СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(30.11–13.12)

2015 № 22

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(30.11–13.12)
№ 22

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

У світі стрімко набирає популярність Flipagram – сервіс, що дає змогу створювати короткі (30–60 секунд) ролики з аудіосупроводом. Про це пише Еспресо.TV із посиланням на Forbes.

За рік роботи Flipagram набрав 30 млн активних користувачів. Щоб зібрати таку аудиторію, Facebook знадобилося три роки, а Snapchat – два.

У США додаток входить у десятку найпопулярніших додатків для пристроїв, які працюють на iOS, у категорії фото і відео. У III кварталі поточного року кількість «фліпів» (тих самих роликів) зросла на 165 % порівняно з аналогічним періодом минулого року.

«Це властиво людям. У всіх є історії, які їм хочеться розповісти», – каже власник Flipagram Ф. Мохіт, який два роки тому придбав додаток у його розробників Д. Фелдмана і Р. Багумяна.

Одним з козирів Flipagram є аудіосупровід. У каталозі додатка містяться мільйони мелодій. У свій час на договори з правовласниками Ф. Мохіт витратив значну частину із 70 млн дол. інвестицій, виділених йому компаніями Sequoia Capital, Kleiner Perkins Caufield & Byers і Index Ventures. Тепер користувачі Flipagram можуть додавати до своїх роликів музику, що недоступно користувачам Instagram.

«Музичні лейбли дійсно впевнені в тому, що Flipagram стане великим медіа-сервісом, порівнянним з Twitter», – говорить Д. Дорр із Kleiner Perkins.

Коли Flipagram керували Д. Фелдман і Р. Багумян, додаток коштував 0,99 дол., але Ф. Мохіт зробив його безкоштовним. Утім, користувачі платять 1,99 дол., якщо вони хочуть прибрати фірмовий логотип додатка зі своїх роликів. Тепер Ф. Мохіт прагне перетворити Flipagram у повноцінну соціальну мережу, а прибуток видається другорядним завданням ***(Нова соцмережа Flipagram б'є рекорди популярності // Еспресо.TV (http://espreso.tv/news/2015/12/04/nova_socmerezha_flipagram_bye_rekordy_popularnosti). – 2015. – 4.12).***

***

Популярна соцмережа для спілкування за професійними інтересами LinkedIn провела наймасштабніший за свою історію редизайн мобільних клієнтів, зробивши їх максимально подібними до Facebook та інших додатків соцмереж.

Про це йдеться на сайті Cossa.

Як і Facebook, новий додаток LinkedIn фокусується на стрічці новин користувачів, яка показує оновлення мережі контактів та розширений контент.

Схоже до Facebook News Feed клієнт фільтрує, які новини показувати в першу чергу залежно від інтересів власника акаунту. Крім того, LinkedIn стверджує, що ця функція «еволюціонує» у міру використання додатку.

Домашня сторінка розроблена за принципом нещодавно перезапущеного сервісу Pulse – користувачі можуть бачити, наприклад, пости тих людей, у котрих схожа робота.

Додаток LinkedIn також містить оновлений інтерфейс особистих повідомлень та покращену пошукову систему, яка, за словами LinkedIn, працює на 300 %, аніж у попередній версії.

Всі нові функції мобільних клієнтів LinkedIn доступні для пристроїв на iOS та Android ***(LinkedIn оновила додаток у Facebook-стилі // MediaSapiens (http://osvita.mediasapiens.ua/web/social/linkedin_onovila_dodatok_u_facebookstili/). – 2015. – 3.12).***

***

Социальная сеть Facebook запускает функционал прямых видеотрансляций Live для рядовых пользователей. Ранее он был доступен лишь владельцам подтверждённых профилей, пишет searchengines.ru

Первым доступ к новой функции получит небольшой процент пользователей iPhone, проживающих в США. В будущем масштаб запуска будет расширен.

Facebook также представила новый формат публикаций – «коллажи». С его помощью можно размещать несколько фото или видео в одном посте. Новый формат запущен в приложении для iOS. В Facebook для Android он появится в следующем году.

В связи с этими нововведениями социальная сеть также тестирует новое выпадающее меню для обновления статуса. При нажатии на What's on your mind пользователи смогут выбрать между различными видами действий, включая запуск видеотрансляции и публикацию фото/видео коллажа.

Напомним, что функционал видеостриминга изначально был запущен в августе этого года в приложении для знаменитостей Facebook Mentions. На тот момент запускать прямые трансляции в Facebook могли лишь владельцы подтверждённых публичных страниц – актёры, спортсмены и другие известные личности. В сентябре социальная сеть открыла доступ к этому функционалу подтверждённым пользователям. А в ноябре в видеотрансляциях Facebook Live появилась кнопка подписки. Теперь начать трансляцию можно будет из основного приложения Facebook ***(Прямые трансляции в Facebook станут доступны рядовым пользователям // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45520/118/lang,ru/). – 2015. – 4.12).***

***

Facebook изменила настройку ленты, чтобы показывать лучшие вирусные посты. Решение об исключении принимают на основе опроса «десятков тысяч» людей ежедневно. Лайков, комментариев и расшариваний недостаточно. Пользователям предложат поучаствовать в опросе и выбрать, какой из двух постов они хотели бы видеть в ленте.

Если выбор пользователей и популярность поста совпали, все идет по плану. Если наоборот – есть над чем работать.

Как сообщают в блоге Facebook, причина проверки – высокий рейтинг фейковых постов. Так как вирусные посты – аномалии, на продвижении страниц сообществ нововведение не отразится ***(Facebook изменил настройку Ленты // InternetUA (http://internetua.com/Facebook-izmenil-nastroiku-lenti). – 2015. – 7.12).***

***

Facebook закрывает филиал Creative Labs, который должен был подготовить ряд инновационных приложений для крупнейшей социальной сети в мире.

Подразделение работало над созданием ряда известных программ, таких как Slingshot, Rooms, Riff и Paper, но все указывает на то, что они не очень хорошо были встречены пользователями. Первые три приложения были удалены из магазинов Google Play и App Store, и, вероятно, в ближайшее время они перестанут работать на устройствах пользователей, которые их установили. На данный момент остается нерешенным вопрос об утилите Paper, которая до сих пор доступна для скачивания для пользователей мобильных устройств.

О Slingshot стало известно еще в мае 2014 г. Приложение должно было стать интересной альтернативой чрезвычайно популярного Snapchat, который ранее пыталась купить Facebook за 3 млрд дол. К сожалению, сервис не был встречен с таким же интересом, как и его прототип. Creative Labs также подготовила программу Rooms, которая позволяла создание закрытых дискуссий, посвященных теме, выбранной пользователем, и Riff, позволяющую монтировать видео на основе записей, полученных от друзей. Paper являлась аналогом Flipboard и Facebook Home, а ее задача заключалась в том, чтобы предложить владельцам смартфонов и планшетнов просмотр в режиме ленты.

В настоящее время известно, что Rooms будет исключена из списка 23 декабря этого года. Трудно сказать, какая судьба ждет Riff и Slingshot. Возможно, приложения перестанут работать, хотя трудно сказать, что компания в конечном счете может решить не делать этого и провести их интеграцию с IM Messenger или WhatsApp. Также непонятно будущее Paper. Программу все еще возможно загрузить, поэтому есть шанс, что Facebook будет продолжать поддерживать ее ***(Facebook закрывает Creative Labs // Hi-Tech Новости (http://hi-tech-news.com/news/1229/). – 2015. – 9.12).***

***

Сервис микроблогов Twitter тестирует новый способ формирования ленты – не в хронологическом порядке, сообщает The Next Web. Пользователи возмутились, заметив такое нововведение. В техническую поддержку соцсети поступило множество вопросов и жалоб.

«Это всего лишь эксперимент. Мы продолжаем разрабатывать способы формирования лучшего контента для пользователей Twitter», – прокомментировали в компании.

Пока трудно сказать, какие результаты покажет тестирование, и будет ли введена новая технология формирования ленты. Twitter часто предлагает пользователям перемены, но далеко не всегда они встречают отклик ***(Twitter стал формировать ленту не в хронологическом порядке // InternetUA (http://internetua.com/Twitter-stal-formirovat-lentu-ne-v-hronologicseskom-poryadke). – 2015. – 8.12).***

***

Сначала в сервисе Twitter появились «лайки», которые многими были восприняты с негативом, теперь же компания решила переработать способ отображения фотографий. Основное изменение – это тот факт, что теперь снимки в ленте будут отображаться необрезанными. Поэтому, листая сообщения в Twitter, теперь не нужно будет постоянно нажимать на картинку, чтобы увидеть её полную версию. Впрочем, это не касается удлинённых портретных снимков – они по-прежнему будут показываться немного обрезанными.

Также были внесены изменения в способ отображения серий снимков. Например, теперь вместо четырёх изображений одинакового размера Twitter будет показывать одно большое фото и три маленьких – похожая технология используется в социальной сети «ВКонтакте». По словам менеджера по продуктам компании А. Кумара, изменения были сделаны для того, чтобы фотографии можно было показывать пользователям такими, какими они должны были быть изначально ***(Фотографии в Twitter стали отображаться в полном размере // InternetUA (http://internetua.com/fotografii-v-Twitter-stali-otobrajatsya-v-polnom-razmere). – 2015. – 10.12).***

***

Видеохостинг YouTube добавил в мобильные приложения новую вкладку, в которой показаны набирающие популярность ролики в сети. Изменение вступили в силу на десктопной версии сервиса, а также устройствах с iOS и Android без обновления клиентов.

Вкладка «Набирающие популярность» доступна и на iPhone, и на iPad. Компания не анализирует историю просмотров человека, а только отбирает наиболее популярные ролики за последнее время. При подборке видеоклипов учитывается такой критерий, как местоположение.

Примечательно, что у Android-версии YouTube функциональность новой вкладки шире, чем у аналога для iOS: приложение для «гуглофонов» позволяет увидеть набирающие популярность видео в разных категориях.

YouTube также решил добавить в свои мобильные приложения возможность полной буферизации видео. У ряда пользователей в приложении появилось уведомление при установке ролика на паузу – в окне указан полный

вес видео и объем загруженных данных. Процесс буферизации доходит до конца, вне зависимости от длины ролика, даже если поставить паузу в самом начале.

Функция полной буферизации видео находится в стадии тестирования, когда она будет доступна для всех пользователей, неизвестно ***(YouTube добавил в мобильное приложение новые возможности // IGate (http://igate.com.ua/lenta/11937-youtube-dobavil-v-mobilnoe-prilozhenie-novye-vozmozhnosti). – 2015. – 10.12).***

***

Комментировать посты в Facebook с мобильных устройств теперь можно без подключения к сети. О появлении новой функции сообщается на сайте для разработчиков. Комментарии будут сохраняться в памяти устройства до того момента как оно снова окажется в зоне действия сети, после чего приложение будет автоматически обновлять содержимое ленты. Новая функция пока доступна только устройствам на Android.

Также представители корпорации заявили, что в настоящее время тестируют новый функционал, который в дальнейшем позволит приложению загружать свежие новости в тот момент, когда владелец устройства пользуется другими онлайн-программами. Вероятно, некоторые пользователи не будут рады такому нововведению, так как приложение Facebook и без этого съедает большую часть заряда батареи как на Android, так и на iOS устройствах.

Отметим, в октябре Facebook обновила свое приложение для Android. Некоторые старые посты теперь загружаются не из сети, а из памяти смартфона ***(Оставлять комментарии в Facebook теперь можно в офлайн-режиме // InternetUA (http://internetua.com/ostavlyat-kommentarii-v-Facebook-teper-mojno-v-oflain-rejime). – 2015. – 11.12).***

***

Социальная сеть «ВКонтакте» запустила новый алгоритм рекомендации аудиозаписей, который, по утверждению представителей соцсети, работает в два раза быстрее предыдущего. Об этом сообщает новостной проект LIVE.

Возле каждой песни появилась кнопка «Показать похожие», которая работает и в тот момент, когда аудиозапись не воспроизводится. Рекомендации можно получить как по отдельной песне, так и по целому альбому.

По утверждению представителей соцсети, система рекомендаций стала работать в два раза быстрее – вне зависимости от источника (песня, альбом или весь треклист). Алгоритм основывается на добавленных и прослушиваемых песнях из раздела аудиозаписей пользователя.

Чем больше в списке действительно интересных вам песен, которые вы готовы слушать постоянно, и чем чаще вы их слушаете, тем точнее будут рекомендации. Чтобы выдать рекомендации по одной песне, система ищет всех пользователей, добавивших этот трек, анализирует их список аудиозаписей и выбирает наиболее часто встречающиеся.

Система рекомендаций – одна из основных составляющих популярных стриминговых сервисов. Разделы с персональными подборками присутствуют в таких проектах, как Apple Music, Spotify, «Яндекс.Музыка» и Google Play Music ***(«ВКонтакте» запустила обновлённый алгоритм музыкальных рекомендаций // VC.RU (https://vc.ru/n/vk-relevant-music). – 2015. – 12.12).***

***

Російська соціальна мережа «Одноклассники» за підсумками листопада випала з ТОП-10 найпопулярніших сайтів, якими користуються українці. Про це свідчать дані щомісячного дослідження CMeter, компанії TNS ***(Rozetka.ua витіснила Однокласники з ТОП-10 найпопулярніших сайтів серед українців (дослідження TNC) // UkrainianWatcher (http://watcher.com.ua/2015/12/11/rozetka-ua-vytisnyla-odnoklasnyky-z-top-10-naypopulyarnishyh-saytiv-sered-ukrayintsiv-doslidzhennya-tns/). – 2015. – 11.12).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Українські лідери думок у соціальних мережах

Бум соцмереж на тлі підвищенної соціальної активності українців примусив суспільство по-новому споживати новини. Українські лідери думок сьогодні керують країною і конкурують із пресою, пише «Новое время» (http://nv.ua/ukr/publications/ukrajinski-lideri-dumok-v-sotsialnih-merezhah-kerujut-krajinoju-i-konkurujut-z-presoju-83345.html).

К. Волох, один з найвідоміших у Facebook українських блогерів, колись завів акаунт тільки для того, щоб просувати власну клініку. Писати на політичні теми він і не думав. Більш того, К. Волох зізнається, що тривалий час не міг опанувати клавіатуру – ніяк не вдавалося запам'ятати розташування клавіш. «Тому перший час залишав коментарі максимум на півречення», – згадує він.

Сьогодні аудиторія блогера порівнянна з цілком успішним виданням і становить 55 тис. читачів, а сам він упевнений, що життєвий досвід дає змогу йому висловлюватися по суті практично на будь-яку тему – від політики до економіки і судової реформи. На питання, навіщо йому, успішному підприємцю з Ізраїлю, у якого до недавнього часу не було навіть тутешнього громадянства, впрягатися у віз української політики, він упевнено відповідає: «Мені ніяково про це говорити, але, наприклад, я абсолютно точно знаю, що без мене не було б закону про люстрацію [закон України Про очищення влади]».

Власним впливом і чималою кількістю передплатників К. Волох зобов'язаний не лише своїй інформованості та громадянській позиції, а й зростанню популярності соціальних мереж у країні. За підрахунками Watcher,

вітчизняного видання про інтернет-бізнес та маркетинг у соціальних медіа, за останні шість років кількість українських користувачів Facebook зросла в 64 рази: у квітні 2009 р. у мережі було зареєстровано 62 тис. співвітчизників, а тепер їх кількість перевалила за 4 млн. Як мінімум 40 з них мають понад 100 тис. передплатників, тобто їх точка зору вважається авторитетною, а самі вони – впливовими.

Бум соціальних мереж, що стався на тлі зростання соціальної активності українців, призвів і до зміни структури споживання новин. За даними дослідження міжнародної компанії Nielsen, проведеного серед 30 тис. онлайн-респондентів у 60 країнах світу (в тому числі в Україні), у соціальних мережах свіжу інформацію про останні події черпає 47 % співвітчизників. Для порівняння: майже стільки ж – 48 % українців отримують новини з інтернет-видань, а 51 % – з телепрограм.

«Соціальні мережі – це дуже особистий простір для кожної людини. Це його клуб за інтересами, його приватна вечірка, його сімейне застілля, якщо хочете, – вважає Е. Нагорний, директор з маркетингу литовської соціальної мережі Plag, екс-директор українського медіа-холдингу UMH. – Все, що відбувається там, дуже особисте, і викликає більше довіри і емоцій, ніж все, що відбувається на вулиці або в ЗМІ».

Колективні честь і розум

Є. Гендін, популярний блогер та автор кабаре Веселий ПесецЪ, відомого своєю політичною сатирою, і не помітив, як його «затишний щоденничок» у соціальній мережі перетворився в публічну бібліотеку. На пости Є. Гендіна у Facebook підписано понад 20 тис. осіб, а особливий інтерес до дніпропетровського сатирика, який раніше вважався людиною незаангажованою, з'явився після того як він публічно підтримав свого друга, лідера партії УКРОП Б. Філатова.

Через цю підтримку частина фейсбучних друзів покинули Є. Гендіна, вважаючи Б. Філатова одіозним політиком. Хоча сатирик не сумує, стверджуючи, що тут же чимало і підписалося. «Я в підсумку в плюсі», – запевняє він.

Є. Гендіна можна назвати типовим українським лідером думок, людиною, що має десятки тисяч передплатників, який відмінно розбирається в політиці, по суті своїй є соціальним активістом і хоча б одного разу потрапив в епіцентр фейсбучного скандалу. Є і ще одна спільна риса: більшості вітчизняних лідерів думок вже виповнилося 40. Практично всі ці якості різняться з західними стандартами соціальних мереж, де більше затребуваний не політичний, а розважальний контент, і тому там правлять бал переважно 25-річні – співаки, актори, футболісти та інші знаменитості.

Причина лідируючих позицій українських політиків і навколополітичних блогерів у рейтингу найвпливовіших лідерів думок – надмірна заполітизованість суспільства, констатують експерти.

«Дурість (що частіше) або мудрість (майже ніколи) наших політиків впливає на життя кожного, що і викликає інтерес до їхніх думок, – розставляє

крапки над і О. Дерев'янко, керівний партнер агентства PR-Service та віце-президент Української PR-ліги. У стабільних мирних країнах цього немає, тому що там громадяни відчувають себе в більшій безпеці».

З іншого боку, фахівці називають активність українців у Facebook прикметою часу: якщо тебе немає в соцмережах, тебе немає ніде. Тому соціальні мережі і облюбували політики, які часто використовують ці майданчики не стільки для спілкування з народом, скільки для піару. Утім, у Facebook панує демократія: схвальні лайки тут отримують не за портфелі, а за точно сформульовані і актуальні пости.

Більше того: колективний розум соціальних мереж перетворився у свого роду орієнтир для влади. Наприклад, після того як лідери думок Facebook назвали прийняття закону від 2 липня 2015 р. про повернення кредитів фізичними особами за курсом на момент взяття їх згубним для банківської системи, це не на жарт налякало багатьох депутатів. Багато з них стали публічно виправдовуватися, намагатися відкликати голоси, і в результаті одіозний закон скасували.

Ще один знаковий епізод: 8 червня 2015 р., коли у Васильківському районі виникла масштабна пожежа на нафтобазі мережі БРСМ, міністр екології І. Шевченко був у неузгодженій із Прем'єр-міністром відпустці в Ніцці. Після кількох резонансних постів від лідерів думок І. Шевченко був звільнений.

А найсвіжіший приклад – відсторонення від посади київського поліцейського О. Савчина після того, як блогери знайшли в мережах його запис в підтримку «Беркута» часів протистояння на Грушевського.

Як стати зіркою

Політичні зірки та громадські активісти, які «оселилися» в соціальних мережах, набувають ще більший вплив, – так багато хто вважає. Вчасно зайнявши потрібну нішу, можна стати одним з найбільш цитованих блогерів у соцмережах, не маючи в реальному житті для цього вагомих підстав. Популярний блогер О. Барабошко наводить як приклад Д. Тимчука, керівника Центру військово-політичних досліджень, який першим почав систематизувати інформацію про події в АТО і «подавати її під соусом інсайду».

Тепер у Д. Тимчука понад 245 тис. послідовників у Facebook, 297 тис. у Twitter, і він сьомий у списку лідерів думок, складеному НВ. Більше того, слідом за віртуальною впливовістю до нього прийшла реальна – він став народним депутатом.

