст даже создал приложение для iOS, через равные промежутки напоминавшее ему о необходимости занести новые данные в заметки.

По словам самого Н. Фэлтона, его отчеты показывают уровень развития технологий сбора персональных данных. Так, его последний отчет полностью составлен из информации, полученной с помощью приложений для смартфона. Кроме того, энтузиаст также хотел привлечь внимание общественности к проблеме массового сбора персональных данных ***(Бывший работник Facebook 10 лет самостоятельно собирал свои персональные данные // InternetUA (http://internetua.com/bivshii-rabotnik-Facebook-10-let-samostoyatelno-sobiral-svoi-personalnie-dannie). – 2015. – 21.10).***

***

По данным исследования компании ProtectMyID, большинство потребителей опасаются стать жертвой кибермошенников во время совершения онлайн-покупок и использования интернет-банкинга.

73 % респондентов опасаются за свои личные данные, которые они указывают при использовании банковских сайтов. При этом почти две трети из более чем 1 тыс. взрослого населения США заявили, что чувствуют подобный страх при осуществлении онлайн-покупок.

Около 70 % опрошенных беспокоятся за свою безопасность во время использования публичного Wi-Fi. Примерно такое же количество респондентов обеспокоены безопасностью во время входа в интернет-банкинг.

Почти половина всех респондентов на сегодня используют дополнительные меры безопасности для предотвращения кражи личных данных. Тем не менее, исследование также показало, что люди не пользуются простыми мерами, которые могут значительно повысить безопасность их данных.

Так, например, более 50 % пользователей не проверяют есть ли на сайте иконка с замком, которая свидетельствует о безопасном соединении с сайтом (эта иконка находится в адресной строке браузера, слева от введенного веб-адреса).

Кроме того, 50 % не защищают паролем свои смартфоны. 55 % не закрывают веб-браузер, после того как заканчивают пользоваться своим интернет-банкингом. 15 % сохраняют записи своих паролей и PIN-кодов в бумажниках, мобильных устройствах и компьютерах.

Несмотря на все эти опасения, 80 % респондентов заявили, что хотели бы чаще, чем сейчас использовать интернет-соединения ***(Чего опасаются онлайн-покупатели? // InternetUA (http://internetua.com/cego-opasauatsya-onlain-pokupateli). – 2015. – 21.10).***

***

Несколько моделей жёстких дисков компании Western Digital с самошифрованием обладают многочисленными уязвимостями, позволяющими при получении доступа к диску получить доступ и к хранящимся на нём данным, зачастую даже не имея ключа дешифрования. Об этом говорится в опубликованной недавно работе группы исследователей. Уязвимостями затронуты внешние жёсткие диски под брендами My Passport и My Book (было рассмотрено шесть моделей), и сохранить данные не помогают даже длинные пароли. Функция самошифрования данных призвана избавить пользователей от необходимости установки специального программного обеспечения для полного шифрования дисков.

Большинство рассмотренных дисков при шифровании и дешифровании данных использовали мост USB для подключения компьютера к интерфейсу SATA диска. Доступ к интерфейсу должен быть закрыт, пока пользователь не введёт пароль. Чтобы противостоять атакам, при которых злоумышленник подбирает миллиарды вариантов пароля в секунду, пароль шифруется и тысячу раз обрабатывается функцией SHA256.

Однако ошибки реализации этого метода всё же позволяют подобрать пароль весьма быстро. В одном случае ключ был предсказуемым, генерируясь на основе текущего времени на компьютере. Эта уязвимость была закрыта в прошлом году, однако обновления установили далеко не все обладатели данных дисков. В другом случае хэш (зашифрованный пароль) можно было извлечь с диска на компьютер и взламывать уже там.

Ещё одна уязвимость даёт доступ без знания пароля вовсе. Диски поставляются с паролем по умолчанию, и при его смене ключ для дефолтного пароля продолжает храниться на диске, что даёт возможность расшифровать его. Этой проблемы можно избежать, сменив пароль дважды.

Во избежание кражи данных в подобных случаях рекомендуется всё же использовать приложения для шифрования от зарекомендовавших себя производителей, вроде Symantec ***(В жёстких дисках Western Digital с самошифрованием обнаружили множество уязвимостей // InternetUA (http://internetua.com/v-j-stkih-diskah-Western-Digital-s-samoshifrovaniem-obnarujili-mnojestvo-uyazvimostei). – 2015. – 23.10).***

***

Представители Международной ассоциации Independent Systems Audit and Control Association (ISACA) сообщили, что предприятия еще не готовы к отражению APT-атак. Такое заявление они сделали на конференции по кибер-безопасности CSX 2015, которая с 19 по 21 октября нынешнего года прошла в Вашингтоне, округ Колумбия, США.

Согласно данным проведенного ISACA опроса, более четверти респондентов (28 %) столкнулись с APT-угрозами в текущем году. По словам председателя международного совета директоров ISACA Х. Димитриадиса, осуществление атак повышенной сложности стало нормой, а использование

инструментария и методик APT позволило осуществить множество знаковых взломов.

