СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(7–21.04)

2014 № 8

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(7–21.04)
№ 8

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

Головний редактор
В. Горовий, д-р іст. наук, проф.

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2014

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ 4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 21
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 23
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 35
Інформаційно-психологічний вплив мережевого спілкування на особистість 35
Маніпулятивні технології 36
Зарубіжні спецслужби і технології «соціального контролю» 43
Проблема захисту даних. DDOS та вірусні атаки 56

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Согласно исследованию GfK, на конец 2013 г. 50 % наших соотечественников возрастом старше 16 лет регулярно пользовались Интернетом, что на 6 процентных пунктов превысило аналогичный показатель за 2012 г., пишет Marketing Media Review (http://mmr.ua/news/id/polovina-ukraincev-polzuetsja-internetom-iz-nih-dve-treti-socsetjami-39213/).

В декабре прошлого года каждый второй украинец старше 16 лет подключался к всемирной сети минимум раз в месяц. Наиболее популярной причиной для захода в Интернет среди жителей Украины остаются социальные сети – 65 % опрошенных именно из-за проверки своих аккаунтов в соцсетях пользовались Интернетом. Годом ранее этот показатель составил 63 %. Самой активной категорией интернет-пользователей, естественно, является молодежь – 70 % представителей возрастной группы 16–19 лет ежедневно заходили в сеть, тогда как среди старшего поколения (50–59 лет) таких только 14 %.

Все больше украинцев приобретают себе электронные устройства, констатировали аналитики GfK. По итогам исследования в IV квартале 2013 г. 57 % наших сограждан старше 16 лет владели хотя бы одним из перечисленных гаджетов – смартфоном, компьютером, ноутбуком либо планшетом. Аналогичный показатель за 2012 г. был на 5 процентных пунктов меньше. Рост произошел за счет увеличения доли населения, имеющей ноутбук, планшет либо смартфон. При этом 81 % владельцев электронных устройств подключили их к домашнему фиксированному Интернету.

Исследователи отметили, что мужчины и женщины в одинаковой степени пользуются социальными сетями и электронной почтой, но в то же время есть и ряд различи в сетевом поведении между полами. Так, мужчины чаще женщин закачивают музыку и фильмы (48 % против 39 %), смотрят телепрограммы, видеоролики и слушают радио (34 % против 27 %) и играют в компьютерные игры (30 % против 16 %). А вот информацию о здоровье, наоборот, чаще ищут женщины (32 % против 19 %) ***(Половина украинцев пользуется интернетом, из них две трети – соцсетями // Marketing Media Review (http://mmr.ua/news/id/polovina-ukraincev-polzuetsja-internetom-iz-nih-dve-treti-socsetjami-39213/). – 2014. – 9.04).***

***

Українська соціальна мережа WeUA.info, нарешті, розпочала свою роботу. Це відбулося через тиждень після очікуваного запуску. Відкриття ресурсу відклали через масовані DDoS-атаки. Про це повідомляє ain.ua.

1 квітня на сайті weua.info мала розпочатися реєстрація. Натомість відвідувачі побачили на головній сторінці ресурсу повідомлення про

масштабні кібератаки і що реєстрація на сайті буде доступна найближчим часом.

Соцмережа не працювала впродовж усього тижня і, нарешті, запустилася. У ній уже реєструють користувачів, однак не кожен може отримати доступ. Щоб створити аккаунт на WeUA.info, потрібно ввести ключ реєстрації. Їх роздають лише тим, хто підписався на соцмережу ще до відкриття. Кожному такому користувачеві на пошту надсилають три ключі: для себе та для двох друзів.

Такі обмеження адміністратори ресурсу пояснюють тим, що помітили хвилю створення фейкових акаунтів. На сайті повідомили, що реєстрація за запрошеннями є тимчасовою.

Як повідомляє команда WeUA, в Інтернеті вже торгують їхніми ключами доступу. У соцмережі наголошують, що отримання доступу є безкоштовним і закликають не піддаватися на провокації. «Це шахрайство!» – підкреслив засновник сайту Б. Оліярчук.

Скільки часу триватиме реєстрація за запрошеннями адміністратори не повідомляють.

Разом з тим, згідно з інформацією WeUA, у мережі зареєструвалися майже 30 тис. користувачів ***(Українська соцмережа WEUA нарешті запрацювала // Osvita.MediaSapiens (http://osvita.mediasapiens.ua/material/29382). – 2014. – 7.04).***

***

В Google+ появилась метрика Views («Просмотры»). Новинка показывает количество просмотров другими пользователями профиля, публикаций, фото и видео с учётом перепостов и переходов пользователей на страницы контента.

Аналогичная статистика уже функционирует в Google Plus и позволяет получать данные о количестве просмотров фотографий и личных постов на странице пользователей. Расширенные возможности метрика Views распространяются и на другие виды контента.

Желающие могут скрыть информацию о просмотре контента от посторонних глаз в настройках.

Особенно полезной новая метрика может стать для авторов контента, поскольку отражает статистику заинтересованных пользователей.

«Новая метрика подсчитывает количество переходов на страницы публикаций, учитываются и просмотры постов на страницах пользователей, которые поделились ими, разместив ссылку или кликнув по кнопке +1. Принципы работы новой метрики на первый взгляд могут показаться странными, поскольку всё выглядит так, словно количество просмотров будет зависеть только от количества подписчиков. Однако здесь на первый план выступает именно степень активности при взаимодействии с аудиторией», – комментирует нововведение представитель Google Й. Зангер.

Слухи о том, что наличие профиля в Google+ влияет на ранжирование связанного с ним контента в основном поиске Google в среде специалистов ходили давно. Не исключено, что грамотное использование новой метрики поможет авторам еще более эффективно продвигать свой контент в социальной сети ***(Google+ показывает общее число просмотров контента, опубликованного пользователем // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/google_pokazyvaet_obschee_chislo_prosmotrov_kontenta_opublikovannogo_polzovatelem). – 2014. – 7.04).***

***

В веб-версии сервиса микроблогов Twitter появился новый дизайн, отображающий больше информации о пользователях. Об этом сообщается в официальном блоге Twitter.

В новом дизайне профилей пользователей будет фоновое изображение ещё большего размера, чем прежде. Читатели смогут просмотреть лучшие твиты владельца аккаунта, а сам он – «закрепить» вверху какую-то конкретную запись.

Кроме того, в новом дизайне можно будет переключаться между тремя вариантами отображения записей: только твиты, записи с фото и видео и все твиты, включая ответы другим пользователям.

«От момента к моменту ваш Twitter-профиль показывает миру, кто вы. Начиная с сегодняшнего дня, вам станет ещё проще (и, мы думаем, ещё веселее) самовыражаться через новый и улучшенный веб-профиль.Twitter»

Новый внешний вид профилей Twitter станет доступен всем пользователям в течение нескольких недель. Посмотреть, как выглядит новый дизайн, уже можно на примере нескольких страниц.

Разговоры о том, что у Twitter будет более «фейсбукоподобный» дизайн, появились ещё в феврале. Тогда часть пользователей уже получила новые профили ***(Twitter сделал профили пользователей похожими на Facebook // InternetUA (http://internetua.com/Twitter-sdelal-profili-polzovatelei-pohojimi-na-Facebook). – 2014. – 9.04).***

***

Сеть микроблогов Twitter тестирует новую функцию, которая будет как-то связана с показом уведомлений в браузере на компьютерах. Настройку, которую нельзя было активировать, первым нашел пользователь из Голландии М. Уэйстер, зайдя на сайт с тестового аккаунта. Через некоторое время она пропала, но оставалась доступной по прямому URL-адресу в Chrome и Firefox.

Акции Twitter торгуются на бирже, и уже скоро – 29 апреля – компания должна отчитаться о квартальной прибыли. Чтобы заработать больше, сервис стремится как можно дольше удержать пользователей на сайте, а функция оповещений о новых твитах и других событиях ей может в этом помочь. По

официальной статистике, в прошлом квартале Twitter активно пользовался 241 млн человек с ПК и 184 млн с мобильных устройств.

Ранее на этой неделе компания, стремясь стать более привлекательной для широких масс пользователей, переработала внешний вид профилей, сделав их похожими на страницы в Facebook и Google+. А за несколько дней до этого веб-версия Twitter научилась отображать популярные смайлики Emoji.

На смартфонах пользователи уже могут получать push-уведомления о том, если они были упомянуты кем-то из тех, на кого подписаны, о ретвитах и попаданиях в избранное. В браузере на ПК можно настроить оповещения по почте, некоторые из них в режиме реального времени умеет показывать Safari на «маках». Однако в более популярных обозревателях, таких как Chrome и Firefox, такая функциональность достигается за счет установки сторонних расширений ***(Twiter покажет уведомления в браузере // InternetUA (http://internetua.com/Twiter-pokajet-uvedomleniya-v-brauzere). – 2014. – 10.04).***

***

Крупнейшая в мире социальная сеть Facebook планирует удалить возможность обмена личными сообщениями из мобильных приложений для платформ iOS и Android и полностью выведет функцию мобильного чата в отдельное приложение Facebook Messenger, сообщает техноблог TechCrunch.

До сих пор мобильные приложения соцсети всегда содержали полнофункциональную вкладку для обмена личными сообщениями. Несколько месяцев назад для пользователей, у которых на смартфонах установлено отдельное приложение Messenger, Facebook заменила вкладку с сообщениями на ссылку, запускающую мессенджер. Если пользователь хотел продолжать обмениваться сообщениями внутри Facebook, ему нужно было лишь не загружать либо удалить Messenger.

Теперь выбора у пользователей Facebook не будет, пишет TechCrunch. Вкладка с сообщениями уйдет из мобильных приложений, а пользователи получат оповещения с предложением загрузить Messenger. Оповещения уже рассылаются отдельным пользователям в Европе, на переход дается около двух недель. Со временем на новый формат будут переведены все пользователи мобильных приложений соцсети.

Избежать «миграции» на Facebook Messenger смогут либо владельцы недорогих Android-смартфонов, версия платформы которых не поддерживает мессенджер, либо пользователи мобильного веб-сайта Facebook, либо те пользователи, которым доступно приложение-агрегатор контента Facebook Paper.

Можно предугадать, что не все пользователи будут довольны нововведением. Facebook часто используется как единая платформа для общения – как в публичном формате на стене, так и приватно, причем диалоги могут переходить из одного формата в другой. Попытка заставить

пользоваться отдельным приложением для личных диалогов может оттолкнуть аудиторию – рынок мессенджеров в настоящее время на подъеме, и необходимость установки еще одного приложения на устройство может показаться избыточной.

С другой стороны, Facebook часто подвергалась критике за излишнее число вкладок и разделов в мобильных приложениях. Возможно, вывод сообщений в Messenger станет попыткой упростить работу с сервисами Facebook – если только стратегия разработки отдельных приложений для ключевых функций может упростить взаимодействие с соцсетью.

С переводом личных диалогов в Messenger остается неясным план Facebook в отношении сервиса WhatsApp, который соцсеть купила за 19 млрд дол. По сути, Facebook Messenger как кросс-платформенный мессенджер напрямую конкурирует с WhatsApp. Кроме того, обоим сервисам сейчас приходится конкурировать с другими игроками рынка – Viber, Line, Telegram, WeChat, KakaoTalk, myChat и другими.

Мобильные сервисы в настоящее время являются главным приоритетом Facebook – аудитория приложений соцсети насчитывает более миллиарда пользователей в месяц, а на долю мобильной рекламы пришлось 40 % выручки за 2013 г. Глава Facebook М. Цукерберг заявлял, что соцсеть сфокусируется на развитии самостоятельных приложений – Facebook Messenger, Instagram, Poke, Paper и программная оболочка Facebook Home ***(Facebook заставит скачать отдельное приложение для сообщений // InternetUA (http://internetua.com/Facebook-zastavit-skacsat-otdelnoe-prilojenie-dlya-soobsxenii). – 2014. – 10.04).***

***

Администрация соцсети Facebook признала, что многие пользователи не понимают ее настройки безопасности, сообщает TechCrunch.

Пользователи считают, что Facebook слишком часто меняет настройки приватности, и что компания не умеет объяснять, как они работают, признают представители соцсети. Так как пользователи не имеют точного представления, кто именно увидит их посты, они предпочитают не публиковать некоторые вещи.

Ежедневно соцсеть проводит четыре тысячи опросов пользователей на 27 языках, чтобы узнать, насколько им понятны настройки безопасности. Они выявили, что большинству пользователей необходимы всплывающие подсказки, в которых будет говориться о последних изменениях в настройках.

В частности, Facebook будет оповещать пользователей о том, что теперь можно сделать старые обложки профиля доступными определенному кругу друзей, и что перепост поста доступен только общим друзьям. Также подсказки будут предупреждать перед публикацией поста, кто его увидит ***(Facebook признал свои настройки слишком непонятными // InternetUA***

(http://internetua.com/Facebook-priznal-svoi-nastroiki-slishkom-neponyatnimi). – 2014. – 10.04).

***

Facebook анонсировал несколько изменений в алгоритме отображения записей в ленте новостей. Соцсеть сократит объём записей, которые получают больше внимания пользователей, чем они того заслуживают, передает NewsOboz.org со ссылкой на techno.bigmir.net.

Речь идёт о трёх категориях записей. Первая содержит в себе недвусмысленные призывы ставить лайки, оставлять комментарии или делиться с друзьями. По словам представителей Facebook, пользователи действительно чаще реагируют на записи такого рода, однако опросы выявляют, что они на 15 % менее релевантны для читателей, чем другие статусы со сравнимыми показателями вовлечения.

Для борьбы с такими записями Facebook научился автоматически определять «попрошайничество». Их приоритетность в ленте новостей будет понижена, что не позволит им вытеснять другой важный контент от друзей пользователей.

Изменение в алгоритме не затронет страницы, «по-настоящему поощряющие дискуссии», а скорее коснется тех, кто часто публикует прямые призывы к социальным действиям, отмечают в Facebook. Примера того, как правильно стимулировать обсуждения с читателями, пресс-служба Facebook не приводит.

Две другие категории записей связаны с однотипным контентом и спамными ссылками. Facebook научился определять, какие страницы регулярно публикуют фотографии или видео, которые уже многократно появлялись в соцсети, и будет также понижать их приоритет. Первые результаты тестирования нового алгоритма показывают, что это на 10 % снижает количество записей, которые пользователи скрывают из ленты новостей.

Под спамными в Facebook понимают такие записи, которые уводят пользователя на внешний сайт, заполненный рекламой и второсортным контентом. Благодаря модификации алгоритма пользователи стали на 5 % чаще кликать на внешние ссылки, замечают представители Facebook.

Лента новостей в Facebook устроена таким образом, что пользователь видит не все записи, а только те, которые алгоритм посчитал для него наиболее важными. Каждая запись имеет показатель видимости так называемый EdgeRank на который влияет, например, то, кто её написал (насколько близок он по социальному графу к пользователю) и оставили ли под ней лайки или комментарии друзья читателя. Facebook не раскрывает деталей алгоритма, в связи с чем пользователи часто жалуются на непонимание принципов его работы ***(Facebook примерно накажет за «баяны» и попрошайничество // NewsOboz***

(http://newsoboz.org/it_tehnologii/facebook-primerno-nakazhet-za-bayany-i-poproshaynichestvo-14042014012400). – 2014. – 14.04).

***

Дислексик из Британии создал соцсеть, которой могут пользоваться молчуны и анонимы

Социальная сеть Slight, доступная пользователям устройств, работающих по управлением iOS, позволяет оставлять анонимные записи, привязывая их к точному месту на карте. Вокруг этих точек могут завязываться диалоги, но пользователи не знают ничего про человека, с которым ведут беседу.

«Мы не авторизуем пользователей, они не оставляют в системе никаких данных о себе, кроме геолокации», – пишут разработчики нового сервиса. Один из создателей Slight Д. Нэш рассказал, как ему в голову пришла идея новой соцсети. «Однажды я сидел на конференции DLD, европейском аналоге TED-Talk. На сцену вышла пара с каким-то жутким докладом, они без конца цитировали Н. Манделу и М. Л. Кинга. Все это было бы очень тоскливо, если бы не было так смешно. Я написал SMS своему другу: «What a Bullshit?!» («Что за отстой?!») Потом открыл Twitter-ленту конференции, но там не было ни шуток, ни комментариев. Люди предпочитали промолчать и переждать. Если бы у нас была возможность в некоторых ситуациях оставлять анонимные комментарии, мы могли бы рассказать друг другу куда больше».

С момента появления приложения Slight в AppStore его скачало несколько десятков тысяч пользователей. При этом едва ли не все пользователи очень быстро привыкли к новой соцсети и пользуются ей ежедневно.

Slight – далеко не первая соцсеть, дающая возможность анонимного общения, однако Д. Нэш верит, что все, кто скачает Slight, смогут улучшить мир. Издание отмечает, что аналогичное мнение высказывали и разработчики близкого аналога Slight – сети YikYak, популярного сервиса для студентов. Однако массовое использование этого сервиса в университетах и школах закончилось плохо. Произошло несколько суицидов среди подростков, уставы поведения учебных заведений регулярно нарушались. В итоге, разработчики заблокировали YikYak.

Д. Нэш страдает дислексией, из-за этого ему трудно читать и писать. Ему было трудно учиться в школе, и он изобрел собственный способ получения новых знаний. Вместо обычных книг Д. Нэш читал сотни pdf-файлов особым образом. Он находил ключевое слово, читал два абзаца вверх и два вниз, терял внимание и переключался на другой.

Д. Нэш полагает, что анонимная сеть Slight может найти самые разные применения. С его точки зрения, суть сервиса заключается в том, что вместо одного места с миллионом пользователей существует миллион мест с

несколькими пользователями, которые гораздо больше заинтересованы в общении в привязке к конкретному месту, но не собеседнику.

Например, с помощью Slight чиновники получат возможность передавать информацию о фактах коррупции или нарушения закона в стенах того ведомства, в котором они работают. В то же время анонимные сообщения могут использоваться для общения без давления офисной иерархии ***(Дислексик из Британии создал соцсеть, которой могут пользоваться молчуны и анонимы // InternetUA (http://internetua.com/disleksik-iz-britanii-sozdal-socset--kotoroi-mogut-polzovatsya-molcsuni-i-anonimi). – 2014. – 11.04).***

***

Согласно анонсу компании Nokia, приложение Facebook Messenger будет выпущено для линейки смартфонов Nokia X, Asha и Lumia. Хотя Nokia X основана на Android, но внесённые серьёзные модификации в платформу сделали невозможным использование служб Google, включая магазин Play. В этой связи разработчикам необходимо отдельно выпускать свои приложения для смартфонов Nokia X. В отдельных случаях речь идёт не только о публикации, но и внесении корректив в код ввиду отсутствия поддержки служб Google.

Facebook Messenger не предоставляет таких функций социальной сети, как просмотр своих и чужих лент, система отметок и публикаций – приложение нацелено исключительно на общение с друзьями посредством чата, голосовых и видеозвонков. Поддерживается коллективное общение и пересылка фотографий. При этом Facebook Messenger работает самостоятельно и не нуждается в предварительной установке полнофункционального приложения социальной сети.

У пользователей смартфонов Nokia Lumia список друзей Facebook будет добавлен в раздел «Люди» и уведомления о сообщениях будут выводиться в виде всплывающей панели сверху. У владельцев же Nokia X и Asha эти уведомления будут появляться в разделе Fastlane ***(Анонсирован Facebook Messenger для серий Asha, Lumia и Nokia X // InternetUA (http://internetua.com/anonsirovan-Facebook-Messenger-dlya-serii-Asha--Lumia-i-Nokia-X). – 2014. – 12.04).***

***

Почти половина Twitter-пользователей никогда не писала сообщений.

Около 44 % из 974 млн зарегистрированных пользователей Twitter никогда не отправляли из своего аккаунта ни одного сообщения, информируют «Экономические известия» (http://news.eizvestia.com/news_technology/full/285-pochti-polovina-polzovatelej-twitter-okazalas-mertvymi-dushami).

Около трети пользователей разместили меньше 10 сообщений за все время пребывания на сервисе. При этом 13 % пользователей публиковали

твиты более 100 раз. В то же время представители Twitter отказались подтверждать данные Twopcharts.

В компании заявили, что не комментируют статистику, которую собирают третьи лица. Однако, в компании отметили, что по их данным, каждый месяц сервисом пользуются около 241 млн человек. В этом показателе учитываются пользователи, которые хотя бы раз в месяц зашли в свой аккаунт.

Однако, в своих расчетах, сеть микроблогов под «активностью» не предусматривает обязательную публикацию сообщений. Это может быть просто чтение ленты интересных юзеру людей. Отметим, многие пользователи регистрируются на сервисе не для того, чтобы активно публиковать сообщения, но чтобы подписаться на интересные им аккаунты и читать их обновления ***(Почти половина пользователей Twitter оказалась «мертвыми душами» // «Экономические известия» (http://news.eizvestia.com/news_technology/full/285-pochti-polovina-polzovatelej-twitter-okazalas-mertvymi-dushami). – 2014. – 14.04).***

***

Число мобильных пользователей соцсети «Одноклассники» в марте составило 38 млн, сообщила компания.

«При этом общая ежемесячная аудитория «Одноклассников», по данным TNS Web Index за февраль 2014 г. составила более 41 млн пользователей», – прокомментировал «Ленте.ру» пресс-секретарь «Одноклассников» И. Грабовский. Таким образом, почти 93 % пользователей соцсети являются мобильными.

Самыми популярными смартфонами у пользователей «Одноклассников» стали Samsung и Nokia, собрав, соответственно, 24 и 23 % мобильной аудитории. Смартфоны от Apple заняли третье место с долей в 13 %. Замкнули топ-5 смартфоны HTC и LG с показателями 4 и 3 %, соответственно.

Другая крупная российская соцсеть – «ВКонтакте» – не предоставила официальных данных по мобильной аудитории. В то же время, по данным сервиса LiveInternet, в марте число мобильных пользователей «ВКонтакте» составило около 27 млн. По данным TNS за февраль 2014 г., общая месячная аудитория соцсети составила более 52 млн пользователей. Мобильные данные «Одноклассников» в LiveInternet закрыты.

По информации «Одноклассников», с помощью платформы Android в соцсеть заходят 19 млн пользователей, с помощью iOS – 6 млн. По данным LiveInternet, во «ВКонтакте» с помощью Android заходят около 15 млн пользователей, с помощью iOS – 7,8 млн ***(Почти все пользователи «Одноклассников» являются мобильными // Версии.com (http://www.versii.com.ua/news/301612/). – 2014. – 15.04).***

***

Старший вице-президент LinkedIn Д. Хенке, инженер Yahoo! Д. Тралл и первый лоббист Facebook А. Коннер работают над новым проектом – политическим сервисом Brigade. В этом им помогает сооснователь Napster Ш. Паркер, вложивший в стартап 9 млн дол. Он же и будет его CEO. Об этом сообщает hopesandfears.com

Предполагается, что Brigade станет социальной платформой, на которой смогут объединяться жители одного города или штата. Функционал сервиса будет использоваться для повышения их политической активности. В настоящее время она крайне мала: важные городские вопросы зачастую приходят обсудить лишь 10–15 человек.

Стоит отметить, что у проекта уже есть конкурент – сервис MindMixer, ранее привлёкший 4 млн дол. ***(Выходцы из Facebook, Yahoo! и LinkedIn создадут политический сервис // Media бізнес (http://www.mediabusiness.com.ua/content/view/39058/126/lang,ru/). – 2014. – 15.04).***

***

Совсем недавно соцсеть объявила о том, что уберет чат из своих мобильных приложений, не оставив пользователям других вариантов, кроме использования для чатов приложения Messenger. Р Тейт из The Verge считает, что этот шаг свидетельствует о том, что в мобильной среде Facebook, каким мы его знали, приходит конец.

Facebook – это компания, которая зарабатывает миллиарды на том, что объединяет людей. Теперь же она собирается усложнить для своих пользователей сам процесс общения. Недавно соцсеть объявила о планах убрать из своих мобильных приложений функционал мессенджера, по факту, заставив пользователей вдобавок к основному приложению скачивать еще и Facebook Messenger. Это нововведение, безусловно, кому-то покажется раздражающим, но, скорее всего, дело этим не ограничится. По мнению многих наблюдателей, удаление чата – это лишь первый шаг процесса ухода Facebook от единого средства, объединяющего в себе функции многих приложений.