Хоча наявність сотень тисяч передплатників у блогера аж ніяк не гарантує, що всі вони читають кожен його пост. Facebook, залежно від налаштувань, показує в стрічці не всі пости, і алгоритми формування стрічки постійно змінюються. Також фахівці вважають, що для впливовості блогеру вистачить 10 тис. передплатників, а Е. Нагорний переконаний, що іноді і 5 тис. передплатників достатньо, щоб бути почутим.

Впливовість у соціальних мережах тримається на трьох китах – лайку, шерах і коментарях. Приміром, О. Барабошко знає тисячу і один прийом, як

створити пост «на три тисячі лайків». А самий перевірений – писати те, що аудиторія хоче чути.

Цим прийомом майстерно користується О. Ляшко, народний депутат і лідер Радикальної партії, зауважує М. Саваневський, керівний партнер PlusOne DA та засновник видання Watcher. У 2014 р. О. Ляшко потрапив у число топових авторів і тримається там досі. У рейтингу НВ він займає десяте місце із сумарною аудиторією передплатників у Facebook і фоловерів у Twitter 445 тис. осіб. «У нього були нахабні, на межі фолу пости, в яких він пропонує “дати під зад держимордам-депутатам”», – саме це, вважає М. Саваневський, хотіли чути люди.

Автори, які регулярно отримують тисячі схвальних кліків, крім визнання, мають можливість монетизувати свою популярність. Є. Гендін зізнається, що регулярно отримує такі пропозиції – від реклами меблів або мобільного зв’язку до політичної реклами.

Заробляти на лідерах думок – світова практика. Однак якщо в західних країнах популярні блогери працюють в основному з комерційними брендами, в Україні, як висловлюється О. Барабошко, вони «сидять на партійних касах», і їх не цікавить співпраця з брендами за 100 дол.

Вдень і вночі обертаючись у віртуальному світі, більшість стає заручниками лайків: нерідко блогер, зробивши в соціальній мережі кілька вдалих записів і отримавши масове схвалення, починає переживати, якщо його нові записи не отримують бажану кількість лайків знову.

«Ще товариш Маслоу [автор піраміди потреб психолог А. Маслоу] казав, що кожна людина прагне визнання, – міркує психолог і бізнес-тренер В. Вавілов. – Люди люблять, коли їх хвалять, а тут [в соцмережах] є простий спосіб отримати довгоочікувану похвалу: постиш фото котика або анекдот – і ти зірка».

Коли залежність від соціальної мережі стає хворобливою, вихід тільки один – видалити свій акаунт, вважає В. Вавілов. «Шкода, що таких людей я не знаю», – зізнається він.

Герої з мережі

Альтернативним джерелом новин і медіа-інструментом Facebook стала в Україні у 2013 р. У травні 2013 р. у країні було два топових автори – М. Найєм, який тоді був журналістом, і В. Кличко, який тоді був боксером, – в обох було по 25 тис. передплатників, тобто в п’ять разів менше, ніж у деяких топових блогерів зараз, згадує М. Саваневський.

Уже через рік Facebook стала однією з найпопулярніших соціальних мереж, аудиторія деяких топових блогерів приравнялася до аудиторії більшості рейтингових інтернет-ЗМІ.

«Соцмережі знищили ефект сакралізації селебріті, раніше створюваний таблоїдами, і будь-яка людина може написати будь-якому політику, художнику або журналістові все, що вона про нього думає», – наводить приклад С. Іванов, популярний луганський блогер і журналіст.

За словами О. Дерев'янко, враховуючи, що багато реальних ЗМІ перестали сприйматися як джерело об'єктивної інформації, люди шукають тих, кому можна довіряти, у соціальних мережах. Крім того, виросло покоління digital native, яким складно спілкуватися особисто і набагато легше жити в соціальних мережах.

До того ж є люди, яким просто необхідний лідер чи кілька лідерів, щоб вони могли їм «поклонятися», додає В. Вавілов.

У той самий час соціальні мережі – це ідеальний живильний бульйон для маніпуляцій будь-якого роду. О. Барабошко, який за домовленістю веде кілька акаунтів публічних політиків, переконаний, що репутацію навіть найбільш одіозних людей можна змінити декількома постами. «Всього-то потрібно написати щось на зразок: "До мене приходили SMM-щики, просили купу грошей за піар моєї сторінки, так краще я ці гроші віддам людям, – пояснює свої прийоми О. Барабошко. – Скільки лайків буде під цим постом – стільки я відправляю грошей в дитячий будинок". І ті люди, які раніше його таврували, тепер будуть брати в цьому участь».

Також О. Барабошко знає випробуваний рецепт, як стати героєм України. Наприклад, у момент, коли в Донецьку тільки все починалось, все, що потрібно було зробити, – анонсувати у себе в акаунті, що ось, мовляв, хочу поїхати в Донецьк. Потім переключити IP-адресу з київської на донецьку, «відзначитися» в декількох місцях, потім організувати жорстку фотосесію в прилеглому лісі на тему «Сепаратисти катують укропа», показати її на донецьких форумах і зникнути з інформаційного поля на кілька днів. А потім «винирнути» з жалісливою історією героїчної втечі з полону. О. Барабошко стверджує, що знає кількох людей, які скористалися таким прийомом.

Саме за це соціальні мережі деколи називають королівством кривих дзеркал, яке спотворює до невпізнання дійсність і робить актуальними проблеми, яких у реальному житті практично немає. «Це кола на воді», – скептично каже О. Дерев'янко.

Також вона, як і багато інших експертів, упевнена, що людство ще довго буде тішитися новою іграшкою і все більше заплутуватись у соцмережах.

Утім, еволюційно глухим кутом це не стане. «З часом напруження спаде, довіра до лідерів думок зменшиться, кожен почне більше думати своєю головою», – прогнозує перебіг подій Е. Нагорний ***(Іванова К. НВ презентує ТОП-50 українських лідерів думок в соціальних мережах // Новое время (http://nv.ua/ukr/publications/ukrajinski-lideri-dumok-v-sotsialnih-merezhah-kerujut-krajinoju-i-konkurujut-z-presoju-83345.html). – 2015. – 2.12).***

***

Соціальна мережа науковців Scientific Social Community визнала сайт відділу міжнародних зв'язків Львівського національного університету ім. Івана Франка та його Facebook-сторінку найкращими серед україномовних сайтів, які спільнота рекомендує для перегляду молодим ученим.

Про це йдеться на офіційній сторінці Scientific Social Community, – передає прес-центр ЛНУ ім. Івана Франка.

За оцінками соціальної мережі науковців, міжнародний відділ ЛНУ ім. Івана Франка найбільш повно висвітлює освітні програми, зокрема Erasmus+, цікаві зустрічі, партнерські й «відкриті» стипендії у європейських університетах, дає поради з написання англомовних статей.

Рейтинг 10 спільнот у Facebook, рекомендованих для перегляду і коментарів науковому світу, від читачів Scientific Social Community:

1. Scholarships, Fellowships and Grants for Former Soviet Republics.
2. Про: Гранти. Проекти. Стипендії.
3. Гранти, стажування, конкурси в соціальних і гуманітарних науках.
4. Ivan Franko National University of Lviv – International Office.
5. Grants&Projects UA Гранти та проекти для України («Конгрес Активістів Культури»).
6. Science Slam Україна.
7. Наукова ініціатива.
8. Ради молодих вчених України.
9. Форум «Наука. Бізнес. Інновації».
10. Kyiv Scientific ***(Сайт відділу міжнародних зв'язків ЛНУ – в ТОП-10 наукових спільнот // Львівська газета (http://gazeta.lviv.ua/news/2015/12/07/51208). – 2015. – 7.12).***

***

У мережі поширюється звернення до української влади від колективу авторів на честь річниці «Маршу мільйонів».

У зверненні українських можновладців попередили про те, що люди все менше вірять нинішній владі і дають останній шанс на проведення справжніх реформ:

«…Уважаемые президент Украины и премьер-министр!

Люди все видят и понимают. Они уже не верят вашим оправданиям. Коррупционная возня и имитация реформ уничтожают доверие украинского общества и уважение зарубежных партнеров.

Мы не хотим новой революции, которую вы бессознательно приближаете. Мы готовы нести ответственность за будущее нашей страны. Поэтому мы не просим, мы требуем:

1. Начать реальную борьбу с коррупцией. Сконцентрироваться на высших эшелонах власти и разорвать круговую поруку, назначив эффективного генерального прокурора, завершить люстрацию и реформировать государственную службу по европейским стандартам.

2. Восстановить справедливость. Привлечь к ответственности людей, разворовавших страну и приведших к насилию и убийствам на Майдане.

3. Добиться верховенства права. Интенсивно и решительно проводить судебную реформу, в которой были сделаны важные шаги, но общество не ощущает уверенности в успехе.

4. Обеспечить прозрачность власти. Открыто проводить назначения на государственные должности, прекратив практику подковерных договоренностей и распределения должностей по политическим квотам в угоду серым кардиналам.

5. Озвучить четкий план. Как нам вместе преодолеть экономический и гуманитарный кризис, как мы планируем возвращать Крым и оккупированные территории.

У вас все еще есть выбор, кем войти в историю: реальными реформаторами, которые пожертвовали личными интересами ради будущего страны, либо теми, кто привел страну к развалу из-за коррупции и неэффективного управления» ***(У Мережі поширюють звернення до влади, присвячене другій річниці «Маршу мільйонів» // Depo.ua (http://www.depo.ua/ukr/politics/u-merezhi-poshiryuyut-zvernennya-do-vladi-prisvyachene-richnitsi-02122015082500). – 2015. – 2.12).***

***

Среди украинских пользователей Twitter уже третий раз проводится обмен подарками и открытками ко Дню Святого Николая – эта традиция ежегодная: нужно подать заявку на специальный аккаунт в сети микроблогов, внести благотворительный взнос и получить подтверждение.

Регистрация завершается 30 ноября. После этого все участники получат своего «подопечного», которому и будут отправлять подарок – отправить его нужно до 19 декабря, чтобы «подопечный» успел его получить. Для отправки и доставки все участники используют «Новую почту», а количество участников, получатели и ход всей кампании будут отображаться в Twitter по хэштегу #ТвіМиколай. Инициатива некоммерческая и не связана с какими-либо брендами; но в этом году организаторы инициативы сотрудничают с ГО «Свіжа Кров», и все взносы участников пойдут на помощь донорской службе крови нового типа, которую создаёт «Свіжа Кров» ***(Украинские пользователи Twitter запустили обмен подарками ко Дню Святого Николая // Блог Imena.UA (http://www.imena.ua/blog/twitter-st-nicolas-day/). – 2015. – 30.11).***

***

Socialbakers назвали топ-10 читаемых украинских СМИ в Facebook. По данным международной компании в сегменте социального маркетинга, на сегодня в тройку лидеров входят ТСН (498,3 тыс. подписчиков), «Украинская правда» (467,7 тыс.), Hromadske.tv (444,7 тыс.), сообщает rbc.ua. Четвертое и пятое места занимают телеканалы «1+1» (408,2 тыс.) и «5 канал» (379,7 тыс.).

В сегменте онлайн-медиа, по версии Socialbakers, лидируют «Украинская правда», ИА «РБК-Украина» и «Обозреватель». В категории «Новости» самые читаемые в Facebook СМИ являются ТСН, Hromadske.tv и BBC Ukrainian ***(Socialbakers назвали топ-10 читаемых украинских СМИ в Facebook // Marketing Media Review (http://mmr.ua/show/socialbakers_nazvali_top-10_chitaemyh_ukrainskih_smi). – 2015. – 30.11).***

***

Волинський священик дає інтернет-консультації у Facebook

Протоієрей, клірик кафедрального собору Святої Трійці в Луцьку, голова інформаційно-видавничого центру Волинської єпархії УПЦ КП, представник єпархії у Волинській раді Церков В. Собко запровадив інтернет-консультації для вірян краю, пише ВолиньPost (http://www.volynpost.com/news/61590-volynskyj-sviaschenyk-daie-internet-konsultacii-u-facebook).

Священик створив персональну сторінку «Консультація священика луцького собору» в мережі Facebook, на якій відповідає на запитання допитливих городян.

«Слава Ісусу Христу! Що? Де? Коли? Як? Навіщо? Ставлю собі завдання відповісти на запитання, пов'язані з усім, чого Ви потребуєте від Церкви й що вона очікує від Вас, – пише отець Віталій. – Хрещення, Сповідь, Причастя, Вінчання, Соборування, чин похорону, освячення, молебні, подавання записок «За здоров'я», «За упокій» тощо. А якщо буде можливо, то не тільки відповісти на запитання, але й надати практичну допомогу».

Протоієрей наголошує, що, за потреби, до роботи в консультації священика запрошуватимуться інші душпастирі ***(Волинський священик дає інтернет-консультації у Facebook // ВолиньPost (http://www.volynpost.com/news/61590-volynskyj-sviaschenyk-daie-internet-konsultacii-u-facebook). – 2015. – 2.12).***

***

Житомирська міська та обласна ради оновили керівний склад та депутатський корпус. У голів вже є заступники, у міської ради новий секретар та керуючий справами. І всі розпочали виконання обов'язків – керувати справами міста та області і звітувати про виконану роботу своїм виборцям.

Житомир.info відшукав сторінки нових керівників міської та обласної рад у мережі Facebook і подивився, з ким дружать і про що пишуть чиновники.

Житомирський міський голова С. Сухомлин у Facebook має 3392 друга, постійно оновлює стрічку та публікує інформацію про заходи, які відвідує. Свою сторінку веде самостійно, остання публікація написана 24 листопада 2015 р. Підписників немає.

Секретар міської ради Н. Чиж систематично наповнює свою сторінку новою інформацією, часто Н. Чиж відмічають у своїх записах друзі. У Facebook дружить із 4851 користувачами і має 372 підписника.

У першого заступника міського голови О. Ясюнецького 960 друзів та 58 підписників у Facebook. Останній пост О. Ясюнецький написав 30 листопада. На сторінку постійно додає нові публікації.

Активний у соцмережі заступник міського голови з гуманітарних питань М. Хренов. У Fasebook має 1190 друзів. Останній запис зроблений М. Хреновим 15 листопада. Його сторінку часто відмічають у своїх записах друзі.

Сторінка заступника міського голови з питань транспорту Д. Ткачука активна та насичена записами. У Facebook Д. Ткачук дружить із 2195 людьми. В останніх записах, розміщених на сторінці, друзі вітають Д. Ткачука з призначенням на посаду заступника. За сторінкою Д. Ткачука стежать 665 користувачів Facebook.

Керуюча справами міської ради О. Пашко часто оновлює стрічку публікаціями. В останньому записі на своїй сторінці в мережі Facebook подякувала всім за підтримку. У соцмережі має 393 друга.

Активно висловлює свою думку та ділиться новинами на своїй сторінці у Facebook голова обласної ради А. Лабунська. Має найбільше друзів у мережі – 4851. За сторінкою стежать 2900 підписників. Останній запис був зроблений 1 грудня.

Не вдалося знайти сторінки заступників голови обласної ради В. Ширми та Н. Рибак ***(Хто з нових керівників Житомирської міської та обласної ради «зависає» у Facebook // Zhitomir.info (http://www.zhitomir.info/news_152827.html). – 2015. – 1.12).***

***

У київського метрополітену з'явився власний акаунт в Instagram

На сторінці kyivmetrogram обіцяють публікувати як фотографії з щоденного життя метрополітену, так і знімки найпотаємніших куточків підземки, яких ніколи не бачили пасажири.

«Це ще один вектор наших соціальних ініціатив, який дасть змогу показати нові сторони роботи підприємства», – сказав начальник столичної підземки В. Брагінський Platforma.

Перші фотографії акаунту було створено групою українських інстаграмерів у рамках ініціативи #empty. Тепер «фоловити» КП «Київметрополітен» в Instagrami може кожен бажаючий.

Також київський метрополітен має власний Twitter-акаунт, де можна оперативно дізнаватись про зміни в роботі підземки. А про цікаві новини та ініціативи метро – на сайті або на Facebook-сторінці підприємства ***(У київського метро з'явився власний Instagram // MediaSapiens (http://osvita.mediasapiens.ua/web/social/u_kiivskogo_metro_zyavivsya_vlasniy_instagram/). – 2015. – 4.12).***

***

Бразильские правозащитницы из организации Criola начали кампанию против тех, кто пишет в Facebook и Twitter расистские комментарии к записям, передает BBC News.

Активистки собирают оскорбления и размещают их на билбордах поблизости от домов авторов, затирая имена и фотографии. Адрес проживания вычисляют с помощью геолокационных меток.

Акцию назвали «Виртуальный расизм, реальные последствия». По заявлению авторов, цель их кампании – мотивировать людей действовать, когда

они видят проявления расизма. «Люди, которые оставляют оскорбительные комментарии, считают, что могут спокойно сидеть дома и делать в Интернете все, что им заблагорассудится. Мы этого не допустим», – заявила основательница Criola Д. Вернек.

Афробразильцы составляют 7,6 % от общего населения страны согласно переписи 2010 г. Еще 43 % – бразильцы-метисы.

По словам активисток, поводом для акции послужил инцидент с опубликованной на странице новостной программы Nacional Journal в Facebook фотографией популярной чернокожей телеведущей М. Коутиньо. Ряд комментаторов отреагировали на снимок расистскими высказываниями. При этом фото опубликовали 3 июля, в день борьбы с расовой дискриминацией.

Реакция пользователей оказалась смешанной. Некоторые комментаторы одобрили действия активистов, однако другие заметили, что в Интернете оскорбительные комментарии получают все, а не только чернокожие ***(Бразильские правозащитницы ответили интернет-троллям билбордами // InternetUA (http://internetua.com/brazilskie-pravozasxitnici-otvetili-internet-trollyam-bilbordami). – 2015. – 30.11).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Как бизнесу, работающему для бизнеса, следует продвигаться в Интернете.

В последнее время бизнес активно осваивает возможности Интернета, не ограничиваясь лишь корпоративными сайтами, а выходя и в социальные сети. Интернет фактически стал медиа №1 для всех сфер бизнеса. И это правильно – «акулы» Интернета, Facebook и Google ныне суммарно занимают 15 % мирового трафика, пишет UBR (http://ubr.ua/business-practice/own-business/facebook-v-pomosh-kak-internet-mojet-pomoch-b2b-biznesu-367951).

На первый взгляд, продвижение в Интернете кажется актуальным лишь для бизнеса формата B2C. Отличие B2B от традиционного маркетинга лежит в том, что у первого достаточно небольшое число клиентов. В этом материале с помощью экспертов, выступивших на Первом международном B2B форуме, мы объясним, как грамотно продвигать B2B в Интернете.

Комбинация методик

Эксперт по цифровому маркетингу и рекламе Б. Картер утверждает, что в нынешние времена ценность компании создается на основе осведомленности ее клиентов. Как это делается? Чаще всего – через рассылку по электронной почте. Затем отслеживаются продажи – подписчикам звонят, приглашают на мероприятия, так отслеживаются продажи, что в итоге приносит и прибыль, и новых клиентов.

Чтобы оставаться на плаву, компания постоянно должна показывать себя лидером. Это нужно для авторитета компании и лояльности клиентов, говорит

Б. Картер, для того, чтобы они были удовлетворены, что работают с вами. «При традиционном подходе к продвижению для понимания нужно использовать целый набор ориентиров, по которым можно понять, хороши ли вы продвигаетесь вперед – как клиенты взаимодействуют с рассылкой, сколько кликов это дает и т. д.», – поясняет эксперт.

Все это можно упростить, используя Facebook. Социальная сеть – очень экономный способ увеличить осведомленность клиентов и создать спрос, ведь при помощи Facebook можно генерировать желания потенциальных клиентов, потребность, которая может быть как осознанной, так и неосознанной. В целом, Facebook, по словам Б. Картера, является наиболее сильным маркетинговым инструментом, который когда-либо существовал. Конечно, прежние подходы не стоит полностью забывать – реклама на Facebook и наработки из баз данных e-mail'ов дает очень хорошую базу, с которой и далее могут работать торговые агенты.

Привлечение внимания

«Привлечь внимание – очень большая проблема в современном бизнесе», – утверждает Б. Картер. По его словам, причина проблемы кроется в том, что никогда ранее не было такого количества разных материалов, которые привлекают внимание людей – текстовые сообщения, социальные сети, электронная почта, телевидение. Эти факторы порождают конкуренцию за внимание людей с перечисленным обилием маркетинговых инструментов. А это означает, что маркетинг должен быть интересным для клиентов. «Вы не можете что-то продавать, если вас не видят. А чего хотят люди? Наслаждаться, решить все их проблемы – вот так предприниматель может прорваться через все преграды», – говорит эксперт.

