# СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

*Огляд інтернет-ресурсів*
*(1–15.03)*

**2015 № 5**

# Соціальні мережі
## як чинник інформаційної безпеки

**Інформаційно-аналітичний бюлетень**
**Додаток до журналу «Україна: події, факти, коментарі»**
Огляд інтернет-ресурсів
(1–15.03)
№ 5

**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 2015

**ЗМІСТ**

## РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Компанія Gemius Україна представила дані щодо 20 найбільш популярних сайтів українського Інтернету за охопленням за січень 2015 р. У першій трійці й далі продовжують залишатися Google та російські Mail.Ru і «ВКонтакте». Facebook збільшує розрив від «Одноклассники».

У січні підвищили свої позиції сайти електронної комерції: інтернет-магазин Rozetka піднявся з 12 на 10 місце, OLX також піднявся на дві позиції – 11 місце, а Prom.ua розмістився на 13 місці.


Згідно з даними gemiusAudience, розмір ПК інтернет-аудиторії в січні 2014 р. – 18 млн осіб (real users, 14+) ***(Facebook збільшує розрив від Одноклассників (дослідження Gemius) // UkrainianWatcher (http://watcher.com.ua/2015/03/03/facebook-zbilshuye-rozryv-vid-odnoklasnykiv-doslidzhennya-gemius/). – 2015. – 3.03).***

***

Компания Google выпустила обновленную версию приложения YouTube Creator. В нем появилась возможность вырезать из видео несущественные фрагменты.

Инструмент редактирования появляется непосредственно перед загрузкой записи. На раскадровке синим прямоугольником выделен фрагмент, который можно вырезать. Редактирование очень точное – буквально покадровое. Полученный результат можно посмотреть прямо в приложении.

По сведениям сайта Android Police, в будущем в этом приложении появятся видеофильтры в духе Instagram и возможность добавлять в видео музыку со свободным копирайтом ***(Видео для YouTube теперь можно редактировать на смартфоне // InternetUA (http://internetua.com/video-dlya-YouTube-teper-mojno-redaktirovat-na-smartfone). – 2015. – 2.03).***

***

Современные мобильные приложения меняют способ потребления новостей во всем мире, пишет Marketing Media Review (http://mmr.ua/news/id/whatsapp-stal-sredstvom-massovoj-informacii-43475/).

Среди интернет-пользователей Испании, Италии и Бразилии возросла популярность WhatsApp как источника новостей. Но для таких развитых рынков, как США, Франция и Великобритания подобное поведение все еще редкость.

В среднем один из двадцати пользователей хотя бы единожды запускал WhatsApp для того, чтобы ознакомиться с новостями. К такому выводу пришли аналитики Reuters после опроса почти 20 тыс. человек в 2014 г. Вероятно, в текущем году эта цифра превысит 6 %, предположили в BI Intelligence.

На тех рынках, где WhatsApp популярен, он «затмевает» собой Facebook, а не только традиционные источники новостей. На глобальном сайте популярной испанской футбольной команды «Валенсия» на кнопку WhatsApp нажимал каждый третий посетитель. Посетители интернет-страницы могли выбирать среди четырех встроенных приложений, причем WhatsApp появился недавно. Из всего числа обращений к сайту «Валенсии» 48 % сгенерировали указанные четыре кнопки, причем WhatsApp опередил Facebook.

В BI Intelligence собрали свидетельства, что подобное поведение распространяется и в США. Вначале 2015 г. на спортивном сайте FTW посетители чаще нажимали кнопку «поделиться» в WhatsApp, чем Twitter ***(WhatsApp стал средством массовой информации // Marketing Media Review (http://mmr.ua/news/id/whatsapp-stal-sredstvom-massovoj-informacii-43475/). – 2015. – 4.03).***

***

Заработал децентрализованный сервис для анонимных микроблогов Twister

Twister – это платформа для p2p-микроблоггинга, разработанная на базе протоколов Bitcoin и BitTorrent. В частности, речь идёт о технологиях

Bitcoin Block Chain, Bittorrent DHT и Bittorrent Swarm, пишет Блог Imena.UA (http://www.imena.ua/blog/twister-secure-web/).

Помимо использования децентрализованных протоколов, которые исключают возможность цензуры и слежки, Twister не предусматривает запись и передачу IP-адресов пользователей, что подразумевает анонимность общения.

Разработчик сервиса – программист М. Фрейтас – считает, что микроблоги играют важную роль в различных акциях протеста. Политика информационной безопасности государств не предполагает сохранение анонимности пользователей, так что власти наблюдают за гражданами, фактически, осуществляя цензуру в Интернете.

В свою очередь, децентрализованный p2p-микроблог сделает выдачу информации о пользователях невозможной, потому что не существует центрального сервера, где хранятся такие данные ***(Заработал децентрализованный сервис для анонимных микроблогов Twister // Блог Imena.UA (http://www.imena.ua/blog/twister-secure-web/). – 2015. – 2.03).***

***

Twitter анонсировал первый официальный плагин для WordPress, который даст ресурсам простой доступ к функционалу сервиса микроблогов.

Плагин дает издателям WordPress следующие возможности:

– создание Twitter Cards – карточки с картинками и заголовками могут автоматически генерироваться для каждой страницы сайта;

– кастомизация оформления встроенных твитов (включая цвет ссылок и границ);

– возможность напрямую встроить Twitter-видео на страницы;

– добавление кнопки «твитнуть» к постам с возможностью кастомизации;

– добавление кнопки «Подписаться» на каждую страницу ресурса;

– привязка с рекламной платформе Twitter с поддержкой отслеживания конверсии и возможностью создавать tailored audiences;

– аналитика.

Плагин требует версию PHP 5.4 и выше ***(Twitter выпустил официальный плагин для WordPress // ProstoWeb (http://www.prostoweb.com.ua/sozdanie_sayta/novosti/twitter_vypustil_ofitsialny_plagin_dlya_wordpress). – 2015. – 4.03).***

***

Google анонсировал новую версию Контактов в почтовом сервисе Gmail и Google+. Обновление призвано облегчить отслеживание знакомых людей и ускорить получение нужной информации. Новые Контакты Google удобно группируют контакты, круги и людей, с которыми пользователи наиболее часто общаются с помощью Gmail.

Google обновил функцию «Найти дубликаты», чтобы облегчить и ускорить поиск неизбежно возникающих повторяющихся записей.

Поскольку люди иногда меняют работу, города и фамилии, новые Контакты помогают оставаться в курсе последней информации, используя профиль Google пользователей.

Кроме того, теперь можно увидеть последние письма и встречи с человеком непосредственно в его карточке контакта, вне зависимости от того, произошли ли они два дня или два года назад.

Новые контакты пока не доступны пользователям приложений Google. Пользователи Gmail получат доступ к обновлению через несколько недель ***(Google обновляет Контакты // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/internet_dlya_chaynikov/novosti/google_obnovlyaet_kontakty). – 2015. – 10.03).***

***

Facebook внедрила возможность поиска интересных пользователей в приложение по обмену исчезающими сообщениями Slingshot.

Новый раздел «Explore» был презентован в официальном блоге сервиса:

«Explore – это место для открытия интересных, вдохновляющих и творческих людей по всему миру. В этом разделе представлены популярные пользователи, активные в сервисе. Вы можете просмотреть их снимки и затем решить, хотите ли вы подписаться на их обновления. Если вы не хотите, чтобы вас добавляли в друзья посредством Explore, включите Approve Followers (подтверждение запросов пользователей) в настройках».