Совершенно очевидно, что необходимость что-то отдельно скачивать для общения элементарно приведет к снижению числа людей, с которыми можно будет поговорить в Facebook с помощью мобильного приложения. Зачем же соцсеть пошла на такой шаг?

Многие эксперты, с которыми удалось поговорить, считают, что все дело в том, что Facebook меняет свою идеологию и теперь будет вести себя как компания, создающая приложения с четкой и конкретной функциональностью. Число пользователей может увеличиваться и благодаря старому подходу, когда Facebook объединял в себе множество разных функций, но в Долине все больше сторонников приобретает мнение о том,

что пользователи ждут от приложения отличного выполнения какой-то одной конкретной вещи.

М. Мерфи, который руководит в венчурной фирме Kleiner Perkins подразделением iFund, с этим совершенно согласен: «Мы видим, что в мобильной среде побеждает более простой, ясный и четкий опыт. Если вы решаете сделать приложение более сложным, это может «размыть» все впечатления от работы с ним».

Facebook: опыт второго класса

Соцсеть, фактически, подтвердила этот тезис применительно к своему мобильному приложению, раскрыв статистику, согласной которой в Messenger пользователи отвечают на сообщения на 20 % чаще, чем в главном приложении. Даже сам М. Цукерберг жаловался, что чат внутри Facebook App – это опыт «второго класса».

В принципе, так можно сказать вообще про любую функцию флагманского приложения. Поэтому компания на протяжении последних двух лет последовательно выносит из него большие куски функциональности (например Paper и Camera). CEO компании по аналитике мобильных приложений Flurry С. Халаф так описывает мобильный Facebook: «Опыт использования Facebook складывается из трех отдельных компонентов. Во-первых – это фотошэринг, затем идет стена – то есть лента новостей, а третье – коммуникация. И все это они разбивают на три разные приложения».

Для обмена фотографиями у Facebook есть приложение Photos и, конечно же, Instagram. Для новостей есть Paper, а для коммуникаций – Messenger.

Подготовка путей отступления

Какая же функциональность останется в главном приложении Facebook спустя несколько лет? На больших рынках вроде США число пользователей соцсети почти не растет. При этом, переходя с десктопной версии на мобильную, они совсем не обязательно продолжают использовать соцсеть так же интенсивно. Более того, иногда люди даже уходят к конкурентам вроде SnapChat или WhatsApp (который, впрочем, теперь уже не конкурент).

Бывший главный редактор TechCrunch и основатель блога Inside Facebook Э. Элдон считает, что все последние шаги М. Цукерберга очень похожи на подготовку плацдарма для отступления. «Если взглянуть на ситуацию скептически, то можно подумать, что Facebook готовится к тому, что будет делать, когда флагманский корабль (основное приложение) начнет тонуть. Более мягкое мнение заключается в том, что они пытаются сделать более четким и понятным использование тех функций Facebook, которые имеют нераскрытый потенциал [...] Я думаю, что компанию беспокоит влияние долгосрочных трендов на ядро Facebook и растущая популярность конкурирующих приложений-мессенджеров».

Нет никаких сомнений в том, что решение «выпилить» возможность обмена сообщениями из основного приложения в краткосрочной перспективе негативно скажется на активности общения в Facebook. Приложение

Facebook App остается одним из самых скачиваемых как в AppStore, так и в Google Play, и раньше любой, кто открывал его, одновременно был залогинен и в чате – но теперь этому придет конец.

Безусловно, купив WhatsApp, М. Цукерберг теперь может позволить себе небольшую «просадку» в активности обмена сообщениями. В конце концов, у его компании только что появилось больше 500 млн новых пользователей. Основной вызов, стоящий перед Facebook, заключается в трансформации из франкенштейнообразного создания, включающего в себя самые разные функции, в фабрику по производству качественных социальных приложений, которые работают отдельно, но объединены благодаря социальному графу Facebook.

Заставляя мобильных пользователей устанавливать Messenger и не оставляя им никакого выбора (если не считать выходом использование старых версии Android, которые мессенджер не поддерживают), компания четко дает понять, что не собирается ради сиюминутного удовлетворения потребностей приносить в жертву будущие инновации. Если Facebook продолжит действовать столь смело, то вполне может подорвать устоявшееся в технологических кругах мнение о том, что компании, совершившие прорыв в какой-то области, затем «закисают» и неизбежно проигрывают следующему поколению ***(Конец Facebook, каким мы его знали // InternetUA (http://internetua.com/konec-Facebook--kakim-mi-ego-znali). – 2014. – 15.04).***

***

Зачем Facebook тратит миллиарды на приложения типа WhatsApp и Instagram, дублирующие функции, встроенные в соцсеть? Оказывается, у М. Цукербрега есть хитрый план трансформации компании в нечто совсем другое, который он назвал «Креативными Лабораториями».

В конце прошлой недели регуляторы одобрили сделку по приобретению мессенджера WhatsApp соцсетью Facebook за баснословные 19 млрд дол. А на этой неделе стало известно, что Facebook уберет из своего клиента функцию личных сообщений, таким образом вынуждая пользователей скачать отдельное приложение-мессенджер для общения с друзьями по соцсети, Facebook Messenger. Такая последовательность действий выглядит несколько шизофренично: отдать бешеные деньги за один IM-сервис, чтобы потом заставить свою аудиторию пользоваться другим IM-сервисом, разработанным внутри компании, в чем смысл? И вообще, что за стратегия такая: покупать дублирующие уже существующие в соцсети сервисы? Сегодня WhatsApp, вчера Instagram. А ведь еще была неудачная попытка приобрести Snapchat за 3 млрд дол. При этом собственные нововведения Facebook, мягко говоря, не впечатляют: не вызывает восторга ни поиск Social graph, ни фирменный экран блокировки для Android Facebook Home.

Каждый раз, когда Facebook выпускает очередной широко разрекламированный продукт, который никого не впечатляет, каждый раз,

когда она тратит миллиарды на покупку чужих идей, компании предрекают скорую кончину. Однако основатель и гендиректор Facebook М. Цукерберг не унывает, хоть и признает, что двигатель инноваций Facebook в последнее время барахлит. «Зак» работает над пересмотром подхода Facebook к созданию и дистрибуции новых сервисов. Новый подход он называет Creative Labs (Креативные Лаборатории). Его суть можно свести к одному слову – приложения. Много, много разных приложений.

«В рамках Creative Labs мы разбиваем “большое синее приложение” Facebook на отдельные составные части», – рассказывает М. Цукерберг в интервью газете The New York Times. В прошлом, говорит он, Facebook был одной большой вещью, вебсайтом или мобильным приложением, которое позволяло людям удовлетворять сразу все свои социальные потребности. В ближайшем будущем, и особенно это касается мобильных устройств, Facebook раздробят на несколько узконаправленных сервисов, некоторые из которых не будут брендированы соцсетью, и, возможно, даже не потребуют авторизации в ней. Первым таким сервисом стал Paper, приложение для iPhone, позволяющее просматривать новостную ленту Facebook через систему жестов. Недавнее объявление о том, что из «большого синего» клиента соцсети исчезнет функция мессенджера, – тоже шаг в сторону нового подхода. Это рискованный шаг, многим пользователям он может прийтись не по душе. Но если Facebook хочет играть на новом, огромном мобильном рынке, придется рискнуть. Любовь мобильных пользователей компании завоевать жизненно важно: уже сегодня на них приходится основная часть визитов и рекламных доходов Facebook.

По мнению М. Цукерберга, новая стратегия позволит адаптировать Facebook к особенностям использования мобильных устройств. В мобильном мире ценятся узконаправленные приложения, решающие одну задачу, и предоставляющие при этом лучшее юзабилити, уверен гендиректор Facebook. Экраны смартфонов слишком малы для больших многофункциональных приложений. Маленькие программы имеют более простой и интуитивно понятный дизайн, и при этом быстрее работают, не «съедая» львиную долю ресурсов мобильного устройства. Например, через приложение Facebook Messenger сообщения доходят на 20 % быстрее, чем через большой клиент соцсети, выяснили в компании в ходе эксперимента.

Стратегия Creative Labs позволит Facebook создавать сервисы, которые раньше не вписывались в функционал социальной сети, открывая гигантское поле для экспериментов.

В новую стратегию вписывается недавнее открытие М. Цукерберга: некоторые сегменты мобильного Интернета больше и сложнее, чем он раньше думал. Например, сравнив базы пользователей WhatsApp и Facebook Messenger, он выяснил, что хотя эти приложения номинально идентичны, сценарии их использования различаются, а аудитории – не пересекаются. Это объясняет стремление Facebook поглощать успешные стартапы. На огромном поле мобильного Интернета такие сервисы, как Instagram и WhatsApp, могут

извлечь огромную выгоды из базы пользователей Facebook, при этом никак ее не сократив и сохранив собственную аудиторию.

Если новая стратегия будет успешной, в один прекрасный день Facebook может перестать выглядеть как Facebook. Да и называться будет, возможно, по-другому. Зато корпорация будет владеть каждым вторым приложением в вашем смартфоне и знать о вас больше, чем вы сами ***(В лабиринтах "креативных лабораторий" Facebook // InternetUA (http://internetua.com/v-labirintah--kreativnih-laboratorii--Facebook). – 2014. – 19.04).***

***

Компания Facebook добавила в приложения для доступа в соцсеть с мобильных устройств функцию Nearby Friends, с помощью которой можно в реальном времени узнать о нахождении неподалеку друзей по социальной сети, говорится в сообщении Facebook. Местоположение пользователя соцсети можно посмотреть на карте, если он разрешил это.

Функция Nearby Friends начнет распространяться на этой неделе среди пользователей США, она будет доступна на устройствах под управлением iOS и Android.

При включении функции пользователь получает всплывающие сообщения на экране мобильного устройства о друзьях, которые находятся недалеко от него. Можно отметить среди них одного или нескольких человек и предложить им встретиться. Предполагается, что этот сервис позволит организовывать спонтанные совместные походы в кафе или кино.

Пользователь имеет возможность выбрать категории «френдов», которые будут видеть его местоположение (друзья, близкие друзья или избранные пользователи), а также включать и отключать функцию в любое время. При отключении функции пользователь будет недоступен для обнаружения.

Функция Nearby Friends позволяет также выбрать определенный период, в течение которого можно видеть ваше точное местоположение. Это позволяет, например, коллегам найти друг друга перед встречей, но в дальнейшем не раскрывать, где они находятся.

Кроме друзей, находящихся близко, функция отображает местоположение путешествующих пользователей, если они включили соответствующую опцию. Таким образом, появляется возможность дать совет о достойных внимания достопримечательностях других городов ***(Facebook ввел функцию слежки за друзьями // InternetUA (http://internetua.com/Facebook-vvel-funkciua-slejki-za-druzyami). – 2014. – 18.04).***

***

Украинскую соцсеть «Друзі» создали десятеро одесситов. О себе они говорят не очень охотно и еще не привыкли к публичности. Большинство из

них – сотрудники одесских IT-компаний и для многих из них социальная сеть стала первым личным проектом. AIN.UA удалось уговорить их ответить на несколько вопросов (http://ain.ua/2014/04/18/520626).

Мысль о создании украинской соцсети родилась на фоне революционных событий в Киеве. Один из будущих разработчиков ресурса, устав ругаться с российскими «троллями», крикнул товарищу в соседний кабинет: «Юра, а давай сделаем свою социальную сеть?». После краткого обсуждения, было решено создать ресурс только для украинцев, где не будет пророссийской пропаганды, а обсуждать будущее страны смогут только соотечественники.

8 марта 2014 г. команда зарегистрировала домен druzi.org.ua, а через две недели того же месяца соцсеть запустилась и для пользователей. Первые несколько дней сайт практически не открывался из-за DDoS-атак. По словам разработчиков соцсети, по большей части атаки шли с территории Украины.

На сегодня в «Друзях» зарегистрировалось уже более 150 тыс. пользователей и эта цифра постоянно растет. Помимо этого, в социальной сети уже создано свыше 10 тыс. сообществ, загружено около 200 тыс. аудиозаписей и 60 тыс. видеороликов. Недавно проект поддержало Госагентство по науке, инновациям и информатизации, а один из украинских регистраторов подарил «Друзям» домен Друзі.укр.

AIN.UA удалось расспросить одного из основателей ресурса В. Пономарева о том, зачем Украине еще одна соцсеть, как в «Друзях» относятся к пиратскому контенту и где находятся сервера ресурса.

Как вы собираетесь конкурировать с существующими сетями? В чем ваша особенность?

Если речь идет о мировых социальных сетях, то, наверное, нам рано еще говорить о конкуренции, к тому же аудитория у нас может отличаться. У нас не регистрируются «все, чтобы найти всех», у нас регистрируются те, кто считает себя патриотом своей страны. Что касается конкуренции с украинскими социальными сетями, то мы и понятия не имели, что будет столько попыток создать локальную соцсеть.

Главная наша особенность в том, что проект имеет признаки народного – идеи создаем не только мы, но и активные пользователи. Каждый имеет возможность написать предложение, жалобу, указать на ошибку, мы это все анализируем, исправляем и делаем выводы. К примеру, наши пользователи очень хотели иметь раздел «гости», чтобы видеть, кто был на их страницах. Мы это сделали, но другие начали жаловаться, желая оставаться анонимными. Отключили, и снова начались жалобы: «Верните!». Нашли решение – у каждого пользователя теперь есть в настройках пункт «Показывать меня в гостях?», где можно выбрать «да» или «нет». Все счастливы.

Какое у вас отношение к пиратскому контенту? Будут ли его блокировать в «Друзьях»?

Мы против распространения пиратского контента и довольно долго думали над этим вопросом. Например, что делать с видео (фильмы, клипы и тому подобное)? Мы не загружаем видео на наши серверы, а добавляем только ссылки на видеоресурсы, где видео прошло модерацию.

Где находятся сервера ресурса?

Сервера ресурса находятся в Украине. Подробности мы раскрывать не хотим, чтобы не давать лишней информации нашим недругам.

Планируете ли вы привлекать инвестиции?

Мы создавали проект собственными силами и на свои деньги. Инвесторы нам сейчас не нужны, пока справляемся сами.

Какие планы на ближайшее время?

Сейчас мы активно работаем над созданием мобильного приложения для «Друзей». Мы поняли, что большинство пользователей хотят пользоваться соцсетью не только с помощью компьютера, но также с планшетов и смартфонов. Надеемся, что в ближайшее время уже сможем показать первую версию приложения под Android ***(Ворона Т. Зачем Украине еще одна социальная сеть – 5 вопросов основателям проекта «Друзі» // AIN.UA (http://ain.ua/2014/04/18/520626). – 2014. – 18.04).***

***

Как Facebook хранит 300 петабайт и развивает инфраструктуру

В социальные сети попадает всё больше людей, которые стремительно наполняют их контентом. Хранилище данных Facebook возросло втрое за последний год, достигнув объёма в 300 ПБ. Основная проблема компании в том, что эти триста петабайт должны оставаться легкодоступными миллиарду пользователей. Как же крупнейшая социальная сеть справляется с этой задачей?

Для сотрудников Facebook «большие данные» – ежедневная действительность, бросающая всё новые вызовы. Целый отдел специалистов из разных областей постоянно разрабатывает перспективные методы хранения данных. Любую новую систему сначала тестируют на реальных массивах, после чего принимают решение: внедрять её, отправить на доработку или полностью изменить предлагаемый подход.

На аппаратном уровне в Facebook используются такие традиционные технологии, как дисковые системы хранения данных и RAID-массивы. Особенность в том, что они могут быть легко масштабированы «на лету» за счёт кластерной платформы.

Для упрощения процессов репликации и синхронизации в дата-центрах Facebook применяется иерархическая распределённая файловая система HDFS. Однако это не совсем типовое решение на основе платформы Hadoop.

Основу инфраструктуры Facebook составляет программная надстройка Hive, которая с целью ускорения обработки использует систему индексов и обеспечивает SQL-подобный язык запросов HiveQL. Хранение метаданных в

СУБД значительно ускоряет выполнение семантической проверки при выполнении запросов.

Перед записью файлов в HDFS они предварительно сжимаются, причём алгоритм и настройки компрессии выбираются эвристически для каждого блока данных. Реализация системы обработки запросов Map-Reduce под названием Corona также имеет свои отличия. Она оптимизирована для работы с большими таблицами.

В большинстве реляционных баз данные организованы в виде двумерных таблиц, анализ которых осуществляется построчно. В Hive используется гибридный многоколонный формат записей (RCFile), адаптированный для хранения реляционных таблиц на кластерах.

Структура размещения данных RCFile представляет собой систематическое сочетание нескольких компонентов, включающих формат хранения данных, подходы к их сжатию и методы оптимизации чтения. Он обеспечивает четыре ключевых преимущества: быструю загрузку данных, высокую скорость обработки запросов, эффективное использование дискового пространства и хорошую адаптивность динамических шаблонов доступа к данным.

В общем случае перевод табличных данных в битовую последовательность выполняется сначала по строкам, а затем по колонкам, но в RCFile сделана важная оптимизация: столбцы таблиц записываются друг за другом смежными блоками и сжимаются индивидуально с помощью кодека Zlib / LZO, снабжаясь описанием в виде метаданных.

Благодаря такому подходу при операции чтения можно ограничиться выполнением выборочной распаковки данных. Поэтому при выполнении запроса пропускаются долгие этапы декомпрессии и десериализации ненужных столбцов. Специалисты Facebook указывают, что применение структуры RCFile позволяет им сжимать исходные данные примерно в пять раз. Без неё компании потребовалось бы сегодня хранилище на полтора эксабайта, а в ожидании загрузки ленты новостей пользователи успевали бы вздремнуть.

С дальнейшим распространением Facebook в развивающихся регионах размеры пользовательских профилей стали расти быстрее, а связка Hive + RCFile перестала быть достаточно эффективным решением.

Выход был найден при сотрудничестве с командой инженеров Hortonworks. Они разработали формат ORCFile, в котором оптимизация распределённого хранения данных в экосистеме Hadoop получила дальнейшее развитие.

Когда Hive записывает с помощью ORCFile табличные данные, они индивидуально сжимаются и разбиваются на блоки по 256 МБ, называемые полосами. Такой алгоритм был создан после многочисленных экспериментов с реальными базами. Размер полос в 256 МБ оказался оптимальным, а итогом проделанной работы стал вывод о неэффективности применения одинаковых настроек сжатия и постоянного использования словаря.

Программисты Facebook изменили код ORCFile так, чтобы целесообразность использования разных методов компрессии определялась для каждого блока данных заранее и без ухудшения производительности. Объём памяти, занимаемый словарём, сократился на 30 %, а скорость записи возросла в 1,4 раза.

Другим важным преимуществом нового формата стала возможность индексировать столбцы и строки с указанием их смещения, устраняя необходимость в частом использовании разделительных знаков.

Применив все эти улучшения, команда Facebook обеспечила значительную экономию дискового пространства. Степень сжатия данных последовательно довели сначала до пятикратной, а теперь и до восьмикратной. Причём, скорость их обработки также увеличилась.

Сегодня ORCFile уже успешно используется для хранения десятков петабайт данных. Модификация ORCFile, выполненная Facebook, демонстрирует в среднем втрое более высокую производительность, чем её изначальный вариант с открытым исходным кодом. Все наработки по оптимизации были переданы в проект Apache Hive ***(Как Facebook хранит 300 петабайт и развивает инфраструктуру // InternetUA (http://internetua.com/kak-Facebook-hranit-300-petabait-i-razvivaet-infrastrukturu). – 2014. – 21.04).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Политика продолжает вытеснять все прочее из информационного поля украинцев. По данным новостного агрегатора Mediametrics, который анализирует переходы пользователей социальных сетей на сайты СМИ, за прошедшую неделю все самые популярные статьи в Украине носили политический характер. В российском сегменте социальных сетей политические медиахиты недели немножко разбавил шоу-бизнес и сторителлинг (http://ain.ua/2014/04/14/519742).

Самой популярной статьей среди украинских пользователей социальных сетей за прошедшую неделю (за точку отсечения редакция AIN.UA взяла 21.00 воскресенья) стал материал сайта uainfo.org, который содержит данные свежего соцопроса граждан России. Согласно результатам опроса, большинство россиян поддерживает военное вторжение в Украину. Причем 52 % готовы сами идти на такую войну, а свыше половины опрошенных согласны при этом терпеть международные санкции. «Поздравляю Путина. Ему удалось создать государство такого сферического

быдла, что мне уже не страшно. Мне просто мерзко», – заключает автор статьи.

Половина всех статей из топ-10 приходится на долю «Украинской правды». Интересно, что в этот раз наиболее читаемыми стали блоги УП, а именно злободневные колонки известных журналистов Р. Шрайка, С. Лещенко и Д. Гнапа. В тройку попала и новость «Корреспондента» о том, что министр спорта Д. Булатов во время Евромайдана отдыхал в Доминикане.

Если взглянуть, какие материалы интересовали украинских пользователей лишь за последние сутки, то там, само собой, преобладают новости из Славянска, который в настоящее время превратился в главный оплот сепаратизма.

Тем временем, в России пользователи соцсетей тоже активно переходят на новости и статьи о происходящем в Донбассе. Особенно если посмотреть на срез за последние сутки. Здесь преобладают совсем другие настроения и источники, часто фигурирует «Правый сектор». Анонс очередного заявления В. Януковича оказался на четвертом месте за сутки, онлайн-трансляция из Славянска – на пятом ***(Судольский Р. Украина vs Россия: чем интересуются пользователи социальных сетей // AIN.UA (http://ain.ua/2014/04/14/519742). – 2014. – 14.04).***

***

Исполняющий обязанности министра внутренних дел Украины А. Аваков стал самым популярным украинским пользователем в социальной сети Facebook, сообщает «Обозреватель» со ссылкой на Watcher (http://tech.obozrevatel.com/news/09476-avakova-priznali-samyim-populyarnyim-ukrainskim-polzovatelem-v-facebook.htm).

Последние данные рейтинга украинских пользователей в Facebook показывают, что А. Аваков по своей популярности обошел журналиста М. Найема, который почти полгода возглавлял рейтинг.

Популярность А. Авакова была обеспечена во многом благодаря постоянному информированию пользователей Facebook о действиях возглавляемого им Министерства внутренних дел. Однако чрезмерная активность А. Авакова в социальной сети вызывает у многих раздражение, которое часто выражается в появлении специфического сетевого юмора ***(Аваков признан самым популярным украинским пользователем в Facebook // Обозреватель (http://tech.obozrevatel.com/news/09476-avakova-priznali-samyim-populyarnyim-ukrainskim-polzovatelem-v-facebook.htm). – 2014. – 15.04).***

***

Всплеск патриотизма в Украине, а также пылко встреченный обществом бойкот российских товаров и услуг, породил в уанете новый тренд. Всего за две недели запустилось сразу пять украинских социальных

сетей, которые надеются перетянуть на себя пользователей «Одноклассников» и «ВКонтакте». Надежды этих стартапов небезосновательны. Согласно результатам опроса, который AIN.UA проводил совместно с компанией 1 World Online, от российских социальных сетей в пользу украинских аналогов готовы отказаться 46 % интернет-пользователей (http://ain.ua/2014/04/19/520639).

Вопрос был сформулирован так: «Будете ли вы пользоваться украинскими социальными сетями?». В голосовании поучаствовало около 2700 человек. Из них 45 % (более 1200 респондентов) предпочло первый вариант ответа. Они не просто готовы стать пользователями украинских соцсетей, но и откажутся ради них от российских аналогов. 24 % опрошенных готовы пользоваться украинскими соцсетями наряду с другими популярными сервисами – Facebook и «ВКонтакте».

Лишь 17 % проголосовавших считают национальные соцсети полностью ненужными. Наконец, 14 % пользователей решили, что выводы делать рано и отложили решение на потом.

Сервис 1 World Online составил интерактивную карту, на которой можно посмотреть, как голосовали в опросе пользователи из разных уголков Украины и мира. В Украине примерно половина пользователей высказалась в пользу украинских соцсетей и отказа от российских.