Первый шаг. В Facebook можно отправлять рекламу, не используя электронную почту. Люди начинают видеть вас повсюду в своей ленте и думают, что ваша компания – сверхважна и нужна им. Кроме того, социальные сети гораздо более экономны, чем другие виды рекламы – в США в Facebook можно рекламироваться всего лишь за один доллар в день.

Второй шаг. Социальные сети значительно облегчают маркетинговые исследования потенциальных клиентов – при помощи Facebook вы можете получить такие личные данные, как образование, статус в отношениях, возраст, пол, заинтересовавшие пользователя страницы.

Третий шаг. Грамотно составляйте расписание постов. Можно выкладывать посты хоть каждый час, однако, если они недостаточно интересны и их смотрят менее 3 % подписчиков, положительного результата не будет. Обычно компании B2B размещают от одного до восьми постов в день. К примеру, четыре поста об услугах компании и четыре поста на близкие темы. Также не стоит забывать о времени постов – это должно быть время, когда потенциальные клиенты или потребители услуг наиболее активны.

Для понимания того, какой способ продвижения услуг эффективнее, генеральный директор AllBiz Д. Лисицкий советует вести учет, через какой канал связи поступил тот или иной заказ, и таким способом выяснять

эффективность того или иного метода. Упростить эту задачу можно, создав разные посадочные страницы для разных способов связи (Google, Facebook и т. п.) с разными контактными данными (телефонами), советует Д. Лисицкий.

Альтернативные и дополнительные методы

Еще один инструмент рекламы в B2B – ремаркетинг. Под этим термином подразумевается демонстрация рекламы сайта, который вы однажды уже посетили. По словам экспертов, инструмент действительно эффективный.

«Если у человека один раз уже была потребность и желание зайти на нужную страничку, то существует вероятность, что ему это понадобится еще раз. И она в 20–30 раз выше, чем если просто показывать рекламу всем подряд», – утверждает генеральный директор AllBiz.

В ремаркетинге важно не допустить ошибок, которые уничтожат всю эффективность этого метода. Среди них – отсутствие связи между содержимым баннера и тем, что ищет пользователь; неверный подход к частоте показа рекламы и к аудитории для нее. Важны и сроки сбора аудитории – для разных сфер они разнятся.

Конверсия в ремаркетинге в некоторых случаях может достигать целых 100 %, утверждают эксперты.

Рассмотрим и то, как бизнес ищет поставщиков. Касательно Интернета, в настоящее время поиск поставщика услуг в Украине работает таким образом – либо через поисковики, либо через советы знакомых в Facebook. После этого идет сравнение вариантов, обдумывание и приобретение товара или услуги, в общем-то, наобум. Все это можно исправить отзывами.

Отзывы влияют на тех людей, которые на этапе сравнения и оценки выбирают себе поставщика, утверждает Е. Шевченко, руководитель агентства UaMaster. По статистике, 2/3 украинцев перед тем, как совершить покупку читают отзывы о товарах, услугах и компаниях не на официальном сайте продавца или производителя, а в независимых источниках. Использование же официальных источников позволяет получить обратную связь от поставщика, но большие блага это несет самому поставщику. Так, через обратную связь в отзывах можно повышать авторитет компании и лояльность клиентов, использовать отзывы для улучшения работы (не каждый эксперт сможет определить те недостатки, которые увидит пользователь), а положительными отзывами повысить мотивацию сотрудников.

И не забывайте, что главное в различных методах продвижения – эффективность рекламы, конверсия и экономия рекламного бюджета. Опираясь на эти критерии, следует выбрать стратегию, наиболее подходящую вашей компании ***(Шевченко Л. Facebook в помощь: как интернет может помочь B2B-бизнесу // UBR (http://ubr.ua/business-practice/own-business/facebook-v-pomosh-kak-internet-mojet-pomoch-b2b-biznesu-367951). – 2015. – 1.12).***

***

Социальные сети способствуют росту рынка электронной коммерции

Розничные продавцы во всем мире массово уходят в онлайн, а продажи в существующих интернет-магазинах показывают стремительные темпы роста. Не последнюю роль в активном развитии электронной торговли во всем мире играют социальные сети, ставшие, по сути, платформами для прямых продаж. Какие преимущества продавцам предоставляет новый сервис электронной коммерции «ВКонтакте» и насколько важным это направление является для социальной сети – об этом рассказал Ю. Иванов, директор по электронной коммерции «ВКонтакте», с которым нам удалось встретиться на конференции eCom21 в Риге, пишет PaySpaceMagazine (http://psm7.com/socialnye-seti-sposobstvuyut-rostu-elektronnoj-kommercii-yurij-ivanov-vkontakte.html).

«В этом году я выступил с докладом о нашем новом сервисе для онлайн-магазинов “Товары “ВКонтакте”, который был запущен два месяца назад. Также я участвовал в дискуссии о так называемых disruptors, то есть возмутителях спокойствия. Это компании, которые не являются традиционными для рынка e-commerce, но начинают этим заниматься.

Это не первый наш поход в электронную коммерцию. В 2010–2011 годах существовал сервис “Желания”. Тогда мы были интегрированы с крупнейшими онлайн-магазинами, такими как Ozon.ru. Пользователь мог приобрести товары из каталогов этих магазинов или добавить их в свой список желаний, а другие пользователи могли ему эти товары подарить. Функционирование этого сервиса обеспечивала наша собственная платежная система “Рубли “ВКонтакте”. Но грянул закон “О национальной платежной системе”, согласно которому, чтобы сохранить собственную платёжную систему, нам нужно было бы выполнить ряд требований. Мы тогда решили, что нам стоит сконцентрироваться на развитии социальных и коммуникационных сервисов, и закрыли сервис “Желания”.

С того времени популярность покупок в Интернете только возрастала. Мы видели это по большому количеству магазинов, которые в том или ином виде занимались торговлей на нашей площадке. Однако у них не было удобного инструмента, который позволил бы им полноценно заниматься торговлей, и они были вынуждены использовать другие сервисы не по назначению, например, фотографии. Поэтому мы запустили сервис Товаров, который позволяет десяткам миллионов покупателей получить доступ к предложениям сотен тысяч продавцов в едином интерфейсе.

Решение запустить подобный сервис заново было вызвано большим спросом

На данный момент для нас это скорее эксперимент, но первые его результаты уже внушают оптимизм. За два месяца более 200 тыс. сообществ подключили раздел Товаров и создали более 3,2 млн товарных карточек. Мы считаем, что это очень хорошие показатели, которые демонстрируют высокий спрос на подобный сервис.

На данный момент наш сервис не предусматривает оплату непосредственно с нашей помощью. То есть сделка купли-продажи проходит вне зоны нашего внимания. По сути, сейчас наш сервис работает как площадка,

на которой встречаются продавцы и покупатели. Если же говорить о платежных предпочтениях наших пользователей, то высока доля банковских карт, также популярны электронные кошельки. Таким образом, наша аудитория пользуется современными методами оплаты, предпочитая выгоду и удобство.

Ближайшие планы по развитию новых сервисов электронной коммерции "ВКонтакте".

ВКонтакте – это амбициозная команда, поэтому и планы у нас соответствующие. Безусловно, мы рассматриваем возможность внести свою лепту в изменение рынка электронной коммерции в Рунете, потому что 88 % аудитории Рунета – это наши пользователи. То есть мы на этот рынок имеем определенное влияние. Главное здесь – делать правильные шаги. Они не будут поспешными, они будут уверенными. Мы будем ориентироваться на обратную связь от наших пользователей и стараться делать то, что действительно будет полезно нашей аудитории. Сервис "Товары ВКонтакте" будет активно развиваться в 2016 г.

Также мы предлагаем рынку платежи с помощью социальных привязок. Этот новый инструмент позволяет посетителю стороннего интернет-магазина пройти авторизацию с помощью "ВКонтакте" и совершить платеж с карты, привязанной к его аккаунту в социальной сети. Использование социальных привязок повышает конверсию платежей такого магазина на 13–17 %. Секрет кроется в высоком доверии пользователя к бренду любимой социальной сети. Направление интересное, мы планируем развивать его» ***(Крузова Н. Социальные сети способствуют росту рынка электронной коммерции – Юрий Иванов, «ВКонтакте» // PaySpaceMagazine (http://psm7.com/socialnye-seti-sposobstvuyut-rostu-elektronnoj-kommercii-yurij-ivanov-vkontakte.html). – 2015. – 2.12).***

***

Відкритий доступ до соцмереж на роботі є тільки у 60 % офісних працівників України. При цьому кожен третій співробітник заходить у соцмережі кілька разів на день. Найпопулярніша Facebook, на другому місці «ВКонтакте» – показують результати опитування кадровго порталу HeadHunter Ukraine.

Про це повідомляє ain.ua.

Більш ніж 80 % офісних працівників заходять у будь-яку із соціальних мереж мінімум раз на тиждень. Читають переважно новини і розважальний контент. Крім того, соцмережі – один з найбільш популярних та ефективних каналів для пошуку нової роботи.

Найпопулярніша соцмережа серед офісних працівників Facebook. Тут шукають і розміщують професійні статті та огляди. На другому місці «ВКонтакте» і YouTube, які використовують для розваг. Дані отримали в липні 2015 р. за результатами опитування 1155 респондентів з різних регіонів України.

Рейтинг соцмереж серед офісних працівників:

Facebook (68 %)
«ВКонтакте» (58 %)
YouTube (32 %)
LinkedIn (28 %)
«Одноклассники» (24 %)
Mail.ru (23 %)
Instagram (13 %)
Twitter (9 %)
LiveJournal (4 %)
Evernote (3 %)
Pinterest (3 %)

Проте доступ до соцмереж мають лише 60 % опитаних. Кожен четвертий український роботодавець не дозволяє своїм співробітникам користуватися соцмережами в робочий час.

Найчастіше так відбувається у великих компаніях. Співробітника, який розміщує неробочий контент у робочий час, можуть за це звільнити. В Україні досі мало компаній, які просувають бізнес у соцмережах. Тільки одна з десяти компаній заохочує співробітників розміщувати інформацію про компанію в соцмережах ***(Facebook – найпопулярніша соцмережа серед українських офісних працівників // Телекритика (http://www.telekritika.ua/go_telek/2015-12-09/112754). – 2015. – 9.12).***

***

Facebook пошла навстречу рекламодателям и изменила политику в отношении Instant Articles, статей, которые можно читать, не покидая соцсеть. Как сообщает Wall Street Journal, рекламодатели смогут разместить одно объявление через каждые 350 слов. Ранее интервал был в 500 слов.

Instant Articles появились в веб-версии Facebook летом, в октябре – на iPhone. Благодаря Instant Articles издатели публикуют материалы напрямую в Facebook ***(Facebook покажет больше рекламы в Instant Articles // Состав.ua (http://sostav.ua/publication/facebook-pokazhet-bolshe-reklamy-v-instant-articles-69469.html). – 2015. – 10.12).***

***

Twitter почав тестування демонстрації реклами для тих, хто не має акаунту в сервісі мікроблогів

Про це повідомляється в офіційному блозі компанії, передає Еспресо.TV.

Тепер деякі незареєстровані користувачі, що зайшли на чийсь профіль на Twitter, наприклад, через пошуковик Google, побачать промопости. Включно з твітами посилань на сайт бренду та відеороликами. За заявою компанії, кількість незареєстрованих користувачів, які відвідують Twitter щомісяця, становить близько 500 млн осіб.

При цьому йдеться про те, що таргетинг в такому випадку буде не зовсім точний. Зазвичай користувачам Twitter показують рекламу на основі їх

підписок, ретвітів, зазначених у профілі особистих даних, місцезнаходження тощо.

Перші тестування нової функції почнуться в США, Великій Британії, Японії та Австралії. Спершу реклама буде відображатися тільки у веб-версії Twitter. Компанія заявила, що послугу запустять і в інших країнах ***(Twitter хоче нажитися на незареєстрованих користувачах // Еспресо.TV (http://espreso.tv/news/2015/12/10/twitter_khoche_nazhytysya_na_nezareyestrovanykh_korystuvachakh). – 2015. – 10.12).***

***

В Великобритании начали страховать от интернет-«троллей»

Компания Chubb начала страховать пользователей от нападок интернет-«троллей», угроз с их стороны и нанесение ущерба репутации в сети. Выплаты могут достигать 50 тыс. фунтов стерлингов: за консультации юристов, вынужденные переезды и необходимость бросить работу.

В случае с Chubb страховыми случаями признаются те, в которых насчитывается три и более нападок со стороны «троллей» (это могут быть как отдельные личности, так и группы): речь идет об угрозах, преследовании и запугивании. Ввести новый тип страхования компания решила после проведенных опросов клиентов и агентов, пишет The Stack.

Страхование, как считают в компании, будет популярно среди родителей, которые волнуются за своих детей, проводящих все больше времени в Интернете. Однако покупателями страховки могут стать и взрослые. Так, страховку можно использовать для найма PR-специалистов, которые специализируются на восстановлении деловой репутации ***(В Великобритании начали страховать от интернет-«троллей» // InternetUA (http://internetua.com/v-velikobritanii-nacsali-strahovat-ot-internet--trollei). – 2015. – 13.12).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Любители размещать на своих страницах в социальных сетях «глубокомысленные» цитаты, размещенные на фоне пейзажей, отличаются более низким уровнем интеллекта.

В этом убеждены ученые, сообщает Joinfo.ua со ссылкой на Daily Mail. Соответствующее исследование британские психологи разместили в журнале Judgment and Decision Making.

Материал под названием «О восприятии и распознавании псевдомудрой чепухи» посвящен тому, являются ли одни люди более восприимчивыми к воодушевляющим цитатам, чем другие.

В ходе эксперимента 845 добровольцам демонстрировались «глубокие» мысли («Ты силен настолько, насколько силен твой следующий ход», «Посреди движения и хаоса сохраняй спокойствие внутри себя» и т. д.), которые в избытке можно найти в Интернете. При этом часть цитат была фиктивной – ее либо генерировали случайным образом, либо же это были очевидные утверждения наподобие «большинству людей нравится музыка».

Как выяснилось, участники исследования не чувствовали разницы между реальными мотивационными цитатами и фиктивными – и тем, и другим они выставляли примерно одинаковые оценки по шкале «глубины мысли».

После этого участников эксперимента попросили пройти серию психологических тестов и заполнить анкету с вопросами о собственных верованиях.

Как выяснилось, ценителей «глубокомысленных» цитат оказалось около 27 %. При этом ученые выяснили, что они не склонны к рефлексии, у них хуже математические навыки, они медленнее думают, придерживаются суеверий и склонны к вере во всемирный заговор ***(Ученые: у любителей вывешивать в соцсетях цитаты проблемы с интеллектом // Joinfo.ua (http://joinfo.ua/hitech/scince/1136969_Uchenie-lyubiteley-viveshivat-sotssetyah-tsitati.html). – 2015. – 8.12).***

***

Американские ученые выяснили, что Facebook оказывает негативное влияние на здоровье женщин. При просмотре ленты в соцсети девушки могут впадать в депрессию.

Ученые из Университета Окленда в США провели исследование, в котором приняли участие примерно 11 тыс. человек. 63 % из общего числа добровольцев составили женщины, а 37 % – мужчины.

Как оказалось, девушки, имеющие аккаунты в Facebook, начинают сравнивать свои фотографии со снимками других представительниц женского пола в социальной сети, в том числе звезд шоу-бизнеса и знаменитых моделей, чьи изображения зачастую отредактированны фотошопом. Если девушка решит, что она выглядит хуже остальных, то у нее может развиться депрессия.

При этом выяснилось, что мужчин в целом не волнует, как они выглядят по сравнению с другими представителями сильного пола. Ученые сделали вывод, что Facebook отрицательно влияет на здоровье женщин и рекомендуют им ограничить время пребывания в социальных сетях ***(Ученые доказали, что соцсети опасны для девушек // GoGetNews.info***

(http://www.gogetnews.info/news/society/110344-uchenye-dokazali-chto-socseti-opasny-dlya-devushek.html). – 2015. – 6.12).

***

Опитування мешканців США, проведене на замовлення NBC News, показало, що понад 70 % американців переконані, що сучасні технології роблять стосунки між людьми не такими міцними, як були колись.

Про це повідомляє «Українська правда. Життя».

Водночас 68 % безпосередніх користувачів сайтів Facebook, Twitter та Instagram вважають, що «живі» взаємини страждають від впливу соціальних мереж. Серед тих, кого немає в соцмережах, злом їх назвали усі 83 %.

Тих, хто вважає, що новітні технології лише йдуть на користь взаєминам – 35 %. Прихильників соціальних медіа найбільше серед учасників 18–34 років.

У групі 35–64 років упевнених у позитивній ролі технологій виявилося 20 %. Прикметно, що після 65 років симпатія до соцмедіа зростає – із тим, що вони сприяють зміцненню зв'язків між людьми, погодилися 28 % респондентів цієї вікової групи.

Серед любителів соцмедіа 30 % змушені визнати, що такі сайти пробуджують найгірше, що криється в людині.

«60 % респондентів зізналися, що блокували когось або відфренджували. 69 % жінок назвали серйозною проблемою цькування в Інтернеті. Серед чоловіків чутливими до цього виявилася лише половина», – повідомляє «УП.Життя».

Як повідомляв Media Sapiens, кількість українських користувачів соціальної мережі Facebook за останній рік (з вересня 2014 по вересень 2015 року) зросла на 30 %, або на 1 мільйон осіб ***(70 % американців вважають, що соцмережі псують стосунки між людьми // MediaSapiens (http://osvita.mediasapiens.ua/web/social/70_amerikantsiv_vvazhayut_scho_sotsmerezhi_psuyut_stosunki_mizh_lyudmi/). – 2015. – 9.12).***

***

Як з'ясувалось, 90 % матусь – у списку друзів своїх дітей на Facebook. Але психологи впевнені, це велика помилка – намагатися стежити за дітьми в мережах. Адже у віртуальному просторі людина часто не та, ким є насправді. Тому таке стеження може мати мінімум користі та максимум недовіри з боку дитини.

1. У мережах є кожен другий школяр, хоча реєстрація неповнолітніх і заборонена, як і фальсифікація даних про себе та свій вік. Це не заважає школярам представлятися студентами та щосили спілкуватися з дорослими.

2. У 86 % батьків є акаунт у тій же соцмережі, де проводить час їхня дитина. Але це не заважає дітям приховувати інформацію про себе саме від батьків.

3. 90 % матерів френдять своїх дітей на Facebook, але при цьому 46 % із них обмежують доступ своїм дітям у свої профілі. Саме такі результати «підлої» поведінки мами оприлюднили журнали Parenting і Babytalk.

4. У деяких батьків є вигадані профілі, які вони використовують, щоб завести дружбу зі своїми дітьми в соцмережах.

5. Але не такі й строгі батьки. За даними дослідження The Parenting Group, 33 % мам дозволяють дітям створювати у Facebook сторінки в 12 років. Хоча це заборонено до 13 років.

6. 73 % мам, які не зафрендили своїх дітей на Facebook, стежать, як діти користуються Facebook, під іншими ніками.

7. А от дружити з друзями дітей мами дуже навіть хочуть. 77 % матерів «дружать» із друзями своїх дітей у соцмережах.

8. Більшість мам (87 %) прагнуть обмежити дітям використання соцмереж. 52 % батьків дозволяють своїм дітям бути на Facebook тільки 1 годину на день.

9. Для багатьох дітей соцмережі – це бонус за виконане домашнє завдання. Таких бідолах серед підлітків налічується 30 %.

10. Для 20 % дітей Facebook доступний лише в присутності дорослих.

11. У світі 50 % батьків щотижня, 35 % щодня, 10 % раз на місяць стежать за акаунтами своїх дітей у соцмережах, за даними компанії TRUST.

12. 84 % батьків упевнені, що точно знають, скільки часу їхні діти проводять у мережах, і вважають, що діти відповідально ставляться до поширення персональної інформації в соціальних мережах.

13. А поки батьки такі впевнені у своєму контролі, 67 % підлітків підчищають історію перегляду у своїх браузерах, як заявила компанія Microsoft.

14. 40 % мам дозволяють своїм дітям грати в ігри на своїх смартфонах кожен день, це з'ясувала The Parenting Group.