49 % опрошенных ИБ-специалистов выделяют APT в отдельную разновидность кибер-атак, в то время как остальные эксперты считают их традиционными угрозами. Более половины респондентов считают, что существует большая угроза APT-атаки на их организацию.

Исследователи отметили, что крупные бизнес-структуры в целом полагаются на технические средства защиты от атак. В то же время тренингу сотрудников почти не уделяется внимания, вследствие чего злоумышленники могут получить доступ к внутренним сетям компаний, применяя технологии социальной инженерии.

В то же время наблюдаются положительные тенденции. Руководящее звено стало уделять больше времени обеспечению информационной безопасности компаний. 80 % ИБ-специалистов ощутили заметный рост поддержки со стороны высшего руководства.

Справка: APT (сложная постоянная угроза) является высокоточной кибер-атакой. С другой стороны, APT можно назвать группу, спонсируемую государством либо иным покровителем, оплачивающим целевую атаку ***(Готовность организаций к отражению APT-атак оставляет желать лучшего // InternetUA (http://internetua.com/gotovnost-organizacii-k-otrajeniua-APT-atak-ostavlyaet-jelat-lucsshego). – 2015. – 23.10).***

***

Как хакеры могут приблизить смерть смартфона

Редкая генетическая аномалия под названием «прогерия» приводит к появлению признаков старости у молодых людей. Сюжет раннего старения обыгрывался во многих романах и художественных фильмах. К примеру, в фильме «Джек» Р. Уильямс сыграл мальчика, взрослеющего в четыре раза быстрее сверстников. Создание «Загадочной истории Бенджамина Баттона» также было вдохновлено этим расстройством. Но недавно исследователи Нью-Йоркского университета опубликовали работу, где рассказали, как можно заразить устройства, вроде смартфонов, цифровой версией этой болезни, пишет TechCrunch.

В статье под названием «Магия: Злонамеренное старение в схемах/ядрах» (MAGIC: Malicious Aging in Circuits/Cores) программисты университета описали серию методов, позволяющих атаковать аппаратную составляющую устройства. При этом интегральные схемы перегружаются и быстрее изнашиваются. К примеру, атакованный смартфон начинает работать медленнее или даже отказывает.

«Обычно, когда компании производят интегральные схемы, они проектируются на определенную продолжительность “жизни”. Но когда мы изучали процесс старения, то обратили внимание, что он зависит от программной составляющей. Если вы запускаете определенные программы, то можете заставить деградацию происходить быстрее, – говорит А. Канупарти, один из авторов исследования. – Так что мы смогли создать вредоносную

программу, которая, будучи запущенной на смартфоне, сможет уничтожить его за месяц».

Зачем кто-то может делать подобное? Есть много причин, по которым потребители, или даже сами компании, могли бы попытаться использовать подобные программы для «убийства» устройств.

Первый сценарий, который описывает исследование, называется гарантийным сценарием. «Допустим, вы купили новый телефон, но производитель объявляет о выпуске новой модели. Вы хотите этот более новый телефон, – говорит А. Канупарти. – Тогда достаточно загрузить приложение, запустить его на своем смартфоне, а затем сказать, что он сломан и поменять на более новую модель». По сути, программа просто мучает процессор телефона до смерти. «Думайте об этом следующим образом. Если вы будете есть слишком много сырных шариков и пить много сладкой газировки, что с вами произойдет? По сути, мы делаем то же самое: устраиваем транзисторам на интегральной схеме стресс, принудительно нагружая их», – говорит А. Канупарти.

Запланированное устаревание

Второй сценарий – сценарий запланированного устаревания. В этом случае компания, стремящаяся продать больше новых устройств, может преднамеренно ухудшить работу более старой версии, чтобы вынудить пользователей проводить апгрейд. «Компании могут принуждать пользователей покупать более новые устройства, – утверждает А. Канупарти. – Было несколько случаев, все они описаны в исследовании, когда крупные компании подозревались в использовании метода запланированного устаревания. К примеру, Blu-ray плеер, ломающийся за день до истечения гарантийного срока. Или телефон, который начинает работать медленнее после очередного обновления накануне выхода новой модели. Тогда вы идете в магазин, пробуете эту новую модель, видите потрясающий прирост производительности, и вынуждены покупать новый аппарат».

Третий сценарий – спонсируемые государством аппаратные «черные ходы». «В этом сценарии, к примеру, одна страна закупает военную технику у другой. У страны-продавца сегодня могут быть дружественные отношения со страной-покупателем, но ведь никто не знает, что произойдет завтра», – говорит А. Канупарти. Страна-продавец может захотеть состарить и испортить проданную технику, активировав предустановленный вредоносный код.

Исследователи продолжают изучать как возможности порчи устройств, так и способы смягчения подобных атак. Многие производители интегральных схем смогут использовать эти данные для противодействия злонамеренному старению. Будущие исследования будут направлены на смягчение атак на архитектуру процессора. Учитывая недавние примеры, вроде скандала с компанией Volkswagen, когда встроенное программное обеспечение обманывало экологические тесты, потребительские контрольные комиссии и другие регуляторы обязаны обратить особое внимание на возможность злонамеренного старения техники. Каждый подозрительный случай должен быть тщательно изучен ***(Как хакеры могут приблизить смерть смартфона //***

InternetUA (http://internetua.com/kak-hakeri-mogut-priblizit-smert-smartfona). – 2015. – 22.10).