Киев был более сдержан в оценках – 32 % высказали украинским соцсетям полную поддержку, 22 % готовы использовать их наряду с международными аналогами, а 26 % считают, что WEUA, «Друзі» и их аналоги никому не нужны. Именно этот вариант пользовался наибольшей поддержкой в России. Из 60 проголосовавших россиян три четверти не видят смысла в украинсих соцсетях. Из голосований по миру интересны данные по Италии – там проголосовали девять человек, причем все 100 % поддержали первый вариант ответа ***(Судольский Р. Украинцы готовы отказаться от «ВКонтакте» и «Одноклассников» – итоги опроса AIN.UA // AIN.UA (http://ain.ua/2014/04/19/520639). – 2014. – 19.04).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Краудсорсинг – это метод сбора идей, контента, поддержки или других типов решений от группы людей. Профессионалы во всем мире увеличивают прибыль путем краудсорсинга. Они устраивают конкурсы, опросы, получают мгновенную обратную связь, слушают и используют данные/идеи от клиентов.

Благодаря развитию социальных медиа, собирать информацию и идеи от ваших фолловеров стало гораздо проще. Представляем четыре способа, которыми можно углублять взаимодействие аудитории с вашими продуктами, повышая их лояльность и ваши продажи.

1. Спросите ваших клиентов, что они хотят.

Независимо от того, работаете ли вы в B2C секторе или предоставляете услуги для B2B компаний, чем лучше вы можете соответствовать потребностям потребителя, тем больше шансов, что они будут покупать у вас и станут вашими постоянными клиентами.

Простой способ вовлечь их и показать, что вы слышите их потребности – спросить их мнение.

Вот пример одного небольшого интернет-магазина, занимающегося продажей игрушек, которому нужно было узнать, какие LEGO продукты будут пользоваться большим спросом. Они создали простой опрос, в котором попросили клиентов напрямую проголосовать, какой набор им больше хотелось иметь. В качестве мотивации компания обещала отдать в подарок одному из участников тот набор LEGO, который наберет большее количество голосов.

Четкий призыв поделиться тем, что клиенты хотят, будет увеличивать социальное взаимодействие, а также повысит лояльность к бренду.

2. Проведите исследование потребительских предпочтений

Вы можете подумать, что исследование потребительских предпочтений – это очень трудоемкий процесс с фокус-группами, телефонными интервью и анкетными опросами.

С социальными медиа собирать статистику и получать понимание того, что хотят ваши клиенты, стало гораздо проще.

Создайте опрос на Facebook и попросите своих поклонников проголосовать:

За их любимый продукт;

Предпочтительные цвета продукции;

Лучшее использование вашего продукта;

Любимый способ шоппинга (онлайн/офлайн магазины), и т. д.

Crocs, например, проводит конкурс New release shoesday на Facebook. Они вовлекают своих фанатов, спрашивая о любимых новых ботинках на этой неделе. Фанаты, которые участвуют в опросе, имеют шанс выиграть обувь Croc. А бренд в свою очередь получает глубокое представление о рыночных предпочтениях.

Регулярно проводя опросы/конкурсы, вы получаете обратную связь, давая вашей аудитории то, что они с нетерпением ждут и за что голосуют каждую неделю.

3. Запустите конкурс «Название нового продукта».

Вовлеките ваших клиентов в такое важное бизнес решение, как выбор названия, и вы дадите им почувствовать, что они вносят важный вклад в ваш бизнес.

Чем больше пользователей почувствуют себя связанными с вашим бизнесом, тем больше шансов, что они купят товар у вас и поделятся информацией об этом со своими друзьями.

Sony наделала много шума в прошлом году, запустив конкурс «Помогите нам с именем». Они попросили общественность помочь разработать название для своей новой беспроводной акустической продукции: круглых динамиков белого, розового и черного цвета.

Sony опубликовала условия конкурса на своем блоге и продвинула его по всем социальным площадкам. Участники предлагали свои варианты названий новой продукции.

Менее чем за две недели Sony собрала 39 страниц с вариантами названий.

Окончательное название было выбрано руководителями компании. Имена пяти победителей были размещены на странице Sony в Facebook.

4. Попросите клиентов придумать новый вариант вашей продукции.

Краудсорсить можно не только названия к готовым продуктам, но и идеи новых товаров бренда. Когда вы просите ваших клиентов о такой услуге, вы даете им чувство расширения их прав и возможностей. Вы также способствуете тому, что клиенты думают о тех типах продуктов, которые у вас уже имеются, что увеличивает и лояльность и продажи.

Например:

Владелец ресторана может попросить постоянных посетителей придумать новый десерт.

Фирма по дизайну интерьера может собрать с пользователей новые идеи дизайна светильника.

Компания, занимающаяся приложениями, может краудсорсить идеи нового эффективного инструмента для бизнеса.

Известный бренд картофельных чипсов произвел настоящий фурор в мире краудсорсинга, когда предложил любителям чипсов шанс создать новейший вкус Lay’s в кампании Do Us a Flavor.

Lay’s максимально упростил условия участия. Участникам просто нужно было выбрать имя, назвать три ингредиента и затем поделиться записью в Twitter. Автоматически размещенные посты в лентах участников повышали охват аудитории конкурса.

Один выбранный победитель получил 1 млн дол. Lay’s получил не только огромную базу идей для будущих вкусов, но и увеличил продажи и узнаваемость бренда благодаря сарафанному маркетингу.

Советы по проведению опросов и исследований с помощью социальных медиа:

Устраивайте опросы в любых социальных сетях, где у вас есть официальное представительство (ВКонтакте, Twitter, Facebook. Pinterest, Google Plus или даже в вашем блоге).

На Twitter постите обновления о вашем конкурсе в разное время в течение дня и используйте соответствующие хэштеги, чтобы увеличить охват постов.

Следите, чтобы вопросы были простыми, используйте картинки и задавайте один вопрос за один раз.

Стимулируйте участие, раздавая подарки, непосредственно связанные с темой вопроса.

Распространите охват вашего исследования с помощью кросс-продвижения его по другим социальным сетям.

Сразу обговорите, что ваша компания будет иметь право «последнего слова» в выборе победителя (в случае, если компания выберет название из предложенных вариантов).

Просите пользователей предлагать идеи к продуктам, связанным с уже существующими товарами, чтобы углубить их лояльность к вашей продукции и увеличить объем продаж.

Не забудьте публично похвалить победителя (-лей), представив их имена публике в социальных медиа.

Ваша очередь!

Краудсорсинг для ваших бизнес-продуктов увеличивает вовлечение, повышает лояльность аудитории и показывает, что вы инновационная, современная компания. Добавление конкурсного элемента только даст им больше мотивации для участия ***(4 способа краудсорсить идеи в соцсетях // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/4_sposoba_kraudsorsit_idei_v_sotssetyah). – 2014. – 7.04).***

***

Как пишет The Wall Street Journal, в течение полугода в ленте новостей Twitter появится 15 новых разновидностей рекламных сообщений.

Один из новых видов рекламы будет продвигать приложения и игры для мобильных устройств. Пользователь, нажавший рекламный баннер, перейдет на страницу приложения, а сразу после начала установки будет переброшен обратно в Twitter в то место, на котором был прерван просмотр ленты новостей. Похожую рекламу можно увидеть на Facebook. Информации о других 14 видах рекламы пока нет.

По сведениям издания, увеличение разновидностей рекламы не приведет к росту ее объема, а лишь усилит заинтересованность пользователей продвигаемыми продуктами ***(Twitter тестирует 15 новых видов рекламы // InternetUA (http://internetua.com/Twitter-testiruet-15-novih-vidov-reklami). – 2014. – 7.04).***

***

Краткая инструкция по использованию LinkedIn для бизнеса

Если взглянуть на графики роста социальных сетей, то можно узнать не только о том, что Instagram стремительно растет, но и то, что на третьем месте по скорости роста находится LinkedIn.

Объективно – это важная информация, но понять, как именно все это можно использовать, не так-то просто. Несмотря на то что LinkedIn как соцсеть не настолько «заанализирована» всевозможными экспертами, все же

существует несколько интересных статистических наблюдений, которые полезно было бы учитывать.

LinkedIn отправляет на вашу главную страницу в четыре раза больше людей, чем Twitter и Facebook

Сервис микроблогов и соцсеть М. Цукерберга хороши, когда речь идет о вирусном распространении контента, но в плане прямого трафика на сайта, LinkedIn куда более интересный инструмент.

Аналитическая компания Econsultancy подтвердила этот факт своим исследованием 60 корпоративных сайтов с 2 млн визитами в месяц, которое продолжалось на протяжении двух лет. Переходы из LinkedIn составили почти две трети от всего социального трафика, что практически в четыре раза больше, чем у Facebook, занявшего второе место.

LinkedIn: 64 % социального трафика

Facebook: 17 %

Twitter: 14 %

Прежде всего, то, что зная о таком отличном свойстве LinkedIn, вы можете соответствующим образом изменить свой аккаунт и подачу материала в нем, фокусируясь на публикации контента, который будет генерировать лиды для вашего сайта.

Например, вот как «Лаборатория» с помощью LinkedIn приводит пользователей соцсети на свой главный сайт и рекламирует продукты:

Самый востребованный контент – это инсайты индустрии

Согласно данным самой соцсети, шесть из 10 пользователей LinkedIn заинтересованы в различных инсайтах индустрии, в которой трудятся. Следующим по популярности типом контента являются новости компаний (53 % заинтересованных пользователей), а на третьем – анонсы новых продуктах и услугах (43 %).

Что это означает:

Нужно делиться своей экспертизой. Не стесняйтесь объяснять людям интересные и сложные вещи, будьте прозрачны – и абсолютное большинство вашей аудитории оценит это. Большую часть публикуемого вами в LinkedIn контента должны составлять экспертные статьи и интересные новости компании, именно таким образом следует формировать контент-план.

Сам LinkedIn формулирует это так:

Ваши подписчики пользуются LinkedIn поскольку хотят быть более продуктивными и успешными профессионалами. Информативные, полезные посты имеют наивысшую степень вовлеченности, потому что именно такую информацию от компаний и хотят видеть пользователи».

Избегайте публикаций поздно вечером, после обеда и в выходные

Чтобы увеличить охват своих публикаций, имеет смысл делать их, когда число потенциальных читателей больше всего. Самым активным временем в LinkedIn является утро и день в будни. Грубо говоря, наибольшего охвата можно добиться в часы работы большинства компаний,

конечно, для конкретных страниц и бизнесов результаты могут немного отличаться, так что надо тестировать разное время публикации.

Что это означает:

Нужно публиковать контент так, чтобы посты выходили тогда, когда это удобно аудитории. Поэтому, если вдруг вы занимаетесь подбором контента для публикации по вечерам, лучше распланировать отправку сообщений на следующий день с помощью специальных сервисов.

Следует делать как минимум 20 публикаций в месяц

Теперь когда вы знаете, когда именно следует публиковать контент, стоит задаться вопросом частоты публикаций. По данным самой соцсети, необходимо делать не менее 20 постов в месяц – это позволяет охватить 60 % уникальной аудитории.

Более частые публикации помогут увеличить охват, но уменьшат число возвращающихся пользователей. Кого-то из подписчиков никогда не удастся охватить так как эти люди не заходят в социальную сеть, поэтому нацеливаться стоит на тех, кто ею пользуется. Конечно, никто не даст вам стопроцентную гарантию того, что вы сможете охватить 60 % аудитории, сделав 20 публикаций, но все же шансы на это довольно велики.

Есть и такие компании, у которых есть время, ресурсы и, самое главное, контент для более чем 20 публикаций. Лучшие корпоративные маркетологи, работающие с LinkedIn, делают 3–4 публикации в день – это около 80 постов в месяц.

В общем и целом, универсальный совет может звучать так: публикуйте так много постов, на сколько у вас хватает контента.

Что это означает:

Начните с 20 качественных публикаций в месяц и увеличивайте это число, если поймете, что это принесет дополнительную пользу. Число «20» отлично соотносится с рекомендуемыми окнами для публикации – если вы будете делать один пост в день на протяжении четырех недель (исключая выходные), то как раз наберется 20 публикаций.

Одним постом можно охватить 20 % вашей аудитории

Если вас интересует, кто вообще может прочитать то, что вы публикуете, то знайте – охват поста на LinkedIn составляет 20 % от аудитории страницы.

Что это означает:

20 % – это много или мало? Естественно, все зависит от общего числа подписчиков, если их много, то охват в двадцать процентов будет вполне неплохим результатом. С другой стороны, соотношение 1 к 5 – это не мечта маркетолога, так что есть смысл делать больше постов, чтобы добиться лучших результатов.

Помогите своим сотрудникам помочь компании

Активность на корпоративной странице, а именно вовлеченность подписчиков, может сыграть большую роль в привлечении новых людей. Если кто-то просто «проходил мимо» и увидел, что у вас все довольно

активно, то он может остаться с вами надолго. А в плане увеличения вовлеченности, нет никого лучше собственных сотрудников.

Вероятность того, что сотрудник компании кликнет на опубликованную ею ссылку, прокомментирует пост или сделает шейр на 70 % выше, чем у среднестатистического пользователя LinkedIn.

Что это означает:

Не стоит пренебрегать таким активом, как собственные сотрудники. Отправляйте им оповещения о постах на корпоративной странице каждый раз, когда что-то публикуется.

Изучайте процент вовлеченности и оптимизируйте стратегию

Используйте LinkedIn Analytics – панель администратора страницы – для того, чтобы изучать процент вовлеченности пользователей.

С главной страницы администраторской панели вы сможете увидеть общую информацию о посещениях вашего профиля, включая интересные демографические данные (например, местоположение пользователей – полезно для понимания, в каких временных зонах вы популярнее всего), распределение посетителей по должностям, отраслям и даже о том, как много посещений было от ваших собственных сотрудников.

Для получения более полной информации нужно нажать на ссылку в самом верху страницы – это позволит увидеть полную статистику по опубликованным постам.

Процент вовлеченности высчитывается исходя из общего числа взаимодействий, кликов и приобретенных подписчиков для каждого поста в вашем аккаунте. Другими словами, процент вовлеченности говорит вам, как много людей из тех, кто видел вашу страницу, как-либо с ней взаимодействовали.

Что это означает:

Вовлеченность скажет вам о том, где следует поднажать и что изменить в том, как и что вы публикуете на своей Linkedin-странице. Оценивайте категорию опубликованного контента, целевую аудиторию, а также день недели и время публикации. Все это поможет вам лучше оптимизировать контент-стратегию и добиться лучших результатов для следующих постов.

Кстати, не так давно в LinkedIn появились и некоторые другие полезные для маркетологов инструменты – в частности, Content Marketing Score, который «измеряет вовлеченность рекламных постов, публикаций на корпоративной странице, в группах LinkedIn, постов сотрудников и лидеров мнений», а также дает возможность сравнить свои показатели с результатами конкурентов. Страницы для сравнения можно подбирать по разным показателям, например, по размеру компании и индустрии.

Как видно, LinkedIn становится все более измеримой социальной сетью, что, вкупе с упомянутой выше перспективностью в плане аудитории, делает ее очень привлекательным средством для использования в маркетинговой стратегии ***(Краткий гайд по использованию LinkedIn для***

бизнеса // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/kratkiy_gayd_po_ispolzovaniyu_linkedin_dlya_biznesa). – 2014. – 8.04).

***

Компания объявила о Шлеме Twitter (Twitter Helmet) 8 апреля – носимое устройство, которое охватывает полностью всю голову пользователей, одновременно позволяя «взаимодействовать с миром вокруг них (виртуальным) исключительно через пользовательский интерфейс», говорится в блоге компании.

Устройство также обладает функцией отправлять твиты простым «клюющим движением» (кивком) головы, и стоит новинка всего 139,99 дол., несмотря на то что изготовлен гаджет из высококачественных материалов, таких как ударопрочное стекло с олеофобным покрытием.

Шлем появятся в продаже в начале сентября и будет включать в себя множество аксессуаров птичьей тематики, такие как «кожаный чехол с ручным тиснением, перо-образный Wi-Fi и усилитель сотового сигнала, подбородочный ремень из углеродного волокна с восковице образным микрофоном», согласно компании ***(Twitter анонсировал шлем виртуальной реальности // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_anonsiroval_shlem_virtualnoy_realnosti). – 2014. – 8.04).***

***

Сайт поиска недвижимости Address.ua теперь показывает пользователям в том числе и объявления о продаже/аренде квартир в социальных сетях. Когда зарегистрированные пользователи сервиса авторизуются на нем через аккаунты во «ВКонтакте» и Facebook и начинают искать жилье на сайте, первыми в результатах выдачи они видят объявления из этих сетей, пишет AIN.UA (http://ain.ua/2014/04/08/519018).

Пользователи сразу видят объявления от лиц из списка друзей, которые также авторизовались на сайте через социальные сети. Затем показываются объявления других пользователей «ВКонтакте» и Facebook, которые связаны общим кругом общения (друзей друзей), а затем – все остальные. В настоящее время на сайте зарегистрировано около 80 тыс. пользователей, из которых около 3 тыс. – через социальные сети.

Таким образом, сначала пользователи видят объявления от людей, которых они лично знают. Чем больше друзей с привязкой аккаунтов в социальных сетях, тем больше объявлений появится в списке.

Руководство сайта уверено, что такая функция очень упростит пользователям поиск жилья. Ведь позвонить по квартире легче человеку, которого знаешь лично. Такой список практически нивелирует недоверие первого контакта, считает CEO проекта М. Школьник ***(В Address.ua теперь***

можно искать жилье в Facebook и «ВКонтакте» // AIN.UA (http://ain.ua/2014/04/08/519018). – 2014. – 8.04).

***

Сервис микроблоггинга Twitter приобрел приложение Cover, популярную замену страницы блокировки для устройств на базе Android. Условия сделки пока неизвестны.

Welcome to the flock @coverscreen! We're excited too.

– Twitter Mobile (@twittermobile) April 7, 2014

Cover автоматически помещает на страницу блокировки шесть приложений, которые чаще всего запускает пользователь в зависимости от местоположения – дома они одни, на работе другие, в дороге третьи. В блоге Cover написано, что приложение не исчезнет из Play Маркета, но как оно будет интегрировано с Twitter, не сообщается.

Facebook, один из конкурентов Twitter, в прошлом году выпустил лаунчер для Android, однако этот опыт оказался для социальной сети неудачным – приложение так и не стало популярным ***(Twitter купил приложение для страницы блокировки Android // InternetUA (http://internetua.com/Twitter-kupil-prilojenie-dlya-stranici-blokirovki-Android). – 2014. – 8.04).***

***

Сегодня присутствие в соцсетях для брендов – это необходимость. Социальные медиа стали неотделимой частью любого современного бизнеса: именно с их помощью компании генерируют продажи и поддерживают общение с покупателями. Если посмотреть глазами пользователя, то можно увидеть одни преимущества – они получают общение в реальном времени и ответы на все волнующие вопросы, не выходя из дома.

Community-менеджер имеет дело с неостанавливающимся потоком сообщений сразу на нескольких платформах, и очень часто в голову приходит вопрос: «Во сколько можно уйти в офлайн? Может ли вообще клиентский сервис быть офлайн?»

Ответ прост: нет. В реальной жизни это очень сложно осуществить, множество факторов этому препятствуют. Socialbakers опубликовали данные, которые необходимо проанализировать, прежде чем приступить к работе 24/7:

1. Покупатель.

Популярные бренды получают вопросы и сообщения круглосуточно, и речь уже не идет о границах рабочего дня. Независимо от того, во сколько написал клиент – это время становится рабочим для community-менеджера. А если компания международная, то про эти сроки вообще стоит забыть.

Если вы не понимаете, почему ваши клиенты закидывают вас сообщениями в 4 часа утра, то выход один – подключайте аналитику.

2. Цель.

Сейчас в социальных сетях время стратегий и метрик. Каждый бренд должен определить точные цели продвижения и сформировать понимание того, почему присутствие необходимо именно на этой площадке.

Объем запросов может быть огромным. Создание раздельных аккаунтов для «поддержки» и «новостей» – это единственное жизнеспособное и наиболее часто практикуемое решение. Это отличный способ отфильтровать покупательские вопросы от других менее важных сообщений.

Иногда для пользователя жизненно важно, чтобы кто-то на другом конце быстро ответил на его вопрос или комментарий, особенно после выхода нового контента.

3. Проблемы.

Никто не любит недругов. Но, к всеобщему сожалению, киберпространство переполнено ими. Некоторым особенно стрессовым сферам бизнеса, таким как продажа авиабилетов или мобильные операторы, свойственны случаи «социального суицида». Так называется момент, когда кнопка «опубликовать» становится врагом, и с ее помощью можно разрушить репутацию бренда. Постоянный мониторинг даст вашему бренду возможность своевременно придумать подходящий ответ. Если вы этого не делаете, то рискуете вдвойне: критические проблемы могут остаться незамеченными, а небольшие противоречия могут перерасти в крупные сложности.

К сожалению, многие бренды еще не выучили этот урок. Данные Socialbakers о среднем времени ответа на вопросы пользователей говорят о том, что пользователям зачастую приходится в два раза больше ждать по вечерам или выходным, в отличие от дневного времени в обычные дни – от 4 до 7 часов.

Запомните:

Интернет никогда не спит. Пребывание в офлайне может повлечь за собой негативные последствия: очень важные сообщения могут так и остаться непрочитанными, а бренды перестанут замечать проблемы своих покупателей ***(Круглосуточный мониторинг соцсетей – ключ к успеху // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/kruglosutochnyy_monitoring_sotssetey_klyuch_k_uspehu). – 2014. – 9.04).***

***

Компании Facebook и Google усиливают собственные рекламные агентства, чтобы разрабатывать кампании для таких крупных брендов, как Budweiser и Ford. Об этом пишет The Financial Times.

Как напоминает газета, Facebook и Google уже зарабатывают в общей сложности 60 млрд дол. в год на продаже рекламного пространства на своих сайтах.

Внутренние подразделения Google и Facebook по производству рекламы, известные как The Zoo и The Creative Shop соответственно,

являются все еще небольшими агентствами, говорится в заметке. В The Zoo работают около 100 человек, в The Creative Shop – 70.

«Однако они быстро расширялись после своего создания несколько лет назад», – отмечает газета и добавляет, что Facebook и Google хотят изменить то, как бренды воспринимают их платформы ***(Facebook и Google усиливают собственные рекламные агентства // Версии.com (http://www.versii.com.ua/news/301232/). – 2014. – 10.04).***

***

Facebook заявила, что увеличит размер рекламных объявлений, отображаемых в правой колонке на веб-сайте, в попытке привлечь внимание пользователей и осчастливить рекламодателей.

Новый вид объявлений в правой колонке появится в конце этого месяца. Они будут больше по размеру и иметь то же соотношение сторон объявлений, что и в ленте новостей. Объявления охватывают всю ширину правой колонки, что означает возможность для маркетологов использовать одно и то же изображение в любом из своих объявлений. Больший размер также означает, что пользователи увидят меньше объявлений, отображаемых в правой колонке.

В конечном счете, эти изменения призваны повысить взаимодействие и сделать формат рекламных объявлений более привлекательным для рекламодателей и для пользователей. Facebook заявила, что первоначальные тесты повысили взаимодействие пользователей в три раза по сравнению с меньшим форматом.

При эмуляции формата ленты новостей, объявления в правой колонке могут стать значительно более качественными. Блоки столбцов заработали репутацию менее привлекательных по неверным причинам.

Более крупные, с меньшим количеством текста – более наглядны, заметны и эффективны.

Социальная сеть должна предоставить доходы своего первого квартала 23 апреля. Акции торгуются на отметке 61 дол. за штуку, или на 5 % выше после закрытия во вторник на отметке в 58,19 дол. ***(Facebook запускает новый формат рекламы // Marketing Media Review (http://mmr.ua/news/id/facebook-zapuskaet-novyj-format-reklamy-39247/). – 2014. – 11.04).***

***

Социальная сеть Facebook продолжает экспансию на непривычные для IT-компании рынки, став, кроме крупнейшей социальной сетью, еще и интернет-банком

Как сообщает издание The Financial Times, соцсети осталось всего несколько недель до получения одобрения от государственного регулятора Ирландии, что позволит пользователям Facebook приобретать и передавать новую Facebook-валюту, передает NewsOboz.org со ссылкой на Gazeta.ua.