15. Та й самі матусі заохочують знайомство дітей з комп'ютерами. Кожна з них у середньому завантажує 11 додатків на свій смартфон, і 4 із них – для дитини.

Чи контролювати дітей у соціальних мережах, вирішувати лише тобі. Адже все залежить від дитини, від її відповідальності та довіри до тебе. І якщо вдалося побудувати з дитиною довірчі стосунки, це краще за будь-які шпигунські ігри з чужими ніками й акаунтами ***(Дитина і батьки в соцмережах: про що варто знати? // Nashamama.com (http://nashamama.com/simia/18739ditina-i-batki-v-socmerezhah-pro-szo-varto-znati.html#). – 2015. – 9.12).***

***

Які небезпеки підстерігають наших дітей у мережі?

Контент 18+, небезпечні незнайомці, необдумані покупки: Kaspersky Lab розповідає про небезпеки для дітей у мережі, пишуть «АКЦЕНТИ. СЬОГОДНІ» (http://accents.today/news/yaki-nebezpeky-pidsterihayut-nashyh-ditej-u-merezhi/).

Сучасні діти оточені великою кількістю гаджетів – комп'ютерами, смартфонами, планшетами. З їх допомогою маленькі користувачі виходять в Інтернет і почуваються там не менш вільно, ніж у реальному житті.

Це лякає мам і тат: згідно з опитуванням Kaspersky Lab, 53 % батьків бояться, що їхня дитина побачить у мережі небажаний контент, і кожен десятий упевнений у тому, що це вже сталося.

Досліджуючи інтереси молодшого покоління в Інтернеті, експерти виявили, що батьків також сильно турбує можливість спілкування дитини з небезпечними незнайомцями (44 %). Такі співрозмовники можуть ображати дитину, виманювати у нього конфіденційну інформацію, пропонувати реальні зустрічі.

Цей страх має під собою підставу, адже найбільше в Інтернеті дітей цікавлять саме засоби спілкування, переважно соціальні мережі. На категорію «Засоби інтернет-комунікації» (соціальні мережі, веб-пошта і чати) припадає 77 % від загальної кількості дитячої інтернет-активності.

Ще одна зростаюча небезпека в соцмережах – це кібербулінг, тобто цькування і приниження в мережі, що часто стає причиною серйозної психологічної травми, особливо якщо віртуальний конфлікт переростає в реальний.

Також діти заходять у мережу заради комп'ютерних ігор (11 %) і для оплати покупок в інтернет-магазинах або платіжних системах (4 %). Несанкціонований доступ малюків до онлайн-гаманцях батьків призводить не тільки до фінансових втрат, але й може забезпечити дитині доступ до небажаного контенту.

Меншою мірою серед дітей популярні інші активності, такі як пошук піратських програм, відео, музики, порно та еротики, принципів роботи блокуючих програм, поставлених батьками, і способів їх обходу, а також відвідування сайтів категорій «Зброя», «Насильство» та «Нецензурна лексика».

Незважаючи на велику кількість можливих ризиків, кожен п'ятий дорослий не робить ніяких захисних заходів, щоб захистити свою дитину, і лише 22 % встановили засоби батьківського контролю.

Тому сайт Kaspersky Lab радить таке:

– рзкажіть своїм дітям про потенційні загрози, які є в Інтернеті;
– якщо це можливо, встановіть комп'ютер у спільній кімнаті;
– намагайтеся проводити час за комп'ютером усією родиною;
– попросіть дітей розповідати про все, що викликає у них неприємні почуття або дискомфорт під час відвідування Інтернету;
– обмежте кількість матеріалів, доступних для дітей через комп'ютер;
– поясніть дітям, що їм дозволено, а що заборонено робити в Інтернеті:
– реєструватися в соціальних мережах і на інших сайтах;
– робити покупки в Інтернеті;
– завантажувати музику, ігри та інший контент з Інтернету;
– використовувати програми миттєвого обміну повідомленнями;
– відвідувати чати;

– якщо дітям дозволено використовувати програми миттєвого обміну повідомленнями або відвідувати інтернет-чати, розкажіть їм про небезпеки спілкування або надсилання повідомлень людям, яких вони не знають і яким не довіряють ***(Які небезпеки підстерігають наших дітей у Мережі? // АКЦЕНТИ. СЬОГОДНІ (http://accents.today/news/yaki-nebezpeky-pidsterihayut-nashyh-ditej-u-merezhi/). – 2015. – 4.12).***

Маніпулятивні технології

В Украине действуют десятки курируемых спецслужбами России сетевых сообществ

Сегодня в социальных сетях существует более полутора тысяч антиукраинских сообществ и групп, которые информационно поддерживают пророссийских сепаратистов и сеют ненависть к любым проявлениям всего украинского.

В соцсети «ВКонтакте» по запросу «Новороссия» можно найти свыше 900 пабликов. В самом большом из них 78 167 участников. По запросу «ЛНР» найдем 131 сообщество, по запросу «ДНР» – 397. В «Одноклассниках» по тем же запросам поисковик выдаст порядка 300 групп.

Есть среди них и многочисленные местные группы, ориентированные на жителей определенных районов и населенных пунктов. Большая часть, понятное дело, охватывает жителей временно оккупированной части Донбасса.

Но и на контролируемой украинской властью территории такие сообщества все еще можно найти (к слову, в «ЛНР» также действуют местные проукраинские группы – но речь в данном случае не о них). Справедливости ради, стоит отметить, что участников в таких группах немного – обычно по несколько сотен.

Фабрика ботов

В принципе, интернет-пользователи имеют возможность ознакомиться с разными сепаратистскими сетевыми ресурсами, ориентированными на представителей различных регионов. Бросается в глаза несомненное сходство их содержания. Везде фимиам В. Путину и анафема всему европейскому, американскому, украинскому, а теперь еще и турецкому. Месседжи одни и те же, одинаковые мнения, одни и те же слова, одни и те же картинки. Год назад все хором твердили о крушении Украины как о свершившемся факте, теперь тем же хором практически в одних и тех же выражениях славят «великую миссию» России в Сирии.

Последний тренд – тотальная истерика по поводу обесточенного Крыма и сбитого турками российского истребителя, с неизменным ликом сурового В. Путина, который всем покажет «кузькину мать». Все как один участники антиукраинских сообществ испытали приступ отвращения к турецким курортам (на которых большая часть никогда не была) – в пабликах развернута агитационная кампания. Слова «ополченцы» и «ополчение» все как-то вдруг и

дружно выкинули из лексикона, но вместе с тем синхронно перепечатали текст «рупора» боевиков А. Жучковского о том, сколько миллиардов Россия тратит на поддержку сепаратистских банд в Украине (местные боевики боятся, что Россия их сольет).

Если убрать со страниц этих виртуальных сообществ местные новости и не несущие смысловой нагрузки переклички ботов – останется голый костяк российского имперского мышления. И элементы информационной войны – нагнетание нелепых слухов и страхов вроде белиберды о запрете на выезд за пределы Украины мужчинам до 45 лет, приказа ВСУ стрелять по всему, что движется, и прочей глупости.

«Сегодня на территории области (в том числе, на оккупированной части) действует порядка 30 пророссийских сетевых сообществ, – рассказал сотрудник одного из подразделений СБУ. – В общей сложности, ими руководит от 15 до 20 человек, находящихся на оккупированной территории. Отсюда – сходство контента. Концепция-то одна.

Если группа создается для украинской территории, то ее создатели и (за редким исключением) администраторы находятся на территории России и являются сотрудниками ФСБ или контролируются ими. Если речь идет о локальных группах для “ЛНР”, то этих людей все равно опосредованно курирует ФСБ РФ. Многие группы создавались еще в 2014 г. специально под неудавшийся проект “Новороссия”, хотя в основном старые сепаратистские группы нами заблокированы. Но некоторые функционируют. Их создатели стремятся максимально охватить влиянием активную часть Интернет-пользователей до 40 лет, представляющих по возможности разные слои населения».

Правоохранительные органы Украины имеют и законодательные, и технические возможности, позволяющие пресечь функционирование подобных интернет-ресурсов, и эта работа активно ведется. Лица, которые создают такие ресурсы и участвуют в их работе, привлекаются к ответственности за содействие террористической организации (ст. 258-3 КК Украины) или по ст. 110 (посягательство на территориальную целостность и неприкосновенность Украины).

Редакторы – местные

Функционирование сообществ обеспечивает вертикаль «создатели – редакторы – администраторы».

Возглавляют процесс создатели, находящиеся в России. Они назначают администраторов, редакторов, создают и по необходимости меняют контент. Администраторы назначают редакторов сообществ, размещают новости, выставляют фильтры и цензуру. Их задача – следить за тем, чтобы на странице никто не писал ничего хорошего об Украине и ничего плохого – о России, о «ДНР» и «ЛНР». При появлении «неправильных» точек зрения их немедленно удаляют или троллят, тем самым создавая у простых пользователей иллюзию полного единства мнений: буквально все боготворят Путина, ненавидят «хунту» и «гнилой Запад».

Кстати, о единодушии и массовости. Количество участников сепаратистских пабликов – еще один способ воздействия на коллективный мозг целевой аудитории. В самом большом – ЛНРовском сообществе «ВКонтакте» 27 322 участников, в «Одноклассниках» – 74 840 участников. И на всех – одно мнение.

Как единичному пользователю устоять перед стереотипом «большинству виднее»? Самостоятельную точку зрения сохранить трудно. А между тем наш собеседник из СБУ уверяет, что при желании такое количество аккаунтов фейковых участников можно насоздавать в течение суток, не выходя из комнаты. Социальная сеть «ВКонтакте» насчитывает 75 млн российских аккаунтов, из них минимум половина – это фэйки.

Была бы на то воля российских манипуляторов – они бы, конечно, изготавливали весь продукт самостоятельно и в готовом виде вкладывали в голову «целевой аудитории». Но особенность подобных сообществ в соцсетях состоит в том, что они не могут существовать без информационного обмена с живой местной средой. Поэтому руководители стараются подыскивать редакторов групп среди жителей того района, на который направлено пропагандистское воздействие. Обычно в сетях их и находят.

Задача редакторов – размещать готовый контент. Через администраторов они получают от россиян информационные задания на день и отрабатывают их. Озвучивают определенные кураторами темы дискуссий, заранее подготовленные мнения, готовые итоги дискуссий. Те же принципы лежат в основе организации работы СМИ «ЛНР». Полученный контент редакторы разбавляют местными сообщениями, объявлениями и т. п.

Но этим их работа не ограничивается. Нередко, помимо редакторских функций, им поручается сбор разведывательной информации, что вообще-то чревато для них серьезными последствиями. Это касается в первую очередь, территорий Донбасса, находящихся неподалеку от линии разграничения. Российские доброжелатели хотят, чтобы их информировали о дислокации и перемещении украинской техники, наличии ремонтных баз, о личном составе подразделений и прочих вещах, за которые можно, грубо говоря, надолго «сесть» по обвинению в содействии террористической деятельности или в госизмене.

В Луганской области известны случаи, когда по поручению кураторов местные интернет-воины пытались собирать такую информацию, в том числе, вовлекая в это дело других пользователей. Правоохранители их находят и привлекают к ответственности.

Добровольцы и наемники

Получают ли сетевые воины деньги за свою работу? Тут тоже не все просто. Условно их можно разделить на две группы, назвав для ясности «бесплатные» и «беспринципные».

Первая группа – бесплатная рабсила. Люди с навязчивыми идеями: «Путин придет – порядок наведет», «Не буду получать загранпаспорт – дождусь, пока везде будет Россия» и т. п. Приобщаясь к чему-то, по их мнению,

великому (например, к культу личности президента соседней страны) они чувствуют себя увереннее в этом опасном мире, который их не ценит и не понимает. А вообще им страшно жить. Они обидчивы. С ними трудно. Они на своей волне.

Вторая – меркантильные граждане, для которых работа в антиукраинских пабликах не более, чем зарабатывание денег. С таким же успехом они могли бы сбывать наркоту или заниматься мошенничеством. Но сидеть за компьютером легче и вроде как интеллигентнее. Они получают оплату за труд, плюс отчисления от рекламы. Эти трезвомыслящие (по-своему) и беспринципные люди, как правило, ищут неадекватных и странноватых фанатов «русского мира», т. к. их бескорыстная и бестолковая нелюбовь к Украине при правильной организации для корыстных становится хорошим источником доходов. Информационная война – тоже бизнес ***(В Украине действуют десятки курируемых спецслужбами России сетевых сообществ // АНТИКОР (http://antikor.com.ua/articles/76436-v_ukraine_dejstvujut_desjatki_kuriruemyh_spetssluhbami_rossii_setevyh_soobshchestv). – 2015. – 7.12).***

***

Сторонники боевиков Донбасса уверены, что депутат Николаевского областного совета Н. Скорый, который позволил себе сидеть во время звучания государственного гимна Украины, станет руководителем области после победы российско-террористической организации «Новороссия».

Такое заявление появилось в открытой группе «Правда в Новороссии» «ВКонтакте», подписчиками которой являются более 2600 человек.

Также в сообщении обещают казнить патриотов Украины.

«В Николаеве еще много наших парней, которые отстаивают идеалы Новороссии, и им нужна поддержка всех жителей Донбасса. Честь и хвала Николаю Скорому, который поставил на место укропов в сессионном зале облсовета. Не ровен тот час когда над Николаевом мы установим флаг Новороссии, и тогда заиграет на весь ЮГ гимн Великой Новой Державы. И такие люди как Николай Скорый будут руководить регионом», – сказано в сообщении ***(Сепаратисты восхваляют николаевского депутата, который отказался встать под гимн Украины // НикВести (http://nikvesti.com/news/incidents/79692). – 2015. – 8.12).***

***

В украинском сегменте Facebook активно обсуждается проект «Слобожанщина», призванный «автономизировать» Харьковскую область от Украины. Участники общественного совета «Слобожанщина» регулярно выступают за усиление полномочий региональных властей якобы для решения социальных проблем области. Пользователи социальных сетей считают, что «Слобожанщина» может стать сепаратистским проектом. В частности, украинский журналист П. Шуклинов на своей странице в Facebook отмечает,

что «Кремль развивает новую волну сепаратизма в восточных областях Украины и не демонстрирует желания прекратить терроризм». Об этом сообщает replyua.net со ссылкой на журналиста, пишет Багнет (http://www.bagnet.org/news/politics/272911).

Он отметил, что сепаратизм на Востоке Украины активно пытаются привить бывшие коммунисты. В частности, экс-соратница Симоненко А. Аллександровская развивает в Харькове желание граждан получить особый статус для города. «Причем упирает на то, что этого якобы хочет молодежь. Проводит чистую манипуляцию в заголовке и тексте», – сетует блоггер. «Все делается настолько явно, что даже клише не считают нужным менять. Термин "киевские власти" звучит постоянно и демонстрирует "желание" харьковчан отделиться от киевских властей», – отмечает журналист. Также П. Шуклинов обратил внимание на список СМИ, активно обсуждающих данную тему. Журналист призывает СБУ обратить внимание на проект «Слобожанщина» и принять незамедлительные меры по пресечению сепаратизма в Харьковской области ***(В соцсетях массово призывают арестовать Александровскую за сепаратизм // Багнет (http://www.bagnet.org/news/politics/272911). – 2015. – 2.12).***

***

Два типа крымчан. Кто чаще пишет в соцсетях

Во всей ситуации с Крымом есть главная проблема – отсутствие внятной социологии. Чаще всего мы делаем вывод о настроениях на полуострове, ориентируясь на комментарии в соцсетях. А они не вполне релевантны, пишет П. Казарин для «Крым.Реалии», сообщает «Обозреватель» (http://obozrevatel.com/blogs/10753-dva-tipa-kryimchan--kto-chasche-pishet-v-sotssetyah.htm).

Если собрать коллективный портрет крымского комментатора, то создается ощущение, что он всецело рад российской реальности, презирает Украину, ждет входа российских войск в Киев и царапает на деревьях «Обама – чмо». Одновременно он ждет скорого краха американской модели и предвкушает, как презираемые им беженцы растопчут презираемый им Евросоюз.

Знакомый персонаж, верно?

Самой большой ошибкой было бы думать, что подобные настроения – средняя температура по больнице. Существует важный фактор, определяющий уровень «непримиримости» и «радикальности» поведения человека в соцсетях. Этот маркер очень прост: что будет с человеком, если в Крыму снова сменятся флаги?

Потому что все крымчане сегодня оказались разделены на два лагеря. И этот водораздел заключается даже не в том, проукраински или пророссийски они настроены. Дело в другом. Сложилось так, что по одну сторону баррикад – те, кто поставил себя вне рамок украинского законодательства. По другую – те, кто подобных шагов не совершал.

Первые отчетливо понимают, что в случае смены флагов им придется покидать территорию полуострова из-за угрозы судебных преследований. Они даже не рассматривают возможность возвращения Украины в Крым, потому что в их личном случае это будет означать персональное поражение. Абсолютно закономерно, что они – наиболее непримиримы в своих высказываниях и комментариях. И наиболее активны – потому что им, по большому счету, нечего терять. Сохранение российского присутствия – это единственная возможность для них сохранить свое персональное статус-кво.

И есть вторая группа людей. Те, кто не нарушал украинского законодательства. Кто не нарушал присягу – военную или чиновничью. Они могут даже не быть проукраински настроенными – более того, они вполне могут питать симпатию к Москве. Но, с юридической точки зрения, в их действиях Киев не сможет найти ни малейшего состава преступления. Просто потому, что они жили и живут, не соприкасаясь с государством. Условно говоря, в этот лагерь попадают все те, кто могут выезжать сегодня из Крыма в Херсонскую область, не опасаясь вопросов со стороны украинских силовиков.

Эта вторая группа куда менее активна в соцсетях. Именно потому, что для них смена флагов в Крыму не означает обязательных изменений в личной судьбе. Более того, они куда осторожнее в высказываниях, потому что это позволяет им не знакомиться (ни сейчас, ни в перспективе) ни с российской, ни с украинской силовыми системами. Причем в этой группе есть как те, кто ждет возвращения в Крым Киева, так и те, кто просто сосредоточен на обычном бытовом выживании.

И специфика данной ситуации именно в том, что в публичном пространстве слышны голоса только ребят из первой группы. Тех, кому нечего терять, а потому они яростно обличают Украину. Тех, кому некуда отступать, а потому они защищают Москву и ее политику. Это не тролли, им не платят зарплату за комментарии – они всего лишь защищают нынешнюю реальность, потому что не уверены, что в случае ее изменения им попросту найдется место на полуострове.

Составлять мнение о настроениях в Крыму, исходя из их активности, заведомо бессмысленно. Они загнали себя в ситуацию, когда им придется защищать любое действие Кремля, сколь бы сомнительным оно ни было. Они вынуждены служить адвокатами любых властных капризов – просто потому, что присутствие триколора гарантирует их персональное будущее. Их невозможно убедить аргументами, потому что для них это не отвлеченный теоретический спор о будущем. Для них любой разговор о судьбе Крыма – это разговор об их персональной дальнейшей судьбе. Эмоции для них – это способ интуитивной защиты.

Помните об этом, когда будете сталкиваться с теми, кто рассказывает, что крымский вопрос закрыт раз и навсегда ***(Казарин П. Два типа крымчан. Кто чаще пишет в соцсетях // Обозреватель (http://obozrevatel.com/blogs/10753-dva-tipa-kryimchan--kto-chasche-pishet-v-sotssetyah.htm). – 2015. – 9.12).***

***

В четверг вечером, 3 декабря, оба аккаунта и «публичная фигура» российского финансиста и блогера Славы Рабиновича в Facebook были заблокированы на 30 дней.

Как он сам сообщил «Обозревателю», это произошло в шестой раз за период с августа 2014 г. (http://obozrevatel.com/politics/08673-facebook-zablokiroval-rabinovicha-iz-za-zhalob-fabriki-trollej.htm).

По словам С. Рабиновича, так называемая фабрика троллей российской пропаганды выбрала абсолютно случайный его пост, после чего на него последовала чреда «жалоб».

«Главное, чтобы количество “жалоб” на этот пост было реально огромным, лавинным. Далее в Facebook автоматически срабатывает “робот” на блокировку, который может быть, в ручном режиме, проверен (и отменен или не отменен) русскоязычным модерационным центром в Дублине. Бывают случаи, когда этот центр модерации секретно подчиняется “неофициальным просьбам” российских властей заблокировать тот или иной аккаунт», – объяснил С. Рабинович.