Социальная сеть запустила Slinshot в июне 2014 г. С того времени приложение было подвергнуто двум значительным обновлениям:

– изменение механики получения и отправки сообщений в сентябре 2014 г.;

– расширение функционала в декабре 2014 г.

В декабре 2014 г. Facebook также добавила поисковый функционал в автономное приложение-форум Rooms ***(Facebook добавил поисковый функционал в Slingshot // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_dobavil_poiskovyy_funktsional_v_slingshot). – 2015. – 12.03).***

***

Facebook объявила о закрытии социальной сети FriendFeed, купленной в 2009 г. «Самый простой способ поделиться материалами в сети», – до сих пор утверждается на главной странице сервиса, которая давно не обновлялась и сегодня выглядит архаично.

Целью FriendFeed, одного из пионеров социальных медиа, был обмен ссылками, фотографиями и текстовыми сообщениями посредством

«настраиваемой ленты». Теперь уже официально известно, что сервис прекращает свою работу 9 апреля.

Причина проста и очевидна: FriendFeed почти никто не пользуется. В заявлении Facebook говорится: «Мы поддерживали этот сервис последние пять лет, но его использование стабильно падает, сегодня его аудитория составляет лишь малую толику от того, что было раньше».

В течение всего апреля контент во FriendFeed будет доступен в режиме чтения, но затем полностью исчезнет.

Вхождение FriendFeed в состав Facebook было громким событием в сфере социальных сетей, её сооснователь Б. Тэйлор стал техническим директором Facebook. Социальный гигант выложил за покупку 50 млн дол. Тогда это были немалые деньги, но с тех пор бизнес социальных медиа ушёл далеко вперёд ***(Facebook официально закрывает сервис FriendFeed // InternetUA (http://internetua.com/Facebook-oficialno-zakrivaet-servis-FriendFeed). – 2015. – 14.03).***

## СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Президент сделал подарок на день рождения сообществу «Ай Лав Кременчуг», подписавшись на обновления.

Говоря о жизни политиков, невозможно не вспомнить их «Интернет жизнь». Так, А. Аваков и Ю. Бирюков славятся своими достижениями в Facebook, а Президент П. Порошенко начал продвигаться «ВКонтакте». Как говорится, ближе к украинской молодежи…

Особенно приятным является то, что теперь в его обозрение попал и Кременчуг – на днях П. Порошенко подписался на официальную страницу общественного движения Кременчуга с одноименным названием, которое освещает жизнь Кременчуга. «Ай Лав Кременчуг» радует кременчужан уже два года, у страницы сейчас около 10 тыс. подписчиков, среди которых теперь и почетный гость.

В самом сообществе Президенту рады и считают это лучшим подарком на предстоящий день рождения: «“Ай Лав Кременчуг” 13 марта празднует свой 2-летний юбилей... Видимо, П. Порошенко тоже хочет оказаться в списке приглашенных на вечеринку!» – шутит по этому поводу лидер общественного движения А. Редькин.

«Кременчуг Today» проверил страничку Президента «ВКонтакте» и убедился в том, что это его официальная страница. Не можем не зачитаться статусами и записями Президента на его стене, например:

«В країні не вдасться розхитати внутрішню стабільність батальйонами “все пропало”, батальйонами “все кінець”, брехнею про 200 і більше

загиблих учора, брехнею про оточені блокпости, про українських військових, які нібито перебувають там без боєприпасів, їжі і води.

Це сценарій не український. І впевнений, що ті, хто його розповсюджував, чекали абсолютно іншого результату. Ні, на щастя сьогодні ми маємо вдало завершену операцію. Будемо мати можливість і далі боронити державу….»

А нам же, дорогие читатели, остается ждать от П. Порошенко позитивных постов о нашем городе и самих прекрасных кременчужанках, в чем ему поможет сообщество «Ай Лав Кременчуг»... ***(Президент Порошенко отслеживает Кременчуг «Вконтакте» // Кременчуг Today (http://kremenchugtoday.com.ua/news.php?id=40954). – 2015. – 10.03).***

***

Нещодавно запустився сайт «IT Толока» (it.volnytsia.org). Проект має на меті посприяти, щоб молоді IT-спеціалісти та інші фахівці на волонтерських засадах допомагали неурядовим організаціям.

Як повідомляє AIN.UA, сайт був створений за підтримки громадських організацій «Вольниця» та «Воля Громади».

Допомога волонтерів, відповідно до ідеї проекту, може полягати у створенні сайту, написанні прес-анонсу, розробці дизайну логотипа, буклету, мобільного додатка тощо.

Як нагороду волонтер отримає запис у портфоліо та рекомендацію від тих, кому він допоміг. Можливий також невеликий гонорар чи сувенір.

Засновники «IT Толоки» мають на меті налагодити співпрацю між студентами, веб-студіями, PR-агентствами та волонтерами.

«Для студентів – це можливість долучитися до вирішення соціальної проблеми та вдосконалити свої практичні навички ще до того, як закінчиться навчання», – вважає керівник проекту С. Сучок.

Молоді веб-студії чи PR-агентства, на його думку, можуть створити собі за допомогою сайту якісне соціальне портфоліо.

Ресурс пропонує громадським організаціям заповнити форму, вказати свої потреби, сферу, до якої належить завдання, а також кінцевий термін виконання та можливу винагороду. Завдання з'являється на головній сторінці сайту після модерації ***(За допомогою проекту «IT Толока» громадські активісти шукають волонтерів для соціальних проектів // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/web/online_media/za_dopomogoyu_proektu_it_toloka_volonteri_shukayut_rozrobnikiv_dlya_sotsialnikh_proektiv/). – 2015. – 10.03).***

***

В соцсети Facebook активисты создали клуб знакомств с бойцами АТО. Группа создана для знакомств единомышленников, в которой кому-то интересно просто общение, а кто-то ищет романтику.

По словам администратора проекта Н. Коваль, идея создать такой паблик возникла в ответ на запрос, как со стороны парней, так и девушек.

В настоящее время в группе выбирают названия для альбомов, в которых разместят фотографии желающих познакомиться, а пока что объявления размещают на стене паблика.

При этом бойцы больше настроены на конкретику, а девушки просто стремятся поболтать, отметила активист.

«Многие холостые парни хотят познакомиться не для развлечения, а для создания семьи. Война меняет ценности и восприятие мужчин. В то же время не до знакомств раненным бойцам, для которых на первом месте восстановление. А некоторые здоровые ребята, которые ждали создания группы, говорят, что в настоящее время не хотят ни к кому привязываться, пускай война закончится», – рассказала Н. Коваль.

Также администратор проекта добавила, что пока что люди немного стесняются знакомиться, тогда как за пределами Интернета интерес к этой теме намного больший.

«Наверное, еще не все готовы во всеуслышание заявить о том, что хотят найти свою пару», – отметила Н. Коваль.

На момент публикации в группе состоит 721 участник ***(В Facebook создали клуб знакомств с бойцами АТО // МОСТ ДНЕПР – новости Днепропетровска и Украины (http://most-dnepr.info/news/society/116239.htm). – 2015. – 3.03).***

***

Немало севастопольцев в социальных сетях активно интересуются способами их восстановления украинского внутреннего паспорта, пишет «Пресса Украины».