***

Ученый из Университета Глазго совместно со своим коллегой из исследовательской лаборатории Symantec проанализировали сложность интеллектуального подбора пароля и выяснили, что добавление символов верхнего регистра и цифр не делает пароль значительно устойчивее по сравнению с первоначальным. Большую эффективность показало банальное удлинение пароля или использование специальных символов. Результаты своей работы авторы опубликовали в сборнике ACM CSS 2015.

Исследователи использовали для атаки интеллектуальные алгоритмы, которые предварительно были обучены на базе данных, представляющей собой десять миллионов слитых в сеть в открытом виде паролей. После обучения они проверили эффективность алгоритмов на 32 млн других паролей.

Авторы использовали различные методы атак, основанные на N-граммах, вероятностной контекстно-свободной грамматике и экспоненциальной выдержке, из которых наилучшие результаты при подборе показал последний. Суть этого алгоритма заключается в правильном подборе частоты некоторого процесса с помощью проверок, расстояние между которыми растет экспоненциально.

Например, в некоторых сетях алгоритм экспоненциальной выдержки используется для определения подходящего времени между запросами к определенному, часто довольно загруженному, узлу. Время между запросами изменяется примерно как степень двойки.

На основании этой проверки авторы предложили новую шкалу сложности угадываемого пароля. Оказалось, что наиболее эффективными способами для усложнения взлома пароля являются удлинение пароля и добавление символов, не являющихся цифрами или алфавитными буквами, а использование символов верхнего регистра и цифр не позволяет достичь такого же эффекта.

Исследователи объясняют это тем, что люди в своих паролях обычно используют символы верхнего регистра в начале пароля, а цифры в конце. По словам авторов, основной способ сделать пароль более надежным тривиален – надо сделать его менее предсказуемым ***(Регистр и цифры в пароле оказались бесполезными для его устойчивости к взлому // InternetUA (http://internetua.com/registr-i-cifri-v-parole-okazalis-bespoleznimi-dlya-ego-ustoicsivosti-k-vzlomu). – 2015. – 26.10).***

***

Наш смартфон – это приложения, которые мы используем. Без них он был бы просто бесполезным экраном с набором микросхем. Разумеется, все мы используем разные приложения и с разной интенсивностью. Однако есть самые популярные приложения, а еще есть приложения, которые активнее других используют ресурсы смартфона. Команда AVG поделилась своими данными о тех приложениях, которые больше всего нагружают смартфон, съедают память и разряжают аккумулятор. Стоит быть с ними повнимательнее.

AVG собирают анонимные данные с пользователей своих антивирусных приложений для Android из США, Великобритании и Австралии. Затем они распределяют приложения, используемые пользователями, на четыре категории: влияющие на производительность, потребляющие трафик, разряжающие аккумулятор и отнимающие место на накопителе.

На этот раз самым требовательным приложением оказался Snapchat. Неудивительно, ведь он одновременно использует камеру, данные о местоположении и подключение к сети. Приложение Snapchat было замечено в пятерке худших в трех категориях.

Однако гораздо страшнее те приложения, которые начинают свою работу с момента запуска смартфона. Facebook закрепляет за собой звание главного врага вашего смартфона, лидируя по трем категориям. Стоит также отметить, что Chrome – единственный браузер, обвиняемый в излишнем потреблении памяти, а предустановленные приложения от Samsung вообще не должны были показываться в подобных рейтингах, но они попались ***(Социальные сети – злейший враг вашего смартфона // InternetUA (http://internetua.com/socialnie-seti---zleishii-vrag-vashego-smartfona). – 2015. – 26.10).***

***

У ніч перед виборами, 24 жовтня, прихильники однієї з політичних партій зламали сервер сайтів телеканалу ICTV та його редакції новин «Факти» і запустили на них відеорекламу однієї з політичних партій. Про це повідомила прес-служба каналу.

Проблему виправили, однак через хакерську атаку відеофайли ICTV, які були опублікуванні сайті за останні три місяці, не підлягають відновленню.

«По факту завданої шкоди телеканал проведе службове розслідування. Наразі відомо, що атака хакерів була здійснена на всі інтернет-ресурси групи StarLigtMedia», – зазначили в прес-службі ***(У ніч виборів хакери атакували інтернет-ресурси StarLigtMedia // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/u_nich_viboriv_khakeri_atakuvali_internetresursi_starligtmedia/). – 2015. – 25.10).***

***

В ночь с 24 на 25 октября произошла хакерская атака на контроллеры доменов во внутренних сетях ведущих телевизионных групп Украины: StarLightMedia, Медиа Группы Украина и Интер Медиа Групп. Вследствие этих действий большинство сайтов не работала, а IT-инфраструктура некоторых телеканалов была парализована. Об этом сообщается в распространенном релизе.

Этими действиями было нарушено право граждан на доступ к информации, размещенной на сайтах телеканалов. Этот факт особенно неприятен, поскольку именно 25 октября в Украине проходили всеукраинские выборы в местные советы.