После блокировки блогер не может запостить никаких текстов и не может комментировать свои посты, кроме того личная переписка С. Рабиновича не работает ***(Facebook заблокировал Рабиновича из-за жалоб «фабрики троллей» // Обозреватель (http://obozrevatel.com/politics/08673-facebook-zablokiroval-rabinovicha-iz-za-zhalob-fabriki-trollej.htm). – 2015. – 4.12).***

***

Шулеры заводят фальшивые страницы в социальных сетях с фотографиями бойцов АТО и требуют денег «на пополнение счета» у новых друзей.

Об этом пишет издание ИНФОРМАТОР со ссылкой на публикацию волонтера Е. Любинецкой на странице в Facebook.

«Опять аферисты атакуют. За два дня уже третий. Вот из-за таких уродов потом страдают нормальные ребята. И что только не придумают, от пополнения счета и до срочной оплаты счета его беременной жены. Сначала они внимательно рассматривают Вашу страницу с лайками – при возможности добавляются в друзья.

При этом у самих страницы зарегистрированы не более недели. На вопросы при переписке, отвечают поверхностно и обобщенно – ничего конкретно и путаются. Если припрете к стенке – обложат с головы до ног, при этом сразу удаляют свою страницу», – описала Е. Любинецкая ***(«Волки из Facebook»: как аферисты наживаются на имидже бойцов АТО // ІНФОРМАТОР (http://www.informator.su/volky-yz-facebook-kak-aferystyi-nazhyvayutsya-na-ymydzhe-bojtsov-ato/). – 2015. – 13.12).***

В России впервые назначено реальное лишение свободы за пост в соцсетях

Сургутский городской суд впервые приговорил к реальному лишению свободы жителя Сургута О. Новоженина, обвиняемого в распространении в социальных сетях экстремистских материалов.

Согласно материалам дела, расследованием которого занимались следователи регионального управления ФСБ по Тюменской области, молодой человек выложил аудио- и видеофайлы, которые пропагандировали деятельность украинской националистической партии «Правый сектор» (запрещена в России) и добровольческого батальона «Азов».

Интересно, что обычно по данным составам суды привлекают подсудимых в основном к штрафу или назначают условный срок. Реальное лишение свободы на срок один год в колонии-поселении было назначено впервые в России ***(В России впервые назначено реальное лишение свободы за пост в соцсетях // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45467/118/lang,ru/). – 2015. – 01.12).***

***

«Фонд электронных рубежей» (Electronic Frontier Foundation, EFF) направил жалобу в Федеральную торговую комиссию США (Federal Trade Commission) и обвинил компанию Google в слежке за несовершеннолетними пользователями ноутбуков Chromebook. Специалисты EFF уверены, корпорация нарушает американское законодательство и собственную политику конфиденциальности.

По словам представителей «Фонда электронных рубежей», проблема затрагивает всех пользователей Google Chromebook и набора программ Google Apps for Education. Последний представляет собой набор образовательных online-приложений, широко используемых в школах и высших учебных заведениях во всем мире.

В целях защиты персональных данных Google подписала Заявление о неприкосновенности личных данных учащихся (Student Privacy Pledge) – документ, обязывающий компании не собирать и не использовать персональные данные учеников без предварительного согласия родителей. За нарушение условий Заявления Google может быть привлечена к ответственности в соответствии с законодательством США.

Согласно заявлению EFF, Google действительно не собирает персональные данные школьников во время интернет-браузинга. Тем не менее, в настройках ноутбука Chromebook по умолчанию включена опция синхронизации. Это позволяет Google собирать, хранить и анализировать персональные данные учащихся, включая историю посещений веб-сайтов, логины, пароли и другие данные. Компания действует без предварительного разрешения родителей.

Google отреагировала на претензию EFF и пообещала отключить синхронизацию в ноутбуках Chromebook, поставляемых в учебные заведения.

Заявление о неприкосновенности личных данных учащихся обеспечивает защиту персональных данных учеников школ на юридическом уровне. Подписавшие документ компании (206 на момент написания новости) обязуются не собирать конфиденциальную информацию школьников в каких-либо целях, выходящих за рамки образовательных программ, а также обеспечивать защиту данных всеми возможными способами. Заявление подписали такие компании, как Apple, Google и Microsoft.

Electronic Frontier Foundation (EFF), Фонд электронных рубежей – основанная в июле 1990 г. в США некоммерческая правозащитная организация с целью защиты заложенных в Конституции и Декларации независимости прав в связи с появлением новых технологий связи.

Хромбук – лэптоп, работающий под управлением операционной системы Chrome OS ***(Google следит за несовершеннолетними пользователями Chromebook // InternetUA (http://internetua.com/Google-sledit-za-nesovershennoletnimi-polzovatelyami-Chromebook). – 2015. – 5.12).***

***

В связи с террористическими атаками давление на социальные сети растет, и государство требует от таких сайтов, как Facebook, YouTube и Twitter, более тщательного мониторинга экстремистского контента, пишет gazeta.ru

На прошлой неделе Facebook удалила страницу, которую, как предполагается, использовали двое подозреваемых в стрельбе в Сан-Бернандино. Представитель социальной сети отказался говорить о том, как данный профиль был найден, а также о том, как была определена его подлинность.

«Когда дело доходит до террористического контента, то это сложная ситуация для компаний, и я им не завидую. Тем не менее, я волнуюсь, что, опасно давать не демократичным по своей природе компаниям больше возможностей регулировать свободу слова», – сказал изданию глава Фонда электронных рубежей США Д. Йорк.

Отмечается, что количество материалов является вызовом для компаний. Около 400 часов видео загружается на YouTube каждую минуту. Сайт не удаляет ролики самостоятельно, а делает это лишь после того, как кто-то из пользователей присылает жалобу. Facebook заявляет, что компания старается обрабатывать подобные отчеты пользователей более оперативно ***(WSJ: от социальных сетей требуют мониторинга экстремистского контента // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45527/118/lang,ru/). – 2015. – 7.12).***

***

Начиная с 1 января 2016 г., правительство Казахстана собирается прослушивать весь пользовательский трафик, включая зашифрованные HTTPS-соединения. Для этого были внесены соответствующие поправки в Закон «О связи». Для реализации глобальной прослушки будет выпущен специальный корневой сертификат, который создаст Комитет связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан.

Новость о внедрении «национального сертификата безопасности» была опубликована на сайте АО «Казахтелеком», однако позже загадочным образом оттуда исчезла. Но кэш Google все помнит.

Как можно заметить, технических подробностей пока мало, но в целом схема работы «национального сертификата безопасности» ясна. Пользователей обяжут загрузить и установить на все устройства правительственный сертификат, через который будет проходить весь защищенный трафик зарубежных веб-сайтов. Можно предположить, что дешифровке подвергнется не только весь HTTPS-трафик, но и прочие TLS-соединения.

Фактически, это означает, что во время установки SSL-соединения настоящий сертификат сайта будет подменяться фальшивкой, сгенерированной на лету. Такой подставной сертификат будет завязан на «национальный сертификат безопасности», который всех пользователя страны заставят добавить в список доверенных корневых сертификатов. В результате браузер сочтет фальшивку доверенной.

Без установки корневого сертификата браузеры будут пугать пользователей предупреждениями о том, что сертификат недействителен. Чтобы не возникло паники, «Казахтелеком» обещает провести разъяснительную работу с пользователями в декабре 2015 г. и опубликовать соответствующие инструкции и пояснения на официальном сайте.

Если все пройдет именно так, как запланировано, начиная с января 2016 г., власти страны действительно получат полный доступ к трафику пользователей, и наступит эра «Великого казахского файрвола». Однако ни одно защищенное соединение в стране после этого не сможет считаться по-настоящему защищенным. Соединение с банком или платежной системой, сессия с iCloud или Dropbox, всё будет как на ладони.

Похожие схемы использует правительство Китая и «Великий китайский файрвол» он же «Золотой щит». Так, в апреле текущего года Google забанила в удостоверяющем центре Chrome китайский корневой сертификат, созданный с аналогичной целью. Реакции от других компаний на действия Поднебесной, впрочем, не последовало ***(Казахстан собирается контролировать и прослушивать весь HTTPS-трафик // InternetUA (http://internetua.com/kazahstan-sobiraetsya-kontrolirovat-i-proslushivat-ves-HTTPS-trafik). – 2015. – 05.12).***

***

Следственный комитет вызвал на допрос крымскотатарского общественного деятеля и правозащитника Эмир-Усеина Куку за его посты в социальной сети Facebook. Об этом сообщает Главное со ссылкой на «События Крыма».

«Предъявляют то, что в сети Интернет в своем аккаунте в Facebook размещал ряд материалов. В ФСБ считают, что эти материалы экстремистские. К такому выводу они пришли в результате проведения лингвистической и криминалистической экспертизы моих высказываний, комментариев. ФСБ передала дело в Следственный комитет России», – рассказал Э.-У. Куку.

По словам активиста, проверка Следственного комитета коснулась его постов, сделанных даже до аннексии Крыма. В общей сложности сотрудники ФСБ и Следственного комитета на странице правозащитника зафиксировали более 40 публикаций, к которым они имеют претензии.

«Как я понимаю, они проштудировали мою переписку начиная еще со времен Украины с 2013–2014 года. Насобирали в общей сложности более сорока эпизодов, я увидел 42, возможно даже и больше. Туда входят ссылки на различные интернет-сайты, как российские, так и украинские. В том числе, ссылки на сайт YouTube. В первую очередь их интересовало обращение к мусульманам Крыма, видеоролики, в том числе и зарубежные, с переводами, где к мусульманам Крыма обращаются со словами поддержки, сочувствия, призывами быть терпеливыми, в связи с тем, что мы оказались в таком положении. Даже они зацепились к словам “Вы славные, веруете в Аллаха”. Они начали проводить лингвистический анализ этой фразы. Все это они склоняют к межнациональной розни – 282 статья УК РФ», – сообщил Э.-У. Куку.

«Ссылки на высказывания М. Джемилева, в отношении того, что против крымских татар и крымских мусульман будут применяться репрессии, выдавливания из Крыма, то же самое в отношении политических активистов. Все то, что они насобирали, касается критики властей. Так или иначе, все у них подогнано так, что целью является создание негативного образа России, негативной позиции России и так далее», – добавил он.

На допрос в Следственный комитет также вызывают супругу активиста для дачи показаний. Если же вина Э.-У. Куку будет доказана, ему грозит до пяти лет лишения свободы.

Эмир-Усеин Куку является членом контактной группы по правам человека в Ялтинском регионе. В середине апреля этого года по дороге на работу его задержали сотрудники спецслужб России и доставили домой, где провели обыск. В доме правозащитника изъяли два ноутбука, мобильный телефон, несколько книг, не входящих в список запрещенной литературы. По словам Э.-У. Куку, когда его везли в ялтинское отделение ФСБ на допрос, всю дорогу его били. На его теле остались побои, которые он засвидетельствовал в медучреждении. Правоохранители этому делу хода не дали, а наоборот, попытались его самого обвинить в нападении на сотрудников ФСБ ***(В Крыму***

ФСБ «шьет» правозащитнику экстремизм за посты в соцсети // Главное ™ (http://glavnoe.ua/news/n251527). – 2015. – 2.12).

***

Российские власти готовят законопроект, который будет регулировать работу мессенджеров в России, сообщают «Ведомости».

Авторы предлагают внести в законы «Об информации...» и «О связи» понятие «информационно-коммуникационных сервисов». Под их деятельностью подразумевается передача «текстовых, голосовых и графических сообщений, технологически неразрывно связанных с услугами связи, оказываемыми третьими лицами на сетях передачи данных операторов связи».

Источники «Ведомостей», ознакомившись с документом, пришли к выводу, что речь прежде всего идет о мессенджерах, хотя теоретически под действие закона могут попасть и соцсети.

Авторы законопроекта предлагают сделать так, чтобы компании-разработчики таких сервисов могли работать в России только по договору с операторами связи. Также они хотят заставить их уведомлять о своей работе Роскомнадзор ***(Россиян могут ограничить в использовании месседжеров // Телекритика (http://www.telekritika.ua/internet-svit/2015-12-09/112751). – 2015. – 9.12).***

***

Британська спецслужба зізналася в хакерській діяльності

Центр урядового зв’язку (ЦУЗ) Великобританії вперше зізнався в суді, що займається комп’ютерним хакерством.

Кілька інтернет-компаній та активістів, які виступають за дотримання норм про конфіденційність інформації, подали скаргу до спеціального трибуналу, який розглядає справи про зловживання органів влади.

Поки справу не почали розглядати, ЦУЗ відмовлявся підтвердити або спростувати, чи допускав він у своїй роботі хакерські прийоми (клас операцій Computer Network Exploitation, CNE). Проте потім відомство зробило кілька офіційних зізнань, уточнивши, що таку діяльність вело не тільки стосовно об’єктів у своїй країні, а й за кордоном.

ЦУЗ заявив про використання «стійких» закладок CNE, які функціонують у зараженому пристрої і передають потрібну інформацію протягом тривалого періоду, і «непостійних» процесів, коли закладка припиняє існування наприкінці інтернет-сесії користувача.

Провайдери і організація Privacy International стверджують, що дії ЦУЗ є незаконними, і просять суд досліджувати питання про те, чи дотримувалися норми внутрішнього законодавства та акти про захист прав людини під час встановлення шкідливих програм.

Позивачі також висловили побоювання з приводу шпигунства через мобільні пристрої. У письмових доказах є посилання на свідчення колишнього

підрядника американських спецслужб Е. Сноудена. Він розповів, зокрема, про програму Nosey Smurf, що дозволяє за допомогою встановленого хакерського ПО активувати мікрофон на смартфонах.

У свою чергу ЦУЗ наполягає, що використання CNE є законним. Спецслужба стверджує, що не займалася невибірковим масовим стеженням. Як приклад свого успіху центр згадав, що до вересня 2015 р. завдяки цій діяльності було розкрито шість імовірних терористичних змов.

ЦУЗ зазначає, що в деяких випадках CNE може бути єдиним способом отримання розвідувальної інформації про терористичну діяльність підозрюваного або про серйозний злочин на території іншої країни.

Центр урядового зв'язку (Government Communications Headquarters, GCHQ) – британська спецслужба, відповідальна за ведення радіоелектронної розвідки і забезпечення захисту інформації урядових органів і збройних сил ***(Британська спецслужба зізналася в хакерській діяльності // LB.ua (http://ukr.lb.ua/news/2015/12/02/322418_britanska_spetssluzhba_ziznalasya.html). – 2015. – 2.12).***

***

Турция оштрафовала Twitter из-за экстремистских записей

Управление информационных и коммуникационных технологий Турции обязало сервис микроблогов Twitter выплатить штраф в размере 150 тыс. лир (около 3,6 млн р.) в связи с бездеятельностью в отношении экстремистских записей, передает lenta.ru Согласно ведомству, администраторы Twitter не удаляют записи, в которых содержится террористическая пропаганда. Примеры подобных экстремистских твитов чиновники приводить не стали. Правительство Турции впервые штрафует Twitter. Ранее деятельность сервиса на территории страны несколько раз временно запрещали, называя в качестве причины неспособность адекватно реагировать на запросы об удалении контента ***(Турция оштрафовала Twitter из-за экстремистских записей // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45597/118/lang,ru/). – 2015. – 11.12).***

Проблема захисту даних. DDOS та вірусні атаки

Исследователь безопасности О. Флисбек обнаружил, что сервис для обмена сообщениями Telegram раскрывает третьим лицам метаданные пользователей. Используя командную строку клиента мессенджера для настольных платформ, злоумышленник может получить доступ к определенной информации, которая может быть использована для слежения за жертвой.

Проблема заключается в том, что приложение Telegram для Android отправляет всем контактам пользователя специальное уведомление при

переходе в фоновый режим и повторной активации. Используя эти данные, злоумышленник, у которого есть несколько общих контактов с жертвой, может узнать, с кем она общается и в какое время.

Поскольку осуществление такого типа атаки само по себе требует, чтобы пользователь знал номер телефона жертвы, злоумышленник может добавить ее в список контактов. Каждый раз, когда жертва будет сворачивать приложение Telegram или возвращаться к нему, клиент будет втайне уведомлять всех пользователей в списке контактов, включая и злоумышленника.

Это не единственная проблема безопасности, затрагивающая Telegram. В четверг, 19 ноября, ИБ-исследователь под псевдонимом Grugq заявил, что сервис по обмену зашифрованными сообщениями далеко не настолько безопасен, как кажется на первый взгляд ***(Telegram раскрывает метаданные третьим лицам // InternetUA (http://internetua.com/Telegram-raskrivaet-metadannie-tretim-licam). – 2015. – 1.12).***

***

Хакеры публикуют скомпрометированные платежные данные в Twitter

Киберпреступники взломали систему безопасности банка Sharjah Islamic Bank (ОАЭ) и публикуют скомпрометированные платежные данные клиентов финучреждения в социальных сетях.

Мошенники утверждают, что не остановятся до тех пор, пока руководство банка не заплатит им выкуп в криптовалюте. Сумма, которую требуют хакеры, не разглашается.

Сотрудникам банка удалось договориться о временном блокировании Twitter-аккаунтов преступника. Однако отсрочить публикацию платежных реквизитов клиентов надолго не удалось. Хакеры создали новый аккаунт и продолжили распространять конфиденциальную информацию.

Только в одном приложении к твиту были опубликованы данные 500 вкладчиков исламского банка.

Тем временем недовольство среди клиентов продолжает нарастать. Пользователи и бизнес обвиняют банк в ненадежной системе защиты информации ***(Хакеры публикуют скомпрометированные платежные данные в Twitter // InternetUA (http://internetua.com/hakeri-publikuuat-skomprometirovannie-platejnie-dannie-v-Twitter). – 2015. – 1.12).***

***

Популярный китайский производитель электронных игрушек для детей VTech объявил о хакерском взломе магазина приложений. В опубликованном заявлении VTech сообщается, что в результате несанкционированного доступа 14 ноября к хакерам попала информация о клиентах магазина приложений Learning Lodge. Этот магазин предоставлял возможность родителям скачать приложения, игры, электронные книги и обучающий контент к игрушкам VTech.

База данных содержит сведения о клиентах VTech, включая имя, адрес электронной почты, пароль, IP-адрес, почтовый адрес и историю загрузок. Компания сообщила, что в базе данных нет информации о кредитных картах клиентов и банковских счетах, а также социальных номерах.

Вместе с тем VTech не раскрыла, как много пользователей пострадало в результате хакерского взлома. По данным ресурса Motherboard, первым сообщившего об инциденте, был получен доступ к данным о 200 тыс. детей и 4,8 млн родителей.

Motherboard был оповещён о взломе неизвестным хакером, который взял на себя ответственность за проникновение в систему. Он сообщил, что не собирается предпринимать никаких действий с полученной информацией. Как утверждает Motherboard, иногда хакеры взламывают систему для того, чтобы продемонстрировать её уязвимость, а также указать на то, что она нуждается в более надёжной защите.

Сведения о VTech были добавлены в базу данных сервиса Have I Been Pwned?, где взлом компьютерной системы производителя игрушек стал четвёртым в истории самых крупных взломов сайтов, уступив лишь взлому Adobe (152 млн аккаунтов), Ashley Madison (30 млн аккаунтов) и 000webhost.com (13,5 млн аккаунтов) ***(Из-за взлома VTech к хакеру попали данные о 200 тыс. детей и 4,8 млн родителей // InternetUA (http://internetua.com/iz-za-vzloma-VTech-k-hakeru-popali-dannie-o-200-tis--detei-i-4-8-mln-roditelei). – 2015. – 30.11).***

***

Хакери Anonymous заявляють, що одна з компаній Силіконової долини – CloudFlare – допомагає поліпшувати та зміцнювати онлайн-безпеку ресурсів терористів ISIS.

Про це повідомляє Daily Mail.

Хакери, які націлилися на інтернет-діяльність бойовиків після терактів у Парижі, звинуватили CloudFlare у захисті веб-сайтів ISIS. Компанія надає послуги близько 4 млн клієнтів, прискорюючи час завантаження веб-сайтів і допомагаючи захиститися від кібер-атак. Вона зупиняє DDoS-атаки. Це означає, коли хакери Anonymous намагаються «покласти» сайт, технологія від CloudFlare зупиняє їх.