Вот, к примеру, на наиболее украинофобском интернет-форуме «севастополь.інфо» один пользователь под ником «ЭМ 531» хочет восстановить украинский паспорт.

«Кто знает, как восстановить украинский внутренний паспорт. (По глупости в состоянии эйфории я и мои знакомые повыбрасывали так как поездки в Украину изначально не планировались)», – говорится в сообщении.

Ему знающие коллеги сразу же сообщили, что попасть на материковую Украину у него просто так не получится.

«Не пустят 100 %. Единственный выход (если и загранпаспорт Украины в патриотическом порыве тоже порвали):

1. Оформить российский загранпаспорт.

2. Выехать через Керченскую переправу или вылететь на самолете из Крыма в материковую часть РФ.

3. Въехать в Украину по российскому загранпаспорту через официальные пограничные пункты.

4. Прибыть в Херсон или Новотроицк и объяснять там украинской паспортной службе, что вы прозрели и хотите иметь документы,

подтверждающие украинское гражданство. (Но учтите, что крымской прописки – даже если паспорт вам восстановят – там скорее всего не будет) ***(Крымчане уже думают, как восстановить украинские паспорта // Типичный Херсон (http://www.t.ks.ua/krymchane-uzhe-dumayut-kak-vosstanovit-ukrainskie-pasporta). – 2015. – 5.03).***

***

Український інститут національної пам'яті запросив українців публікувати улюблені вірші Т. Шевченка. Про це йдеться на Facebook-сторінці інституту.

Український інститут національної пам'яті обрав для флешмобу уривок з поеми «І мертвим, і живим, і ненародженим…».

Підтримали ініціативу і в Національному музеї Т. Шевченка, опублікувавши вірш «Мені однаково, чи буду».

Приєдналися до флешмобу вже багато інтернет-користувачів. Свої дописи вони доповнюють хештегом #Шевченко ***(Українців запрошують до Facebook-флешмобу з нагоди дня народження Тараса Шевченка // Osvita.MediaSapiens.ua (ttp://osvita.mediasapiens.ua/web/social/ukraintsiv_zaproshuyut_do_fleshmobu_z_nagodi_dnya_narodzhennya_tarasa_shevchenka/). – 2015. – 9.03).***

***

Вінничани влаштували флешмоб на сторінці В. Коровія у Facebook

«Ви людина на своєму місці!»

«Для винничан очень правильно»

«Зрозуміло, що в такий час йому буде непросто, але він сильний – впорається!»

«Наконец-то во главе области встал опытный экономист»

«Баланс профессионализма, лидерства и человечности – это то, что нам так необходимо сейчас», – такими є відгуки на сторінці новопризначеного голови Вінницької ОДА В. Коровія. До того ж не від анонімних «тролів-ботів», покликаних прославляти або ганьбити будь-який інформаційний привід, а від цілком конкретних людей, які реєструються у соціальних мережах під власними прізвищами.

Вітають не лише вінничани (хоча їх більшість), а й мешканці інших міст України, ті, з ким В. Коровію доводилося працювати раніше.

Показово, що коментарі такої тональності на сторінках вітчизняних політиків у соціальних мережах – швидше виняток, аніж правило. Користувачі, які не надто поділяють захоплення політиків віртуальними перемогами на тлі цілком реальних соціальних негараздів, не втрачають випадку, коли можновладцям можна сказати все, що про них думаєш. Тому й можемо спостерігати в соціальних мережах «пости» з характеристикою – від стриманого скепсису, до відвертої лайки.

Однак не в цьому випадку. Відрізняються зазначені дописи і від коментувань на сторінці попереднього губернатора – А. Олійника. Там були поради, або ж стримані побажання успіху.

Відмінність у тональності реакції користувачів можна пояснити, насамперед, тим, що В. Коровій є для вінничан – представників місцевого регіонального істеблішменту – своїм, людиною, з якою вони працювали багато років, і результати діяльності якої вони бачили на власні очі. Навзаєм А. Олійник, при усьому толерантному ставленні до нього, і розумінні непростої ситуації, у якій довелося йому діяти в умовах фактичної агресії з боку Кремля, визнавався представником виконавчої вертикалі, який отримав посаду «за призначенням». Проте не був органічно вписаний у сталу традицію саме вінницького політикуму ***(Вінничани влаштували флешмоб на сторінці В. Коровія у Facebook // Vinnytsia PressPoint (http://vn.presspoint.in.ua/2015/03/09/33710). – 2015. – 9.03).***

***

Начальник ГУМВД в Киевской области В. Троян поручил своим подчиненным завести страницы в Facebook. Об этом говорится в его сообщении в соцсети.

«Учитывая то, что время течет быстро, информация о событиях разносится молниеносно, а чиновники, как правило, сидят в кабинетах и не знают, что происходит за их пределами, мной было принято решение – каждому руководителю милиции районного звена создать страницу в социальной сети Facebook», – сообщил В. Троян.

По его словам, адреса руководителей милиции области вскоре будут размещены на сайте ГУМВД в Киевской области ***(Начальник милиции Киевской обл. поручил подчиненным завести страницы в Facebook // InternetUA (http://internetua.com/nacsalnik-milicii-kievskoi-obl--porucsil-podcsinennim-zavesti-stranici-v-Facebook). – 2015. – 13.03).***

## БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Pinterest запускает рекламные объявления, состоящие из нескольких изображений, – так называемую «карусель». Новый формат позволит рекламодателям презентовать более одного продукта в одном объявлении, или же различные ракурсы одного и того же товара.

Недавно о запуске похожего продукта под названием «динамические товарные объявления» объявила Facebook.

«Новый формат – всего лишь один аспект агрессивной стратегии монетизации Pinterest. Он запускается в рамках усилий, направленных на привлечение 500 млн дол. венчурного финансирования при оценке компании в 11 млрд дол. Кроме того, Pinterest сталкивается со скептицизмом в

отношении функционирования его существующей рекламной платформы», – сообщает Digiday после общения с представителями компании.

Не все оптимистично восприняли нововведение в Pinterest.

По словам Д. Брайт, директора по работе с социальными сетями в цифровом агентстве DigitasLBi, Facebook и Twitter предлагают аналогичные рекламные продукты – объявление, состоящее из нескольких изображений, в Facebook и возможность публикации нескольких фото в одном твите в Twitter. Однако до сих пор эти форматы не очень активно использовались рекламодателями. По её мнению, та же участь может коснуться и продукта Pinterest.

Напомним, что Pinterest также готовит запуск кнопки «Купить» (Buy), которая позволит пользователям приобретать товары непосредственно со страниц социальной сети вместо перенаправления их на сторонние коммерческие сайты.

Кроме того, Pinterest убирает партнёрские ссылки со своего сайта ***(Pinterest внедряет рекламные объявления формата «карусель» // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42625/118/lang,ru/). – 2015. – 3.03).***

***

Instagram объявила о запуске рекламных объявлений формата «карусель», позволяющих продемонстрировать пользователям несколько изображений в одном объявлении. Новый функционал будет внедрён в ограниченном масштабе в течение ближайших нескольких недель, пишет Marketing Media Review (http://mmr.ua/news/id/instagram-zapuskaet-reklamnye-objavlenija-formata-karusel-43489/).

«Мы получили обратную связь от сообщества Instagram – нашим пользователям интересно узнать больше о бренде или продукте после того, как они просмотрели спонсированное фото или видео», – сообщается в блоге компании.