Кроме того, разрешение Ирландии, которая является членом ЕС, позволит менять Facebook-валюту на евро и будет действительна по всей Европе, а также, скорее всего, станет массово использоваться для онлайн-покупок ***(Социальная сеть Facebook запускает собственные деньги // NewsOboz (http://newsoboz.org/it_tehnologii/facebook-zapustit-sobstvennye-dengi-14042014133446). – 2014. – 15.04).***

***

Сервис микроблогов Twitter запустил полноценный рекламный функционал для разработчиков мобильных приложений на базе существующей рекламной платформы. Инструмент разработан на основе технологии MoPub, приобретённой компанией Twitter в сентябре 2013 г. Об этом пишет Marketing Media Review (http://mmr.ua/news/id/twitter-zapustil-reklamnyj-funkcional-na-baze-mopub-dlja-razrabotchikov-mobilnyh-prilozhenij-39372/).

Технология позволяет разработчикам мобильных приложений управлять размещением рекламы из различных источников – контекстной рекламой, рекламой на главной странице, объявлениями из сетей и аукционов в едином аккаунте MoPub Marketplace.

В настоящее время новый функционал проходит стадию закрытого бета-тестирования и представляет своим клиентам разнообразные настройки таргетинга; а также инструменты для измерения эффективности рекламы.

Новый продукт позволяет рекламодателям создавать объявления «нативной» рекламы и блоки рич-медиа, совмещая успешный опыт использования «Карточек Twitter» и «Продвигающих твитов». Пользователи смогут взаимодействовать с приложениями и загружать их к себе на устройства прямо из ленты.

Первыми партнёрами Twitter, пожелавшими протестировать функционал стали сервисы Spotify, HotelTonight, Kabam и Deezer.

Помимо данного функционала, рекламодатели Twitter получили возможность запускать и настраивать кампании в Twitter Publisher Network на ads.twitter.com. Twitter Publisher Network позволяет встраивать рекламные объявления в тысячи приложений, которые ежемесячно запускаются на 1 млрд мобильных устройств. Процесс назначения ставок происходит автоматически.

Возможность уже доступна ограниченному числу рекламодателей из США и по завершении беты будет представлена широкой аудитории.

«Сегодня платформа MoPub охватывает более 1 млрд мобильных устройств и ежемесячно обрабатывает свыше 130 млрд запросов на размещение рекламы в приложениях для Android и iOS. Это одна из самых крупных в мире бирж по размещению мобильной рекламы. В настоящее время рекламодатели могут запускать кампании, адресованные 241 млн активных пользователей Twitter, используя специальный интерфейс на

ads.twitter.com», – комментируют запуск представители сервиса микроблогов.

Впервые информация о том, что Twitter готовится представить новый формат рекламы мобильных приложений – App-install Ads – появилась в отраслевых СМИ начале марта 2014 г. Планировалось, что новинка привлечёт дополнительное число рекламодателей из числа представителей e-commerce и лидеров игровой индустрии ***(Twitter запустил рекламный функционал на базе mopub для разработчиков мобильных приложений // Marketing Media Review (http://mmr.ua/news/id/twitter-zapustil-reklamnyj-funkcional-na-baze-mopub-dlja-razrabotchikov-mobilnyh-prilozhenij-39372/). – 2014. – 18.04).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Социальные сети связаны с эмоциональной и физической изменой, разрывами отношений, показало новое исследование. Как оказалось, активные пользователи сети Twitter чаще сталкиваются с конфликтами со своим партнером, спровоцированными именно социальной сетью, пишет Health India. Причем продолжительность романтических отношений не играет никакой роли, заявляет Р. Клэйтон из Университета Миссури.

Р. Клэйтон исследовал 581 пользователя Twitter разных возрастов. Людей опрашивали на предмет активности пользования социальной сетью (учитывалось количество входов, написания твитов, просмотр сообщений по подписке, число сообщений другим пользователям и ответов подписчикам). Также ученый интересовался, были ли конфликты с партнером, связанные с использованием Twitter. Выяснилось: чем чаще свою активность человек проявлял в Twitter, тем больше был риск конфликта с партнером.

Ранее Р. Клэйтон проводил похожее исследование Facebook. Тогда было доказано: частота использования социальной сети предсказывала наличие связанных с ней конфликтов, которые приводили к разводу и расставанию. Но, что касается Facebook, риск расставания был особенно высок у людей, находивших в отношениях максимум 36 месяцев. В любом случае, ученый советует сократить время пользования социальной сети, если имеются проблемы в личной жизни. Дело в том, что люди, слишком активно пользующиеся социальными сетями, могут отстраняться, а это сопровождается ростом недоверия к партнеру ***(Социальные сети***

разрушают романтические отношения, – ученые // Утро.UA (http://www.utro.ua/ru/zhizn/sotsialnye_seti_razrushayut_romanticheskie_otnosheniya_uchenye1397132778). – 2014. – 10.04).

***

Популярность социальных сетей вынуждает ученых проводить все новые и новые исследования о том, какое влияния они оказывают на человека. Большинство выводов экспертов пока, увы, неутешительны. Особенно это касается женщин, сообщает IT Expert со ссылкой на meddaily.ru.

Так, по данным ученых, использование дамами социальной сети Facebook негативно сказывается на их самооценке и, в частности, на восприятии собственной фигуры.

Специалисты опросили 881 студентку и выяснили, что в среднем каждая из них проводила в соцсети около 80 мин. в день. Чаще всего девушки читали френд-ленту и разглядывали фотографии других пользовательниц.

При этом чем дольше они находились в соцсети, тем выше была вероятность того, что они начинали сравнивать себя с другими. Причем сравнение это было отнюдь не в их пользу.

При том, что средний вес участниц исследования составил 67,59 кг, они хотели весить меньше примерно на 9 кг. В среднем, девушки хотели достичь идеального веса около 58,97 кг.

Такие результаты были особенно характерны для девушек, которые пытались похудеть. Те же, кто не стремился к этому, отличались более высокой самооценкой после просмотра фотографий в соцсети ***(Соцсети внушают женщинам недовольство своим телом // IT Expert (http://itexpert.org.ua/rubrikator/item/35106-sotsseti-vnushayut-zhenshchinam-nedovolstvo-svoim-telom.html). – 2014. – 16.04).***

Маніпулятивні технології

История кубинского аналога Twitter заставила задуматься о «темной» стороне соцсетей

После того как стало известно, что «кубинский Twitter» под названием ZunZuneo тайно финансировался США и мог быть создан с целью организации оппозиционно настроенных жителей острова, многие задумались о природе более крупных интернет-сервисов и социальных сетей.

«Все слышали о том, как социальные сети вроде Twitter, Facebook и YouTube способствуют распространению демократии в мире, мобилизуя массы и упрощая свержение диктаторов. Теперь мы видим их более мрачную сторону», – написал обозреватель газеты The Washington Post Д. Басулто в блоге на сайте издания. Обзор его записи публикует портал InoPressa.

Пример ZunZuneo выглядит очень показательным. Он лишний раз доказывает, что социальные сети действительно можно использовать в политических целях. Они могут быть частью правительственных кампаний по дезинформации, направленных на усмирение оппозиционных движений. Список приемов обширен: от цифровых «медовых ловушек» до сложнейших попыток разрушить репутацию. В странах вроде Египта и Турции данные соцсетей используют также с целью установить местоположение протестующих по GPS или IP-адресам, говорится в статье.

Новая сторона социальных сетей имеет множество последствий для американской дипломатии, полагает Д. Басулто. Изначально Twitter, Facebook и YoTube помогли рассказать всему миру, что Америка – страна бейсбола, яблочного пирога и демократии для всех. Однако чем сильнее впечатление, что соцсети подчиняются АНБ и ЦРУ, тем менее эффективна их роль в распространении американских ценностей за рубежом. «Если американский образ жизни подразумевает слежку со стороны правительства, а также опасность подрыва онлайн-конфиденциальности и сбора персональных данных в политических целях, можно ли использовать это для завоевания сердец и умов зарубежных стран?» – задается вопросом Д. Басулто.

Тем не менее журналист отдает должное Twitter и Facebook, которые сопротивляются и публично выступают против правительственной слежки за общением онлайн. «Самый заметный пример: М. Цукерберг призвал президента Б. Обаму прекратить использовать АНБ для слежки за активностью более чем миллиардной аудитории соцсети», – пишет Д. Басулто. Впрочем, с точки зрения автора, это не помешает американскому правительству создать «поддельный Twitter» или «поддельный Facebook» ***(История кубинского аналога Twitter заставила задуматься о «темной» стороне соцсетей // InternetUA (http://internetua.com/istoriya-kubinskogo-analoga-Twitter-zastavila-zadumatsya-o--temnoi--storone-socsetei). – 2014. – 11.04).***

***

Соцсеть «ВКонтакте» считает Крым и Севастополь Украиной

Депутат Госдумы Е. Федоров (ЕР) направил администрациям «ВКонтакте» и Facebook запросы: он просит разъяснить, почему эти соцсети считают Крым и Севастополь частью Украины. Два региона вошли в состав России три недели назад. Социальные сети «Одноклассники» и «Мой мир» уже присоединили их к Российской Федерации. Об этом пишет izvestia.ru

«Это первый этап депутатского расследования. Они дадут информацию либо не дадут, тогда уже будем делать выводы – как на них повлиять, – говорит Е. Федоров. – Если они являются врагами российского государства и ставят задачу давления на Россию, то будет одна реакция. Если это случайность – другой ответ».

По мнению депутата Госдумы И. Костунова, если обе социальные сети хотят быть политически нейтральными, они могли бы дать возможность жителям полуострова самим выбирать, с какой страной они себя ассоциируют. При этом существует возможность массовой регистрации ботов, считающих российский город Симферополь частью Украины, но это не приведет ни к каким правовым последствиям.

В картографическом сервисе российской компании «Яндекс» государственная принадлежность Крыма и Севастополя зависит от того, из какой страны пользователь обращается к сайту.

«“Яндекс” – международная компания, которая предоставляет сервисы в соответствии с законами тех стран, где мы работаем. Это Россия, Украина, Казахстан, Беларусь, Турция. Всем пользователям, которые приходят на “Яндекс” из остальных стран, мы будем показывать карты сообразно официальной российской позиции, – сообщили “Известиям” в пресс-службе “Яндекса”. – С технологической точки зрения реализация изменений по Крыму займет некоторое время. Уже сейчас пользователи из России видят Крым территорией России».

По мнению основателя портала liveinternet.ru Г. Клименко, причины того, что «ВКонтакте» и Facebook не присоединили Крым и Севастополь к России, могут быть две: либо техническая, либо политическая. «У Facebook могут быть политические соображения. Это американская компания, и теоретически они могут не признать Крым российским. Я не думаю, что у “ВКонтакте” политические причины. Мне кажется, это техническая история. К примеру, в сервисе статистики liveinternet.ru Крым мы вынесли в отдельное государство, и чтобы считать его регионом России, надо переделывать всю базу. У них может быть подобная история».

Представители «ВКонтакте» и Facebook не прокомментировали задержку со сменой государственной принадлежности двух регионов ***(Соцсеть «ВКонтакте» считает Крым и Севастополь Украиной // Media бізнес (http://www.mediabusiness.com.ua/content/view/39000/126/lang,ru/). – 2014. – 10.04).***

***

С. Аксенов, как истинный пользователь социальных сетей, просто не «вылазит» с Twitter. Там он сообщает все свои мысли и предположения, формируя мышление других по-своему (или скорее Путинскому) образу и подобию.

Но как-то смешно ловить его на вранье, еще смешнее, что российское интернет-издание с четырехмиллионными просмотрами печатает информацию, которая противоречит сама себе.

РИА-Новости: 13:29, 14.04.2014 (обновлено: 16:13 14.04.2014): «Власти Киева втрое сократили объем подачи воды в Крым по Северокрымскому каналу, сообщило агентство Крыминформ в понедельник со ссылкой на первого вице-премьера региона Рустама Темиргалиева».

Интерфакс: 11:50, 14.04.2014 «При норме около 50 кубометров в секунду сейчас идет объем около 16 кубических метров в секунду, и то из-за того, что мы нашли техническое решение, не позволяющее им полностью эту воду перекрыть. Практически в три раза сократили поставки, – сказал Р. Темиргалиев журналистам в Симферополе».

РИА-Новости практически продублировали эту информацию.

А в 9:20 С. Аксенов написал на своей странице Twitter: «Украина сократила поставки воды в Крым почти в 13 раз. Мотив данного заключается в провокации Киевом Москвы, пользуясь положением Крыма».

В ответ ему: «Та нет все нормально течет как надо!», но неугомонный С. Аксенов сразу оправдался: «При сложившейся ситуации уменьшения поставок воды из Украины в Крым, мы перешли на резервные источники. Без воды не останемся!»

Население удивляется: так быстро отреагировали, что даже непонятно, а каким образом уменьшение подачи воды в 13 раз должно сказаться на наличии ее в кране.

С. Аксёнов в тот же день пожаловался Путину о проблемах с подачей воды в Крым. Об этом также написали в РИА-Новости. Он доложил о том, что «Киев сократил подачу воды около 5,5 куба в секунду, при норме около 70 кубов в секунду».

Ну если с подачей как-то можно манипулировать, то нормы, что возросли с 50 до 70 кубов в секунду – удивляют.

Но если эта информация в вечерних новостях России будет подаваться еще более «оптимистическая», то это уже не удивит, а воспримется как должное. Сарафанное радио за кумулятивным принципом. Надо бы С. Киселева послушать, там наверно прозвучит что-то с «ужасные бендеровцы-фашисты подорвали и завалили Северо-Крымский канал, чтобы мирные жители Крыма умерли от засухи…».

Таким образом формируется информационно-фейковое поле российских ЗМИ ***(Кто-то врет: Аксенов или РИА-Новости? // UkrNews24 (http://ukrnews24.com/kto-to-vret-aksenov-ili-ria-novosti/). – 2014. – 14.04).***

***

Для поширення неправдивих новин російська пропаганда використовує ботів в Twitter, які розповідають про те, що Слов’янськ штурмують силовики з Західної України.

Нещодавно на сайті російського державного інформаційного агентства РИА Новости з’явилась ще одна неправдива інформація. Цього разу про те, що «Бойовики «Правого сектора» прибули в Слов’янськ для участі в спецопераціі».

При цьому використовується фото «Правого сектору», зроблене кілька тижнів тому в Києві.

Новину, як і попередню про силовиків з Західної України, активно поширюють російські боти в соцмережах ***(Тема №2 для російських ботів:***

Боевики «Правого сектора» прибыли в Славянск для участия в спецоперации // UkrainianWatcher (http://watcher.com.ua/2014/04/13/tema-2-dlya-rosiyskyh-botiv-boevyky-pravoho-sektora-prybyly-v-slavyansk-dlya-uchastyya-v-spetsoperatsyy/). – 2014. – 13.04).

***

Маразм пророссийских пропагандистов не знает границ. Российские пользователи социальных сетей вовсю постят фото С. Джобса, скончавшегося в 2011 г., который поддержал присоединение Крыма Россией. Следует отметить, что картинке в духе «Цитаты великих людей» пользуются особой популярностью в соцсетях, однако зачастую большинство цитируемых великих людей уже не могут оспорить приписываемые им цитаты, какими бы глупыми или бессмысленными они не были.

Так, С. Джобс, легендарный основатель Apple, скончавшийся в октябре 2011 г., несмотря на свою кончину 2,5 года назад, восхваляет Россию за действия в Крыму, начавшиеся в марте текущего года. Распространение картинки в социальных сетях осуществляется с подачи российских средств массовой информации ***(Маразм дня в соцсетях: умерший в 2011 г. Стив Джобс одобрил действия России в Крыму // IT Expert (http://itexpert.org.ua/rubrikator/item/35150-marazm-dnya-v-sotssetyakh-umershij-v-2011-g-stiv-dzhobs-odobril-dejstviya-rossii-v-krymu.html). – 2014. – 17.04).***

***

Как ловят мошенников в социальных сетях. Анализ социального окружения помогает предотвращать мошенничество на финансовом рынке.

В эпоху Интернета и всеобщей глобализации мошеннические сообщества становятся шире, а сами злоумышленники – более умелыми и осторожными. Для предотвращения подобных угроз и серьезных убытков современным организациям необходимо выявлять преступные группы на ранних этапах их развития. Особенно это важно для розничных банков, выдающих большой объем кредитов населению – им необходима «историческая база» для моделирования случаев мошенничества.

Как бороться с этим злом? Традиционные схемы здесь малоэффективны, мошенники постоянно изобретают новые способы обмана. На помощь приходят математические и статистические методы анализа информации, точнее, целый арсенал инструментов углубленной аналитики. Среди них – передовая развивающаяся методика выявления сложных организованных схем мошенничества на основе анализа социального окружения (она получила название Social Network Analysis, SNA, иногда ее называют также «анализ социальных связей»). Практически ни одна разработка в области противодействия мошенничеству не продемонстрировала в последнее время такого потенциала, как SNA.

Нередко словосочетание «анализ социального окружения» наводит на мысль о популярных сервисах Facebook и Twitter. В основе метода SNA для финансовых организаций и популярных интернет-сервисов лежит общая концепция построения сети с узлами и связями. Однако SNA представляет собой более сложный математический аппарат, позволяющий не только строить сеть связей, но и рассчитывать показатели сети, автоматически выявлять скрытые сообщества.

Говоря о «сети связей», мы подразумеваем узлы, типы связей и бизнес-правила для их расчета. Узлами сети могут служить так называемые объекты. Связи между объектами могут быть самыми разными – это, например, и отдельные клиенты, и компании-контрагенты, и банковские счета, и т. д.

Эти связи определяют различные типы отношений между объектами, например, торговые операции компаний, родственные связи клиентов и т. д. Для расчета связей могут применяться как простейшая логика (такая, как совпадение телефонного номера у двух клиентов), так и более сложные бизнес-правила с возможностью нечеткого поиска.

Социальную сеть связей можно строить буквально на любом существующем наборе данных. Если преступное сообщество уже сформировано, то социальная сеть сразу же позволит его выявить с помощью встроенных алгоритмов. Интересно, что модель сети можно использовать не только для «вычисления» сообществ мошенников, но и для выявления принадлежности текущих банковских операций таким сообществам с целью их последующей блокировки.

Метод SNA основан на построении сети взаимосвязей клиентов. Мы считаем, что два клиента связаны, если между ними существует какая-то общая характеристика или общее действие. Например, два клиента будут связаны между собой, если у них общий адрес электронной почты или одинаковый номер телефона.

В страховании в качестве общей связи может выступить владение одним и тем же автомобилем (продавец б/у автомобиля и его покупатель) или участие в одном и том же ДТП.

Как работает SNA? Если мы видим связь клиента с ранее выявленным случаем мошенничества (причем связь может быть неявная), то для нас это является основанием подозревать, что этот клиент тоже может быть мошенником.

Один из крупнейших проектов SNA был реализован в Министерстве финансов Бельгии при раскрытии схемы незаконного возврата экспортного налога на добавленную стоимость, известной как «карусель НДС». В 2001 г. потери бюджета от этой схемы оценивались в 1,1 млрд евро в год. В схему была вовлечена целая сеть фиктивных компаний в нескольких юрисдикциях (Бельгии и Франции), которые занимались последовательной перепродажей одних и тех же товаров друг другу. При перемещении товаров из одной юрисдикции в другую у экспортера возникало право на возмещение НДС, который ранее был уплачен другой аффилированной компанией-

посредником. Однако на деле НДС в бюджет никогда не платился, так как компания-посредник являлась типичной фирмой-однодневкой и в одночасье просто «растворялась». Таким образом мошенники могли неограниченное число раз перепродавать товар по цепочке и возмещать НДС, организуя своеобразную «карусель».

Для борьбы с организованным мошенничеством в Бельгии в 2001 г. была создана Налоговая инспекция специального назначения (ISI). Сложность заключалась в том, чтобы найти мошеннические компании в списке из десятков тысяч организаций и определить мошеннические операции среди миллионов финансовых транзакций по всему Евросоюзу.

Для решения проблемы пригласили экспертов компании SAS, которые предложили использовать методы SNA. На основе электронных баз была построена сеть связей из компаний-экспортеров и торговых операций между ними. С помощью аналитических инструментов SNA были выявлены отдельные скрытые сообщества компаний, которые осуществляли внутри себя циклические операции экспорта-импорта, отобраны сообщества с признаками мошеннических операций и проведено детальное расследование их деятельности. В результате уже в первый год использования SNA потери Бельгии от «карусели» сократились на 80 % до 232 млн евро, а к 2012 г. – на 98 % до 18,5 млн евро в год. Это был потрясающий успех!

В банковском кредитовании крупное мошенничество, как правило, также носит организованный характер. Преступные группы подделывают пакеты документов о финансовом состоянии заемщика, организуют телефонную линию, по которой подставные люди готовы подтвердить банкам любую позитивную информацию о заемщиках. Случается, что в преступную группу оказываются вовлечены и сами сотрудники банков. Такие схемы могут на протяжении долгого периода времени приносить доход преступникам, поскольку их сложно обнаружить без использования современных методов. Например, если в схеме замешан сотрудник офиса продаж банка, занимающийся оформлением кредитов, то именно этот сотрудник может стать «центральным звеном» в SNA-сообществе недобросовестных клиентов, которым он выдал кредит.

Исследования показывают, что вероятность мошенничества клиента банка увеличивается, если среди его родственников, коллег или знакомых присутствуют кредитные мошенники. Именно такие связи позволяет анализировать и учитывать при оценке кредитоспособности заемщика решение SNA.

В страховом бизнесе организованные группы мошенников, как правило, специализируются чаще всего в сегменте автострахования. В мошеннические схемы могут быть вовлечены и сотрудники станций техобслуживания (СТО), которые умышленно завышают стоимость ремонтных работ, и агенты, страхующие за определенное вознаграждение разбитые автомобили, и группы злоумышленников, занимающихся фальсификацией ДТП.

С помощью метода SNA эксперты выявили, что один малоизвестный пункт автосервиса активно проводил калькуляцию стоимости ремонта тех случаев ДТП, где присутствовали признаки фальсификации. Кроме того, у отдельных клиентов автосервиса совпали адреса и телефоны, что позволило страховой компании обнаружить, что здесь замешана организованная группа.

В мировой практике, по статистике, около 10 % всех выплат в автостраховании являются мошенническими.

Инструмент SNA может обнаружить мошеннические схемы в данных, на первый взгляд, представляющих абсолютно разрозненные страховые случаи. Автоматические алгоритмы ищут связи между страховыми случаями и их участниками, учитывая любые мелочи, которые могут ускользнуть от внимания человека. Например, на основании базы данных страховой компании SNA может выявить раннее (с глубиной в несколько лет) вписанных в один и тот же полис ОСАГО лиц, которые, на момент подачи требования могут показаться «случайными» участниками ДТП, а на деле являются мошенниками ***(Как ловят мошенников в социальных сетях // InternetUA (http://internetua.com/kak-lovyat-moshennikov-v-socialnih-setyah). – 2014. – 19.04).***

Зарубіжні спецслужби і технології «соціального контролю»

Еще в декабре прошлого года документы Э. Сноудена о слежке АНБ показали, что спецслужбы используют данные от рекламных трекеров в Интернете. Новая научная работа специалистов из Принстонского университета позволяет понять, как именно используется эта информация. Авторы считают, что 90 % пользовательской активности в Интернете можно восстановить, отслеживая статистику с рекламных трекеров, таких как Google DoubleClick.

Каждая рекламная сеть провозглашает анонимность собираемой статистики, но при этом присваивает каждому пользователю уникальный номер ID, а затем отслеживает его переходы с сайта на сайт, что позволяет восстановить почти полную картину истории серфинга пользователя.

Более того, впоследствии несложно восстановить и реальное имя человека, потому что рано или поздно он авторизуется в социальной сети вроде Facebook или Google+. Так что провозглашаемая анонимность – не более чем рекламный лозунг.

Авторы научной работы говорят, что для обеспечения истинной анонимности нужно использовать сеть маршрутизации Tor, чтобы надежно замаскировать свой настоящий IP-адрес ***(Слежка за пользователями с помощью рекламных трекеров // InternetUA (http://internetua.com/slejka-za-polzovatelyami-s-pomosxua-reklamnih-trekerov). – 2014. – 8.04).***

***

8 апреля Э. Сноуден принял участие в видеоконференции для слушаний, организованных правовым комитетом Парламентской ассамблеи Совета Европы (ПАСЕ). В ходе мероприятия он рассказал общественности об очередной программе слежения, реализуемой АНБ США. В частности, речь идет о проекте под названием Fingerprints.