«Телеканалы готовят обращение в правоохранительные органы с требованием предпринять все необходимые меры и привлечь виновных к ответственности. Рассчитываем, что правоохранители в ближайшее время

обнаружат злоумышленников», – говорится в релизе ***(Хакеры атаковали крупнейшие телегруппы // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45094/118/lang,ru/). – 2015. – 26.10).***

***

«Доктор Веб» предупреждает о появлении новой вредоносной программы, инфицирующей мобильные устройства под управлением операционной системы Android. Зловред получил обозначение Android.BankBot.80.origin.

Троян замаскирован злоумышленниками под официальное приложение-клиент одной из российских кредитных организаций и имеет соответствующее имя, а также значок, скопированный из настоящего банковского клиента для Android. Если обманутый пользователь установит и запустит программу, она попытается получить доступ к правам администратора, демонстрируя соответствующий запрос снова и снова до тех пор, пока жертва не согласится выполнить требуемое действие.

Проникнув на мобильное устройство, зловред сканирует адресную книгу пользователя и отправляет по всем найденным в ней телефонным номерам SMS вида «Привет, проголосуй за меня http://******konkurs.ru/». При переходе по указанному в сообщении веб-адресу пользователи попадают на мошеннический сайт, якобы связанный с проводимым в настоящее время конкурсом фотографии. С этого ресурса на мобильные устройства потенциальных жертв автоматически загружается одна из модификаций вредоносной программы.

Одновременно с рассылкой SMS-спама троян соединяется с управляющим сервером и передаёт на него сообщение об успешном заражении Android-смартфона или планшета. После этого зловред ожидает получения указаний от кибер-преступников, для чего с определённой периодичностью связывается с удалённым узлом на предмет появления новых директив. Троян, в числе прочего, может инициировать переадресацию звонков на указанный номер, а также выполнять USSD-запросы.

Главным предназначением программы является незаметная кража денег у российских клиентов ряда сотовых операторов, кредитных организаций, а также пользователей нескольких популярных платёжных систем. При наличии средств на счёте мобильного телефона жертвы троян пытается осуществить денежный перевод в пользу злоумышленников с использованием специализированных сервисных номеров, таких как 7878 и 3116. А если средства присутствуют на банковском счёте или счёте платежной системы, зловред предпринимает попытки похитить их, отправив соответствующую сервисную команду в текстовом сообщении ***(Новый троян ворует деньги у владельцев Android-устройств // InternetUA (http://internetua.com/novii-troyan-voruet-dengi-u-vladelcev-Android-ustroistv). – 2015. – 27.10).***

***

Специализирующаяся на безопасности компания Palo Alto Networks обнаружила 18 тыс. приложений для Android, которые крадут SMS. Все они

созданы с помощью бесплатного SDK от китайской рекламной компании Toamike.

Всего было обнаружено 63 тыс. приложений на базе SDK Toamike, но только 18 тыс. имели вредоносный код для отправки содержимого SMS (номера и текста) на серверы Toamike.

Шпионские приложения разработаны китайскими компаниями и предназначены для внутреннего рынка. В магазине Google Play их нет ***(Китайские Android-приложения крадут SMS // InternetUA (http://internetua.com/kitaiskie-Android-prilojeniya-kradut-SMS). – 2015. – 26.10).***

***

Расширенный функционал поиска в социальной сети Facebook, который с недавнего времени будет искать информацию среди 2 трлн постов, заставил пользователей вновь задуматься о приватности, передает The Guardian.

Ранее Facebook позволял искать только по публичным страницам, группам и местам, теперь в соцсети индексируются и личные странички. В связи с этим многие из пользователей забеспокоились о том, что посты многолетней давности могут стать доступными для широкой общественности. Несмотря на изменение настроек приватности, более ранние посты, сделанные при других конфигурациях, якобы могут попасть во всеобщий доступ.

Тем не менее вице-президент команды соцсети, занимающейся функциями поиска, Т. Стоки поспешил разъяснить алгоритм работы новой функции. «Результаты вашей поисковой выдачи индивидуальны и уникальны, вы можете видеть те посты, которыми с вами поделились. Кроме этого, вы в любой момент можете настроить “аудиторию” и посты, которые ей доступны», – рассказал Т. Стоки ***(Расширенный поиск в Facebook заставил пользователей позаботиться о приватности // InternetUA (http://internetua.com/rasshirennii-poisk-v-Facebook-zastavil-polzovatelei-pozabotitsya-o-privatnosti). – 2015. – 27.10).***

***

Исследователь из Калифорнийского университета в Лос-Анджелесе представил заслуживающий внимания доклад на конференции ACM CCS 2015. По данным ученого, новая технология передачи данных и голоса по сети LTE (VoLTE) небезопасна.

Технология VoLTE еще совсем новая, внедрять ее начали только в 2014 г., но ее уже используют (или собираются использовать) крупнейшие операторы сотовой связи разных стран мира, включая Verizon, AT&T и T-Mobile. Тем прискорбнее узнать, что технология несовершенна.