У нещодавній доповіді організація звинуватила CloudFare у захисті 40 сайтів, пов'язаних з тероризмом, 37 з яких є відверто пропагандистськими. «Знову CloudFlare були викриті у наданні послуг проісламістським сайтам», – заявили хакери.

У свою чергу співзасновник і генеральний директор CloudFlare М. Принс заявляє, що претензії Anonymous є просто «диванним аналізом від дітей», який важко сприймати серйозно і наполягає на тому, що компанія не матиме жодної користі від підтримки терористичної групи. Він додав, що якщо поліція або представники федеральної влади прийдуть в їхній офіс у Сан-Франциско, то вони будуть співпрацювати.

У 2013 р. компанія CloudFlare вже стикалася з подібними звинуваченнями щодо сайту, пов'язаного з Аль-Каїдою. М. Принс тоді написав у блозі, що вони захищали свободу слова: «Сайт – це мовлення. Це не бомба. Там немає безпосередньої небезпеки». Нагадаємо, раніше хакери Anonymous опублікували плани терористів «Ісламської держави» щодо можливих майбутніх терактів. У ФБР не мали даних про підготовку терактів, але серйозно поставилися до попередження ***(Хакери Anonymous звинуватили компанію CloudFare у захисті сайтів ISIS // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/khakeri_anonymous_zvinuvatili_kompaniyu_cloudfare_u_zakhisti_saytiv_isis/). – 2015. – 30.11).***

***

Согласно прогнозу ИБ-компании Lookout Security, в следующем году коммерческие предприятия столкнутся с ростом кибератак с эксплуатацией уязвимостей в iOS-устройствах. Мобильные гаджеты постепенно приобретают функционал, присущий персональным компьютерам, к примеру, у планшета Apple iPad Pro появилась клавиатура, поясняют в компании.

«Мы не считаем, что атаки из App Store станут нормой. Тем не менее, мы ожидаем рост числа атак на корпоративные iOS-устройства, учитывая хранимые на них большие объемы данных и тот факт, что посредством мобильных гаджетов можно получить доступ к другой важной информации», – отмечают эксперты Lookout.

Вероятнее всего, кибератаки будут комбинированными и включать использование вредоносных приложений, эксплуатацию уязвимостей в легитимных программах и операционных системах, а также социальную инженерию. Также специалисты считают, что пользователи по-прежнему будут создавать себе неприятности, устанавливая слабые пароли на сайтах и в учетных записях. Одним из способов решения этой проблемы является повсеместная реализация двухфакторной аутентификации, и в будущем году использование и доступность этой функции будет расти.

«В настоящее время пароли являются, пожалуй, самой основной проблемой в интернете. Слабые пароли, использование одних и тех же паролей на различных сайтах и восстановленные пароли, которые могут получить лица с доступом к электронной почте пользователя, делают их своеобразной ахиллесовой пятой даже для тех, кто серьезно относится к собственной безопасности», – добавляют в Lookout ***(Эксперты прогнозируют рост атак на iOS-устройства в 2016 году // InternetUA (http://internetua.com/eksperti-prognoziruuat-rost-atak-na-iOS-ustroistva-v-2016-godu). – 2015. – 1.12).***

***

Рекомендуем пользователям PayPal срочно поменять пароли: неизвестные хакеры заявили о краже 23 млрд учетных записей пользователей сервиса. Подлинность аккаунтов пока не доказана, а в сети злоумышленники опубликовали только 1300 аккаунтов PayPal. В компании сообщили, что

опубликованные данные «неточны», проверка продолжается, пишет AIN.UA (http://ain.ua/2015/12/02/619161).

Логины и пароли были опубликованы на Pastebin и обнаружены сканером чешской компании Cybersecurity Help s.r.o., которая специализируется на корпоративной киберзащите, во вторник 1 декабря. Хакеры заявили, что получили доступ к 23,873,667,087 аккаунтам, впрочем, указанная в посте ссылка на полный список не существует. Эксперты попытались проверить подлинность опубликованных учетных записей, но после неудачной попытки входа столкнулись с блокировкой по IP-адресу со стороны PayPal. «Если опубликованные данные подлинны, хакеры могли получить к ним доступ, только взломав сервера PayPal», – сообщают в Cybersecurity Help s.r.o.

Мы также проверили несколько учетных записей и не смогли получить к ним доступ, однако на все 1300 понадобится больше времени. А пока достоверность данных не доказана.

Утечка в целом вызывает множество вопросов не только потому, что ссылка на полный список учеток «убита». В PayPal всего 173 млн активных аккаунтов, а на Земле проживает 7 млрд человек, поэтому цифра 23 млрд аккаунтов звучит неправдоподобно, сообщает издание csoonline.com. Кроме того, журналистам издания удалось отыскать в Интернете аналогичный слив от другого хакера – те же 1300 аккаунтов были опубликованы 28 ноября и тоже на Pastebin.

В PayPal прокомментировали ситуацию так: «Профессионалы по безопасности проверили сведения о том, что данные наших пользователей могли быть скомпрометированы, и мы можем подтвердить, что эти сведения неточны». Однако до сих пор наверняка неизвестно, есть ли среди опубликованных аккаунтов реально скомпрометированные. Логины и пароли могут не быть учетными записями PayPal, однако косвенно могут быть связаны с пользователями сервиса.

К слову, в течение последних нескольких дней некоторые пользователи PayPal столкнулись с некорректной работой сервиса: сайт попросту не открывается ***(Хакеры заявили о краже 23 млрд аккаунтов пользователей PayPal // AIN.UA (http://ain.ua/2015/12/02/619161). – 2015. – 2.12).***

***

В начале октября нынешнего года SecurityLab.ru сообщал об уязвимостях в ряде популярных 3G-маршрутизаторов производства Huawei. Независимый исследователь безопасности П. Ким обнаружил множественные бреши в сетевых устройствах еще в 2014 г., но ответ от производителя получил лишь спустя год. Несмотря на популярность маршрутизаторов, Huawei не собиралась исправлять найденные уязвимости в связи с истечением срока официальной поддержки устройств.

Как оказалось, уязвимостям подвержены не только 3G-маршрутизаторы, но и роутеры серии WiMax. По словам П. Кима, сетевые устройства до сих пор

широко используются во многих странах мира, включая Украину, Бахрейн, Иран, Ирак, Ливию, Филиппины и Кот д'Ивуар.

Уязвимостям подвержены следующие модели маршрутизаторов:

– Huawei EchoLife BM626 WiMax CPE;
– Huawei EchoLife BM626e WiMax CPE;
– Huawei EchoLife BM635 WiMax CPE;
– Huawei EchoLife BM632 WiMax CPE;
– Huawei EchoLife BM631a WiMax CPE;
– Huawei EchoLife BM632w WiMax CPE;
– Huawei EchoLife BM652 WiMax CPE.

Защита доступа к интерфейсу управления устройствами основана на JavaScript-перенаправлении. Злоумышленник может отключить JavaScript в браузере и получить полный контроль над устройством. Кроме фактического отсутствия проверки авторизации, ПО содержит бреши, позволяющие удаленному пользователю раскрыть важные данные, похитить данные сессии и осуществить CSRF-атаку.

Сотрудники Huawei отказались выпустить исправленные версии прошивок, ссылаясь на завершение срока поддержки маршрутизаторов. Компания рекомендует пользователям приобрести новые модели сетевых устройств ***(В WiMAX-маршрутизаторах Huawei обнаружены множественные уязвимости // InternetUA (http://internetua.com/v-WiMAX-marshrutizatorah-Huawei-obnarujeni-mnojestvennie-uyazvimosti). – 2015. – 2.12).***

***

Среди всех аспектов кибербезопасности человеческому фактору уделяется минимум внимания, хотя он уязвим больше всего. Как заявил в ходе выступления на конференции IRISSCON менеджер команды по информационной безопасности компании Trend Micro Б. МакЭрдл, методы социальной инженерии являются более эффективными, нежели инфицирование компьютеров вредоносным ПО.

По словам директора по вопросам учебной подготовки консалтинговой компании SANS Securing the Human Л. Спитцнера, многие предприятия проводят тренинги для своих сотрудников, направленные на обучение мерам предосторожности при работе с корпоративными данными, однако повышают осведомленность пользователей не совсем верным способом. Он отметил, что многие эксперты по кибербезопасности при общении с рядовыми пользователями пытаются донести информацию, используя профессиональную терминологию, которую не владеющие техническими навыками коллеги зачастую просто не понимают. «Большинство программ, направленных на повышение осведомленности пользователей, являются неэффективными не из-за информации, а из-за способа, которым она доносится», – подчеркнул Л. Спитцнер.

Как рассказал вице-президент департамента по исследованию информационной безопасности Trend Micro Р. Фергюсон, повсеместное

использование в компаниях мобильных устройств предоставляет злоумышленникам больше возможностей для доступа к корпоративным системам. Тем не менее, именно мобильные гаджеты чаще всего являются наиболее уязвимыми. С развитием виртуальной и дополненной реальности Р. Фергюсон прогнозирует рост атак, направленных на хищение личности. Также эксперты ожидают увеличение количества кибератак на сферу «Интернета вещей», пишет издание Help Net Security. Проблема заключается в том, что при разработке этих технологий вопрос безопасности стоит не на первом месте, отметил Р. Фергюсон.

По данным добровольческой команды реагирования на компьютерные угрозы Irisscert, в 2015 г. был зафиксирован значительный всплеск DDoS-атак (26 137 против 6 534 в 2014 г.). При этом в более трети из них использовались принадлежащие ирландским компаниям серверы для атак на серверы в других странах. На втором месте оказались атаки с применением вредоносного ПО ***(Человеческий фактор – самый уязвимый аспект кибербезопасности // InternetUA (http://internetua.com/celovecseskii-faktor---samii-uyazvimii-aspekt-kiberbezopasnosti). – 2015. – 3.12).***

***

Facebook планирует обязать пользователей в Бельгии, которые не имеют аккаунта в соцсети, регистрироваться и входить под своей учетной записью для просмотра публичных страниц сайта. Об этом сообщает ComputerWorld.

Данный шаг компания пояснила выполнением требования суда по запрету слежки за теми пользователями, которые не зарегистрированы в соцсети.

Обычно просматривать страницы, доступ к которым не закрыт владельцем, могут все интернет-пользователи, без необходимости регистрации на сайте. В основном, публичные профили заводят малые предприятия, спортивные команды и знаменитости.

Соцсеть также приостановит действие cookie-файлов под названием datr, с помощью которых и осуществлялась слежка, для незарегистрированных пользователей в Бельгии. Facebook заявила, что удалит информацию, относящуюся к таким файлам, с компьютеров жителей. «В связи с этим мы сможем предоставить в Бельгии доступ к контенту только пользователям с аккаунтом на Facebook», – пояснили в компании.

В ноябре суд в Бельгии выпустил временное распоряжение, согласно которому Facebook обязана прекратить слежку за пользователями, которые не зарегистрированы в соцсети. В противном случае компании грозят штрафы. Как выяснилось в ходе разбирательств, отслеживание активности пользователя осуществлялось при помощи datr, которые определяют, залогинился на сайт настоящий владелец аккаунта или нет, а также с какого браузера он зашел.

Бельгийская комиссия по защите неприкосновенности частной жизни подала иск против Facebook в июне. Власти обвинили соцсеть в том, что она нарушает бельгийские и европейские законы, когда отслеживает и

обрабатывает данные как зарегистрированных, так и незарегистрированных пользователей без их согласия.

В апреле 25 тыс. австрийских граждан подали аналогичный иск в суд на Facebook ***(Facebook заблокирует доступ незарегистрированным в соцсети бельгийцам // InternetUA (http://internetua.com/Facebook-zablokiruet-dostup-nezaregistrirovannim-v-socseti-belqiicam). – 2015. – 3.12).***

***

Компания Cisco выпустила несколько бюллетеней безопасности с описанием ряда уязвимостей в некоторых продуктах. Неисправленные бреши затрагивают продукты Cisco Unified Computing System, Cisco Unity Connection и Cisco Unified SIP Phone 3905.

Бюллетень Cisco-SA-20151201-UCS1 описывает уязвимость в платформе для дата-центров Cisco Unified Computing System (UCS), позволяющую удаленному пользователю осуществить CSRF-атаку. Бреши подвержена версии UCS 1.3 и 1.3.0.1. Уязвимость существует из-за недостаточной проверки подлинности HTTP-запросов. Злоумышленник может с помощью специально сформированной страницы выполнить некоторые действия от имени пользователя.

Бюллетень Cisco-SA-20151202-PCA описывает брешь в программе по обмену сообщениями и голосовой почтой Cisco Unity Connection версии 9.1. Уязвимость существует из-за некорректной проверки пользовательских данных. Удаленный пользователь может с помощью специально сформированной ссылки выполнить произвольный код сценария в браузере жертвы в контексте безопасности уязвимого сайта.

В бюллетене Cisco-SA-20151202-SIP описывается уязвимость в SIP-телефоне Cisco SIP Phone 3905. Брешь существует из-за ресурсных ограничений устройства и позволяет удаленному пользователю осуществить DoS-атаку путем отправки большого объема трафика на целевой аппарат.

Вместе с тем компания исправила уязвимость повышения привилегий в Cisco WebEx Meetings for Android. Брешь позволяет злоумышленнику повысить привилегии на системе с помощью предустановленного вредоносного приложения. Уязвимость затрагивает Cisco WebEx Meetings for Android 8.5.1 и более ранние версии приложения ***(Cisco предупреждает о множественных уязвимостях в ряде продуктов // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/12/05/Cisco-warns-of-flaws.html). – 2015. – 5.12).***

***

Производитель сетевого оборудования компания Cisco сообщила об уязвимости (CVE -2015-6394) в USB-драйвере коммутаторов серии Nexus 5000. Брешь позволяет неавторизованному локальному пользователю вызвать отказ в обслуживании. Проблема затрагивает продукты Cisco Nexus 5000 на базе ПО Cisco NX-OS версии 5.2(9)N1(1).

Согласно бюллетеню безопасности производителя, уязвимость существует из-за некорректной обработки вводных параметров USB. Атакующий может проэксплуатировать брешь путем отправки специально сформированного пакета с параметрами USB для обработки ядром устройства и тем самым вызвать отказ в работе целевого устройства.

В настоящее время специалисты Cisco работают над устранением проблемы. Подробности об уязвимости пока неизвестны.

Коммутаторы Cisco Nexus 5000 – оборудование уровня Enterprise, предназначенное для оптимизации сетевой архитектуры центров обработки данных с высокой нагрузкой ***(В Cisco Nexus 5000 обнаружена опасная брешь // InternetUA (http://internetua.com/v-Cisco-Nexus-5000-obnarujena-opasnaya-bresh). – 2015. – 8.12).***

***

Независимый исследователь обнаружил, что роутеры N150 компании Belkin, это крайне опасные девайсы. Предназначенные для домашнего использования маршрутизаторы содержат Telnet-бэкдор, CSRF (cross-site request forgery) уязвимость и ряд других, более мелких, багов. Хуже того, все уязвимости актуальны, так как компания работает над патчем крайне неторопливо.

Р. Сингх – известный исследователь, чью работу не раз отмечали компании Microsoft, Adobe, eBay, ESET и Google. На этот раз Сингх изучил роутеры компании Belkin и в октябре 2015 г. обнаружил, что модель N150, это настоящее решето.

В своем блоге Р. Сингх опубликовал подробную информацию обо всех найденных уязвимостях, а также сообщил, что пытался связаться с компанией Belkin, но не получил ответа.

В частности, исследователь обнаружил, что можно осуществить HTML/Script инъекцию, которая затрагивает параметр language. Р. Сингх опубликовал proof-of-concept видео, которое демонстрирует, что после инъекции пэйлоуда веб-интерфейс устройства становится непригодным к использованию.

Еще один баг: ID сессий представляют собой шестнадцатеричную последовательность, чья длина ограничена восемью символами. Атакующий может воспользоваться обычным брутфорсом, чтобы добраться до информации.

Одна из наиболее серьезных проблем, найденных Р. Сингхом, это поддержка протокола Telnet, который на N150 включен по умолчанию. Сервер запущен на 23 порту и использует стандартную комбинацию логина и пароля: root/root. Если хозяин устройства поленился сменить настройки, хакер с легкостью может получить удаленный доступ к маршрутизатору, с root-привилегиями, просто использовав дефолтные логин и пароль. Также удаленно можно эксплуатировать и CSRF уязвимость.

«Комбинируя эти уязвимости между собой, атакующий может скомпрометировать устройство полностью, – поясняет Р. Сингх. – Атакующий может быть подключен к локальной сети жертвы, что возможно как физически, так и удаленно, к примеру, взломав локальную сеть посредством вредоносного ПО. Затем хакер может использовать Telnet или CSRF уязвимость, чтобы закончить начатое».

По данным исследователя, прошивка 1.00.09 (F9K1009) является наиболее свежей, и она была выпущена в мае 2015 г. Хотя тогда выход новой версии был объяснен исправлением NAT-PMP уязвимости, то есть компания работает над проблемами безопасности, новейшая прошивка всё равно содержит все перечисленные Р. Сингхом баги.

Р. Сингх пытался связаться с компанией Belkin еще в октябре текущего года, но не получил ответа. Выждав некоторое время, исследователь решил обнародовать информацию, надеясь, что это заставит компанию отреагировать. Судя по всему, так и получилось. Журналисты SecurityWeek сумели получить комментарий от представителей Belkin, которые сообщили, что в компании знают обо всех перечисленных проблемах и работают над их исправлением. Точные сроки выхода патча в компании называть не стали ***(Обнаружен ряд активных уязвимостей в роутерах Belkin N150 // InternetUA (http://internetua.com/obnarujen-ryad-aktivnih-uyazvimostei-v-routerah-Belkin-N150). – 2015. – 6.12).***

***

Как показало новое исследование, опубликованное специалистами Veracode, код в скриптовых языках является источником значительного количества уязвимостей в веб-приложениях. Отчет основан на результатах анализа более 200 тыс. приложений на распространенных языках программирования – PHP, Java, Microsoft Classic ASP, .NET, iOS, Android, C и C++, JavaScript, ColdFusion, Ruby и COBOL. Самыми уязвимыми оказались приложения на языках PHP, Classic ASP и ColdFusion, а самыми безопасными – на Java и .NET.

В ходе анализа специалисты использовали метрическую систему, измеряющую количество брешей на 1 МБ кода. По итогам исследования был составлен следующий рейтинг:

– Classic ASP – 1 686,6 брешей/МБ (1 112 критических)
– ColdFusion – 262,8 брешей/МБ (227 критических)
– PHP – 184 брешей/МБ (47 критических)
– Java – 51,8 брешей/МБ (5,2 критических)
– .NET – 32,5 брешей/МБ (9,7 критических)
– C++ – 26,7 брешей/МБ (8,8 критических)
– iOS – 23,4 брешей/МБ (0,9 критических)
– Android – 11,3 брешей/МБ (0,4 критических)
– JavaScript – 8,1 брешей/МБ (0,09 критических)

Согласно отчету, 83 % приложений на ColdFusion, 81 % приложений на PHP и 79 % на Classic ASP не прошли проверку OWASP Top 10.

По данным Veracode, 86 % приложений на PHP содержали по меньшей мере одну XSS-брешь. 56 % программ оказались уязвимы к внедрению SQL-кода. Также приложения позволяли осуществить атаку типа обратный путь в директориях (67 %) и внедрение кода (61 %). В числе других проблем: некорректный процесс обработки учетных данных (58 %), уязвимости в криптографическом протоколе (73 %) и бреши, позволяющие утечку данных (50 %).

Такое положение вещей значительно влияет на общую ситуацию в интернете, поскольку порядка 70 % систем по управлению контентом работают на базе WordPress, Drupal и Joomla, подчеркивают эксперты.

Open Web Application Security Project (OWASP) – открытый проект обеспечения безопасности веб-приложений. Сообщество OWASP включает в себя корпорации, образовательные организации и частных лиц со всего мира. Участники проекта уже 10 лет составляют список Топ-10 самых опасных уязвимостей в веб-приложениях, стараясь привлечь внимание всех веб-разработчиков ***(Названы самые уязвимые языки программирования // InternetUA (http://internetua.com/nazvani-samie-uyazvimie-yaziki-programmirovaniya). – 2015. – 6.12).***

***

«Доктор Веб» изучил новую вредоносную программу, нацеленную на компьютеры под управлением операционных систем Linux: зловред носит имя Linux.Rekoobe.1.