Э. Сноуден утверждает, что используемое для осуществления слежки аппаратное и программное обеспечение позволило разведведомству не только собирать данные об интернет-пользователях, но и анализировать их. По его словам, АНБ следило за посетителями определенных сайтов, даже если пользователь попадал на них случайно или каким-то образом скачивал с них контент.

Помимо прочего, в ходе конференции стало известно, что спецслужбы следили и за правозащитными неправительственными организациями. Также, по словам американца, в рамках Fingerprints АНБ создавала списки и распределяла по категориям пользователей на основе нескольких параметров, в частности по их сексуальной ориентации.

«Массовое отслеживание триллионов единиц коммуникаций невинных людей является грубейшим нарушением прав человека, – передает слова Э. Сноудена The Guardian. – Если политического решения достичь не удастся, необходимо применить технические меры».

Сам Э. Сноуден заявил, что он не намеревался вредить системе национальной безопасности США, несмотря на все попытки правительства страны доказать противоположное. Более того, бывший сотрудник ЦРУ отметил, что пока власти не смогли предоставить доказательства того, что раскрытые им данные привели к гибели людей или негативным образом повлияли на национальную безопасность ***(Сноуден рассказал об очередной программе слежения АНБ США – Fingerprints // InternetUA (http://internetua.com/snouden-rasskazal-ob-ocserednoi-programme-slejeniya-anb-ssha---Fingerprints). – 2014. – 9.04).***

***

Ректорат Санкт-Петербурзького університету профспілок (СПбДУП) доручив деканатам відрахувати з ВНЗ 150 недисциплінованих студентів. Однією з причин відрахування може стати недостойна поведінка у соціальних мережах. Про це повідомляє snob.ru з посиланням на сайт університету.

Згідно з рішенням ректорату в березні – квітні 2014 р. мають бути відраховані студенти зі слабкою успішністю, які «не дотримуються дисципліни та нездатні до поведінки на рівні університетських стандартів». Ідеться про зухвалий зовнішній вигляд, використання ненормативної лексики та неналежну активність у соціальних мережах.

«Увагу буде приділено і поведінці студентів у соціальних мережах. У першу чергу – активності на форумах типу “Підслухано у СПбДУП” і т. п.», – ідеться в повідомленні на сайті.

Як пише snob.ru, в університетській групі «ВКонтакте» користувачі анонімно публікують інформацію про життя свого вишу. Тут можна знайти повідомлення про загублені речі, спортивні змагання, а також про викладачів та ректора закладу.

Декани п’яти факультетів уже підготували перший список кандидатів на відрахування, до якого включили 47 осіб. Цих студентів запрошують пройти кадрову комісію та перевестися до іншого вишу. Вже 20 студентів покинули університет, пише snob.ru.

На підтримку відрахованих студентів виступила Російська студентська спілка, назвавши такі дії ректорату посяганням на свободу думки і слова. У зв’язку з цією ситуацією спілка звернулася до прокуратури та інших відповідальних державних органів РФ ***(У російському університеті студентів відрахують за дописи у соцмережах // MediaSapiens (http://osvita.mediasapiens.ua/material/29376). – 2014. – 7.04).***

***

Оказывается, Агентство национальной безопасности США начало свою вредоносную деятельность в Интернете задолго до того, как это привлекло внимание общественности. Более того, АНБ повлияло на фундаментальные принципы (отсутствия) безопасности Интернета с самого момента создания Всемирной сети в середине 1970-х.

Американские инженеры в процессе первоначальной разработки спецификаций для стека протоколов TCP/IP планировали внедрить в него слой шифрования. В то время криптографы У. Диффи и М. Хеллман опубликовали научную работу, описав основы криптографических систем с открытым ключом. Эта технология была доступна для реализации, а конкретные алгоритмы опубликовали через несколько лет Р. Ривест, А. Шамир и Л. Адлеман (имеется в виду алгоритм RSA 1977 г.).

Спустя десятилетия стало известно, что в разведывательных службах АНБ и ЦРУ криптографические системы с открытым ключом были изобретены задолго до RSA, но эта разработка велась в условиях особой секретности.

Один из отцов-основателей Интернета В. Серф в середине 1970-х годов работал над секретным проектов АНБ в Стэнфорде, сказал он во время обсуждения в Google Hangout тотальной слежки со стороны американских спецслужб. Задача инженера состояла в разработке защищенной версии Интернета, которую спецслужбы собирались использовать в своих целях. В то время ему было запрещено делиться с коллегами наработками. Сейчас он сожалеет о сделанном: «Если бы я мог начать заново, я бы реализовал гораздо более сильную систему аутентификации и криптографии в системе», – говорит В. Серф ***(Почему в TCP/IP нет слоя шифрования // InternetUA***

(http://internetua.com/pocsemu-v-TCP-IP-net-sloya-shifrovaniya). – 2014. – 10.04).

***

ВВС США запустили новий американський розвідувальний супутник з космодрому на мисі Канаверал у Флориді

Ракета-носій Atlas-5 вивела на задану орбіту апарат, відомий як NROL-67, який, згідно з неофіційними даними, призначений для проведення космічної радіоелектронної розвідки і радіоперехоплення даних в інтересах американських спецслужб. Запуск проводила компанія United Launch Alliance.

Відзначимо, що даний старт став причиною перенесення запуску американського комерційної вантажівки SpaceX Dragon, який повинен був стартувати майже місяць тому. Спочатку старт Dragon був відкладений з технічних причин, але потім в SpaceX без оголошення причин знову перенесли запуск. Як тепер стає зрозуміло, він перетнувся зі стартовим вікном для NROL-67 і перевага була віддана останньому.

Відзначимо, що супутники серії NROL є апаратами, специфікації яких публічно не повідомляються, проте відомо, що військові супутники – шпигуни цієї серії є найбільшими і найважчими апаратами на орбіті.

На думку незалежних експертів, запущений апарат збирає дані для розвідки США, працюючи з геосинхронної орбіти. Раніше США також виводили об'єкти подібного класу і всі вони були важкими супутниками, розміщеними на орбіті заввишки 35 900 км. Передбачається, що NROL складається з мережі радіоресіверов і великої антени.

Також незалежні експерти з високою часткою ймовірності говорять про те, що після введення нового супутника до ладу, апарат буде працювати в інтересах Агентства національної безпеки США і проводити «глобальне радіоперехоплення» ***(США запустили гігантський супутник радіоперехоплення // Espreso.tv http://espreso.tv/news/2014/04/11/ssha_zapustyly_hihantskyy__suputnyk_radioperekhoplennya). – 2014. – 11.04).***

***

11 апреля Facebook опубликовала очередной отчет о правительственных запросах на раскрытие пользовательских данных за вторую половину 2013 г. В документе компания впервые предоставляет информацию о запросах на ограничения доступа или удаления контента.

Кроме того, Facebook опубликовала данные о правительственных запросах на раскрытие данных пользователей и ограничение доступа к контенту в Instagram. Тем не менее, эти данные не указываются отдельно, а входят в общее число.

Стоит отметить, что компания получает запросы на ограничение доступа или удаления содержимого в соответствии с законами государств.

Когда запрос юридически озвучен, Facebook ограничивает доступ к контенту в конкретной стране, чье правительство направляло запрос. Если компания определяет, что данный контент нарушает ее собственные стандарты, она делает его недоступным абсолютно для всех пользователей.

Согласно отчету, Facebook не всегда отвечает на запросы правительства, например, если они слишком расплывчаты, или не соответствуют правовым стандартам. Во второй половине 2013 г. компания получила 12,6 тыс. запросов. Отметим, что в предыдущем отчете за первую половину прошлого года этот показатель равнялся 11–12 тыс. Во втором полугодии Facebook удовлетворила 81 % запросов.

Лидером по количеству запросов является США, за ними следует Индия. На третьем месте расположилась Великобритания, далее – Франция и Германия ***(Facebook опубликовала очередной отчет о правительственных запросах // InternetUA (http://internetua.com/Facebook-opublikovala-ocserednoi-otcset-o-pravitelstvennih-zaprosah). – 2014. – 14.04).***

***

Украинское сообщество программистов DOU.ua попало в реестр сайтов, содержащих информацию, распространять которую в Российской Федерации запрещено.

Статья Федерального закона от 27 июля 2006 г/ № 149-ФЗ, на основании которой DOU попал в список:

Статья 15. Использование информационно-телекоммуникационных сетей

1. На территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи, настоящего Федерального закона и иных нормативных правовых актов Российской Федерации.

К моменту написания статьи сайт не открывается ни у кого из сотрудников редакции ЦП, находящихся на территории России, и мы решили обратиться за комментариями к команде DOU. Основатель проекта М. Ищенко прокомментировал ситуацию так: «Да, думаю, попробуем воспользоваться установленной процедурой и выяснить, во-первых, причину блокировки; а во-вторых – разобраться, можно ли выйти из-под запрета. По данным Google Analytics, на DOU – около 7 % пользователей из РФ, и не хочется лишать их доступа к сайту» ***(Роскомнадзор заблокировал DOU – самый крупный украинский ресурс для ИТ-специалистов // InternetUA (http://internetua.com/roskomnadzor-zablokiroval-DOU---samii-krupnii-ukrainskii-resurs-dlya-it-specialistov). – 2014. – 13.04).***

***

Apple защитит пользователей от рекламного шпионажа

Хотя Apple начала отказывать приложениям использующим уникальный идентификатор устройств (UDID) еще в феврале, данный пункт в условиях на одобрение появился только сейчас. Теперь никто другой не сможет шпионить за пользователями iOS устройств.

Напоминаем, что в январе стало известно, что американские и британские спецслужбы собирают личные данные пользователей через дыру в безопастности популярных приложений. В их числе были и сверхпопулярные Angry Birds.

Слежка за пользователями осуществлялась через встроенную в приложение рекламу.

Если вы опасаетесь за свою безопасность, то вот небольшая инструкция по тому, как ограничить рекламу:

Настройки → Приватность → Реклама → Сбросить идентификатор и ограничить трекинг рекламы

О самой уязвимости было известно с 2011 г. Точнее, тогда это никто не знал об использовании UDID для слежки. Apple открыла доступ к нему чтобы пользователи видели только интересующую их рекламу. И вот как оно все повернулось ***(Apple защитит пользователей от рекламного шпионажа // InternetUA (http://internetua.com/Apple-zasxitit-polzovatelei-ot-reklamnogo-shpionaja). – 2014. – 14.04).***

***

Есть подозреваемый в радиослежке за участниками Майдана. История вопроса

После первого разгона Евромайдана с 1 декабря в центре Киева начались серьезные проблемы со связью. Стало очевидным, что кто-то несанкционированно вмешивается в работу мобильных операторов: GPRS и CDMA-доступ в местах проведения массовых акций отсутствовал.

ИнАУ даже пришлось призвать работников офисов в центре города распаролить свои Wi-Fi точки и пододвинуть их поближе к окнам, чтобы люди могли оставаться на связи. «Воля-Кабель» увеличила пропускную способность своего интернет-канала и также призвала своих пользователей, проживающих в центре города, снять пароли на Wi-Fi.

В то же время мобильные операторы МТС и Киевстар сделали заявление о том, что никаких технических сбоев в работе их сетей нет и, скорее всего, связь в центре отсутствует из-за включения «глушилок».

Кроме того, участникам Евромайдана стали приходить смс-сообщения и даже звонки с дезинформацией и угрозами. Первые смс и звонки я, как и большинство журналистов, начала получать ночью 1 декабря 2013 г.

Вторая волна смс прошла ночью 21 января после первых столкновений на Грушевского.

Однако мобильные операторы Life, МТС и Киевстар от рассылки открестились, обвинив в ней пиратские базовые радиостанции. Компании МТС, «Астелит» и «Тримоб» обратились в Украинский государственный центр радиочастот (УГЦР) с просьбой разобраться, кто рассылает угрозы их абонентам.

Кто виноват

28 января, после проведения проверки, начальник УГЦР П. Слободянюк заявил, что на киевском Майдане действуют мобильные пираты, которые создают помехи в работе телефонных сетей. В то же время никаких устройств, способных считывать информацию про абонентов с сетей вроде IMSI – Catcher, о которых заявляли операторы, как и самих виновных, УГЦР в ходе проверки не обнаружил.

По словам П. Слободянюка, оператору life:) мешали свои же дополнительные базовые станции, «Тримобу» – видеокамера на Бессарабской площади, а кетчеры пираты сняли до начала проверки.

Оспорить результаты экспертизы было некому, так как кроме УГЦР такими вопросами в Украине больше никто не занимается, да и оборудование для прослушки есть только в этой структуре.

Наверное, все помнят, что еще до начала кровавых событий, журналистка Т. Черновол проникла в автобус, где находились сотрудники СБУ с прослушивающей аппаратурой, что они позже сами признали. Однако напрашивается вопрос, кому могло принадлежать конкретное спецсредство, с помощью которого работники спецподразделения выявляли радиоканалы управления взрывными устройствами.

Мы решили разобраться, кто же на самом деле обладает возможностью мониторить украинский радиотрафик.

Одновременно из нескольких серьёзных источников, по секрету – мы узнали о том, что на протяжении нескольких лет УГЦР совершал приобретения радиооборудования, которое используется для радиомониторинга радиосетей по всей территории Украины (как мобильных, так и стационарных объектов).

Якобы, после оплат оборудование оставалось в «собственных» фирмочках и передавалось в аутсорсинг УГЦР по завышенной цене. И возможно, именно это оборудование работало на улицах Грушевского и Институтской в ходе «зачистки» Майдана.

Всем известно, что база данных IMEI-кодов, которая позволяет идентифицировать любое радиоэлектронное устройство и отслеживать его перемещение, находится именно в УГЦР (Кстати, законодательство Украины создание таких баз данных не предусматривает). Таким образом в комплексе с оборудованием радиоконтроля, УГЦР имеет техническую возможность отслеживать любые телефонные разговоры.

Кроме того, несмотря на то что, согласно Закону Украины «О радиочастотном ресурсе Украины», УГЦР не имеет полномочий относительно измерения телекоммуникационных сетей, в структуре есть и

такое оборудование. Еще в 2011 г. глава НКРС П. Яцук распорядился передать на баланс УГЦР пять анализаторов сигнализации телекоммуникационных систем (АСТС), которые находились на балансе Государственной инспекции связи. Соответствующее решение можно найти на сайте созданной после ее расформирования НКРСИ. Однако где сейчас находится оборудование, никому неизвестно.

Не так всё просто

Мы обратились с этим вопросом в УГЦР и узнали, что его у них нет. Также нам сообщили, что УГЦР не арендует технику у других предприятий.

Из СБУ нам ответили, что пропавшие АСТС не используются частными лицами, однако где они находятся, не уточнили. Зато добавили, что с их помощью нельзя собирать конфиденциальную информацию.

Но мало этого, неожиданно мы получили неожиданное приглашение приехать и посмотреть на оборудование УГЦР собственными глазами.

Вначале мы встретились с начальником центра П. Слободянюком. Он еще раз рассказал нам, что на балансе УГЦР находится 144 мобильных и 196 стационарных станций радиоконтроля и что центр ничего не арендует у других предприятий. Кроме того, П. Слободянюк заверил нас в том, что решение о передаче на баланс УГЦР пяти АСТС было всего лишь проектом решения и оборудование по-прежнему находится в НКРСИ. Впрочем, оказалось, что у Центра радиочастот есть свои анализаторы, которые нам обещали показать.

Кроме того, П. Слободянюк пытался убедить нас в том, что ни один аппарат, который находится на балансе УГЦР, не может перехватывать контент. «Наши аппараты в принципе лишены возможности перехватывать контент. Если говорить об ользовании АСТС, то мы работаем только со служебной информацией, с номерами абонентов. Когда СБУ обращается к нам в рамках оперативно-розыскного или другого дела за получением какой-то информации в рамках закона, они эту информацию получают. Но только ту, которая у нас есть. А наше предприятие никогда не занималось изучением, хранением контента. Мы не вникаем в то, что передается. У нас нет таких возможностей, они у нас не заложены. Более того, когда мы проектируем аппаратуру, никогда не закладываем в нее возможность анализа контента. Если речь идет о радиочастотах, то для нас важны только параметры передачи: частота, ширина полосы частот, мощность, ничего другого мы не измеряем …Если нужно пообщаться с абонентом, ему звонят по обычному телефону. Но вникнуть в эту информацию мы вообще не можем. Интернет-трафик мы не контролируем».

Также П. Слободянюк убеждал нас в том, что на самом деле проверка УГЦР выявила «мобильных пиратов», которые действовали во время событий киевского Майдана.

«Во время событий на Грушевского были выявлены мешающие средства связи, эта информация есть у операторов связи. Одно из них находилось на улице Банковой. Мы эти помехи выявили и устранили. А

фантомные станции на Грушевского мы не увидели, потому что для этого нужно было поставить там постояннодействующий копмлекс радиомониторинга. Но у нас нет столько денег».

Впрочем, по словам директора УГЦР, средств хватает на ежемесячные плановые и внеплановые проверки радиостанций, выезды по заявкам операторов и регулярное внедрение современного оборудования, в чем мы не преминули убедиться.

На всех автомобилях наклейки УГЦР, однако, мы заметили и машины «без опознавательных знаков». Как рассказал нам начальник управления радиочастотного мониторинга УГЦР В. Бондарчук, они предназначены для выполнения конфиденциальных работ, например проверки своих же коллег.

На крышах мобильных станций с функцией пеленгования – антенны, рассчитанные на разные диапазоны частот.

В. Бондарчук рассказывает о работе своих подчиненных и объясняет их главные задачи.

«…Мы не радиоразведка. Все антенны одинаковые. А вот куда они подключаются – это уже другой вопрос. Мы покупаем технику только под те задачи, которые перед нами стоят. У нас даже нет средств регистрации в открытых каналах аудиосигнала. Нам запрещено иметь демодуляторы. И у нас нет арендованной техники, вполне достаточно своей в рамках выполнения плановых и внеплановых работ. Кроме этого идет пополнение в тех направлениях, где ее недостаточно».

Также В. Бонадарчук рассказал нам подробности проверки УГЦР во время киевского Майдана.

«По заявке МТС-Украина мы нашли помехи в виде двух ретрансляторов, которые устанавливались в полуподвальных помещениях на Лютеранской. Сотрудники коммерческо-промышленной фирмы «Промикс», чтобы в подвале работала сотовая связь, поставили ретранслятор. Он создавал соответствующую помеху на канале связи, снижал качество. Мы заставили фирму его зарегистрировать. А для того, чтобы поймать мобильных пиратов с Грушевского, нужно было мониторить это место 24 часа в сутки и 365 дней в году. И наша машина должна стоять за 2–3 км до базовой станции, чтобы ее услышать. Во время проверки мы осуществляли объезд, пытаясь не получить коктейль Молотова в машину, но никаких фантомных базовых станций, которые внедряются в работу действующей сети не обнаружили».

Мы спросили у специалиста, кто же может иметь полномочия и необходимое оборудование для полноценного мониторинга радиотрафика в Украине, на что он ответил, что ответа на этот вопрос не существует, однако, скорее всего, государственные органы, которые занимаются защитой информации.

Как рассказал нам заместитель начальника по вопросам телекоммуникаций УГЦР А. Кудрицкий, анализаторы ставят на сеть по просьбе операторов связи.

«Это делается для того чтобы выявить возможность рефайла. То есть операторы, с которыми мы работаем по договору, привлекают нас для того, чтобы посмотреть, кто паразитирует на их сетях. Благодаря АСТС можно определить что такой-то абонент или партнер оператора под видом национального или городского трафика отправляет трафик международный. Разницу в деньгах вы представляете».

А. Кудрицкий, убеждал нас в том, что АСТСы не позволяют анализировать передаваемый контент. «Мы работаем только с системой фиксированной связи. Ставим АСТСы только туда, куда скажет оператор. Анализ контента с их помощью невозможен. Для этого нужно другое оборудование. У нас есть соответствующие бумаги, которые подтверждают, что наше оборудование не дает возможности снятия информации с каналов связи».

На тезу о том, что для возможности анализа контента достаточно поставить дополнительную программу на оборудование, А. Кудрицкий ответил, что у них такой программы нет и если бы в УГЦР ее поставили, был бы скандал с СБУ.

Опровержение

Однако, как мы знаем, было бы желание, а возможность всегда найдется. Например, президент компании «Адамант» И. Петухов до сих пор ищет ответ на вопрос, как в ходе проверки его фирмы сотруднику УДЦР удалось прослушать корпоративную IP-телефонию.

По словам И. Петухова, проверка компаний «Адамант» и «Адамант-Телеком» началась 7 марта 2012 г. и происходила с нарушениями. Предписание было выписано не на тот адрес (причем эту ошибку НКРСИ перед этим уже допустили дважды), а в составе комиссии почему-то принимал участие инженер второй категории УГЦР В. Бреславский.

Как мы помним, сотрудники УГЦР рассказывали нам, что НКРСИ часто привлекает их технических специалистов к проведению инспекторских проверок. Однако, согласно п.6.р.6 Указа Президента о НКРСИ, комиссия может привлекать специалистов только для рассмотра вопросов, которые относятся к полномочиям НКРСИ, но не для участия в проверках.

Кроме того, АСТС, который использовал В. Бреславский, был подключен к ноутбуку с доступом в Интернет.

«Они поставили АСТС в пятницу и писали весь трафик до утра понедельника. Нашли трафик между сервером, который поставил наш клиент на колокейшен и каким-то его офисом. Прицепились к нему и что-то измеряли. Когда я сказал, что это не голосовой трафик, они включили подключенный к АСТСу ноутбук с какой-то программой. И все, кто находились рядом отчетливо услышали разговор между двумя людьми», – вспоминает И. Петухов.

Мы решили узнать немного больше о возможностях анализаторов сигнализаций телекоммуникационных систем и нашли в Интернете описание АСТС Винницкой фирмы ИнноВинн, клиентами которой является УДЦР. В

его функциях четко значится, что каждое записанное анализатором сигнальное сообщение может быть детально декодировано. Кроме того, АСТС поддерживает такие протоколы как SMS, SMS-TP, IP и GPRS/EDGE, что означает возможность совершения массовых SMS-рассылок и слежки за пользователями мобильного Интернета.

Интересно, что бы на это сказал Штирлиц? ***(Есть подозреваемый в радиослежке за участниками Майдана // InternetUA (http://internetua.com/est-podozrevaemii-v-radioslejke-za-ucsastnikami-maidana). – 2014. – 16.04).***

***

Популярных блогеров РФ обяжут регистрироваться в качестве СМИ – эту поправку профильный комитет Госдумы рекомендует к принятию. Замминистра Минкомсвязи говорит, что такой подход противоречит традиционной позиции России, в том числе в международных инстанциях, законодатели считают, что выполняют великую миссию очищения соцсетей от «мерзости».

Комитет Госдумы по информационной политике и СМИ 17 апреля одобрил поправку, которая обяжет «топ-блогеров» регистрироваться в качестве средства массовой информации. Поправку приняли единогласно – все фракции оказались едины во мнении, что соцсетям необходимо дополнительное регулирование.

…Блогеров, у которых на персональном сайте или странице в соцсетях фиксируется минимум 3000 посещений в сутки (впрочем, вероятно, в итоге критерий будет изменен на «10 тыс. подписчиков»), предлагается заносить в особый реестр. Включение в реестр налагает на автора блога обязанность проверять достоверность размещаемой им информации и указывать возрастные ограничения для пользователей. Также он будет обязан соблюдать касающиеся СМИ законы, в том числе о предвыборной агитации, противодействии экстремизму и о распространении сведений о частной жизни граждан. Включение в реестр даст блогеру право размещать рекламу за деньги и обязанность платить с нее налоги.

…Отметим, что в Уголовном кодексе России статья «Клевета» и без того существует и подобные иски к блогерам и так поступают в суды. Так, к примеру, малоизвестный московский муниципальный депутат А. Лисовенко подал недавно в суд на оппозиционного политика А. Навального за твит «Депутат-наркоман считает, что доступом в ЖЖ и Twitter может пользоваться только один человек» ***(Путин уничтожит оппозицию в соцсетях // InternetUA (http://internetua.com/putin-unicstojit-oppoziciua-v-socsetyah). – 2014. – 17.04).***

***

В настоящее время Twitter не заблокирован в Турции, но власти страны не расстались с мыслью о введении цензуры. По словам турецкого министра

связи Л. Элвана, соцсеть и страна договорились, что нежелательный контент будет «нейтрализоваться» с помощью «пикселизации».