Г. Ту рассказал об обнаружении ряда проблем в VoLTE сетях. Ученый «ставил опыты» в сетях сразу двух провайдеров, названий которых он, по понятным соображениям, не раскрывает. При помощи рутованного телефона и компьютера он сумел подделать свой трафик, выдав его за трафик VoLTE. Используя этот метод, исследователь сумел разорвать соединение жертвы DDoS-подобной атакой, а также подделать стоимость вызовов, взвинтив счета ни в чем неповинных пользователей до небес.

Согласно отчету, уязвимости связаны с фундаментальными проблемами, которые возникают вследствие передачи голоса и данных по одним и тем же каналам связи. На сегодня стандарт VoLTE разделяет данные на три канала: обычная сотовая связь, более приоритетные голосовые звонки и канал с наивысшим приоритетом – для пакетов данных, которые координируют вышеупомянутые звонки (их называют signal headers). Распределение данных по этим каналам, как правило, происходит на аппаратном уровне, но ученый обнаружил, что защиту можно обойти, а пакеты данных, к примеру, можно перенаправить в другой канал.

Исследователь пишет, что некоторые найденные им проблемы уже были исправлены сотовыми операторами, но другие баги нельзя «починить», не изменив при этом всю структуру VoLTE вообще. На сегодня Федеральная комиссия связи США требует, чтобы голосовые данные имели приоритет над обычными данными, так как VoLTE должна обеспечивать такое же хорошее качество связи, как и обыкновенная сотовая связь. Если звонок будет прерываться из-за любого обновляющегося на фоне приложения, это не вариант. К тому же система распределения должна обеспечивать взаимодействие между различными операторами, из-за чего им приходится использовать так называемые clear signal, которые можно отреверсить и проделать то же самое, что показал на конференции Г. Ту.

Сам исследователь настаивает на том, что технология нуждается фундаментальных изменениях, хотя этого будет крайне сложно добиться: операторы сотовой связи могут более пристально следить за VoLTE сетями, но самостоятельно изменить протокол им никто не позволит, равно как и изменить «железо» и софт, работающие на среднестатистическом смартфоне.

«Решение этой проблемы потребует объединения усилий операторов сотовой связи, авторов мобильных ОС, производителей чипсетов и организаций, принимающих стандарты. Осуществить такое быстро не получится», – говорит ученый ***(Обнаружены уязвимости в технологии VoLTE // InternetUA (http://internetua.com/obnarujeni-uyazvimosti-v-tehnologii-VoLTE). – 2015. – 27.10).***

***

Как сообщают специалисты компании Incapsula, кибер-преступники активно используют IP-камеры для осуществления DDoS-атак. Такие устройства обычно используются в рамках инфраструктуры «Интернета вещей», из-за чего не отличаются повышенной безопасностью в повседневном применении.

Как пример эксперты Incapsula привели обыкновенную DDoS-атаку на одного из клиентов компании, мощность которой не превысила 20 тыс. запросов в секунду. Во время анализа IP-адресов устройств, с которых осуществлялась атака, было выяснено, что зараженные камеры находятся недалеко от одного из офисов компании. Эксперты вручную удалили вредоносное ПО с жестких дисков камер видеонаблюдения.

Атака осуществлялась на одного из крупных облачных провайдеров. Злоумышленники смогли скомпрометировать камеры, поскольку в них

использовалась заводская учетная запись с логином и паролем по умолчанию. Специалисты отметили, что в связи с огромной численностью таких незащищенных устройств кибер-преступники могут с легкостью создавать крупные ботнеты.

Эксперты Incapsula надеются, что этот пример обратит внимание администраторов на безопасность IP-устройств. В условиях эпохи «Интернета вещей», когда каждый девайс обладает выходом в Интернет, обеспечение безопасности таких устройств становится задачей первостепенной важности ***(Злоумышленники используют IP-камеры для осуществления DDoS-атак // InternetUA (http://internetua.com/zloumishlenniki-ispolzuuat-IP-kameri-dlya-osusxestvleniya-DDoS-atak). – 2015. – 28.10).***

***

В сеть просочился список из более чем 7 тыс. логинов и паролей различных социальных сетей. Изначально было заявлено, что данные входа на платформу Dropbox не являются правдивыми. Но согласно многочисленным комментариям на форумах, оказалось, что пароли для входа были настоящими, их подлинность подтвердили сами пользователи.

Одна из причин, по которым происходит утечка пароля – это то что пользователи используют одни и те же пароли везде. Вот и получается, что один злоумышленник из одного сайта может получить доступ ко всем учетным записям пользователя на других сайтах, или даже счетам. В условиях последней утечки настоятельно рекомендуется изменить пароли всех учетных записей.

Хотя выложенные пароли в большей части не подходят, и с их помощью не возможно войти, существуют пароли которые подходят к учетным записям на Dropbox. Владельцы Dropbox выступили с официальным заявлением:

«Новости в средствах массовой информации, о том что Dropbox был взломан, не соответствуют действительности. Ваши данные в безопасности. Логины и пароли были похищены из других источников, не связанных с Dropbox. Кибер-преступники использовали позже украденные данные, чтобы попытаться войти в разных местах на всем протяжении сети, в том числе и Dropbox. У нас есть инструмент для выявления подозрительной активности – после того, как это определяется автоматически сбрасывается пароль».