«Основываясь на этом интересе, мы представляем новый рекламный формат под названием “карусель”, – новый способ для брендов поделиться бóльшим количеством изображений с людьми, заинтересованными в их публикациях».

По мнению представителей компании, рекламные объявления формата «карусель» дают брендам больше гибкости в рассказе их истории. Проведя пальцем по объявлению влево, пользователи увидят дополнительные изображения и ссылку на сайт, выбранный брендом.

Новый формат позволяет использовать потенциал многостраничных печатных кампаний на мобильных устройствах – направляя людей на сайт, где можно получить больше информации о товаре. Например, компания, работающая в индустрии моды, может использовать «карусель», чтобы соединить отдельные товары в «лук». Компания, занимающаяся продажей

автомобилей, может показать различные детали транспортного средства и дать ссылку на сайт, где можно получить больше информации о новой модели.

Возможно, в будущем публикации, включающие несколько изображений, будут также доступны рядовым пользователям Instagram ***(Instagram запускает рекламные объявления формата карусель // Marketing Media Review (http://mmr.ua/news/id/instagram-zapuskaet-reklamnye-objavlenija-formata-karusel-43489/). – 2015. – 5.03).***

***

Особенности национального YouTube: пять советов украинскому видеоблогеру

Несмотря на то что в январе 2015 г. «Одноклассники» неожиданно вытеснили YouTube из первой пятерки самых популярных сайтов уанета, принадлежащий компании Google видеохостинг остается одним из самых востребованных интернет-сервисов. Украинцы не только смотрят YouTube, но и активно наполняют его. Сегодня для продвижения своих услуг YouTube пользуются все – от крупнейших компаний и до локальных интернет-магазинов. Конечно, при ведении своего канала следует учитывать специфику местной аудитории. AIN.UA начинает цикл материалов «Особенности национального YouTube», в котором мы расскажем об особенностях ведения видеоблога в реалиях нашей страны (http://ain.ua/2015/03/03/567520).

Согласно статистике в Google Trends, украинцев на YouTube больше всего интересуют политические ролики, обзоры популярных гаджетов и игровые видео. Эти темы всегда будут популярны, и для поддержания активности на канале хватит ютубовской методички. Однако, если вы ведете свой аполитичный, не геймерский канал – например, учите одиноких мужчин быстро и вкусно готовить, – помимо понимания условной группы «одинокий мужчина» вы обязательно должны знать аудиторию «русскоговорящий пользователь YouTube». Потому как этот самый пользователь очень отличается от своего западного коллеги.

1. Всегда используйте призывы

«Ставьте лайки, подписывайтесь на мой канал» – эту фразу, наверное, слышал любой пользователь Интернета, посмотревший хоть один видеоролик. Даже официальный гид YouTube в одном из первых уроков советует использовать этот прием, хотя многие блогеры о нем забывают. К сожалению, реальность такова, что средний украинец абсолютно ничего не сделает без призыва автора. Не бойтесь надоесть зрителю: если призыв оставить в конце ролика, вместе с красивой фоновой музыкой, заставкой и ссылками на предыдущие видео (или анонсами следующих), никто и слова вам не скажет. А вот рост подписчиков, как показывает практика, может увеличиться более чем на 100 %. Кстати, голосовой призыв подписаться можно дублировать интерактивной кнопкой, через функцию «аннотация».

2. Научите пользователя распространять ваши ролики

Особенно, если они могут быть интересны любому зрителю. Конечно, можно использовать и призыв, но лучше дать прямые ссылки, нажатие на которые приведет к тому, что пользователь поделится видео в одной из социальных сетей. В таком случае, каждый поделившийся будет приносить вам в среднем по 50–80 новых просмотров и потенциальных распространителей.

3. Ловите тренды

Даже если они не касаются основной тематики вашего канала. Полиция Аризоны устроила погоню за ламами? Вставьте в ролик шутку в поддержку свободного передвижения лам! Завтра пройдет церемония вручения «Оскар»? Запишите спецвыпуск блога: поделитесь своим мнением, сделайте ставки, предложите зрителям поучаствовать в обсуждении. Украинские пользователи любят общение, которое выходит за рамки тематики канала – особенно, если это касается событий, которые ему интересны. Подобные вещи позволяют «оживить» канал. Да, постороннему зрителю может быть неинтересно мнение Павла П. о сливе фотографий Д. Лоуренс, однако ваши подписчики это оценят.

4. Но не трогайте политику

Если вы не политический эксперт, и тематика блога далека от политики в целом, никогда не касайтесь этого вопроса. Он всегда разделит аудиторию пополам, причем одной половине ваше мнение будет совершенно непонятно. Да, на этом тоже можно вырастить свою новую аудиторию, которая восторженно будет поддерживать вашу реакцию на политические события, но тогда готовьтесь к тому, что ваши основные видео по начальной тематике перестанут просматриваться совсем. Деление аудитории на группы хорошо, когда предметом их обсуждения становится, например, научная значимость нового открытия или прическа Э. Уотсон. Такие споры не способны рассорить людей, разделить их на враждующие стороны, взрывающие ваши комментарии потоками мата и оскорблений. Поэтому помните: «располовинивание» аудитории по политическому признаку приведет к располовиниванию ваших подписчиков. На тех, кто вас поддерживает и тех, кто отписался. Хотелось бы отметить в этом пункте ребят из kreosan, о которых мы писали в прошлом году: живя по сей день в Луганской области, они никогда не касались политических вопросов.

5. И не стесняйтесь заимствовать форматы

Но в этом вопросе придется ориентироваться на западных блогеров. Так уж сложилось, что YouTube в СНГ отстает от западного примерно на полтора года. То есть штуки и форматы, которые сейчас популярны в США, до нас дойдут минимум через несколько месяцев. Посмотрите европейские тренды YouTube (отбросив летсплеи – похоже, эти ребята будут популярны всегда). Краткие новостные выпуски а-ля телестудия на дому, уличные розыгрыши, опросы. Мировые тренды показывают, что YouTube станет гораздо более социальным, и постепенно начнет заменять телевидение в

казалось бы «телевизионных» форматах. К слову, практически все сегодняшние русскоговорящие топ-пользователи YouTube вдохновлялись западными блогерами. Так что не бойтесь пробовать что-то новое: оценку всегда дадут ваши подписчики ***(Особенности национального YouTube: 5 советов украинскому видеоблогеру // AIN.UA (http://ain.ua/2015/03/03/567520). – 2015. – 3.03).***

***

Как создать эффективную видеорекламу в Facebook – советы маркетологов

Чуть более года назад Facebook представила функцию автоматического воспроизведения видеорекламы, а в рамках последнего ежеквартального отчета о прибыли сообщила о том, что в соцсети ежедневно просматривается свыше 3 млрд видео, пишет Marketing Media Review (http://mmr.ua/news/id/kak-sozdat-effektivnuju-videoreklamu-v-facebook-sovety-marketologov-43474/).

Тем не менее, до сих пор многие маркетологи (и даже крупные бренды) не знают, как использовать все возможности этой опции. Агентство Jack Morton Worldwide попросило маркетологов со всего мира поделиться опытом создания эффективного видеоконтента на Facebook.

Правило трех секунд

В новостной ленте Facebook видеореклама начинает воспроизводиться автоматически и прекращается сразу же, как только пользователь пролистывает ее. Это значит, что ролик должен привлекать внимание практически моментально – в течение трех первых секунд.