Он не объяснил, что имеется в виду под пикселизацией, но, видимо речь идёт о том, чтобы замещать спорные изображения и тексты крупной мозаикой. Впрочем, вполне возможно, Л. Элван просто имел в виду не это, а то, что сервис будет скрывать конкретные твиты от посетителей из Турции. Если нет, то всё это выглядит достаточно безумно.

Министр сказал, что в ходе двухсторонних переговоров было достигнуто соглашение о «нейтрализации вредоносного контента» и возможности самостоятельно удалять некоторые спорные твиты. Если вы не помните, к чему это всё, то вот предыстория: сейчас в стране идёт предвыборная гонка, и нынешний премьер-министр Турции Р. Т. Эрдоган пытается всеми правдами и неправдами избежать распространения компромата на него и на правительство в целом ***(Twitter согласился «пикселизовать» твиты в Турции // InternetUA (http://internetua.com/Twitter-soglasilsya--pikselizovat--tviti-v-turcii). – 2014. – 19.04).***

***

Генеральный директор «ВКонтакте» П. Дуров рассказал о требованиях ФСБ выдать данные организаторов сообществ сторонников «Евромайдана» в Украине и увязал их с продажей собственной доли в компании. Копию требования он опубликовал на своей странице в соцсети.

По словам П. Дурова, 13 декабря 2013 г. от ФСБ пришло требование «предоставить регистрационные данные» авторов и организаторов ряда групп, названия которых связаны с «Евромайданом» и революцией на Украине. Судя по опубликованному им запросу, речь идёт о 39 сообществах.

П. Дуров заверил читателей, что «ВКонтакте» не стала выполнять требование спецслужбы. Объясняется это тем, что российская юрисдикция не распространяется на украинских пользователей соцсети.

Выдача личных данных украинцев российским властям была бы не только нарушением закона, но и предательством всех тех миллионов жителей Украины, которые нам доверились.

П. Дуров также отметил, что «в процессе» ему пришлось «пожертвовать многим», включая его собственную долю во «ВКонтакте». Он подчеркнул, что не жалеет о случившемся, так как лишившись собственности, он сохранил «нечто более важное» – чистую совесть и идеалы, которые он готов защищать.

В другой записи П. Дуров рассказал о требовании закрыть группу сторонников А. Навального, которое он также отказался выполнять. Он добавил, что не будет блокировать и «сотни других сообществ», к которым предъявляют претензии власти, несмотря на оказываемое на него давление.

Ни я, ни моя команда не собираемся осуществлять политическую цензуру. Мы не будем удалять ни антикоррупционное сообщество

А. Навального, ни сотни других сообществ, блокировки которых от нас требуют.

К записи П. Дуров прикрепил копию обращения Генпрокуратуры, связанного с сообществом «Война коррупции – поддержка Алексея Навального». В документе говорится, что эта страница призывает к участию в несогласованных акциях, из-за чего она должна быть заблокирована – как и блог Навального в LiveJornal, его страница в Facebook и аккаунт в Twitter.

Ранее о претензиях к двум последним страницам не сообщалось, а LiveJornal оппозиционера был заблокирован на территории России в середине марта.

П. Дуров уже высказывался в поддержку «Евромайдана» в начале декабря 2013 г. Тогда он напомнил, что оборудование «ВКонтакте», изъятое полугодом ранее госорганами Украины, так и не было возвращено, и пожелал успеха протестующим.

«Надеюсь, что текущие гражданские выступления в Киеве приведут к позитивным изменениям. Очевидно, что этот замечательный народ заслуживает более высокого интеллектуального и морального уровня своих правителей» ***(Дуров: я продал долю «ВКонтакте» из-за требований ФСБ раскрыть сторонников «Евромайдана» // InternetUA (http://internetua.com/durov--ya-prodal-dolua--vkontakte--iz-za-trebovanii-fsb-raskrit-storonnikov--evromaidana). – 2014. – 16.04).***

***

Мережа «ВКонтакте» перейшла під контроль друзів Путіна

Засновник російської соціальної мережі «ВКонтакте» П. Дуров більше не є генеральним директором компанії і вважає своє звільнення незаконним. Про це П. Дуров написав на своїй сторінці «ВКонтакте»

«Судячи з новин, в результаті моєї публічної відмови минулого тижня, сьогодні мене звільнили з посади генерального директора “ВКонтакте”… Таким чином, сьогодні “ВКонтакте” переходить під повний контроль І. Сечіна і А. Усманова. Напевно, в російських умовах щось подібне було неминуче, але я радий, що ми протрималися 7 з половиною років. Ми багато що встигли. І частина того, що було зроблено, вже не анулюється», – додав він.

Про звільнення П. Дурова з посади генерального директора заснованої ним соцмережі компанія заявила в понеділок, 21 квітня.

…За версією того ж Forbes, І. Сечин є ключовою фігурою у владній вертикалі президента Росій В. Путіна і є його близьким другом.

А. Усманов – бізнесмен, зоряний час якого наступив саме за правління В. Путіна. Нагороджений В. Путіним орденом «За заслуги перед вітчизною» ***(Мережа «ВКонтакте» перейшла під контроль друзів Путіна // iPress.ua (http://ipress.ua/news/merezha_vkontakte_pereyshla_pid_kontrol_druga_putina_60848.html). – 2014. – 21.04).***

Проблема захисту даних. DDOS та вірусні атаки

В сети зафиксирована активность новой версии банковского трояна ZeuS, которая распространяется в приложении для Windows-устройств с подлинной цифровой подписью. Программа содержит руткит, позволяющий злоумышленнику получить доступ к компьютеру жертвы.

Авторам вируса удалось заполучить личный ключ цифровой подписи, который принадлежит стороннему разработчику Microsoft, зарегистрированному в Швейцарии. Они использовали этот ключ для того, чтобы криптографически подписать вредоносное приложение.

Использование подлинного ключа позволяет программе обойти защиту Microsoft и других антивирусных решений.

Как утверждают ИБ-эксперты Comodo, им удалось зафиксировать по крайней мере 200 случаев инфицирования компьютеров. Для этого они использовали телеметрию, полученную от пользователей антивирусного ПО компании.

По их данным, новый вариант троянского вируса находится на веб-странице с логотипом Internet Explorer. Но на самом деле, это вредоносное приложение, которое под видом настоящего устанавливает выполняемой файл, пытающийся загрузить на компьютер жертвы руткит. Последний позволяет вирусу работать таким образом, чтобы его не могли обнаружить другие программы, в частности антивирусные ***(Банковский троян ZeuS распространяется с подлинной подписью приложения // InternetUA (http://internetua.com/bankovskii-troyan-ZeuS-rasprostranyaetsya-s-podlinnoi-podpisua-prilojeniya). – 2014. – 7.04).***

***

Китайская антивирусная компания 360 Mobile Security сообщила о распространении опасного трояна Oldboot, который располагается во встроенной флеш-памяти инфицированных Android-устройств и функционирует как буткит, запускаясь на ранней стадии загрузки операционной системы. Это позволяет ему минимизировать возможность своего удаления без вмешательства в структуру файловой системы. Специалисты утверждают, что упомянутое вредоносное ПО активно на миллионах «гуглофонов» по всему миру и является самым продвинутым в истории троянским приложением для Android-платформы.

Для распространения троянца создатели «зловреда» используют нестандартный метод, размещая один из компонентов программы в загрузочном разделе файловой системы и соответствующим образом изменив скрипт, отвечающий за последовательность активации компонентов ОС.

При включении устройства скрипт инициирует работу троянской библиотеки, которая в процессе своей работы извлекает файлы libgooglekernel.so и GoogleKernel.apk и помещает их в каталоги /system/lib и /system/app соответственно. Таким образом, часть троянца Android.Oldboot

устанавливается в систему как обычное Android-приложение и в дальнейшем функционирует в качестве системного сервиса, подключаясь к удаленному серверу и получая от него различные команды – в том числе, для установки или удаления определённых приложений.

Специалисты говорят, что Oldboot.B Android Bootkit может незаметно загружать вредоносные программы, внедрять инфицированные модули в системные процессы, блокировать удаление троянских приложений, менять стартовую страницу в браузере, отправлять SMS-сообщения на платные номера, удалять и отключать установленное в системе антивирусное ПО. Вредонос способен также выполнять код, скрытый в графических файлах – эта техника известна как стеганография.

Опасность Oldboot.B Android Bootkit заключается в том, что даже в случае успешного удаления элементов вредоносного приложения, которые были проинсталлированы после включения мобильного устройства, находящийся в защищённом разделе флеш-памяти компонент при последующей перезагрузке вновь осуществит их установку, тем самым повторно инфицировав операционную систему.

Чтобы не стать жертвой этой и других аналогичных вредоносных программ, 360 Mobile Security рекомендует не приобретать Android-устройства сомнительного происхождения и не загружать приложения из источников, отличных от официального магазина Google Play. Хотя и в последнем эксперты нередко обнаруживают вирусы и вредоносное ПО ***(Самый продвинутый Android-троян заразил миллионы устройств по всему миру // InternetUA (http://internetua.com/samii-prodvinutii-Android-troyan-zarazil-millioni-ustroistv-po-vsemu-miru). – 2014. – 7.04).***

***

Хакеры используют популярное приложение Tinder для распространения вредоносных программ среди его пользователей. Для этого злоумышленники используют ботов и методы социальной инженерии.

Поисковые программы завлекают пользователей заманчивыми профилями и изображениями из фотостудии Аризоны, сообщает охранная фирма BitDefender. Некоторые из этих изображений были также похищены для поддельных профилей Facebook.

После того как пользователи нажимают на Tinder, показывая, что им нравится профиль, боты начинают привлекать внимание пользователей автоматизированными разговорами, пока не убеждают их перейти по сомнительной ссылке. Название URL производит впечатление официальной страницы приложения знакомств.

Афера направлена на британских пользователей, которых заманивают на фиктивную ссылку якобы опросами и сомнительными конкурсами на ваучеры ASDA и Tesco, в то время как пользователям Tinder в США предлагают скачать игру Castle Clash.

Tinder является мобильным приложением на основе определения местоположения для iOS и Android, которое использует информацию Facebook, чтобы соответствовать пользователям. Исследователи безопасности под названием Appthority, выразили волнение по поводу приватности игроков, использующих приложение, из-за которого произошла утечка большого количества информации ***(Хакеры используют популярное приложение Tinder для распространения вредоносных программ // InternetUA (http://internetua.com/hakeri-ispolzuuat-populyarnoe-prilojenie-Tinder-dlya-rasprostraneniya-vredonosnih-programm). – 2014. – 8.04).***

***

Как следует из сообщения исследователей безопасности из Internet Storm Center, они зафиксировали вредоносную спам-кампанию, ориентированную на пользователей мобильных устройств на базе Android.

«Первое сообщение подобного рода я получил еще в феврале этого года, – пишет эксперт Д. Клаузинг. – Однако первый образец от пользователей мы получили лишь в начале этой недели».

По его словам, эти сообщения, как правило, содержат очень мало текста и сравнительно короткий URL-адрес. При этом большинство писем рассылаются через ящики электронной почты Yahoo!, которые, по всей видимости, были скомпрометированы хакерами в январе этого года.

Д. Клаузинг также отмечает, что открытие ссылки пользователем операционных систем Linux, Windows или Mac не грозит ничем, кроме открытия страницы с надоедливой рекламой. В то же время владельцы Android-устройств рискуют не только посетить рекламируемый злоумышленниками портал, но и инфицировать систему вирусным приложением «DroidNotCompatible» ***(Вирус для Android распространяется через электронные письма со ссылками // InternetUA (http://internetua.com/virus-dlya-Android-rasprostranyaetsya-cserez-elektronnie-pisma-so-ssilkami). – 2014. – 8.04).***

***

Как сообщают «Комментарии», сайт Генпрокуратуры Украины (gp.gov.ua) подвергся хакерской атаке, в ходе которой злоумышленники удалили все сообщения и новости после 5 апреля.

Однако при переходе на любую из новостей на главной странице Генпрокуратуры, сайт выдает сообщение «Страницу не найдено».

Прочие разделы сайт работают в прежнем режиме ***(Хакеры взломали сайт генпрокуратуры // proIT (http://proit.com.ua/news/internet/2014/04/09/155752.html). – 2014. – 9.04).***

***

Генеральная прокуратура оперативно ликвидировала последствия хакерской атаки на свой официальный сайт. Об этом сообщается на

официальном сайте Генпрокуратуры Украины, передает корреспондент proIT.

«9 апреля 2014 был зафиксирован факт мощной, заранее подготовленной хакерской атаки на официальный веб-портал Генеральной прокуратуры Украины, в результате которой было временно нарушено его нормальную работ», – сообщает Генпрокуратура.

Так, в течение короткого времени работниками соответствующего подразделения Генеральной прокуратуры работа сайта была восстановлена в полном объеме. Кроме того, как подчеркивает Генпрокуратура, приняты все меры по предотвращению его повторного поражения.

Генпрокуратура установила, что данная хакерская атака была направлена на официальный портал Генеральной прокуратуры Украины, но угрозы нарушения целостности других информационных систем не произошло.

В настоящее время проводится проверка по факту несанкционированного вмешательства в работу компьютерной сети и установления лиц, причастных к нему ***(Сайт генпрокуратуры возобновил работу после хакерской атаки // proIT (http://proit.com.ua/news/internet/2014/04/10/134241.html). – 2014. – 10.04).***

***

Невідомі зламали сайт чернігівської прокуратури, який міститься за адресою: chrg.gp.gov.ua/ua/guidance.html.

Натомість, замість сайту прокуратури Чернігівської області «вилазить» сторінка «ВКонтакте» «АнтиМайдан», де люди активно підтримують позицію Росії ***(«Зламали» сайт чернігівської прокуратури. Тепер там «Антимайдан» // Чернігівщина: події і коментарі (http://pik.cn.ua/print/9004/). – 2014. – 9.04).***

***

Кибервойна между Россией и Украиной продолжается. За прошедший месяц проукраинским хакерским группировкам удалось совершить ряд успешных атак на российские ресурсы. В частности, они взломали сайт Госдумы России, серверы крупнейших российских IT-компаний и вестник российской пропаганды телеканал Russia Today. Кроме того, утекли в сеть адреса электронной почты сотрудников Минобороны и Минэкономразвития РФ, а сотни сайтов российских компаний и региональных госструктур были взломаны. AIN.UA отобрал пятерку самых резонансных взломов за последние несколько недель (http://ain.ua/2014/04/11/519557).

Самой успешной на сегодня атакой проукраинских хакеров можно считать взлом сайта Госдумы России. Вечером 9 апреля взломщики разместили антироссийское обращение на странице Комитета Госдумы России по региональной политике и проблемам Севера и Дальнего Востока от имени члена Компартии РФ Н. Харитонова. В обращении речь идет о том,

что вся мощь империи, называемой Российская Федерация, полностью базируется на алкоголизме, страхе и трусости, а заканчивается сообщение призывом «Слава Украине!».

Еще один крупный успех – взлом российской компании SearchInform датированный 11 марта 2014 г. Хакеры назвали SearchInform «топ-лидером российского IT-рынка» и опубликовали тысячи внутренних документов, логины и пароли доступа к серверам клиентов компании, среди которых – крупнейшие российские организации, такие как «Велес капитал», «Русал», «Газпром», «Сухой» и многие другие.

В ночь на четверг, 6 марта, группа хакеров сообщила об удачной атаке на серверы ОАО «Рособоронэкспорт». В своем сообщении они заявили, что намерены «объявить кибервойну российским военным предприятиям». В тот же день на одном из анонимных файлообменников были опубликованы тысячи документов различной степени секретности. По словам хакеров, им удалось инфицировать системы компаний «Сухой», «Оборонпром», «Газфлот», «РУСАЛ» и многих других.

17 марта хакеры опубликовали данные русского промышленного инвестиционного фонда. По словам взломщиков, фонд является одной из крупнейших российских организаций по привлечению инвестиций. В сеть попала информация о бизнес-операциях организации, а также о теневой деятельности фонда.

В ночь на воскресенье, 2 марта, хакеры взломали сайт телеканала Russia Today и добавили слово Nazi (нацист, нацистский) к заголовкам всех англоязычных материалов. Об этом написало российское издание Lenta.ru. В результате взлома заголовки стали выглядеть, например, так: «Российские сенаторы проголосовали за отправку стабилизационных нацистских войск на украинскую территорию» или «Путин: Нацистские граждане и войска подвергаются угрозе на Украине и нуждаются в защите вооруженных сил».

16 марта хакеры «положили» сайт крымского референдума.

Помимо вышеупомянутых атак, хакеры объявили операцию «Покращення» и создали группу в социальных сетях, где идет публичное обсуждение атак на российские ресурсы. Результаты действий хакеров публикуются на сайте «Бімба». Среди множества сообщений о взломах можно найти вот такие результаты:

Взломана база данных сайта корпоративного управления в России;

Взломана база данных сервера поиска работы на государственной службе;

Взломана база данных сайта российской ассоциации маркетинговых услуг (РАМУ);

Выложены в сеть e-mail адреса сотрудников Федеральной службы РФ по контролю за оборотом наркотиков, чиновников Еврейской автономной области, Министерства обороны РФ, Центрального банка РФ и Минэкономразвития РФ.

Помимо российских ресурсов, хакеры успешно атаковали сайт Главного управления юстиции в Одесской области, выложили в Интернет базу почтовых адресов и паролей сотрудников «Эпицентра» к корпоративному сайту, личные данные бойцов Беркута и телефоны депутатов-регионалов.

Напомним, что недавно, во время слушаний в Конгрессе США, американский адмирал М. Роджерс подтвердил, что, впридачу к военному вторжению в Крым, Россия ведет против Украины кибервойну. Этого же мнения придерживается исполнительный директор по кибербезопасности в Bae System Д. Гарфилд. По данным чиновников США, Россия уже нанесла серию кибератак по украинским сетям коммуникаций в рамках кампании по интервенции в Крым ***(Самые громкие атаки проукраинских хакеров на российские веб-ресурсы // AIN.UA (http://ain.ua/2014/04/11/519557). – 2014. – 11.04).***

***

Хакери зламали сторінку депутата Держдуми Російської Федерації, голови транспортного комітету, Є. Москвічева.

На його сторінці, розміщеній на сайті Держдуми, було опубліковано текст, у якому він висловив жаль із приводу тупості одного зі своїх колег по Думі – М. Харитонова. А також закликав усіх сказати «Ні! божевільним чекістам, які ведуть Росію в прірву».

Наразі текст із сайту зник, але він встиг потрапити до веб-архіва.

«Уважаемые коллеги, единомышленники!

Председатель Комитета по транспорту Москвичев Евгений Сергеевич

Я глубоко разочарован трусостью нашего коллеги Николая Харитонова из комитета по региональной политике и проблемам севера и дальнего востока, который разместив резкое, и вместе с тем глубоко верное заявление относительно ситуации в стране, в последний момент струсил и отказался от своих слов, свалив все на мифических “хакеров”.

В тяжелый для Родины час, мы депутаты Государственной Думы Российской Федерации, осознавая лежащую на нас ответственность перед россиянами, должны сказать решительное “Нет!” обезумевшим чекистам, которые ведут Россию в пропасть. Мы должны немедленно вернуть наши вооруженные силы домой, и остановить агрессию по отношению к братской Украине.

Слава Украине!»

Евгений МОСКВИЧЕВ, Председатель Комитета ***(Українські хакери продовжують знущатись над депутатами російської Держдуми // UkrainianWatcher (http://watcher.com.ua/2014/04/15/ukrayinski-hakery-prodovzhuyut-znuschatys-nad-deputatamy-rosiyskoyi-derzhdumy/). – 2014. – 15.04).***

***

18-річний програміст із Греції стверджує, що зміг зламати додаток на iPhone, який дає можливість замінити паперовий квиток спеціальним QR-кодом, який висвічується на екрані смартфона.

Злом додатку Apple Passbook дав змогу студенту без проблем подорожувати літаками провідних авіакомпаній світу абсолютно безкоштовно.

Своїм «досягненням» справжнісінький «кібернетичний заєць» поділиться на спеціальній конференції хакерів. Слід зазначити, що західні компанії дуже цінують таких спеціалістів та пропонують їм офіційну роботу в команді з розробки охоронних програм і систем безпеки ***(Студент-хакер літає «зайцем» по всьому світу завдяки злому додатку для iPhone // InternetUA (http://internetua.com/student-haker-l-ta---zaicem--po-vsomu-sv-tu-zavdyaki-zlomu-dodatku-dlya-iPhone). – 2014. – 9.04).***

***

Фахівці радять користувачам Інтернету змінити паролі на форумах та інших сайтах. Особливо це слід зробити в електронних банківських мережах.

Під загрозою опинилися електронні пошти та сторінки в соціальних мережах. Їх можуть поцупити в законних власників. Причиною тому стала масштабну помилка в шифруванні сторінок. Про неї повідомили майже всі інтернет-гіганти. Серед них Google, Facebook та Yahoo.

Уразливість давала змогу хакерам викрадати персональні дані та паролі. У найгіршому випадку – навіть дані платіжних карт, що прив’язані до профілю.

Однак, як пише ТСН, простим користувачам спеціалісти радять не панікувати. Нині більшість помилок уже виправили, а саму систему захисту – оновили. Утім, людям усе ж радять змінити старі паролі. Бо їх зловмисники могли викрасти раніше ***(Користувачам Мережі радять змінити свої паролі // Паралелі (http://paralleli.if.ua/news/41531.html). – 2014. – 10.04).***

***

По данным «Лаборатории Касперского», количество компьютерных атак, целью которых была кража денег в 2013 г., – возросло на 27,6 %.

По оценкам «Лаборатории Касперского» общее количество подобных атак составило 28,4 млн случаев. В компании сообщают, что, как и в 2012 г., в 2013 г. самым популярным способом кражи денег были банковские «трояны», на их долю пришлось две трети случаев мошенничества. При этом аналитики отмечают снижение количества случаев кражи денег таким способом. В 2013 г. наблюдается значительный всплеск вредоносного программного обеспечения и мобильных приложений нацеленные на криптовалюты, в частности, на Bitcoin.

Аналитики «Лаборатории Касперского» также отмечают рост мошеннических мобильных приложений, которые нацелены на кражу

информации о клиенте и денег с банковских счетов. Эксперты говорят, что за год типология подобных программ увеличилась почти в 20 раз. Основная масса таких вредоносных мобильных приложений приходится на мобильные устройства, на которых установлена операционная система Android.

Руководитель отдела технического позиционирования «Лаборатории Касперского» В. Заполянский сообщил, что новые вредоносные программы и мобильные приложения появляются ежемесячно. Он также обратился к финансовым организациям с призывом более тщательно подходить к вопросам защиты информации о своих клиентах ***(Количество компьютерных атак с целью кражи денег выросло почти на треть // InternetUA (http://internetua.com/kolicsestvo-kompuaternih-atak-s-celua-kraji-deneg-viroslo-pocsti-na-tret). – 2014. – 10.04).***

***

В скором времени Android станет более безопасной платформой. Компания Google готовится к запуску сервиса, который будет периодически проверять установленные на смартфонах и планшетах приложения на наличие вредоносного кода.

В настоящее время приложения сканируются только во время установки. Антивирусная база нового сервиса будет постоянно пополняться, поэтому он сможет отлавливать даже тот вредоносный код, который не был распознан при первоначальной проверке.

Как сообщает Google, сервис проверки приложений при установке был использован в общей сложности более четырех миллиардов раз, и лишь в 0,18 % случаев пользователи, увидевшие уведомление о вредоносном коде, продолжили установку опасной программы. Источники большей части приложений с вирусами – пиратские сайты, однако в 99,9 % случаев пользователи предпочитают устанавливать игры и приложения из Play Маркета, а в них вредоносного кода почти нет ***(Android научится регулярно сканировать установленные приложения // InternetUA (http://internetua.com/Android-naucsitsya-regulyarno-skanirovat-ustanovlennie-prilojeniya). – 2014. – 11.04).***

***

Киберпреступники занялись разработкой вредоносного программного обеспечения, использующего гибкие возможности командной строки PowerShell, реализованной Microsoft в Windows. При помощи Windows PowerShell преступники надеются пройти мимо установленного антивирусного программного обеспечения. Напомним, что Windows PowerShell представляет собой командную оболочку и скриптовую среду одновременно, которые созданы для автоматизации системных задач и приложений с административными заданиями. Изначально PowerShell появилась начиная с Windows 7, однако позже Microsoft выпустила PowerShell и для более ранних Windows, начиная с XP.