Кажется, что Dropbox не виноват и все еще заботится о безопасности своих пользователей. Не все сайты используют подобные решения.

Так что уважаемый пользователь, сейчас настало то «благоприятное время» чтобы изменить свои пароли ***(Хакеры взломали 7.000 логинов социальных сетей – пришло время менять пароли // Новости IT (http://interteam.com.ua/prishlo-vremya-menyat-paroli/). – 2015. – 29.10).***

***

По данным исследования, проведенного в Университете Нью-Хейвена (Коннектикут, США), популярное приложение для обмена сообщениями WhatsApp собирает данные о телефонных звонках пользователей, в том числе о номерах и продолжительности разговоров.

«Наше исследование демонстрирует, какую информацию можно получить во время экспертного анализа WhatsApp, и закладывает фундамент для проведения дальнейших исследований приложений для обмена сообщениями», – говорится в отчете исследователей.

Эксперты обнаружили, что в WhatsApp реализован протокол FunXMPP. Им удалось расшифровать соединение между клиентом и сервером и просматривать пересылаемые сообщения с помощью специально созданного инструмента командной строки.

По данным экспертов, этот случай является первым, когда исследователи «прощупали», каким образом мессенджер обеспечивает возможность осуществления голосовых звонков с помощью сигнальных сообщений. Если быть точнее, они сосредоточили свое внимание на обмене сигнальными сообщениями во время телефонных звонков через WhatsApp на Android-устройствах. Исследователи изучили реализованный в клиентах мессенджера процесс аутентификации и определили, какой кодек используется для передачи голоса (Opus с частотой дискретизации 8-16 кГц).

Анализ трафика позволил определить тип данных, передаваемых клиентом серверу во время голосового звонка. К ним относятся: телефонные номера WhatsApp, метаданные о звонке, продолжительность разговора, а также дата и время ***(WhatsApp собирает данные о телефонных звонках // InternetUA (http://internetua.com/WhatsApp-sobiraet-dannie-o-telefonnih-zvonkah). – 2015. – 29.10).***

***

Сколько стоят данные, украденные хакерами

В публичных отчетах об обнаруженных уязвимостях и кибер-атаках принято фиксировать количество скомпрометированных счетов. Чем оно больше, тем более серьезной считается атака. Но с точки зрения одного конкретного пользователя, ставшего жертвой взлома, вряд ли имеет значение, были ли его данные украдены в числе 10 тыс. или 50 млн других, пишет TechCrunch.

С точки зрения криминальной экосистемы число жертв также не имеет существенного значения. Числа важны лишь в среде хакеров, где получение миллиона записей считается более успешным, чем получение тысячи. Остальной мир кибер-преступности ориентирован, в первую очередь, на актуальность и полноту полученных данных.

В зависимости от подпольного хакерского сайта, портала в «глубоком Интернете» или другого места, какое удастся отыскать, стоимость одной украденной записи может существенно меняться, от 0,0001 до 200 дол. Большая часть персональной информации пользователей стремительно обесценивается после кражи. К примеру, стоимость данных кредитных карт, включающих имена и адреса жертв, номера карт, сроки их действия и CCV-коды, падает на несколько порядков, как только информация о краже становится публичной. Если о краже пишут в прессе, то есть большая вероятность того, что банк уже принял меры и полученные данные стали бесполезными.

В рамках теневой экосистемы существует целый набор криминальных услуг, позволяющих проверять, распределять и отмывать украденные данные. Существует целый институт посредников, которые за передачу информации от продавца покупателю получают около 25 % сумы. Также существуют сервисы, еженедельно анализирующие украденные данные десятков миллионов кредитных карт и проверяющие, «жива» ли карта и какую сумму с нее удастся снять.

Часто во время взломов злоумышленники крадут имена пользователей, адреса электронной почты и связанные с ними пароли. Конечно, такие пароли, как правило, шифруются, но и ключи, необходимые для их расшифровки, зачастую крадутся вместе с остальной информацией. Звучит угрожающе, но для большинства киберпреступников такой вид данных практически бесполезен. Дело в том, что ценность этой информации целиком зависит от профессиональных хакеров, которым придется расшифровать пароли, прежде чем товар найдет своего покупателя. Это может отнять много времени и ресурсов. Но даже если данные будут расшифрованы, их ценность будет минимальной. Например, из миллиона украденных записей злоумышленники смогут вычленить лишь 250 тыс. адресов почты Gmail.

Этот комплект из 250 тыс. записей, включающих имя пользователя, адрес электронной почты и расшифрованный пароль, может быть продан всего за 20 дол. Вероятно, покупатель будет методом перебора применять список имен и паролей к разным сайтам, надеясь, что кто-то из жертв использует один и тот же пароль на разных ресурсах. Стоимость и ценность такого пакета данных снижается буквально каждый час и падает с каждой перепродажей. Если же информация будет опубликована (к примеру, в каком-либо блоге о безопасности), то данные мгновенно обесцениваются. После этого ими могут заинтересоваться разве что исследователи кибербезопасности.