Основатель и исполнительный креативный директор агентства Genuine Interactive К. Пэйп:

Размещая материал в традиционных СМИ, рекламодатели не переживают о том, как привлечь внимание с первых кадров. Можно целых семь секунд баловать зрителя ярким шоу, а лакомый кусок оставить на конец. Так было раньше, но теперь первые три секунды решают все.

Этот промежуток времени является приоритетным даже с точки зрения метрики. Facebook определяет количество просмотров, начиная с третьей секунды видео, и именно по этому показателю оценивает все видеозаписи бренда.

Искусство Чарли Чаплина

Функция «автоплей» предполагает беззвучное воспроизведение видео при прокрутке новостной ленты, поэтому брендам важно уметь донести свой посыл, используя только визуальные средства.

«Facebook (особенно мобильное приложение) – это беззвучная среда», – признается К. Пэйп. – Маркетологи должны развивать своего внутреннего Чарли Чаплина и создавать визуально привлекательный контент. История, которая рассказывается в видео, должна быть понятной и без слов».

Самобытность

Раз и навсегда откажитесь от копирования телевизионного формата. Главное – вовлечь пользователя, а не делать акцент на прямой продаже продуктов. Чтобы понять, в чем суть «сетевого мышления», маркетологам необходимо забыть все, что касается телевизионного формата.

Д. МакКэффри, глава отела по связям с общественностью агентства Huge: «Во время работы с видеорекламой я задумался вот о чем: как же компании собираются повысить ценность бренда, если они просто впихивают свой логотип в новостную ленту пользователей?»

Телезрители морально готовы к рекламной паузе в своих любимых программах. Что же касается Facebook, то сейчас у компаний есть отличная возможность «влиться» – для этого нужно просто делиться с пользователями своим опытом и получать выгоду с помощью социального контента.

Проверка на гибкость

Интернет-реклама не требует многомиллионных расходов, более того, у Facebook есть особые инструменты для наиболее оптимального таргетирования подходящей аудитории. Так что маркетологам следует быть как можно более гибкими при позиционировании бренда.

Руководитель группы по работе с клиентами агентства Genuine М. Кассель: «Здорово, что можно сделать несколько версий рекламного ролика и посмотреть, какая из них достигнет большего эффекта, вместо того чтобы выпускать компромиссный вариант».

«Чтобы оперативно реагировать на из ряда вон выходящие события, нужно обладать гибким мышлением, – добавляет К. Пэйп. – Предвидеть абсолютно все у вас однозначно не получится».

Клиент – на первом месте

Таргетирование в Facebook возможно как на основе профилей пользователей, так и при помощи cookies браузера, что открывает перед компаниями гораздо более широкие возможности для оценки охвата клиентов и частоты появления рекламы на различных устройствах. Также это позволяет им эффективнее находить «своих» клиентов, и создавать такой контент, который вызовет у них максимальный отклик.

Бренд-менеджер Lysol К.Тронг: «Очень важно оставаться верным своим клиентам, и, создавая определенный контент, быть уверенным в том, что он заставит их сопереживать – и дело тут вовсе не в лайках».

Инструменты

На сегодняшний день oCPM (Optimized Cost per Millenium – инструмент Facebook для измерения оптимизированной цены за тысячу показов) и Reach & Frequency (охват и частотность) успели зарекомендовать себя в качестве наиболее эффективных способов продвижения видеорекламы.

Главная цель каждой из этих двух опций – увеличивать количество просмотров, но достигают они ее по-разному.

oCPM следует использовать тогда, когда вы хотите достигнуть наименьшего значения показателя цены за просмотр (cost per view).

Функция Reach & Frequency, которая относится к оптимизации рекламы для достижения целей кампании, позволяет наиболее точно определить доставку контента и приобрести уникальный охват, контролируя частоту появления рекламного ролика.

Если же вы работаете с CPC-рекламой, не используйте ссылки на внешние видео, потому что в этом случае будет недоступна функция автоматического воспроизведения.

Видеореклама особенно эффективна для повышения узнаваемости бренда. Вы можете побудить целевую аудиторию интересоваться продуктом благодаря двум решениям:

Ремаркетинг. Это возможность повторно показывать пользователям ролики, даже если пользовали их однажды их уже видели. В этом может помочь продукт Social Ads Tool, который является партнером Facebook.

Призыв к действию. Другой простой способ увеличить вовлеченность целевой аудитории – это добавить в конце видео один из призывов, среди которых «Зарегистрируйтесь», «Подробнее», «Загрузить» и «Начать покупку».

Общие рекомендации:

Загружайте видео непосредственно в Facebook, избегая ссылок на внешние сайты, например, на YouTube.

В качестве маркетинговой цели задавайте «Просмотры видео» (Video views), чтобы убедиться в том, что объявление имеет корректные настройки характеристик конверсии.

Подумайте, какой инструмент вам больше подходит, – плата за тысячу показов или плата за клики. В случае цены за клик вы сможете максимизировать показатель Cost per View (стоимость одного просмотра), добиться эффективности ремаркетинга и результативности автоматического воспроизведения видео. Преимущества oCPM описаны выше.

Используйте наиболее подходящую метрику для целей своей кампании – охват, частота показов, количество просмотров и CPV ***(Как создать эффективную видеорекламу в Facebook – советы маркетологов // Marketing Media Review (http://mmr.ua/news/id/kak-sozdat-effektivnuju-videoreklamu-v-facebook-sovety-marketologov-43474/). – 2015. – 4.03).***

***

Google анонсировал несколько улучшений в сервисе Мой Бизнес. Нововведения призваны дать владельцам компаний бóльший контроль над тем, как их бизнес представлен в Поиске Google.

Теперь пользователи сервиса могут конкретизировать, какое фото компании должно отображаться в выдаче поисковика. Ранее, любое фото, размещённое в Google+ в качестве фото бизнес-профиля, переносилось в Поиск Google. Теперь, если владелец бизнеса хочет, чтобы в выдаче отображалось одно фото компании, а в Google+ – другое, у него есть возможность это сделать.

Кроме того, предприниматели также получат возможность добавить фото в шесть новых категорий, которые будут отображены в Поиске и в Google+. Эти категории включают основное фото компании, фото интерьера, здания, рабочих мест, персонала и дополнительные фото.

Чтобы воспользоваться преимуществами нового функционала, нужно авторизироваться в бизнес-профиле и зайти в раздел «Фотографии». Здесь можно выбрать фотографии, которые будут представлять компанию в сети.

Кроме того, Google добавил новую функцию, которая рекомендует фото для добавления, основываясь на типе бизнеса. Например, фото интерьера номеров для отелей.

Нововведения уже доступны в десктопной версии Google Мой Бизнес, а также в приложениях сервиса для iOS и Android.

Напомним, что Google представил бесплатный сервис «Мой бизнес», предназначенный для представителей малого и среднего бизнеса, летом 2014 г. Возможности Google Мой бизнес позволяют предпринимателям публиковать и оперативно обновлять информацию о компании и заведениях в Google+, Поиске Google и на Картах Google ***(Google Мой Бизнес дал предпринимателям больше контроля над фото в выдаче // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/internet_dlya_chaynikov/novosti/google_moy_biznes_dal_predprinimatelyam_bolshe_kontrolya_nad_foto_v_vydache). – 2015. – 5.03).***

***

Социальная сеть Facebook объявила, что изменит механику подсчёта общего количества лайков на страницах брендов, компаний и организаций.