Антивирусные лабораториии Symantec и TrendMicro независимо друг от друга сообщили об обнаружении вредоносного кода, имеющего несколько слоев обфускации и способного встраивать вредносный код в системный файл rundll32.exe. Код может прятаться в структуре rundll32 и работать одновременно как бэкдор и как троянец.

При запуске вредоносный скрипт компилирует и исполняет вредоносный код, который встраивается на лету. Скомпилированный код встраивается в rundll32 как системный процесс, что значительно усложняет процесс детектирования. Хакерский код в системном файле также подключается к удаленному серверу и ожидает инструкций от него, которые в будущем исполняются в скрытом режиме.

В Trend Micro говорят, что код также использует модуль Power Worm, работающий с PowerShell. Заражение вредоносом происходит через специально сконструированные Word- и Excel-файлы, которые исполняются во время открытия. После открытия первичный код посредством анонимного прокси Polipo подгружаются дополнительные элементы ***(Новый вредоносный код использует PowerShell и Rundll32 // InternetUA (http://internetua.com/novii-vredonosnii-kod-ispolzuet-PowerShell-i-Rundll32). – 2014. – 10.04).***

***

Организациям предстоит улучшить их методы обнаружения вторжений.

В своем докладе FireEye рассказывает о новых тактиках, используемых для кражи данных. В нем также упоминается о возникающих глобальных угрозах, их возможных мотивах, а также целях.

Время, необходимое для обнаружения вторжения, продолжает уменьшаться

Количество времени, в течение которого хакеры присутствовали в сетях жертвы незамеченными, уменьшилось с 243 дней в 2012 г. до 229 дней в 2013 г. Максимальное количество времени, на протяжении которого злоумышленник присутствовал в сети перед тем, как быть обнаруженным, в 2013 г. составило шесть лет и три месяца.

Организациям предстоит улучшить их методы обнаружения вторжений

В 2012 г. 37 % организаций обнаружили нарушения собственными силами; этот показатель сократился всего до 33 % в 2013 г.

Фишинговые электронные письма играют на доверии к ИТ-подразделениям атакуемых компаний

44 % фишинговых писем были замаскированы под уведомления ИТ-отделений атакуемых хакерами организаций. Большинство таких писем рассылалось по вторникам, средам и четвергам.

Межнациональные политические конфликты способствуют появлению инцидентов информационной безопасности

За прошедший год аналитики Mandiant зафиксировали рост количества инцидентов, вызванных межнациональными политическими конфликтами, затронувшими частный сектор. В частности, они ссылаются на инциденты, связанные с Сирийской электронной армией (СЭА), которая взломала внешние веб-сайты и учетные записи частных организаций в социальных сетях с целью выражения своей политической позиции ***(Киберпреступники могут оставаться незамеченными в течение 229 дней // InternetUA (http://internetua.com/kiberprestupniki-mogut-ostavatsya-nezamecsennimi-v-tecsenie-229-dnei). – 2014. – 12.04).***

***

Миндоходов предупреждает о вирусах, которые рассылаются с поддельных почтовых адресов

В конце марта была зафиксирована новая волна рассылки с поддельных почтовых адресов Миндоходов электронных писем с вредоносным программным обеспечением. Файлы, отправляемые в приложении, имеют форматы «.doc», «.rar», «.zip», пр. и содержат эксплойты для программного обеспечения Microsoft Office. После их открытия (в случае обновления вышеупомянутого программного обеспечения) происходит поражение средств вычислительной техники вредным программным обеспечением. Об этом сообщает IT Expert со ссылкой на пресс-службу Миндоходов.

В ведомстве подчеркивают, что этот вирус позволяет получать несанкционированный отдаленный доступ к компьютерной технике, следить за ней и использовать для осуществления сетевых атак. Все пораженные средства вычислительной техники могут принадлежать к бот-сети.

В случае получения подобных писем пользователям необходимо осуществить блокировку доступа к доменным именам, которые сейчас используются для функционирования бот-сети: nof.su, ohi.su, ohy.su, tknsk.su.

Кроме того, получатели писем должны срочно сообщить об этом Государственную службу специальной связи и защиты информации Украины по адресу cert@cert.gov.ua и отправить образцы вредоносного программного обеспечения.

Для этого их необходимо отдельно хранить в архиве с паролем. Выбор пароля остается на усмотрение отправителя, поскольку известны пароли, такие как «infected», «virus» и другие могут распознаваться почтовыми системами, в результате чего потенциально вредоносный файл, содержащийся в архиве, будут удалены.

В Миндоходов подчеркивают, что объектами массового поражения стали не только компьютеры государственных органов или учреждений, но и граждан Украины ***(Миндоходов предупреждает о вирусах, которые рассылаются с поддельных почтовых адресов // InternetUA (http://internetua.com/mindohodov-preduprejdaet-o-virusah--kotorie-rassilauatsya-s-poddelnih-pocstovih-adresov). – 2014. – 12.04).***

***

В начале года в Украине зафиксирована активность кибермошенников, использующих технологию кредитовых слипов. При этом деньги мошенники воруют со счетов компаний, обслуживающихся в зарубежных банках, а обналичивание этих средств организовано через счета платёжных карт украинских эмитентов.

Специфика такой технологии заключается в имитации операций возврата средств в рамках правил международных платёжных систем. Но на счету получателя средств (в нашем случае клиента украинского банка) после факта обналичивания, как правило, возникает несанкционированный овердрафт на всю сумму.

В нашем случае речь идёт о суммах от 1200 до 3000 дол. США. Для обналичивания украденных средств мошенники в меньшей мере пытаются открывать картсчета по поддельным паспортам, а чаще всего уговаривают доверчивых граждан оформить платёжные карты и передать их вместе с атрибутами счетов. Как правило, предлагая символическое вознаграждение (100–200 грн).

Последствия, которые наступают для лиц, добровольно передавших мошенникам свои платёжные карты и атрибуты счетов, гораздо серьезнее, чем это может показаться на первый взгляд. Такие граждане становятся не только соучастниками международного преступления, но и получают статус «нежелательных персон» в тех странах, банки которых пострадали от действий кибермошенников. То есть в получении визы таким гражданам будет отказано. А за всю сумму несанкционированного овердрафта придется отвечать перед своим банком как за просроченную задолженность и по довольно высоким, – прокомментировал эксперт проекта Независимой ассоциации банков Украины (НАБУ) «Противодействие киберпреступности» в банковской сфере С. Досенко.

Учитывая вышесказанное, настоятельно рекомендуем:

– не оформлять какие-либо банковские продукты в интересах третьих лиц;

– не передавать третьим лицам платёжные карты, доступ к персональным аккаунтам в системах интернет-банкинга и персональном электронном кошельке;

– при подозрительных обращениях лиц, предлагающих такие действия, безотлагательно сообщать милиции и представителям банка, в котором Вы обслуживаетесь;

– по факту утери или кражи карты незамедлительно информировать банк по максимально оперативным каналам (телефоны горячих линий, электронная почта), блокировать карту, используя возможности Интернета или мобильного банкинга, а впоследствии оформить её перевыпуск ***(В Украине зафиксирована активность кибермошенников, использующих технологию кредитовых слипов // InternetUA (http://internetua.com/v-***

ukraine-zafiksirovana-aktivnost-kibermoshennikov--ispolzuuasxih-tehnologiua-kreditovih-slipov). – 2014. – 13.04).

***

После прекращения 8 апреля официальной поддержки Windows XP со стороны Microsoft, хакеры атаковали устаревшую операционную систему, информируют «Экономические известия» (http://news.eizvestia.com/news_technology/full/628-hakery-massovo-atakuyut-polzovatelej-windows-xp).

Злоумышленники зачастую играют на слабой информированности пользователей, заполнив сеть обманными предложениями обновить саму Windows XP или ее отдельные компоненты, такие как Windows Media Player.

При этом наглость злоумышленников достигла апогея – за скачивание зловредных программ они требуют деньги. Доверчивый пользователь, добровольно установив обманные обновления, рискует потерять свои персональные данные, такие как пароли и номера кредиток, а также получить разнообразные рекламные баннеры прямо на рабочий стол, а в некоторых случаях и предложение отправить SMS на короткий номер для разблокирования работы компьютера.

В целом, случилось то, о чем настойчиво предупреждали специалисты, предупреждая пользователей о необходимости перехода на новую операционную систему.

Напомним, что компания Microsoft активно агитировала пользователей перейти на более современные версии Windows, а также предлагала широкий спектр бонусов ***(Хакеры массово атакуют пользователей Windows XP // «Экономические известия» (http://news.eizvestia.com/news_technology/full/628-hakery-massovo-atakuyut-polzovatelej-windows-xp). – 2014. – 15.04).***

***

Heartbleed Bug – три четверти Интернета в опасности

Словосочетание Heartbleed Bug изначально имеет под собой глубоко технические корни, но так уж случилось, что о нем за последнюю неделю рассказывали и в сводках новостей на телевидении, на радио и, конечно же, в Интернете. Почему? Дело в том, что под Heartbleed Bug с прошлой недели стали понимать критически опасный баг, выявленный в крайне популярном программном обеспечении для интернет-шифрования OpenSSL.

Критические баги сами по себе довольно опасны, так как зачастую позволяют скомпрометировать не только данные, находящиеся под управлением уязвимой программы, но и другие сведения в ОС, а когда популярность уязвимой программы таковы, что она используется на 75 % веб-серверов в сети, то картину без преувеличения можно назвать катастрофической. Хуже того, библиотеки OpenSSL используются в сетевом оборудовании таких компаний, как Cisco или Juniper, что ставит под удар

множество корпоративных защищенных сетей, вдобавок к этому, многие мобильные программы для защиты данных и целостности байт-кода подписывают SSL-сертификатами. В Интернете коммерческая подпись SSL-сертификатов – это также прибыльный бизнес, который теперь оказывается под ударом из-за необходимости отзыва почти миллиона сертификатов.

История вопроса

О Heartbleed Bug стало известно еще 14 апреля, тогда как 15 апреля разработчики OpenSSL уже выпустили исправление для библиотеки OpenSSL, которая допускала возможность реализации атаки. С 15 апреля многие серверные операционные системы начали предлагать пользователям возможность обновления программного обеспечения. Однако и здесь не все так просто. OpenSSL – это клиент-серверная система. Она работает так: на сервере генерируются цифровые ключи, которые при подключении передаются клиенту и хранятся на нем (могут очень долго – более года). Проблема была выявлена в механизме генерации ключей и самих ключах. Поэтому если сервер обновляет программное обеспечение, то клиент все равно остается уязвим, так как у него остались старые ключи. Эти ключи нужно вручную удались или отозвать, после чего создать для клиента новые и работать уже через них.

Если учесть, что далеко не все пользователи понимают термин «отзыв цифрового сертификата», а еше меньшее количество понимает, как это сделать, а пользуются сертификатами почти все, то масштаб проблемы становится более или менее очевиден даже для неспециалиста. Хуже того, в некотором оборудовании, например в сетевых маршрутизаторах, SSL-ключи часто вшиваются в программное обеспечение устройства и отозвать их можно только с обновлением программной прошивки в целом.

Так, компании Cisco Systems и Juniper Networks на неделе заявили, что «некоторые» из устройств содержат в себе Heartbleed Bug. Это означает, что потенциальный атакующий имеет техническую возможность перехватывать имена пользователей, пароли и закрытую информацию, проходящую в корпоративных сетях. Крупные операторы связи и поставщики интернет-сервисов, такие как Google, Yahoo, Facebook и Amazon еще 15 апреля сообщили об обновлении их библиотек OpenSSL на серверах. Однако в Cisco и Juniper говорят, что в их случае баг лежит в аппаратном обеспечении и здесь так просто от бага не получится избавиться. Более того, значительная часть оборудования корпоративное, поэтому здесь не получится просто взять и выключить сеть до модернизации оборудования.

Производители говорят, что многие из сетевых устройств, в частности домашние роутеры или маршрутизаторы, которые пользователи купят уже после анонса о Heartbleed Bug, также будут содержать в себе данный баг, ведь выпущены они были раньше публичного раскрытия данных. Дополнительная опасность здесь кроется в том, что защититься от бага не получится ни в случае установки межсетевого экрана, но даже через VPN-сеть.

В Cisco сообщили, что начали процесс обновления программного обеспечения 17 апреля, в Juniper признали, что не смогут его начать раньше следующей недели. Именно поэтому в Juniper пока не разглашают список уязвимых продуктов.

Что делать пользователям?

Что нужно знать обычному пользователю о Heartbleed Bug? Знать нужно следующее: данный баг затрагивает значительную часть Интернета и разом его исправить не получится, поэтому в ближайшие дни (а может и недели) пользователям требуется особая осторожность при передаче данных в сети. На сегодня ИТ-специалисты расходятся во мнениях относительно того, насколько распространенным баг может быть. Также специалисты говорят, что уязвимый компонент OpenSSL присутствовал в программе по меньшей мере два года, а потому «знающие люди» им вполне могли уже давно пользоваться.

В антивирусной компании Sophos не склонны драматизировать ситуацию. По словам Ч. Висниевски, технического консультанта Sophos, данный баг представляет собой традиционый критический баг, которые ранее обнаруживались и в Windows и Linux и других системах, однако в случае с SSL опасность в большей степени кроется именно в громадной пользовательской аудитории бага.

В пресс-службах компаний Google, Yahoo и Facebook признали, что их серверы тоже использовали уязвимый софт, а потому (теоретически) пользователи их систем могли быть под ударом. Однако все указанные компании говорят, что в настоящее время у них системные крипто-библиотеки были обновлены. В Facebook говорят, что обновили OpenSSL еще до публичного анонса, так как задействованы в разработке указаной библиотеки.

Специалисты по ИТ-безопасности дают пользователям в общем-то стандартные рекомендации: обратиться к поставщику услуги и уточнить данные о сертификатах по Heartbleed Bug, по возможности сменить все пароли и не использовать один и тот же пароль для множества аккаунтов.

На сегодня независимые разработчики уже разместили в Интернете ряд программ, которые позволяют установить, работаете ли вы с целевым ресурсом, который обновил библиотеку или же еще нет. Инструменты доступны по адресу: http://filippo.io/Heartbleed/ или https://www.ssllabs.com/ или https://addons.mozilla.org/en-US/firefox/addon/heartbleed-checker/.

Кроме того, в Университете Мичигана в США была разработана система, использующая популярный софтверный сканер ZMap для выявления хостов, подверженных Heartbleed Bug. Он позволяет во время сканирования выявлять наличие на сервере криптографической библиотеки OpenSSL 1.0.1, пытаясь установить защищенное соединение и по заголовкам ответа определяя версии софта.

Публично о баге Heartbleed Bug стало известно 9 апреля. Тогда же в Мичигане провели первое сканирование с ZMap и опубликовали

неутешительные итоги: минимум треть из сайтов, входящих в Alexa Top 1 Million подвержены багу по протоколоу TLS, еще 11 % по HTTPS, 27 % по Heartbeat Extension, тогда как 61 % не используют элементы Heartbeat или уже обновились до безопасной версии. При этом разработчики сканера по понятным причинам пока не приводят полный список уязвимых хостов. Более подробные данные обещаны на предстоящей неделе.

В анонимной беседе авторы говорят, что среди уязвимых сайтов есть социальные сети, сервисы хранения данных, а также проект Twitpic.com, применяемый для фото-шаринга через Twitter, несколько альтернативных Android-маркетов и сетей онлайн-рекламы.

По оценке Sophos, на полную ликвидацию последствий бага может уйти год, который потребуется на обновление системных прошивок, клиентских библиотек и другого софта.

Цунами сертификатов еще предстоит отозвать

Аналитическая компания Netcraft сегодня опубликовала собственные статистические данные, согласно которым в сети более 500 тыс. SSL-сертификатов, затронутых Heartbleed Bug, однако из этого количества только 30 тыс. сертификатов были перевыпущены, еще меньше были отозваны. Новые сертификаты уже были выпущены для таких проектов, как Yahoo, Adobe, CloudFlare, DuckDuckGo,GitHub, Reddit, Launchpad, PayPal, Netflix и Amazon CloudFront. При этом, в Netcraft говорят, что сегодня в веб-среде не отмечается какого-то повышенного темпа отзыва серитификатов. В среднем в сети ежесуточно обновляется по 30 тыс. сертификатов, поэтому пока нельзя говорить о массовом отзыве сертификатов и их обновлении.

При этом организаторы проекта http://heartbleed.com/, посвященного багу, говорят, технически следовало бы отозваать все ранее выпущенные сертификаты, в том числе и те, что применяются для защиты электронной почты, IM-клиентов и некоторых VPN-сетей. Также на сайте heartbleed.com содержится подробное техническое описание бага.

В Netcraft отмечают, что даже если сам пользователь отозвал сертификаты и получил новые от сервера, с которым работает, он технически может быть все равно подвержен атаке, так как нет никакой гарантии, аналогичные процедуры провел администратор сети, из которой пользователь выходит в Интернет (если его соединение изначально защищено).

АНБ?

18 апреля Bloomberg News опубликовало анонимные данные со ссылкой на некие источники, близкие к Агентству национальной безопасности США. Эти источники утверждают, что американская разведка знала о наличии бага в OpenSSL и активно им пользовалась «по меньшей мере два года», то есть с момента его появления. На фоне этого возникает резонный вопрос о причастности АНБ к реализации бага, так как ранее ведомство уже попадалось на искусственном встраивании багов в криптографические алгоритмы, в частности в RSA.

Источники в АНБ также говорят, что heartbleed использовался для получения логинов и паролей пользователей целевых сайтов и перехвата данных. Bloomberg отмечает, что если данные сведения верны, то АНБ потенциально могло иметь доступ к данным сотен миллионов людей по всему миру.

С другой стороны, независимые эксперты говорят, что если АНБ действительно знало о баге, то в его же интересах было его как можно скорее закрыть, так как при помощи SSL защищались многие американские правительственные ресурсы. На фоне постоянно звучавших заявлений Вашингтона о китаской хакерской угрозы, искусственная поддержка багов выглядит несколько нелогичной.

В Управлении по связям с общественностью АНБ опровергли информацию Bloomberg, заявив, что ведомство не имело информации о баге в SSL и ознакомилось с этой информацией только тогда, когда об этом было публично объявлено ***(Heartbleed Bug – три четверти интернета в опасности // InternetUA (http://internetua.com/Heartbleed-Bug---tri-csetverti-interneta-v-opasnosti). – 2014. – 14.04).***

***

Как выяснили исследователи безопасности, находящийся в распоряжении компании Yahoo!, интернет-сервис Flickr, предназначенный для распространения и публикации фотографий, содержит несколько опасных уязвимостей. Эксперты обнаружили возможность удаленного выполнения произвольного кода, а также SQL-инъекции. Под ударом оказались базы данных и серверы веб-ресурса.

Обнаруживший бреши египетский специалист И. Раафат выявил несколько SQL-инъекций в приложении Flickr Photo Books, которое впервые было представлено администрацией ресурса всего пять месяцев назад.

По словам исследователя, уязвимыми являются два параметра (page_id и items), которые подвержены воздействию так называемых слепых инъекций. Еще один параметр (order_id) уязвим к прямым SQL-инъекциям. Успешная эксплуатация этих брешей позволяет похитить пароль администратора MySQL, а также получить доступ к базам данных.

Более того, уязвимости в Flickr способствуют выполнению злоумышленником произвольного кода на сервере – при помощи функции load_file(/etc/passwd) И. Раафат раскрыл содержание конфиденциальных файлов, хранящихся на сайте.

При этом исследователь смог разместить на сервере собственные файлы, запускающие программный код. В настоящее время Yahoo! уже устранила бреши ***(В Flickr обнаружили уязвимость, позволяющую удаленное выполнение кода // InternetUA (http://internetua.com/v-Flickr-obnarujili-uyazvimost--pozvolyauasxuua-udalennoe-vipolnenie-koda). – 2014. – 16.04).***

***

Android-приложение «Фонарик» отслеживало координаты 50 млн пользователей

Даже по стандартам низкого качества бесплатных Android-приложений, которые норовят показать рекламу и собрать информацию о пользователе, программе Brightest Flashlight удалось сделать нечто экстраординарное. Приложение «Самый яркий фонарик», которое установили минимум 50 млн пользователей Android, не просто отслеживало координаты пользователей почти в реальном времени, но еще и продавало эту информацию рекламным сетям и другим покупателям. Автор программы нагло обманывал миллионы пользователей.

Это не ускользнуло от внимания Федеральной торговой комиссии (FTC), которая оформила жалобу и предложила урегулировать ситуацию разработчику – американской компании GoldenShores Technologies, состоящей из одного человека Э. Гейдла. Комиссионеры FTC подробно описали, каким образом Brightest Flashlight в обманных целях использовало настройки приватности при установке приложения.

В настоящее время условия сделки согласованы – и их трудно назвать справедливым наказанием для Э. Гейдла. Он обязан в течение 10 дней удалить всю собранную информацию, а в течение будущих 10 лет информировать FTC о своих новых предпринимательских инициативах. По сути, разработчик отделался легким испугом: ни штрафа, ни возврата нечестно заработанных денег, ни какого-нибудь более сурового наказания. Можно шпионить за 50 млн пользователей – и не выплатить ни цента в качестве штрафа.

FTC предупреждало, что не планирует взыскивать компенсацию, потому что приложение распространялось бесплатно. Но все равно мягкость приговора обескураживает. Мошеннику разрешили оставить себе прибыль от продажи базы данных, собранной нечестным путем. FTC даже не опубликовала названия фирм, которые покупали информацию ***(Android-приложение «Фонарик» отслеживало координаты 50 млн пользователей // InternetUA (http://internetua.com/Android-prilojenie--fonarik--otslejivalo-koordinati-50-mln-polzovatelei). – 2014. – 16.04).***

***

Немецким специалистам по кибербезопасности из группы Security Research Labs (SRLabs) удалось взломать сканер отпечатков пальцев, встроенный в новый смартфон Samsung Galaxy S5. Видео с описанием технологии взлома Touch ID 15 апреля было опубликовано на YouTube-странице SRLabs.

Как следует из видеролика, обмануть сканер можно при помощи известной и весьма распространенной технологии подделки отпечатков пальцев. Достаточно сделать фотографию отпечатка в хорошем разрешении,

отредактировать изображение на компьютере, а затем распечатать на пленке. После этого пленку необходимо покрыть тонким слоем столярного клея.

Приложив вырезанный из такой пленки отпечаток к Touch ID смартфона, любой злоумышленник без проблем разблокирует его и получит доступ ко всей хранящейся на нем информации.

«Хакерам» из SRLabs удалось использовать поддельный отпечаток не только для разблокировки телефона, но и для работы с несколькими его приложениями. Например, фейковый отпечаток позволяет совершать покупки и денежные переводы в приложении PayPal.

При этом даже несколько неудачных попыток не приведут к блокировке телефона или выведению на экран требования ввести пароль – перезагружая гаджет, можно пытаться взломать сканер отпечатков пальцев сколько угодно раз.

Осенью 2013 г. точно такой же метод использовался для взлома Touch ID на вышедшей тогда модели телефона Apple iPhone 5s. То, что спустя более полугода Samsung не учла неудачный опыт своих конкурентов, вызвало у членов Security Research Labs особое удивление.

О взломе сканера стало известно спустя четыре дня с момента выхода нового флагманского телефона Samsung. Продажи Galaxy S5 в России стартовали 11 апреля. Представители корейской компании на момент написания этой заметки пока никак не прокомментировали появившуюся в сети информацию об уязвимости сканера ***(Сканер Samsung Galaxy S5 взломали при помощи фотографий отпечатков пальцев // InternetUA (http://internetua.com/skaner-Samsung-Galaxy-S5-vzlomali-pri-pomosxi-fotografii-otpecsatkov-palcev). – 2014. – 16.04).***

***

«Облачный» сервис Mail.ru содержит вредоносные приложения, способные нанести непоправимый вред информации, которая хранится на пользовательских компьютерах. Об этом говорится в сообщении компании «Доктор Веб», разрабатывающей антивирусные решения.

Эксперты отмечают, что популярный среди интернет-пользователей сервис Mail.ru для хранения файлов в «облаке» привлекает внимание злоумышленников и становится местом для размещения и распространения вредоносных программ. По данным «Доктор Веб», в настоящее время на ресурсе доступны для скачивания сразу несколько опасных троянцев, которые детектируются антивирусом как Trojan.Encoder.102, Trojan.Encoder.427, Trojan.Encoder.432 и Trojan.Encoder.438.