Информация о масштабной краже данных кредитных карт, как правило, особенно сильно привлекает внимание СМИ и вызывает наибольший резонанс. Но, на самом деле, банки и кредитные компании уже давно наладили эффективную систему противодействия мошенничеству. Так что сегодня вероятность того, что кража данных кредитной карты приведет к реальному похищению денег, кране незначительна.

С распространением «умных» кредитных карт со встроенным микрочипами подделывание карт для мошенничества в магазине станет практически невозможным. Соответственно, ценность украденных данных продолжит падать.

Реальные цели киберпреступников

Но если кража адресов электронной почты, паролей и даже данных кредитных карт перестает быть прибыльной, на каких целях могут сфокусироваться злоумышленники?

Сегодня приоритетом для хакеров становится не большой объем данных о разных целях, а получение как можно более подробной информации об одной конкретной жертве. Чем более подробны данные, тем больше способов их применения можно отыскать. И, соответственно, тем дороже будет стоить такой пакет данных в криминальной экосистеме. Например, комплект,

содержащий полное имя жертвы, адрес, дату рождения, номер социального страхования, номер водительских прав, удостоверение личности с фотографией (например, скан страницы паспорта или водительских прав) и номер банковского счета, может стоить целых 100 дол., в зависимости от страны проживания и национальности объекта.

Большинство людей полагает, что с помощью такой обширной информации злоумышленники, в первую очередь, постараются обчистить банковский счет жертвы. Возможно, но для этого им также придется заполучить действительный пароль для онлайн-банкинга. Так что гораздо более вероятно, что информация о жертве будет использована для открытия нескольких новых банковских счетов для отмывания денег или иных преступных целей. Также возможно, что на жертву оформят несколько крупных кредитов.

Так что сегодня не имеет значения, идет ли речь о колоссальной краже миллионов паролей у популярного ритейлера или о похищении сотни аккаунтов с форума флористов. Важна лишь полнота украденной информации. Потому если пользователь стал жертвой хищения данных, ему следует как можно быстрее понять, что именно у него украли. Наиболее опасна та информация, которую нельзя легко и быстро поменять, как пароль от учетной записи. Вероятнее всего, именно она будет целью злоумышленников ***(Сколько стоят данные, украденные хакерами // InternetUA (http://internetua.com/skolko-stoyat-dannie--ukradennie-hakerami). – 2015. – 28.10).***

***

Компания Gemalto на днях провела глобальный опрос среди 900 ИТ-руководителей, по результатам которого пришла к выводу, что безопасность препятствует развитию мобильности.

По данным Gemalto, 92 % ИТ-подразделений компаний по всему миру ограничивают своим пользователям доступ к стратегическим корпоративным данным и ресурсам с мобильных устройств. Главным образом, эти сложности связаны с опасениями за безопасность данных.

Выяснилось, что 94 % респондентов опасаются потенциальной утечки своих данных или взлома своих систем в связи с возможной кражей или компрометацией учетных записей сотрудников или клиентов.

Ситуация усугубляется ростом количества мобильных устройств: в большинстве организаций на каждого пользователя приходится в среднем по два устройства. Кроме того, 20 % обращений в службу ИТ-поддержки связано с тем, что пользователи потеряли или забыли свой логин или пароль.

Чтобы решить проблему обеспечения безопасности при удаленном доступе, 86 % ИТ-подразделений намерены реализовать схему двухфакторной аутентификации. Больше половины опрошенных уже применяют этот подход для защиты внешнего доступа к корпоративным ресурсам.

Что любопытно, облачные технологии становятся ключевой моделью доставки средств двухфакторной аутентификации. 90 % опрошенных соглашаются, что облачная модель стала ключевым фактором в их решении о

приобретении инструментов строгой аутентификации. Главную роль при этом играла общая стоимость владения ***(На чашах весов оказались мобильность и безопасность // InternetUA (http://internetua.com/na-csashah-vesov-okazalis-mobilnost-i-bezopasnost). – 2015. – 30.10).***

***

Эксперты Akamai обнаружили три новых вектора DDoS-атак, проводимых по методу отражения. Злоумышленники смогли направлять на целевые сайты трафик через NS-серверы NetBIOS, PRC-службы контроллера домена, подключаемые через динамический порт, а также серверы WD Sentinel. Отметим, что для осуществления атак по новым векторам в настоящее время используется почти один и тот же скрипт, использующий одинаковые наборы команд.

Атаки с отражением через NetBIOS наблюдались с марта по июль нынешнего года. Эксперты Akamai отмечают, что из-за использования новых векторов количество вредоносного трафика увеличилось почти в четыре раза, и пиковая мощность одной из наиболее опасных атак составила 15,7 Гбит/с.

Использование PRC как вектора было замечено во время одной из мультивекторных атак в августе нынешнего года. По данным Akamai, этот способ осуществления DDoS-атаки увеличило количество вредоносного трафика в среднем в 9,65 раз. Во время одного из инцидентов коэффициент усиления составил 50,53, а мощность превысила 100 Гбит/с.