В ближайшее время Facebook автоматически удалит из общего счётчика лайков неактивные аккаунты. Это касается профилей, чьи владельцы ушли из жизни и об этом стало известно соцсети, а также учётных записей, которые деактивировали добровольно. Кроме этого, со страниц пропадут лайки и комментарии от неактивных аккаунтов к отдельным постам.

Социальная сеть предупреждает, что администраторы могут заметить незначительное сокращение числа подписчиков. Однако обновление, рассчитывают в Facebook, даст компаниям более актуальную информацию о своей аудитории в соцсети ***(Facebook изменил для страниц механику подсчёта лайков // Marketing Media Review (http://mmr.ua/news/id/facebook-izmenil-dlja-stranic-mehaniku-podscheta-lajkov-43515/). – 2015. – 6.03).***

***

Сервис микроблогов Twitter приобрел за 100 млн дол. стартап Periscope, разрабатывающий приложение для просмотра потокового видео, сообщила газета The Wall Street Journal со ссылкой на информированные источники.

Сумма сделки, сообщили они изданию, составила немногим менее 100 млн дол. Большая часть из них была выплачена наличными, другая – акциями компании. Таким образом, еще не запущенный стартап Periscope стал одним из самых дорогих приобретений Twitter.

Сделка была закрыта месяц назад. К настоящему времени состоялось бета-тестирование приложения. Первоначально в нем приняла участие директор по корпоративному развитию Twitter Д. Веррилли, хорошо знакомая с сооснователем Periscope К. Бейкпуром. Позднее к тестированию приложения присоединились CEO Twitter Д. Костоло и сооснователь компании Д. Дорси.

Сделка отражает стремление Twitter к расширению возможностей работы с потоковой передачей видео со смартфонов в реальном времени.

Приложение было куплено одновременно с запуском аналогичного продукта – стартапа Meerkat, позволяющего пользователям Twitter демонстрировать потоковое видео с их телефонов в сервисе микроблогов ***(Twitter приобрел сервис для просмотра видео за $100 млн // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42684/118/lang,ru/). – 2015. – 10.03).***

***

Двадцать восемь правил продвижения в соцсетях: какие работают, какие – нет?

Как разобраться в неписаных правилах этикета соцсетей? Я много наблюдал, экспериментировал, делал много проб и ошибок. Начиная работать с социальными медиа, я руководствовался лишь самыми базовыми правилами и интуицией. Но и сейчас я почти ежедневно узнаю какую-то новую деталь. И вообще-то непросто понять, какие правила вообще существуют, какие незыблемы, а какие вполне можно нарушать, пишет Marketing Media Review (http://mmr.ua/news/id/28-pravil-prodvizhenija-v-socsetjah-kakie-rabotajut-kakie-net-43552/).

Попробую пролить свет на это. Покопавшись в исследованиях, я обнаружил, что есть набор базовых правил для соцсетей, с которыми соглашаются большинство маркетологов.

Вот 28 из них, которые чаще всего называют профессионалы.

Правила для всех социальных сетей

1. Делитесь контентом несколько раз в день, но делайте интервалы в несколько часов.

Исследования показывают, что когда вы заваливаете своих последователей несколькими обновлениями подряд – это один из самых важных факторов, побуждающих людей отписаться от вашей страницы.

2. Отвечайте на все комментарии как можно скорее

Одно исследование социальных сетей показало, что 53 % людей, которые твитят что-то в адрес бренда, ожидают ответа в течение 60 минут.

Twitter – самая оперативная соцсеть, и в ней своевременные ответы жизненно необходимы. Но они весьма важны и в других социальных медиа.

3. Изучайте искусство хэштега.

1 хэштег – хорошо, 10 – плохо Но что значит много? The Next Web рекомендует на всех платформах ограничиваться 1-3 хэштегами для поста. С этого можно начать, но потом вы увидите, что в разных соцсетях дело может обстоять по-разному. Наши собственные исследования показывают, что:

– в Twitter 2 хэштега – лучший вариант;

– в Facebook хэштеги могут даже снижать участие пользователей;

– в Instagram больше всего внимания вы получаете, когда в посте 11 или больше хэштегов;

– в Pinterest хэштеги не рекомендуются. Но не стесняйтесь поэкспериментировать сами.

4. Правило 80/20: сначала развлекайте и информируйте аудиторию, а потом уже продавайте ей что-то

Есть много разных правил на этот счет, но общее в них одно: нужно больше делиться чужим контентом, чем своим. И для многих компаний это будет отличная стратегия. Хотя мы в Buffer попробовали обратное правило: 90 % контента, которым мы делимся – наш собственный. Пока мы не заметили меньше активности от пользователей.

5. Говоря о своем бренде, используйте слово «мы»

Это действительно хорошо работает для компаний. Когда вы говорите о своем личном бренде, «я» или «мне» звучит более естественно.

Правила для Twitter

6. Не нужно автоматически писать прямые сообщения своим последователям

Автоматизация в социальных медиа бывает вполне уместна, но автоматически отсылать новым последователям прямые сообщения – это не тот случай. На заре Twitter это было популярно, сегодня это воспринимается как неискренняя практика.

7. Не используйте все 140 символов.

Оставьте людям место для их собственных замечаний в ретвите Идеальная длина твита – 71–100 символов. Если человек хочет вручную сделать ретвит (скопировать текст из вашего твита и написать в начале RT), он, возможно, захочет добавить и какую-то деталь или слова от себя. Для этого стоит оставить место.

8. Не крадите чужие хэштеги

HubSpot советует: «Когда вы видите, как у других компаний получаются очень успешные хэштеги, не запрыгивайте на их поезд со своим контентом не в тему: это обесценивает не только их хэштег, но и в результате ваш собственный бренд».

9. Не покупайте последователей

Д. Лотан из Betaworks провел эксперимент: он заплатил 5 дол. за 4000 последователей в Twitter. Он чувствовал себя очень неприятно, но все же в

итоге это принесло ему реальный прирост в Twitter. Я лично считаю, что приобретение некоторого количества последователей – как бы ни было это неприятно писать – может ускорить долгосрочный рост и заметность вашего бренда. Хотя это интересный этический момент: если стратегия работает, всегда ли этично ею пользоваться?

10. Не заполняйте ваши твиты ключевыми словами

Как будет звучать ваш твит, если бы вы сказали его словами другу или коллеге? Представьте это и вы поймете, насколько в нем допустимы ключевые слова.

Правила для Facebook

11. Не ставьте лайки на собственные посты

Это потенциально приводит к тому, что контент снова появляется в ленте новостей (в первый раз – когда вы его публикуете, а потом еще раз, когда вы ставите лайк) и вызывает какую-то реакцию. Но все же это дает некий неприятный сигнал, говорит о неком отчаянии с вашей стороны.

12. Не публикуйте (и не ставьте теги) фотографии поклонников, клиентов или сотрудников без их согласия

Многие сайты рекомендуют в таких случаях получить письменное согласие. И тут реально возможны проблемы с защитой частной жизни.

13. Не ставьте теги на людей или страницы, не имеющие отношения к вашему посту

Они получают уведомление о том, что их упомянули в другом обновлении страницы, и некоторые маркетологи пользуются этим, чтобы привлечь дополнительное внимание к своему контенту. Это еще одна тактика, которая потенциально может сработать, но выглядит не очень-то корректной.