Сообщается, что названный троян способен инфицировать устройства с архитектурой SPARC, x86 и x86-64. Для своей работы программа использует зашифрованный конфигурационный файл, прочитав содержимое которого с определённой периодичностью обращается к управляющему серверу для получения команд.

При определённых условиях связь с командным центром осуществляется через прокси-сервер, данные для авторизации на котором троян извлекает из собственного конфигурационного файла. При этом вся отправляемая и принимаемая информация разбивается на отдельные блоки, каждый из которых шифруется и снабжается собственной подписью. Зловред также обладает весьма хитроумной системой проверки подлинности получаемых от управляющего сервера пакетов с закодированными данными.

Однако, несмотря на столь сложный механизм работы, вредоносная программа способна выполнять только три команды злоумышленников: скачивать с управляющего сервера или загружать на него файлы, передавать принимаемые директивы командному интерпретатору Linux и транслировать полученный вывод на сервер, благодаря чему киберпреступники получают возможность удалённо взаимодействовать с инфицированным устройством

(Троян Rekoobe атакует Linux-системы // InternetUA (http://internetua.com/troyan-Rekoobe-atakuet-Linux-sistemi). – 2015. – 5.12).

***

Компания Rayzone Group похвасталась разработкой устройства, которое способно похитить со смартфона электронные письма, пароли от учетных записей в соцсетях, содержимое Dropbox и т. д.

Тактическая разведывательная система разработана для спецслужб. Она имеет название InterApp. Инструмент позволяет скрытно собирать практически всю важную информацию со смартфонов, эксплуатируя существующие уязвимости в мобильных приложениях.

Разработчики обещают полный доступ к электронной переписке жертвы, паролям от учетных записей в соцсетях, списку контактов, истории браузинга, содержимому в Dropbox, фотографиям, истории местоположений, кодам MSISDN и IMEI и пр. Для успешной работы InterApp требуется наличие поблизости смартфона с активным Wi-Fi-передатчиком. Устройство можно прикрепить к стене в аэропорту, торговом центре или любом общественном месте.

Данная система способна одновременно собирать информацию с сотен смартфонов. Устройство обладает возможностью похищать информацию даже в случаях, когда смартфон не подключен к точке доступа Wi-Fi, достаточно просто активированного Wi-Fi-передатчика. Как указывается в рекламной брошюре устройства, InterApp не оставляет следов проникновения на телефоне жертвы и не требует какого-либо взаимодействия от пользователя.

InterApp работает с различными мобильными платформами, в том числе iOS и Android. Данное решение предназначено для разведслужб и правоохранительных органов, поэтому разработчики не раскрывают технические подробности работы системы ***(Создано устройство, способное похитить данные с любого смартфона // InternetUA (http://internetua.com/sozdano-ustroistvo--sposobnoe-pohitit-dannie-s-luabogo-smartfona). – 2015. – 7.12).***

***

Исследователь в области информационной безопасности, известный под псевдонимом slipstream/RoL, обнаружил, что компьютеры и планшеты компаний Dell, Toshiba и Lenovo небезопасны. Отыскав уязвимости в ПО всех трех производителей, хакер обнародовал в отрытом доступе экслплоиты. Так как slipstream/RoL не потрудился поставить компании в известность о своих находках, под угрозой оказались миллионы пользователей.

На своем сайте slipstream/RoL опубликовал все необходимые исходные коды и proof-of-concept эксплоиты. Автор не забыл даже прикрутить к веб-странице бодрый чиптюн, так что осторожнее со звуком.

Интересно, что все три вендора пострадали из-за уязвимостей в собственном предустановленном ПО, иначе говоря – bloatware.

Все три уязвимости позволяют атакующему запустить малварь на системном уровне, вне зависимости от того, какой пользователь был залогинен во время атаки. Для доставки вредоноса в систему хакер предлагает воспользоваться «традиционными методами»: это можно осуществить, заманив жертву на скомпрометированный сайт, или прислав ей эксплоит в почтовом вложении.

Согласно данным CERT, опубликованным 3 декабря, предустановленное ПО Lenovo содержит сразу три уязвимости. Так называемый Lenovo Solution Center предустанавливается на устройства линейки Think: планшеты ThinkPad, ThinkCenter и ThinkStation, IdeaCenter и некоторые IdeaPad, под управлением Windows 7 и более новых версий ОС.

Представители Lenovo уже подтвердили наличие брешей и сообщили, что работают над созданием патча. Компания также признала, что если удалить приложение Lenovo Solution Center, это поможет избавиться от проблемы.

За уязвимость в устройствах Toshiba отвечает предустановленная программа Toshiba Service Station, которая, в частности, ответственна за поиск обновлений для софта. slipstream/RoL рассказал журналистам ZDNet, что приложение позволяет пользователю со стандартным аккаунтом читать некоторые части реестра с более высокими правами. Атакующий не сумеет прочесть данные security account manager или bootkey, но все же сможет получить несанкционированный доступ к некоторым областям реестра.

Уязвимость в устройствах Dell, это уже второй баг, который slipstream/RoL нашел в девайсах компании. В конце ноября 2015 г. исследователь обнаружил, что сконфигурированный определенным образом веб-сайт способен извлечь сервисный код с лэптопа Dell.

На этот раз уязвимость была найдена в предустановленной программе Dell System Detect. Это диагностическое приложение, которое проверяет девайс перед звонком в техническую поддержку. Оказалось, что с его помощью можно обойти защитные механизмы Windows и повысить права в системе.

Пока неясно, сколько устройств подвержено найденным slipstream/RoL уязвимостям. Компании Dell и Toshiba хранят молчание и не дают комментариев. Сам slipstream/RoL подтвердил журналистам, что он не предупреждал никого о найденных багах, так что для производителей эксплоиты стали сюрпризом. В заключение ZDNet цитирует слова исследоватаеля, которые хорошо объясняют его поступок: «Предустановленный фуфлософт, это плохо, ага?» (Preinstalled crapware is bad, m'kay?) ***(Хакер без предупреждения опубликовал эксплоиты для устройств Dell, Toshiba и Lenovo // InternetUA (http://internetua.com/haker-bez-preduprejdeniya-opublikoval-eksploiti-dlya-ustroistv-Dell--Toshiba-i-Lenovo). – 2015. – 7.12).***

***

На прошлой неделе фирма по безопасности Duo Security нашла на компьютерах производства Dell уязвимость, позволяющую злоумышленникам

удаленно просматривать веб-трафик и даже перехватывать пароли. Эта проблема обнаружилась даже в американском Министерстве национальной безопасности. В результате Dell пришлось извиняться и экстренно выпускать заплатки.

Это серьезное открытие было сделано с помощью censys.io – поискового сайта, созданного специально для специалистов по безопасности. Это полностью бесплатный ресурс, позволяющий выявлять уязвимости и другие проблемы Интернета. Он в ежедневном режиме сканирует абсолютно все устройства, подключенные к Всемирной сети. Проект запустила в октябре группа специалистов Мичиганского университета, его программная часть открыта, а аппаратная предоставляется компанией Google.

«Мы хотим создать полную базу данных всего и вся в Интернете», – говорит руководитель проекта З. Дурумерик.

В основу работы Censys положена программа под названием ZMap, собирающая данные – своего рода поисковый робот. Ее разработал З. Дурумерик совместно с коллегами по университету. Каждый день ZMap «пингует» более 4 млрд отдельных IP-адресов, принадлежащих подключенным к Интернету устройствам, и затем обновляет ими базу данных с функцией поиска. Так формируется Censys. Каждый пинг занимает всего несколько часов.

Полученные данные дают большой объем информации об устройствах: тип, используемое ПО, наличие шифрования, настройки и т. д. Это позволяет определить, насколько распространена та или иная уязвимость, какие устройства от нее страдают, как и кем они используются и даже приблизительное местоположение этих устройств.

Идея Censys пришла к З. Дурумерику и его коллегам после того, как их буквально завалили запросами на сканирование устройств с целью выявления потенциальных проблем. В марте этого года они помогли выявить уязвимость в системе шифрования примерно пяти миллионов сайтов, включая сайты Apple, Google и ФБР США. После этого специалисты решили, что пора заняться автоматизацией этого процесса.

У Censys есть конкурент – поисковая система Shodan, которая тоже сканирует подключенные устройства, но делает это несколько иначе и на другом ПО. По словам З. Дурумерика, тесты показали, что у Censys гораздо больше охват Интернета и более актуальные данные, что лучше подходит для поиска проблем.

Впрочем, в Shodan с этим не согласны. Гендиректор Shodan Д. Мэзерли говорит, что покрытие у них не хуже, при этом используются более разнообразные методы сканирования IP-адресов.

Но и в Censys, и в Shodan едины в одном: чем проще специалистам находить уязвимости в оборудовании, тем безопаснее будет Интернет. По словам Д. Мэзерли, благодаря Shodan было настроено и защищено 100 тыс. управляющих промышленных систем, а также закрыто множество серверов, используемых киберпреступниками ***(Censys – поиск от Google, о котором вы***

никогда не слышали // InternetUA (http://internetua.com/Censys---poisk-ot-Google--o-kotorom-vi-nikogda-ne-slishali). – 2015. – 8.12).

***

Программа Enterprise Security Manager (ESM) ориентирована в основном на корпоративных пользователей. ESM, это инструмент для мониторинга и анализа всего происходящего в системах, сетях, базах данных и приложениях в режиме реального времени. Но порой решения, созданные для повышения безопасности, напротив, ее подрывают.

3 декабря 2015 г. компания McAfee, без лишнего шума, представила бюллетень безопасности SB10137. Документ рассказывает о серьезной проблеме в Enterprise Security Manager.

Сообщается, что с помощью «сконструированного определенным образом имени пользователя» можно миновать аутентификацию Security Information & Event Management, проникнув в систему без ввода пароля.

Данный баг срабатывает лишь в том случае, если ESM настроен на использование Active Directory или LDAP. Если настройки соответствуют, атакующий получает доступ к NGCP – дефолтному имени пользователя, которое создается при первой установке. Пароль у злоумышленника опять же никто не спрашивает.

Уязвимость получила идентификатор CVE-2015-8024. Проблема затрагивает McAfee Enterprise Security Manager (ESM), Enterprise Security Manager/Log Manager (ESMLM), Enterprise Security Manager/Receiver (ESMREC) 9.3.x до 9.3.2MR19, 9.4.x до 9.4.2MR9 и 9.5.x до 9.5.0MR8.

Если в конфигурации программ включено использование Active Directory или LDAP, удаленному атакующему достаточно ввести логин NGCP|NGCP|NGCP и любой пароль для проникновения в систему.

McAfee настоятельно рекомендует всем пользователям обновиться. Если такой возможности нет, стоит хотя бы отключить в Enterprise Security Manager аутентификацию через Active Directory и LDAP ***(McAfee security manager содержит опасный баг // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/12/08/esm-auth-bug.html). – 2015. – 8.12).***

***

Хранящаяся на iPhone и iPad персональная информация делает мобильные устройства привлекательной целью для хакеров. В случае, если не удается найти прямой доступ к гаджетам, злоумышленники выбирают обходной путь. Исследователи из Palo Alto Networks обнаружили технику похищения данных с iOS-устройств через резервные копии, хранящиеся на компьютерах.

В общей сложности эксперты идентифицировали 704 образца рекламного ПО и троянов шести семейств для Windows и OS X, использующих так называемую технику BackStab для похищения данных с iOS-устройств и смартфонов BlackBerry, сообщает Securitylab. По данным экспертов,

злоумышленники применяют данный метод уже более пяти лет на территории 30 стран.

Исследователи охарактеризовали BackStab как «атаку, используемую для захвата хранящихся на мобильных устройствах личных данных путем похищения локальных резервных копий с ПК и Mac». Из-за большого количества общедоступных статей и видеоинструкций, описывающих процесс осуществления подобной атаки, BackStab представляет серьезную угрозу конфиденциальности пользователей.

С помощью данного метода злоумышленники могут получить доступ абсолютно ко всем данным на смартфоне. Для успешного осуществления атаки на iPhone и iPad необязательно должен быть установлен джейлбрейк. Более того, вредоносному ПО не требуются привилегии суперпользователя или администратора.

Атака возможна, если на ПК или Mac хранится резервная копия хотя бы одного файла. В некоторых случаях официальное ПО, например, iTunes, автоматически без какого-либо участия пользователя создает незашифрованные резервные копии. Иногда резервные копии создаются вредоносными программами, когда мобильное устройство подключается к инфицированному компьютеру. По словам исследователей, BackStab – не просто теоретический метод, а реально используемый злоумышленниками для атак на iOS.

Эксперты из Palo Alto Networks предложили несколько шагов, позволяющих защитить iPhone и iPAd от такого рода атак. Прежде всего необходимо проверить наличие и удалить незашифрованные и ненужные резервные копий iTunes. При работе с бэкапами нужно активировать функцию шифрования и использовать надежный пароль. То же самое касается iCloud, где, помимо прочего, необходимо активировать двухфакторную аутентификацию. Исследователи также советуют обновить iOS до версии 9.1, использовать антивирусные решения и не делать джейлбрейк ***(Хакеры похищают данные с iPhone и iPad через резервные копии на Windows и Mac // InternetUA (http://internetua.com/hakeri-pohisxauat-dannie-s-iPhone-i-iPad-cserez-rezervnie-kopii-na-Windows-i-Mac). – 2015. – 9.12).***

***

С каждым годом создатели и распространители вредоносного ПО проявляют все больший интерес к пользователям компьютеров Apple – об этом свидетельствует частота появления новых программ, представляющих опасность для операционной системы OS X. Подавляющее большинство таких приложений предназначено для демонстрации нежелательной рекламы или скрытой установки различных программ и утилит. Очередное подобное детище злоумышленников, обнаруженное вирусными аналитиками компании «Доктор Веб», получило имя Adware.Mac.Tuguu.1.

Как и другие представители данного типа программ, Adware.Mac.Tuguu.1 позволяет скрытно устанавливать на «мак» потенциальной жертвы различные дополнительные приложения, обычно – бесполезные, а иногда и вредоносные.

За каждую успешную инсталляцию таких «дополнений» распространители Adware.Mac.Tuguu.1 получают определенное вознаграждение – в этом и заключается их коммерческий интерес.

Adware.Mac.Tuguu.1 распространяется под видом различных бесплатных программ для OS X. При запуске данное опасное приложение считывает содержимое конфигурационного файла «.payload», расположенного в той же папке, откуда была запущена программа, определяет адрес управляющего сервера и определенным образом модифицирует его. Затем с помощью зашифрованного запроса Adware.Mac.Tuguu.1 обращается к командному центру за списком дополнительного ПО, установка которого будет предложена пользователю. Ответ сервера также приходит в зашифрованном виде и содержит несколько полей, определяющих, какие именно дополнительные программы могут быть инсталлированы на пользовательский «мак». Судя по используемой установщиком внутренней нумерации, всего существует 736 различных вариантов. Каждая из предлагаемых к установке программ имеет для Adware.Mac.Tuguu.1 определенный условный «вес»: поскольку максимальное число одновременно инсталлируемых приложений ограничено, установщик по определенному алгоритму пытается создать оптимальный список из неконфликтующего ПО с максимально допустимым «весом».

Перед началом установки Adware.Mac.Tuguu.1 проверяет, совместимы ли предлагаемые им программы друг с другом – так, например, он не станет инсталлировать вместе приложения MacKeeper и MacKeeper Grouped. Также Adware.Mac.Tuguu.1 пытается удостовериться, что такое ПО не было ранее установлено в системе, а перед завершением своей работы проверяет успешность установки.

Поскольку в диалоговом окне Adware.Mac.Tuguu.1 предусмотрен режим Custom Installation, в случае выбора которого на экране будут продемонстрированы флажки, позволяющие полностью отказаться от всех дополнительных приложений, эту программу формально нельзя отнести к категории троянцев. Однако Adware.Mac.Tuguu.1 является типичным рекламным установщиком, который вполне способен «засорить» операционную систему ненужным программным «мусором», пользуясь невнимательностью владельца компьютера. Антивирус Dr.Web для OS X умеет распознавать и удалять эту программу, поэтому она не опасна для пользователей продуктов компании «Доктор Веб» ***(Вредоносная программа устанавливает нежелательные приложения в OS X // ITnews (http://itnews.com.ua/news/79257-vredonosnaya-programma-ustanavlivaet-nezhelatelnye-prilozheniya-v-os-x). – 2015. – 9.12).***

***

Во вторник, 8 октября, компания Adobe выпустила бюллетень безопасности APSB15-32 для Flash Player. Бюллетень исправляет 74 разные бреши, позволяющие выполнить произвольный код на системе с установленной уязвимой версией Flash Player. Еще три уязвимости позволяют обойти

ограничения безопасности. Все бреши могут быть проэксплуатированы удаленно.

Бюллетень затрагивает последнюю версию Adobe Flash Player для Windows и Mac (19.0.0.245), издание расширенной поддержки для всех платформ (18.0.0.261), а также версию для Linux (11.2.202.548).

Две уязвимости (CVE-2015-8438, CVE-2015-8446) существуют из-за ошибок переполнения динамического буфера. Эксплуатация брешей позволяет выполнить произвольный код.

Двенадцать уязвимостей существуют из-за ошибок повреждения памяти. Эксплуатация брешей позволяет выполнить произвольный код.

Три уязвимости (CVE-2015-8453, CVE-2015-8440, CVE-2015-8409) существуют из-за неизвестной ошибки. Эксплуатация брешей позволяет обойти ограничения безопасности.

Одна уязвимость (CVE-2015-8407) существует из-за ошибки переполнения буфера в стеке. Эксплуатация бреши позволяет выполнить произвольный код.

Еще одна уязвимость (CVE-2015-8439) существует из-за ошибки определения типа переменной. Эксплуатация бреши позволяет выполнить произвольный код.

Бреши CVE-2015-8445 и CVE-2015-8415 существуют из-за ошибки целочисленного переполнения и переполнения буфера в стеке соответственно. Эксплуатация уязвимостей позволяет выполнить произвольный код.

Пятьдесят шесть уязвимостей существуют из-за ошибки использования после высвобождения. Эксплуатация брешей позволяет выполнить произвольный код ***(Adobe исправила 77 уязвимостей в Flash Player // InternetUA (http://internetua.com/Adobe-ispravila-77-uyazvimostei-v-Flash-Player). – 2015. – 9.12).***

***

Специалисты компании FireEye совместно с экспертами Mandiant обнаружили новый вид сложного вредоносного ПО, предназначенного для хищения данных с кредитных карт.

Вредонос, получивший наименование Nemesis, обладает возможностью запуска вредоносного кода раньше кода операционной системы благодаря чему может контролировать процесс загрузки ОС. По свидетельствам экспертов, вредоносное ПО довольно сложно обнаружить и удалить даже после переустановки системы.

По данным FireEye, автором Nemesis является хакерская группировка FIN1, базирующаяся в России или русскоязычной стране. Группировка известна атаками, направленными на хищение данных кредитных карт и другой важной финансовой информации.

Экосистема Nemesis включает бэкдоры с поддержкой ряда сетевых протоколов и каналов связи с C&C-сервером. Платформа обладает широким

функционалом, в том числе возможностью передачи файлов, отправки снимка экрана, может работать в качестве кейлоггера, планировщика задач и пр.

После инфицирования целевой системы злоумышленники постоянно обновляют функционал Nemesis. К примеру, в одном из случаев преступники добавили утилиту, модифицирующую главную загрузочную запись (Volume Boot Record). Таким образом хакерам удалось загрузить компоненты вредоносного ПО перед загрузкой ОС Windows ***(Новый вредонос Nemesis предназначен для хищения средств с банковских карт // InternetUA (http://internetua.com/novii-vredonos-Nemesis-prednaznacsen-dlya-hisxeniya-sredstv-s-bankovskih-kart). – 2015. – 9.12).***

***

Специалисты компании Recorded Future сообщают: у хакерской группы Armada Collective, зарабатывающей на жизнь вымогательством, появились последователи. Точно известно, что группа DD4BC (DDoS «4» Bitcoin) тоже наживается на DDoS-атаках и требует выкуп за их прекращение. Однако DD4BC не единственные, кто понял всю перспективность данной тактики.