Атака с помощью Sentinel была впервые проведена в июне текущего года. Злоумышленники пытались вывести из строя сайт Стокгольмского университета. Примерно в то же время специалисты обнаружили уязвимость на сервере лицензий Sentinel, в котором использовался пакет статистического ПО. В сентябре представители Akamai отразили два нападения с использованием Sentinel как вектора. По их словам, в мире существует как минимум 745 уязвимых серверов, с помощью которых можно осуществить DDoS-атаку. Средний коэффициент усиления для таких нападений составляет 42,94, а пиковая мощность не превышает 11,7 Гбит/с ***(Обнаружены три новых вектора DDoS-атак // InternetUA (http://internetua.com/obnarujeni-tri-novih-vektora-DDoS-atak). – 2015. – 31.10).***

***

Неизвестные злоумышленники взломали ряд MySQL-серверов по всему миру, объединили их в ботнет и используют для осуществления DDoS-атак, сообщают исследователи ИБ-компании Symantec. В настоящее время самым крупным атакам подверглись хостинг-провайдер в США и IP-адрес, зарегистрированный в Китае. Имена жертв не разглашаются.

По данным экспертов, инфицированные серверы расположены в 10 странах мира, но большая их часть приходится на Индию, Китай, Бразилию и Нидерланды. Количество зараженных серверов не уточняется.

«Мы полагаем, что злоумышленники скомпрометировали MySQL-серверы из-за их более высокой пропускной способности. С помощью такого

масштабного ботнета можно предпринимать атаки на более высокопрофильные цели», – отметил аналитик Symantec Г. Горман.

Во время атак злоумышленники используют вариант трояна Chickdos, обнаруженного в декабре 2013 г. После инфицирования преступники внедряют SQL-код, который, в свою очередь, устанавливает вредоносную UDF-функцию на целевом сервере. После загрузки в MySQL она исполняется. В этом случае UDF используется как загрузчик, а также для модификации строк регистра с целью активации терминальных сервисов (TerminalServices). Таким образом хакеры получают возможность удаленно контролировать скомпрометированный сервер и создавать новые учетные записи.

После этого с двух вредоносных веб-сайтов загружаются две разновидности Chickdos. Если два года назад во время подобной кампании злоумышленники использовали автоматизированные инструменты или червя для компрометации MySQL-сервера и установки UDF, то в этом случае экспертам не удалось идентифицировать вектор заражения.

Для того чтобы обезопасить себя от атак подобного рода, специалисты Symantec рекомендуют не злоупотреблять правами администратора, регулярно обновлять приложения, для работы с которыми нужны права администратора, а также проверять конфигурацию сервисов, требующих удаленного доступа к серверу ***(Преступники превращают MySQL-серверы в DDoS-боты // InternetUA (http://internetua.com/prestupniki-prevrasxauat-MySQL-serveri-v-DDoS-boti). – 2015. – 1.11).***

***

Как учёные с помощью Twitter бесплатно скачивают исследования

Учёные нашли ещё один способ использования Twitter для своей работы. Они содействуют пиратству с помощью «секретного» хештега, который перестал быть секретом благодаря BBC.

Во многих странах запрещено скачивать материалы, защищённые авторским правом, включая музыкальные треки, фильмы, книги. Научные исследования также подпадают под защиту законов. Эти документы доступны учёным и институтам, у которых есть подписка. Но некоторые учёные не хотят платить за знания, и они считают, что доступ к таким документам должен быть бесплатным и доступным каждому. Поэтому они делятся результатами исследований между собой.

Хештег запустила учёная и писательница А. Кужевски, занимающаяся когнитивистикой. Хештег #icanhazpdf – перефразированный вариант мема «I can haz». Чтобы получить документ, нужно написать твит со ссылкой на нужный файл, хештегом и адресом электронной почты. На этот адрес пользователь очень скоро получит документ от человека, у которого есть к нему оплаченный доступ. После получения файла твит нужно удалить. Так академики из развивающихся стран могут получить доступ к обширной базе знаний различных институтов и исследовательских групп.

Издатели против, и их право подкреплено законом. Они считают такое поведение учёных аморальным. А. Кужевски с этим не согласна. Она уверена, что этот хештег изменит ситуацию с публикациями исследований и доступом к

ним: «Если мы будем продолжать искать и передавать исследования людям бесплатно, и достаточно людей поддержат эту идею, обязательно что-то изменится».

Пиратство в академических кругах не заканчивается этим хештегом. Есть множество сервисов, в которых вы вбиваете номер работы в поисковой строчке и скачиваете документ бесплатно, часто нелегально ***(Как учёные с помощью Twitter бесплатно скачивают исследования // Age of comp (http://ageofcomp.info/wounde/41496-kak-uchyonye-s-pomoshhyu-twitter-besplatno-skachivayut-issledovaniya.html). – 2015. – 26.10).***

Соціальні мережі

як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»

Редактори: Т. Дубас, О. Федоренко, Ю. Шлапак

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, просп. Голосіївський, 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz@pochta.ru
www.nbuv.gov.ua/siaz.html

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.