14. Не просите о лайках, комментах и шерах

Раньше правило было такое: просите поставить лайк только в случае, если вы делаете опрос («Лайкните этот пост, если вы любите собак, и поделитесь им, если любите кошек»). Но вообще просьба о лайках, комментах и шерах – один из тех факторов, которые Facebook учитывает, когда выбирает, что показать в ленте пользователя, и подобные призывы снижают заметность вашего контента.

Правила для LinkedIn

15. Персонализируйте свои запросы о дружбе – объясняйте людям, зачем вы устанавливаете с ними контакт

На личные просьбы обращают внимание, их больше ценят и чаще удовлетворяют, чем стандартные запросы.

16. Когда вы занесли кого-то в друзья, отправьте приветственное сообщение

По моему опыту, это происходит довольно редко – хотя эффект бывает отличный! Если, конечно, у вас много запросов в LinkedIn, в таком масштабе это не работает; но можно делать это в некоторых избранных случаях или когда вы налаживаете связи с влиятельными людьми.

17. Не нужно вступать в группы, чтобы тут же начинать «продавать» себя

Группы в LinkedIn – отличный инструмент связи с людьми (плюс также в том, что в группе вы можете отправить сообщение любому человеку, даже если вы с ним напрямую не в контакте). Одно из главных правил групп в LinkedIn – уважать правила игры. Делитесь и заинтересовывайте людей, прежде чем бросаться в продвижение себя.

18. Не игнорируйте профессиональный тон этой сети

Это вообще одно из главных правил социальных медиа: подстраивайте свой контент и свои сообщения под особенности социальной сети. LinkedIn нацелен на деловых людей и профессионалов, так что учитывайте этот тон.

Правила для Google+

19. Всегда «плюсуйте» пользователей, когда комментируете их посты

Это помогает самим авторам следить за беседой, и это вежливый способ отдать им должное.

20. Когда делитесь постом, обязательно добавляйте к нему свой комментарий

Посты в Google+ приятно читать и писать, это скорее блоги, чем апдейты в привычных соцсетях. В их написании есть особое искусство и наука. Я заметил, что многие люди добавляют свои мысли по теме, потом проводят горизонтальную черту, под которой постят чужую статью.

21. Делитесь с «кругами», чтобы таргетировать контент

Это как прямые сообщения конкретной группе людей. Полезный способ поделиться материалом со строго определенной группой людей.

Правила для Pinterest

22. Не забывайте об описаниях того, что публикуете

Иногда быстро постишь много разных картинок и забываешь прикрепить к ним описание. Но это один из ключевых способов для новых пользователей обнаружить ваши публикации – особенно если вы активно используете ключевые слова.

23. Всегда ставьте линк на первоисточник и отдавайте ему должное

Картинки часто ходят в онлайне туда-сюда, и хорошо, когда можно быстро найти первоисточник. И репостить лучше всего из первоисточника, а не из другой коллекции, которая его использует.

24. Не используйте изображения, которые не имеют отношения к вашему контенту, просто ради кликов и перепостов

Этот прием приносит клики, но вряд ли это будет ценный, стабильный трафик, да и вряд ли у новых посетителей останется о вас очень хорошее впечатление.

25. Не постите только свои материалы

Можно сделать отдельные доски, которые продвигают ваши собственные посты и контент. А помимо этого, постите картинки из самых разных источников.

Правила для Instagram

26. Не просите людей стать вашими последователями и не используйте хэштеги вроде #тегдлялайков

Как и в Facebook, просить о лайках не рекомендуется – дело не в том, что ваши фото будут хуже видны (в Instagram нет алгоритма, подобного ленте Facebook), но ваш бренд будет восприниматься как менее профессиональный.

27. Не постите слишком много – людям не нравится, когда в их ленте доминирует один пользователь

В наших исследованиях идеальной частоты постов в социальных сетях выяснилось, что в Instagram нет конкретного стандарта на этот счет. Одно исследование показало, что крупные бренды в среднем постят 1–2 раза в день. В то же время бренды, которые постят 10 и больше раз в день, все же наблюдают прирост активности пользователей с приростом частоты своих постов.

28. Правильно пользуйтесь хэштегами. «Золотое число» – 11

Как уже говорилось, в Instagram часто уместны гораздо больше тегов, чем в любой другой соцсети. Одно исследование показало, что больше всего взаимодействий получают картинки с 11 и большим числом хэштегов. Причем данные в этом исследовании были получены от пользователей с не более чем 1000 последователей – то есть это группа, в которую, вероятно, и попадают малые бизнесы и те, кто только начал вести аккаунт в Instagram. Иными словами, хэштеги могут оказаться лучшим способом добиться быстрого прироста последователей ***(28 правил продвижения в соцсетях: какие работают, какие – нет? // Marketing Media Review (http://mmr.ua/news/id/28-pravil-prodvizhenija-v-socsetjah-kakie-rabotajut-kakie-net-43552/). – 2015. – 11.03).***

***

Facebook запустила инструмент для изучения мнений аудитории брендов Topic Data

Facebook в сотрудничестве с аналитической компанией DataSift представила Topic Data – новый инструмент аналитики, показывающий маркетологам, о чём говорят их клиенты в социальной сети, и что они думают о темах, имеющих отношение к бизнесу компании и к отрасли в целом, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-instrument-dlja-izuchenija-mnenij-auditorii-brendov-topic-data-43550/).

Эта информация призвана помочь брендам сделать их продукт более релевантным потребителям. Первоначально новый инструмент запускается для рекламодателей в США и Великобритании. В будущем планируется расширение этого функционала на другие страны.

По словам представителей компании, инструмент позволяет рекламодателям видеть, что их клиенты говорят о «мероприятиях, брендах и активностях». Маркетологи могут использовать эту информацию «для принятия решений о продвижении продуктов в Facebook и других каналах».

«Мы хотим убедиться, что информация, которую мы предоставляем, полезна для маркетологов», – сообщается в блоге Facebook. «Поэтому мы используем технологию DataSift».

В качестве примеров использования Topic Data, представители Facebook привели компанию, продающую продукт для выпрямления вьющихся волос. Новый инструмент позволил этому клиенту увидеть демографические характеристики клиентов, обсуждающих, как влажность воздуха влияет на их волосы. Аналогичным образом, компании могут измерить мнение о бренде путём понимания того, что люди говорят о компании или отрасли, в которой она работает.

В блоге отмечается, что подобные данные были доступны рекламодателям и ранее, но размер выборки был не достаточно большим, чтобы компании могли получить полное представление о своих клиентах. Поскольку Topic Data измеряет обсуждения в Facebook, «маркетологи впервые получают целостное и достаточное для осуществления дальнейших действий представление о своей аудитории».

Кроме того, сохраняется конфиденциальность информации, собираемой с помощью Topic Data. «Мы сгруппировали данные и убрали личную информацию из активности в Facebook (за исключением Messenger). «Новый инструмент не может быть использован для нацеливания рекламы непосредственно на пользователей Facebook» ***(Facebook запустил инструмент для изучения мнений аудитории брендов Topic Data // Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-instrument-dlja-izuchenija-mnenij-auditorii-brendov-topic-data-43550/). – 2015. – 11.03).***

***

Facebook и Snapchat переманивают владельцев ТВ-контента у YouTube

Facebook, Snapchat и стриминг-стартап Vessel намерены лишить YouTube контрактов с владельцами ТВ-контента, предлагая им бóльшую долю отчислений от показов рекламы. Об этом пишет Wall Street Journal.