Эксперты Recorded Future пишут, что за последний год жертвами хакерской группы DD4BC стал ряд компаний, преимущественно в финансовом секторе. Злоумышленники действуют точно так же, как ранее делали Armada Collective: инициируют DDoS-атаку на предприятие и требуют от жертвы выкуп за прекращение атаки. В качестве предупреждения DD4BC, как правило, используют слабую атаку, мощностью порядка 10–15 Гбит/с. Она длится всего несколько минут.

Ранее группа DD4BC уже попадала на радары компании Akamai. Исследование, датированное сентябрем текущего года, гласит, что за период с сентября 2014 г. по август 2015 г. хакеры осуществили 141 атаку против компаний в Северной Америке, Европе, Азии и Австралии. По данным Akamai, самая серьезная атака DD4BC достигла мощности 56 Гбит/с, тогда против цели использовали NTP (22 %), SSDP (15 %), UDP (15 %) и SYN (13 %) флуд.

Средняя мощность DDoS-атаки DD4BC составляет 13,34 Гбит/с, хотя хакеры заявляют, что им доступны мощности до 400–500 Гбит/с. Также специалисты Akami подсчитали, что в среднем злоумышленники требуют у своих жертв от 25 (6000 дол.) до 100 (24000 дол.) биткоинов. Если компания не хочет платить, хакеры угрожают атакой на страницы в социальных сетях и угрожают скомпрометировать бренд вообще.

Тогда как из отчета Akamai было ясно, что киберпреступники активно наращивают обороты, то отчет Recorded Future свидетельствует о том, что DD4BC испугались быть пойманными. Более того, эксперты считают, что после недавней кампании против почтового сервиса ProtonMail, родоначальник такого рода атак – группа Armada Collective опасается того же.

Атака на ProtonMail произошла в начале ноября 2015 г. и значительно превосходила по мощности все предыдущие DDoS-атаки, исполненные группами Armada Collective и DD4BC. Хотя хакеры действовали от имени

Armada Collective, позже с сотрудниками ProtonMail связался неизвестный, заявивший о непричастности группы к данному инциденту. Аноним уверял, что он представляет настоящих хакеров Armada Collective. Сами сотрудники ProtonMail тоже подозревают, что стали жертвой какой-то серьезной хакерской команды, спонсируемой правительством. Компания даже попыталась заплатить выкуп, но хакеры из настоящей Armada Collective вернули почтовому сервису деньги и продолжили отрицать свою причастность к происходящему.

Исходя из этих данных, специалисты Recorded Future предполагают, что другие группы уже взяли тактику на вооружение и активно копируют «стиль» Armada Collective и DD4BC. Яркий пример – недавняя атака на греческие банки, якобы тоже произведенная группой Armada Collective. В Recorded Future уверены, что за этим инцидентом стояли совсем другие люди. В частности, хакеры потребовали огромный выкуп (7,2 млн дол. с каждого из трех банков), что совсем непохоже на поведение известных экспертам группировок.

Специалисты Recorded Future также отмечают явный рост интереса к механизмам проведения DDoS-атак в даркнете. Скрипт кидди со всего мира осознали, что кибервымогательство посредством DDoS-атак, это очень перспективное и, главное, простое в освоении направление. Исследователи Recorded Future полагают, что в ближайшем будущем стоит ожидать появления еще большего числа подражателей ***(У хакеров-шантажистов появляется все больше подражателей // InternetUA (http://internetua.com/u-hakerov-shantajistov-poyavlyaetsya-vse-bolshe-podrajatelei). – 2015. – 9.12).***

***

Законодатели и государства-члены ЕС утвердили первый в истории закон, который обяжет интернет-компании, такие как Google и Amazon, сообщать о кибератаках в соответствующие органы ЕС. Об этом пишет psm7.com со ссылкой на Reuters.

Соглашение между депутатами Европарламента и представителями правительств стран ЕС было достигнуто после пяти часов переговоров. Принятый закон стал ответом на растущую обеспокоенность касательно киберугроз, которые нарушают кибербезопасность и конфиденциальность данных жителей ЕС. По мнению представителей властей, принятый закон будет способствовать росту доверия потребителей к онлайн-сервисам, в особенности к трансграничным.

«Интернет не знает границ, и проблема одной страны может по принципу домино затронуть остальные страны в Европе. Именно поэтому нам нужны решения, охватывающие все страны ЕС. Данное соглашение является важным шагом в этом направлении», – отметил А. Ансип, вице-президент Еврокомиссии по вопросам цифрового рынка.

Новый закон, известный как Директива по сетевой и информационной безопасности, устанавливает четкие обязательства для компаний в таких важных отраслях, как транспорт, энергетика, здоровье и финансы. Интернет-компании, такие как Google, Amazon, eBay и Cisco должны будут уведомлять

соответствующие органы о кибератаках и других серьезных инцидентах. В противном случае компаниям могут грозить штрафные санкции. При этом социальные сети, как то Facebook, под действие директивы не подпадают ***(В ЕС приняли первый в истории закон о кибербезопасности // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45558/99999999/lang,ru/). – 2015. – 8.12).***

***

Apple выпустила накопительные обновления iOS 9.2 и OS X El Capitan 10.11.2. Помимо исправлений ошибок и добавления новой функциональности, данные релизы устранили множество уязвимостей, позволяющих скомпрометировать iPhone, iPad и Mac.

В общей сложности, в вышедших 8 декабря заплатках для iOS и OS X было исправлено 54 бреши, отмечает Securitylab. Почти половина всех уязвимостей позволяла скомпрометировать систему и удаленно выполнить произвольный код с привилегиями системы или ядра. Исправление также обновляет ряд сторонних библиотек наподобие libxml2 и OpenGL до последней версии.

В числе прочего, обновление для OS X El Capitan устраняет ряд не связанных с безопасностью ошибок. Например, подключение по Bluetooth более не будет самопроизвольно разрываться, а приложение Mail перестанет удалять сообщения в учетной записи Exchange.

Компания также выпустила обновленную версию iOS. В iOS 9.2 было исправлено 50 уязвимостей. Три бреши были обнаружены разработавшей джейлбрейк для iOS 9 командой Pangu.

Для пользователей, решивших пока не устанавливать OS X El Capitan, было выпущено обновление браузера Safari. Апдейт рекомендуется для установки всем пользователям Mac. Он содержит исправления для 13 уязвимостей, преимущественно затрагивающих движок WebKit. Большинство брешей позволяли удаленное выполнение кода при открытии вредоносных веб-страниц. Одна уязвимость позволяла раскрыть важные данные, если пользователь посетит вредоносный сайт ***(Apple закрыла 54 уязвимости в iOS 9.2 и OS X El Capitan 10.11.2 // InternetUA (http://internetua.com/Apple-zakrila-54-uyazvimosti-v-iOS-9-2-i-OS-X-El-Capitan-10-11-2). – 2015. – 10.12).***

***

Компания Palo Alto Networks предупреждает о новом Android-трояне, которому дали имя Rootnik. Малварь получает root-доступ к устройствам своих жертв, используя коммерческий root-инструмент Root Assistant, а затем похищает данные пользователей.

По данным специалистов Palo Alto Networks, новый вредонос поразил пользователей в США, Малайзии, Таиланде, Тайване и Ливане. Rootnik распространяется путем внедрения в безвредные приложения. Эксперты обнаружили вредоносные версии программ WiFi Analyzer, Open Camera, Infinite

Loop, HD Camera, Windows Solitaire, ZUI Locker и Free Internet Austria. Суммарно компании удалось найти более 600 образцов трояна. Rootnik заражает операционные системы от Android 4.3 и выше.

Для получения root-доступа к устройству жертвы, Rootnik использует легитимную утилиту Root Assistant, созданную в Китае. Инструмент Root Assistant действительно призван помочь пользователям в получении root-доступа к своему устройству. Но авторы программы явно не предполагали, что их разработка найдет признание у злоумышленников.

Есть у трояна и одна интересная особенность – он пытается получить root-доступ к устройству, основываясь на данных о стране использования девайса. Так, малварь вообще не пытается «нападать» на пользователей из Китая.

Авторы малвари имеют в своем распоряжении не менее пяти эксплоитов для платформы Android. Palo Alto Networks сообщает, что злоумышленники используют баги CVE-2012-4221, CVE-2013-2596, CVE-2013-2597 и CVE-2013-6282. Это позволяет хакерам устанавливать и удалять системные и несистемные приложения, не оповещая пользователя о происходящем. Также Rootnik устанавливает в системный раздел пораженного девайса несколько APK-файлов (AndroidSettings.apk, BluetoothProviders.apk, WifiProviders.apk и VirusSecurityHunter.apk), чтобы лучше закрепиться в системе, после получения root-доступа.

Укрепившись в системе, Rootnik способен скачивать исполняемые файлы с командных серверов и пусть их в дело. Основная задача вредоноса – агрессивно насаждать в системе рекламу, показывая полноэкранные баннеры даже на домашнем экране. Кроме того, троян может похищать информацию о Wi-Fi сетях, в том числе пароли, ключи, идентификаторы SSID и BSSID. В опасности также оказывается и личная информация пользователя: Rootnik агрегирует и ворует данные о местонахождении жертвы, MAC-адрес устройства и его ID.

Чтобы защититься от Rootnik и других подобных угроз, специалисты Palo Alto Networks рекомендуют обновить Android до последней версии и не устанавливать приложениях из подозрительных источников ***(Android-троян получает полный доступ к устройству через легитимный root-инструмент // InternetUA (http://internetua.com/Android-troyan-polucsaet-polnii-dostup-k-ustroistvu-cserez-legitimnii-root-instrument). – 2015. – 11.12).***

***

Кибермошенничество заняло первое место в списке основных рисков для финансовой индустрии, опередив традиционные заботы о чрезмерном регулировании и экономическом росте. Об этом стало известно в ходе опроса 113 американских и британских банкиров, регуляторов и риск-менеджеров, проведенного международной консалтинговой компанией PwC.

Один из респондентов отметил: «В какой-то момент мы увидим настолько мощную кибератаку в отношении отдельного банка, что она сможет

“сломать” учреждение и вынудить его обратиться за государственной финансовой помощью».

В глобальном масштабе, проблема киберпреступности возросла в рейтинге на семь позиций – с девятой в прошлом году до второй в этом, вытеснив вопросы регулирования. На первом месте в глобальном рейтинге оказались опасения по поводу хрупкости мировой экономики.

«Исследование показало достаточно сильный консенсус касательно основных угроз безопасности банковских институций, которые исходят от киберпреступников», – заявил С. Хант, глава PwC по рынку банков и капитала ***(Кибермошенничество стало самым большим страхом банкиров // InternetUA (http://internetua.com/kibermoshennicsestvo-stalo-samim-bolshim-strahom-bankirov). – 2015. – 11.12).***

***

Специалисты компании enSilo нашли серьезную проблему, которая оказалась общей для продуктов сразу нескольких антивирусных компаний. Уязвимость позволяет злоумышленнику с легкостью миновать все встроенные средства защиты Windows. Хотя крупные производители уже выпустили исправления, баг может быть по-прежнему актуален для других программ.

Впервые специалисты enSilo заметили проблему в марте 2015 г., когда столкнулись с AVG Internet Security 2015, установленным в системе одного из клиентов компании. Анализ показал, что антивирус распределяет страницы памяти, используя RWX (Read, Write, Execute) и постоянную предсказуемую адресацию. Этот баг может значительно упростить злоумышленнику обход механизмов защиты Windows и последующую эксплуатацию уязвимостей в сторонних приложениях.

«Microsoft встроила в Windows различные механизмы защиты от эксплоитов, к примеру, рандомизацию памяти (ASLR) или функцию предотвращения выполнения данных (DEP). Но когда страницы виртуальной памяти имеют постоянный и предсказуемый адрес, атакующий может узнать, куда именно записать код и откуда его исполнить, – разъясняют в блоге специалисты enSilo. – Из-за использования RWX в системе может быть исполнен вредоносный код, а значит все барьеры, возведенные Windows на пути злоумышленников, оказываются бесполезными».

Специалисты компании полагают, что эта проблема затрагивает не только антивирусы. Баг также могут содержать программы для мониторинга производительности или решения призванные защищать от утечек данных.

Компании AVG, Intel Security и «Лаборатория Касперского» уже отчитались об успешном устранении проблемы в своих продуктах. Но эксперты enSilo не советуют расслабляться и предостерегают пользователей, напоминая, что другие программы тоже могут быть уязвимы. Компания выпустила специальную утилиту, которая поможет отыскать небезопасные приложения в системе. Хотя инструмент не способен автоматически выявить уязвимую программу, он предоставит пользователю развернутую информацию о том,

откуда начинать копать ***(Эксперты обнаружили уязвимость в продуктах AVG, McAfee и Kaspersky Lab // InternetUA (http://internetua.com/eksperti-obnarujili-uyazvimost-v-produktah-AVG--McAfee-i-Kaspersky-Lab). – 2015. – 11.12).***

***

Домашние маршрутизаторы Linksys оказались подвержены уязвимости обхода аутентификации, позволяющей удаленно получить права администратора. Об этом сообщается в бюллетене безопасности, опубликованном компанией KoreLogic.

Брешь затрагивает модели Linksys EA6100, EA6200 и EA6300. Маршрутизаторы входят в линейку продуктов для домашних потребителей. Уязвимость существует из-за ошибок в CGI-скриптах веб-интерфейса устройства. Большинство сценариев предоставляют злоумышленнику неавторизованный доступ для управления маршрутизатором. В дальнейшем атакующий может раскрыть пароль администратора и получить полный доступ к беспроводному маршрутизатору. Ошибки существуют в загрузчике и следующих сценариях: sysinfo.cgi, ezwifi_cfg.cgi, gos_info.cgi и прочих файлах.

Брешь обнаружил эксперт KoreLogic М. Бергин. Специалист опубликовал PoC-код, позволяющий проверить, подвержено ли уязвимости устройство. Если после выполнения кода пароль администратора не изменится, повода для беспокойства нет.

На время написания новости Linksys не выпустила исправление. В качестве меры предотвращения эксплуатации уязвимости KoreLogic рекомендуется отключить средства удаленного администрирования.

CGI (от англ. Common Gateway Interface – «общий интерфейс шлюза») – стандарт интерфейса, используемого для связи внешней программы с веб-сервером.

Linksys – бренд сетевых продуктов для дома и небольших офисов, предлагаемый американской компанией Belkin International ***(Обнаружена опасная уязвимость в маршрутизаторах Linksys // Центр Інформаційної Безпеки (http://www.bezpeka.com/ru/news/2015/12/08/Linksys-flaw.html). – 2015. – 8.12).***

***

Центр НАТО з кіберзахисту опублікував книгу про кібервійну між Україною та Росією «Cyber War in Perspective: Russian Aggression against Ukraine».

Центр займається дослідницькою і навчальною діяльністю у сфері кібербезпеки.

Над створенням книги працювали вчені та експерти, які проаналізували поточну ситуацію з поширенням та захистом інформації, а також стратегічні наслідки кібервійни. В анотації книги зазначається, що даний конфлікт є благодатним підґрунтям для кібервійни, оскільки обидві країни відстоюють

власні геополітичні інтереси, при цьому вони володіють високим рівнем професіоналізму у сфері ІТ і адміністрування комп'ютерних мереж.

Книга охоплює період 2013–2015 рр. Експерти зазначають, що поняття «кібератака» вийшло за рамки тільки інформаційної війни. Тепер поняття включає цифрову пропаганду, DDoS-кампанії, дефейси веб-сайтів, витоки інформації внаслідок атак активістів, а також використання вірусного ПЗ для шпигунства. Завантажити книгу можна за посиланням https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf ***(Дослідники НАТО опублікували книгу про кібервійну України та РФ в інтернеті // Блог Imena.UA (http://www.imena.ua/blog/cyber-war-in-perspective/). – 2015. – 7.12).***

***

Антивирусная компания Symantec прогнозирует всплеск в 2016 г. кибератак на устройства на базе iOS и OS X.

Эксперты отметили, что в уходящем году количество вредоносного ПО, направленного на программные платформы Apple, возросло в два раза. Они сошлись во мнении, что показатель киберугроз, ориентированных на продукты Apple, будет расти. В частности, по данным FireEye, будет атакована платежная система Apple Pay.

Наибольшей опасности подвержены iPhone и iPad, которые были подвергнуты «джейлбрейку» – операции, позволяющей получить доступ к файловой системе аппарата, отмечают в компании.

За первые девять месяцев 2015 г. количество уникальных компьютеров на OS X, которые были заражены вирусами, возросло в семь раз по сравнению с 2014 г. В основном это были программы, которые не несли в себе вредоносного кода, но содержали рекламу или были способны отслеживать веб-активность пользователей. В прошлом году ежемесячно были атакованы до 70 тыс. компьютеров Mac.

В то же время, утверждают исследователи, iOS остается менее уязвимой к вредоносному ПО, чем Windows и Android. По информации FireEye, 96 % вирусов направлены на Android.

Вероятнее всего, кибератаки будут комбинированными и включать использование вредоносных приложений, эксплуатацию уязвимостей в легитимных программах и операционных системах, а также социальную инженерию ***(Владельцам устройств Apple следует запастись антивирусами // InternetUA (http://internetua.com/vladelcam-ustroistv-Apple-sleduet-zapastis-antivirusami). – 2015. – 13.12).***

***

Мошенники распространяют троян через Facebook и Twitter

Эксперты лаборатории Zscaler ThreatLabZ сообщили о новой вредоносной кампании, направленной на пользователей в Бразилии. В ходе кампании злоумышленники распространяют новый вариант банковского трояна Spy

Banker через социальные сети, в основном Facebook и Twitter. В качестве хостинга используются серверы Google Cloud.

Для инфицирования компьютеров жертв преступники применяют методы социальной инженерии, предлагая на Facebook и Twitter бесплатное фальшивое ПО под видом антивируса Avast или мессенджера WhatsApp. Нажав на вредоносную ссылку, пользователь перенаправляется на сервер Google Cloud, служащий для распространения загрузчика Spy Banker. По данным исследователей, переход по ссылке осуществлялся 103 тыс. раз, причем 102 тыс. (99 %) пришлись на долю пользователей Facebook.

Оказавшись на компьютере жертвы, загрузчик устанавливает на систему вспомогательные модули Spy Banker Telax, предназначенные для хищения банковских данных. По словам экспертов, Telax обладает рядом функций, позволяющих избежать обнаружения антивирусными решениями. Первым делом вредонос исследует систему на предмет наличия антивирусов. Троян собирает информацию о версии установленного по умолчанию браузера, операционной системы, антивирусного решения и пр. Затем данные отправляется на C&C-сервер злоумышленников.

Данная кампания – не первая попытка использования мошенниками сервисов Google. В июле нынешнего года специалисты Elastica Cloud Threat Labs обнаружили фишинговую кампанию, эксплуатирующую доверенный сервис Google Drive ***(Мошенники распространяют троян через Facebook и Twitter // InternetUA (http://internetua.com/moshenniki-rasprostranyauat-troyan-cserez-Facebook-i-Twitter). – 2015. – 13.12).***

***

Хакеры из Anonymous заявили, что нуждаются в помощи спецслужб для борьбы с джихадистами в Интернете. Об этом они рассказали в интервью британскому телеканалу Sky News.

По их словам, за последние недели блокированы свыше сотни пропагандистских сайтов, а также более 25 тыс. аккаунтов боевиков «Исламского государства» в соцсетях. Хакеры также размещали на страницах исламистов рекламу «Виагры» и картинки с козами и утками.

Данными операциями управляет небольшая группа, называющая себя Ghost Sec. Она состоит из 12 человек, которые действуют из разных стран мира и ничего друг о друге не знают. Представители Anonymous продемонстрировали Sky News свои возможности по проведению DDoS-атаки и рассказали, что с помощью специальной программы они могут закрыть доступ к сайтам на несколько месяцев.

Однако, подчеркнули хакеры, они исчерпали свой арсенал мер по борьбе с исламистами, поскольку защита их ресурсов стала эффективнее. В связи с этим они считают, что спецслужбы должны активнее включаться в эту работу. «Я думаю, что [они] или игнорируют это, не зная, какие шаги предпринять, либо у них нет времени и ресурсов», – предположил Камеди (Comedi), хакер и отец троих детей ***(Хакеры из Anonymous попросили помощи спецслужб для***

борьбы с ИГ // InternetUA (http://internetua.com/hakeri-iz-Anonymous-poprosili-pomosxi-specslujb-dlya-borbi-s-ig). – 2015. – 8.12).

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Касаткіна** Тетяна

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. 40-річчя Жовтня, 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
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.