Эти вирусные приложения после попадания на компьютер шифруют информацию, делая ее нечитаемой, после чего требуют «выкуп» за возврат файлов в прежнее состояние. Модификация Trojan.Encoder.102 является самой опасной, поскольку содержит алгоритм кодирования, практически не поддающийся расшифровке. Кроме того, для файлов размером более двух гигабайт такое шифрование может оказаться губительным, поскольку

алгоритм шифрования содержит ошибки, приводящие к повреждению данных.

Каким образом вредоносные программы попадают на пользовательские компьютеры, неизвестно.

«Специалисты компании “Доктор Веб”, начиная с 8 апреля, неоднократно обращались в службу технической поддержки и службу безопасности Mail.ru с просьбой удалить опасный контент, – говорится в сообщении антивирусного разработчика. – Однако файлы, размещенные в облачном сервисе Mail.ru в период с 11 января по 19 февраля 2014 г., все еще доступны и могут нанести вред пользователям».

Вредоносный контент, размещенный пользователями, уже удален, заявили представители Mail.ru. «Сегодня мы запускаем проверку всех загружаемых в хранилище файлов, а в ближайшее время будет проверено 100 процентов всех загруженных ранее файлов», – подчеркнули в компании ***(Сервис Mail.ru обвинили в распространении вирусов // InternetUA (http://internetua.com/servis-Mail-ru-obvinili-v-rasprostranenii-virusov). – 2014. – 16.04).***

***

Вредоносные программы, созданные злоумышленниками с целью обогащения за счет демонстрации пользователям Интернета назойливой рекламы, имеют чрезвычайно широкое распространение, однако до недавнего времени они досаждали, в основном, пользователям ОС Windows. Именно поэтому несколько троянцев, исследование которых недавно провели вирусные аналитики компании «Доктор Веб», выглядят весьма необычно на фоне других аналогичных приложений, поскольку заражают компьютеры, работающие под управлением Mac OS X.

Несколько пользователей Mac OS X опубликовали на официальном форуме компании Apple жалобы на навязчивую рекламу, которая демонстрируется в окне браузеров Safari и Google Chrome при просмотре различных веб-ресурсов. Источником проблем оказались вредоносные надстройки (плагины), которые устанавливаются в систему при посещении определенных сайтов. Плагины распространяются в комплекте с легитимными приложениями, способными выполнять на компьютере некоторые полезные функции.

Одна из таких программ носит наименование Downlite и распространяется с сайта популярного торрент-трекера: нажав на кнопку Download, пользователь перенаправляется на другой интернет-ресурс, с которого загружается само приложение, при этом перенаправление осуществляется таргетированно: пользователям Apple-совместимых компьютеров отдается файл StartDownload_oREeab.dmg – установщик Downlite, пользователи других операционных систем могут быть перенаправлены на иные сайты. После загрузки файла начинается установка приложения Downlite.app.

Данный установщик (Антивирус Dr.Web идентифицирует его как Trojan.Downlite.1) обладает любопытной особенностью: он устанавливает легитимное приложение DlLite.app и несколько надстроек к браузеру, при этом в процессе установки запрашивается пароль пользователя Mac OS X, и, если он является администратором системы, приложения устанавливаются в корневую папку. Для работы DlLite.app на компьютере требуется наличие Java, однако вредоносные плагины написаны на языке Objective-C и благополучно запускаются при открытии окна браузера. Также в систему устанавливается приложение dev.Jack, предназначенное для контроля над браузерами Mozilla Firefox, Google Chrome, Safari и детектируемое антивирусным ПО Dr.Web как Trojan.Downlite.2.

Кроме того, рекламные плагины распространяются вместе с другими приложениями (MacVideoTunes, MediaCenter_XBMC, Popcorn-Time, VideoPlayer_MPlayerX). Одним из таких приложений является, например, MoviePlayer (MacVideoTunes): на первом этапе его установки пользователю предлагается запустить программу-инсталлятор без цифровой подписи:

Затем – установить некий «оптимизатор», при этом пользователь лишен возможности сбросить соответствующий флажок, чтобы отказаться от инсталляции приложения. Данный установщик, детектируемый Антивирусом Dr.Web как Trojan.Vsearch.8, с точки зрения своего функционала очень похож на Trojan.Downlite.1, однако вместо программы dev.Jack он дополнительно устанавливает на компьютер приложение takeOverSearchAssetsMac.app (Trojan.Conduit.1).

Во всех упомянутых случаях установщик осуществляет инсталляцию в систему полезной нагрузки, реализованной в виде файлов VSearchAgent.app, VSearchLoader.bundle, VSearchPlugIn.bundle, libVSearchLoader.dylib и VSInstallerHelper ***(Новые Мас-вредоносы показывают рекламу // InternetUA (http://internetua.com/novie-Mac-vredonosi-pokazivauat-reklamu). – 2014. – 17.04).***

***

Компания «Доктор Веб» зафиксировала массовое распространение нежелательных СМС-сообщений, которые содержали ссылку на загрузку Android-троянца Android.SmsBot.75.origin, предназначенного для кражи конфиденциальных данных у южнокорейских пользователей, а также незаметной отправки СМС. За несколько дней злоумышленники произвели около 40 спам-рассылок, а общее число пострадавших владельцев мобильных Android-устройств может составить несколько десятков тысяч человек.

Зафиксированные специалистами компании «Доктор Веб» спам-сообщения информировали потенциальных жертв о якобы неполученном почтовом отправлении, о статусе которого можно было узнать, перейдя по предоставленной в тексте короткой ссылке. В случае перехода по указанному веб-адресу пользователь перенаправлялся на страницу мошеннического блога, размещенного на платформе Blogger от корпорации Google и

оформленного так, чтобы создать ложное впечатление его принадлежности к службе курьерской почтовой доставки. При попытке ознакомиться с предлагаемой информацией на мобильное устройство жертвы загружался троянец Android.SmsBot.75.origin, размещенный в облачном хранилище Dropbox, где у киберпреступников имелась специальная учетная запись.

Таким образом, данная спам-кампания практически ничем не отличается от множества других подобных, организованных в Южной Корее, однако по своим масштабам она является одной из самых крупных за последнее время. Так, злоумышленники произвели почти 40 спам-рассылок, а также задействовали как минимум пять различных вариантов блогов, содержащих ссылки, которые вели на загрузку трех модификаций Android.SmsBot.75.origin.

В свою очередь, согласно открытой статистике, имеющейся на одной из этих страниц, число посетивших ее потенциальных жертв за несколько дней составило более 30 тыс. Учитывая общее количество использованных мошеннических блогов, конечное число пострадавших пользователей может во много раз превышать эту цифру.

Чтобы не вызывать лишних подозрений, после своего запуска Android.SmsBot.75.origin обращается к сайту реально существующей почтово-транспортной компании и загружает его в режиме WebView, т. е. отображает в качестве веб-приложения. Одновременно с этим происходит удаление значка вредоносной программы с главного экрана мобильного устройства и активизация троянского сервиса MainService, который незаметно выполняет всю вредоносную деятельность. В частности, троянец загружает информацию из телефонной книги на удаленный сервер и затем в постоянном режиме ожидает от него поступления команды, в которой будут указаны параметры для отправки СМС-сообщения, – номер получателя и текст. Кроме того, вредоносная программа создает список номеров, звонки и СМС с которых не будут видны пользователю. Таким образом, Android.SmsBot.75.origin может быть использован не только как шпион или СМС-троянец, но и как средство кражи денежных средств из систем мобильного банкинга.

Помимо упомянутой спам-кампании, Android.SmsBot.75.origin уже распространялся злоумышленниками с применением и других нежелательных смс-рассылок, в которых он выдавался за некое уведомление, поступившее из полиции, поэтому не исключено, что в будущем мошенники предпримут новые попытки атак на пользователей ***(Десятки тысяч пользователей могли стать жертвами Android-троянца // InternetUA (http://internetua.com/desyatki-tisyacs-polzovatelei-mogli-stat-jertvami-Android-troyanca). – 2014. – 18.04).***

***

Как сообщают исследователи безопасности из Cyber Forensics Research & Education Group (UNHcFREG), пользователи приложения WhatsApp,

использующие его функцию Location Share, находятся под угрозой компрометации со стороны хакеров.

Это связано с тем, что в программе присутствует уязвимость, позволяющая похитить информацию о местоположении владельца мобильного устройства, сообщает издание The Hacker News.

«Основная проблема состоит в том, что прикрепленные к изображениям геолокационные данные хранятся в незашифрованном виде, что оставляет эту информацию открытой для перехвата», – поясняют специалисты. По их словам, потенциальному злоумышленнику достаточно провести любую из множества существующих сегодня MitM-атак. И даже если для среднестатистического хакера сложность эксплуатации этой бреши весьма высока, то для таких спецслужб, как АНБ, она не представляет особой сложности.

В настоящее время разработчики WhatsApp работают над выпуском соответствующего исправления ***(WhatsApp позволяет раскрыть местоположение пользователя // InternetUA (http://internetua.com/WhatsApp-pozvolyaet-raskrit-mestopolojenie-polzovatelya). – 2014. – 18.04).***

***

Akamai выпустила новый отчет о количестве совершенных DDoS-атак, который показывает, что в I квартале этого года злоумышленники меньше полагались на традиционный ботнет. Вместо этого они использовали технику отражения и усиления. При помощи обновленных инструментов для DDoS можно совершать атаки на протоколы для Интернета, которые доступны на открытых или уязвимых серверах и устройствах.

Наиболее часто атакам подвергаются служба стека протоколов TCP/IP (CHARGEN), протоколы NTP и системы доменных имен (DNS). Эти протоколы, основанные на UDP, позволяют злоумышленникам скрыть свою личность. Кроме того, атаки могут стать причиной утери и распространения личных данных.

Новые инструменты отражения и усиления атаки могут нанести большой вред пользователю. В I квартале количество кибератак увеличилось до 39 %. Одним из самых крупных киберинцидентов стала DDoS-атака на Prolexic. В ходе нее для генерации пикового трафика более чем 200 Gbps (гигабит в секунду) и 53,5 млн пакетов в секундубыли использованы несколько методов отражения в сочетании с традиционным ботнетом. В этом квартале также произошло большое количество кибератак на СМИ и ресурсы индустрии развлечений (54 %).

Инновации на рынке DDoS-атак стали возможными благодаря наличию простых в использовании DDoS-инструментов. Эти инструменты были созданы хакерами, чтобы создать большую мощность и удобство для взлома ***(Хакеры используют технику отражения и усиления для совершения***

DDoS-атак // InternetUA (http://internetua.com/hakeri-ispolzuuat-tehniku-otrajeniya-i-usileniya-dlya-soversheniya-DDoS-atak). – 2014. – 19.04).

***

Новый руткит-вариант банковского трояна Zeus распространяется под видом электронных писем от Starbucks. Как сообщает «Лаборатория Касперского», в сообщениях речь идет о том, что некий друг жертвы приобрел в одном из заведений сети напиток, и решил устроить небольшой праздник. Для того чтобы просмотреть «особенное меню и узнать адрес и точное время, когда можно прийти и отметить этот день с другом», пользователям предлагается открыть вложение.

Чтобы письма выглядели максимально легитимно, злоумышленники добавили в них логотип компании, а сами письма рассылались с пометкой «Очень важно» (High importance).

Тем не менее, они допустили несколько ошибок, благодаря которым опытные пользователи смогут с легкостью понять, что письма поддельные. По данным экспертов компании, в ходе вредоносной кампании были использованы адреса на Gmail и Yahoo.

«Киберпреступники не удосужились замаскировать его (ред. – вложение) в архиве или при помощи двойного расширения названия файла. Кажется, они были уверены в том, что счастливый получатель сразу откроет вложение безо всякого подозрения», – отметила в блоге «ЛК» М. Вергелис.

По данным специалистов компании, адреса, с которых отправлялись вредоносные письма, генерировались случайным образом, «к примеру, incubationg46@, mendaciousker0@ и пр.».

Известно, что вирус может устанавливать на компьютеры жертв руткит Necurs, который не позволяет антивирусным решениям фиксировать деятельность вредоносного ПО ***(Новый вариант Zeus распространяют под видом писем от Starbucks // InternetUA (http://internetua.com/novii-variant-Zeus-rasprostranyauat-pod-vidom-pisem-ot-Starbucks). – 2014. – 19.04).***

***

За последние три месяца количество мобильных банковских вирусов-«троянцев» увеличилось почти вдвое. И основная их часть писалась под платформу Android.

При этом спам вырвался вперед, на первом месте среди мобильных «зловредов» оказались рекламные модули, транслирующие навязчивую рекламу, а долгое время лидирующие SMS-«троянцы» сместились на второе место – их доля уменьшилась с 34 до 22 %.

Таковы данные «Лаборатории Касперского».

Выяснилось, что активно в Интернете действуют и вирусы-шпионы. В I квартале эксперты компании обнаружили новое поколение бэкдоров Icefog – на этот раз Java-версию зловреда, получившую название Javafog.

Жертвами новой атаки стали три организации, находящиеся в США, причем одной из них оказалась крупная международная нефтегазовая компания. Еще более важной находкой стало обнаружение масштабной кампании кибершпионажа «Маска», целями которой были государственные учреждения, посольства, исследовательские институты и другие компании в 31 стране мира.

Воруют и криптовалюту, заражая компьютеры пользователей, чтобы за счет дополнительных ресурсов генерировать больше небезызвестных биткоинов. По этому принципу действует, например, Trojan.Win32.Agent.aduro, который занимает 12-е место в рейтинге наиболее часто обнаруживаем объектов в Интернете по результатам I квартала 2014 г.

Интересна и еще одна тенденция этого года: резкий рост числа пользователей Tor – программы, обеспечивающей анонимную работу в интернете. Tor не только стал решением для защиты от кражи персональных данных, но и снискал большую популярность среди киберпреступников, которым особенно выгодна анонимность.

Например, в феврале эксперты «Лаборатории Касперского» обнаружили первый Android-троянец, который использует в качестве командного центра домен в псевдо-зоне .onion ***(Количество мобильных банковских вирусов увеличилось почти вдвое // InternetUA (http://internetua.com/kolicsestvo-mobilnih-bankovskih-virusov-uvelicsilos-pocsti-vdvoe). – 2014. – 19.04).***

***

Хакеры крадут данные Apple ID

Вместе с джейлбрейком ідевайсов пользователи должны полностью осознавать необходимость тщательного отбора устанавливаемых твиков. На этой неделе пользователями Reddit была обнаружена специальная библиотека Unfold.dylib, которая предназначена для мониторинга трафика по защищенному протоколу SSL.

Из этих соединений злоумышленники извлекают данные и пароли идентификаторов Apple ID. Установка дополнительной библиотеки, входящей в состав MobileSubstrate происходит вместе с твиком Unfold.

Пока нет никакой точной информации о том, кто ответственен за разработку этого вредоносного кода, но некоторые специалисты предполагают, что за его созданием могут стоять китайские специалисты.

Если вы устанавливали твик Unfold, то обязательно удалите его и библиотеку Unfold.dylib ***(Хакеры крадут данные Apple ID // InternetUA (http://internetua.com/hakeri-kradut-dannie-Apple-ID). – 2014. – 19.04).***

***

Российские хакеры осуществили самое большое в истории США кибернападение. Нападение на мировую платежную систему привело к краже более 950 тыс. карт и потерь сотен миллионов долларов.

Житель России В. Дринкман обвиняется в причастности к группе российских хакеров и участии в компьютерном взломе десятка крупных американских и международных корпораций и краже номеров 160 млн кредитных и дебетовых карт. Незаконная деятельность преступников длилась на протяжении семи лет. 28 июня 2012 г. злоумышленник был арестован и находился под стражей в Нидерландах. Теперь США и Россия требуют выдать им преступника. В свою очередь Роттердамский суд в Нидерландах постановил, что одновременные запросы из США и России о выдаче им российского хакера являются допустимыми, поскольку он обвиняется в причастности к краже самого большого объема данных в истории США, сообщает издание Bloomberg ***(Российские хакеры осуществили самое большое в истории США кибернападение // InternetUA (http://internetua.com/rossiiskie-hakeri-osusxestvili-samoe-bolshoe-v-istorii-ssha-kibernapadenie). – 2014. – 21.04).***

***

Участники последнего экономического форума в Давосе среди глобальных опасностей для мировой экономики поставили киберугрозы на третье место. По прогнозам экспертов, через полтора года они поднимутся на ступеньку выше и займут второе место. Эти опасения подтверждаются данными специалистов Symantec. У компании есть своя система отслеживания киберугроз Global Intelligence Network Symantec, которая действует в 157 странах. Она состоит из более чем 40 тыс. датчиков, которые регистрируют тысячи событий в секунду в режиме онлайн.

Рост утечек информации в Интернете в 2013 г. составил 62 % по сравнению с 2012 г. Было похищено более 552 млн записей. Киберпреступность превращается в серьезную угрозу как для рядовых пользователей, так и для бизнеса. Такие выводы опубликовала компания Symantec в своем ежегодном отчете.

Одна из последних тенденций – стремительный рост активности хакеров в сфере мобильных устройств. По данным специалистов Symantec, в прошлом году атаки киберпреступников испытали на себе 38 % пользователей смартфонов. При этом половина хозяев умных телефонов не предпринимает никаких мер для защиты своих гаджетов.

Статистика не радует. Лишь 56 % пользователей мобильных устройств (включая планшеты) сразу удаляют письма от неизвестных отправителей. Среди пользователей ПК таковых 90 %. Лишь на трети гаджетов установлены хотя бы простейшие базовые антивирусные программы.

«Естественно, и качество и количество вредоносного программного обеспечения, направленного на мобильные устройства будет расти, – утверждает главный научный сотрудник Symantec Security Response К. Вёст. – А ПО, обеспечивающее безопасность, пока не совершенно. Оно, конечно, будет улучшаться. Но также очень важен и человеческий фактор. Люди должны осознать важность использования защитных программ. Конечно,

если поставить сканер, который будет сканировать каждые пять минут, он будет тратить ресурсы. Но он такой и не нужен. Для большинства устройств защита нужна, прежде всего, в тот момент, когда вы загружаете какое-то приложение или файл из интернета. Это не должно занимать большое количество времени и энергии».

Возможно, еще большую угрозу безопасности данных несет развитие «Интернета вещей». Бытовые электронные устройства в массовом порядке «умнеют» и подключаются к сети. Но при этом большинство из них не оснащены никакими системами безопасности. А ведь даже подключенная к Интернету зубная щетка (что скоро, видимо, станет нормой) может стать для хакера черным ходом, удобной лазейкой для доступа к вашему компьютеру, личным данным и банковской информации.

Минувший год специалисты компании назвали годом «Мега-утечек». Поведение киберпреступников меняется. Все чаще это не разрозненные хакеры-одиночки, а организованные группировки, которые тщательно разрабатывают и готовят свои акции. Ущерб от таких действий в десятки раз больше, чем от мелких атак.

Вполне возможно, что некоторые хакерские группировки действуют при поддержке правительственных структур разных стран. Кэндид Вёст не исключает, что в ближайшем будущем политические и экономические конфликты будут решаться боевыми действиями в киберпространстве.

«У спецслужб китайских, американских, российских и других государств есть такие возможности, – считает главный научный сотрудник Symantec Security Response. – Мы отслеживаем целевые нападения. Но определить, совершает их независимая группировка, поддерживает ли ее правительство или это вообще государственные структуры действуют, очень тяжело, а иногда и невозможно. В будущем вопрос контроля над киберпространством будет играть очень важную роль. Прежде всего в плане информационных войн и пропаганды, конечно. Информация является очень мощным средством, которое способно коренным образом изменить ситуацию в стране. «Арабская весна» и события в других странах тому подтверждение».

Кстати, серьезность опасности интернет-угроз подтверждает также появление нового вида страховых услуг. Многие крупные западные компании уже разрабатывают тарифы страхования ущерба, причиненного киберпреступниками ***(Зубная щетка как инструмент хакера // InternetUA (http://internetua.com/zubnaya-sxetka-kak-instrument-hakera). – 2014. – 21.04).***

***

Троянское приложение для Android-устройств iBanking научили обходить двухфакторную авторизацию на основе кодов подтверждений, сообщают специалисты антивирусной компании ESET. Будучи установленным на устройство, «зловред» может шпионить за пользователем, фиксируя его активность, перехватывать входящие и исходящие SMS-

сообщения, перенаправлять голосовые вызовы и даже записывать звук с помощью микрофона устройства.

По данным экспертов ESET, на одном из подпольных форумов произошла утечка исходного кода этой вредоносной программы в свободный доступ. Утечка этих данных, среди которых находились исходные тексты панели управления ботами, а также сам билдер, может помочь злоумышленникам переориентировать iBanking на другие цели. Из-за попадания исходных текстов в свободный доступ, злоумышленники стали использовать мобильный троян более активно.

На основе исходных кодов хакеры разработали новый тип веб-инъекций и мобильный бот, который устанавливается с ее помощью. Веб-инъекция использует JavaScript для компрометации веб-страницы социальной сети Facebook. Она позволяет злоумышленникам заманить ничего не подозревающего владельца Android-аппарата на страницу установки вредоносной программы.

Как только пользователь входит в свой аккаунт Facebook, вредоносный код пытается внедрить вышеприведенный скрипт на веб-страницу, что приводит к появлению специального окна. После того как пользователь введет свой номер телефона, он перенаправляется на следующую страницу (в случае выбора ОС Android в меню). Если sms-сообщение со ссылкой не было доставлено мобильному устройству пользователя, он также может использовать прямую ссылку для скачивания, либо воспользоваться инструкцией по установке ***(Шпионские трояны для Android научились обходить двухфакторную авторизацию // InternetUA (http://internetua.com/shpionskie-troyani-dlya-Android-naucsilis-obhodit-dvuhfaktornuua-avtorizaciua). – 2014. – 21.04).***

***

Пользователи Reddit обнаружили вредоносное ПО для iOS-устройств, на которых был осуществлен джейлбрейк. Вирус, получивший название Unflod Baby Panda, направлен на похищение пользовательских данных. В четверг, 17 апреля, пользователи устройств от Apple с джейлбрейком столкнулись с необычной активностью, приводившей к аварийному закрытию таких приложений как Snapchat и Google Hangouts.

Эксперты немецкой ИБ-компании SektionEins обнаружили на зараженных устройствах неизвестный файл Unfold.dylib. По их словам, вредонос похищает пароли и Apple ID пользователей в то время, как они заходят на интернет-ресурсы, использующие SSL-шифрование, и отправляет их на китайские сайты.

Исследователи сообщили, что похищенная информация направляется на сервер с IP-адресом 23.88.10.4, который, предположительно, контролируется лицами из Китая. В пользу этого говорит тот факт, что цифровой сертификат подписан именем разработчика B. Синь.

Владельцы инфицированных устройств считают, что для того чтобы удалить вредоносное ПО, достаточно удалить файл Unfold.dylib и изменить Apple ID. Тем не менее, пока неизвестно, не устанавливает ли Unflod Baby Panda какие-либо дополнительные вредоносные программы. В связи с этим эксперты утверждают, что по-настоящему надежным способом избавиться от вируса является полное восстановление iOS-устройства, то есть, полный отказ от джейлбрейка.

Жертвами Unflod Baby Panda являются 32-битные iOS-устройства (например, iPhone 5), на которых был осуществлен джейлбрейк. Вредонос не затрагивает 64-битные iPhone 5S, iPad Air и iPad Mini с дисплеем Retina.

Как удалить вредоносно ПО:

1. Загрузить из Cydia приложение iFile и проверить устройство на наличие вирусов.

2. Зайти в /Library/MobileSubstrate/DynamicLibraries/.

3. Наличие файлов Unflod.dylib или Unflod.plist, или/и framework.plist или framework.dylib свидетельствует о заражении устройства Unflod Baby Panda.

4. С помощью iFile удалить вредоносные файлы.

5. Перезагрузить устройство и сменить Apple ID ***(Обнаружена вредоносная кампания, направленная на iOS-устройства с джейлбрейком // InternetUA (http://internetua.com/obnarujena-vredonosnaya-kampaniya--napravlennaya-na-iOS-ustroistva-s-djeilbreikom). – 2014. – 21.04).***