По данным издания, Facebook , Snapchat и Vessel уже ведут переговоры с партнерами YouTube, основными дистрибьюторами ТВ-контента в США: Viacom Inc., Time Warner Inc., Comcast Corp., NBCUniversal и 21st Century Fox. Источники WSJ отмечают, что сейчас сервис от Google отдает медиакомпаниям около 55 % доходов от показа рекламы перед их роликами.

Как стало известно изданию, Facebook предложила как минимум одной компании из списка контракт, по которому соцсеть будет отдавать 65 % рекламной выручки. Vessel и Snapchat предлагают медиакомпаниям около 70 % доходов от рекламы, отмечают источники.

Ранее стало известно, что YouTube, несмотря на миллиардную посещаемость в месяц, все еще находится на грани рентабельности. По мнению экспертов, большая часть пользователей пользуется встроенными на сайты плеерами и редко посещает сам сайт сервиса, где отображается большая часть рекламы. Аналитик Pivotal Research Б. Вайзер говорит, что

YouTube не хватает профессионального контента, чтобы удержать аудиторию, а собственных «звезд» у компании не так уж и много.

В ноябре 2014 г. объем публикаций видео на Facebook с помощью встроенного проигрывателя впервые превысил долю YouTube. По мнению зарубежных изданий, в ближайшее время крупные бренды все чаще будут отказываться от сервиса Google и переходить на сторонние площадки ***(Facebook и Snapchat переманивают владельцев ТВ-контента у YouTube // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_i_snapchat_peremanivayut_vladeltsev_tv_kontenta_u_youtube). – 2015. – 11.03).***

***

Від 12 березня користувачі Twitter отримали доступ до оновленої статистики Twitter. Вона доступна як напряму з Twitter-стрічки, так і за посиланням analytics.twitter.com.

В аналітиці ви можете переглянути інформацію про те, скільки разів вас ретвітнули, скільки людей бачили ваші твіти, відвідали профіль, згадали вас або почали фоловити, скільки разів люди поділилися вашим посилання, скільки нових фоловерів ви отримали за місяць.

Трохи більше місяця тому компанія представила функцію «швидкого просування», яка дає змогу користувачам вибирати свої твіти та платити за їх рекламу безпосередньо з панелі аналітики.

Тепер процес просування твітів ще більше спростився – є можливість рекламувати їх безпосередньо з вашого профілю.

Нагадаємо, що Twitter ще у 2013 р. попри обіцянку відкрити статистику для всіх користувачів, так цього й не зробив. Переважна більшість користувачів за півтора року так і не змогли скористатись цим сервісом. Тепер ситуація змінилась ***(Twitter зробив аналітику доступною для всіх користувачів та спростив рекламні інструменти // UkrainianWatcher (http://watcher.com.ua/2015/03/13/twitter-zrobyv-analityku-dostupnoyu-dlya-vsih-korystuvachiv-ta-sprostyv-reklamni-instrumenty/). – 2015. – 13.03).***

***

У компанії Facebook заявили про купівлю шопінг-пошуковика The Find. Про це пише Associated Press.

Умови угоди не розголошуються. Передбачається, що операція буде завершена в найближчі кілька тижнів.

TheFind, яка була заснована у 2006 р., буде закрита, а частина її співробітників перейдуть працювати у Facebook.

Пошуковик, що дає можливість відшукати потрібні товари в довколишніх магазинах, буде інкорпорований у соцмережу з метою вдосконалення її рекламних сервісів.

TheFind заснований у Маунтін-В'ю, штат Каліфорнія ***(У Facebook заявили про купівлю пошуковика The Find // Економічна правда (http://www.epravda.com.ua/news/2015/03/15/533847/). – 2015. – 15.03).***

# СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

## Інформаційно-психологічний вплив мережевого спілкування на особистість

Новости и соцсети мешают украинцам работать

Примерно 10 % офисных сотрудников не могут сконцентрироваться на работе, поскольку постоянно отвлекается на новости. А еще довольно заметная часть работников не только сама отвлекается на новости, но и отвлекает коллег. Такие данные продемонстрировал опрос, проведенный порталом «HeadHunter Украина» (http://ain.ua/2015/03/02/567266).

Правда, по словам участников опросов, в основном они отвлекаются на новости и их обсуждение с коллегами во время обеденного перерыва (57 %).

Интересно, что доля тех, кто общается с коллегами по поводу последних новостей тем выше, чем больше людей работает в компании. К примеру, в каждой третьей компании от 50 до 100 человек не обсуждают новости с коллегами. Что касается больших компаний (свыше 100 человек) и очень крупных (до 1000 человек) – только в каждой четвертой не принято говорить с коллегами по поводу новостей.

Если у сотрудника есть неотложная работа, около 30 % признались, что закрывают все посторонние сайты и стараются сосредоточиться на задании.

Но 50 % из всех респондентов заметили, что и в этом случае будут работать и висеть в социальных сетях одновременно. А 8 % заявили, что будут жертвовать количеством и качеством выполненной работы ради новостей, выполняя только необходимый минимум ***(Новости и соцсети мешают украинцам работать // AIN.UA (http://ain.ua/2015/03/02/567266). – 2015. – 2.03).***

***

Ученые из Амстердамского свободного университета и Филиппинского университета заявляют: Facebook помогает поддерживать отношения на расстоянии.

В наши дни такие отношения очень распространены. А если вторая половина живет в том же районе или городе, общение по Facebook – это не лучший выбор, пишет «Обозреватель» (http://tech.obozrevatel.com/news/52478-facebook-spasaet-otnosheniya-na-rasstoyanii.htm).

Эксперты отмечают, что люди, состоящие в отношениях на расстоянии, чаще пользуются соцсетями. По словам специалистов, Facebook позволяет влюбленным, находящимся далеко друг от друга, быть в курсе происходящего в жизни партнера. То есть социальные сети могут влиять на романтические отношения как позитивно, так и негативно.

В другом исследовании, проведенном ранее, ученые выяснили, что социальные сети разрушают отношения. Чем чаще люди проявляли свою активность в Twitter, тем больше у них был риск конфликта с партнером. Причем продолжительность романтических отношений не играла никакой роли ***(Facebook спасает отношения на расстоянии // Обозреватель (http://tech.obozrevatel.com/news/52478-facebook-spasaet-otnosheniya-na-rasstoyanii.htm). – 2015. – 14.03).***

***

Молоді користувачі соцмереж втомилися ділитись кожною деталлю особистого життя в Інтернеті і частіше вдаються до кроків, які захищають їхню приватність. Про це свідчать дані дослідження однієї з найбільших дослідних спільнот – The Market Research Society, повідомляє TCH.ua (http://tsn.ua/nauka_it/pidlitki-kardinalno-zminyuyut-svoyu-povedinku-u-socmerezhah-doslidzhennya-415428.html).

Підлітки стали частіше викладати до мережі фотографії, не вказуючи свого місцезнаходження, залишають неправдиві записи на своїх сторінках, заводять по кілька фейкових акаунтів. Також останнім часом розповсюджене розміщення дуже розпливчастих і загадкових повідомлень, розрахованих на те, щоб близькі друзі тільки в приватному чаті дізнавалися подробиці, пише Mail Online.

У доповіді К. Стронг із дослідної компанії окремо відзначається підвищений попит до мобільних додатків, які видаляють розміщену на них інформацію через певний нетривалий проміжок часу. Наприклад, популярністю користується додаток Snapchat, який повністю видаляє розміщені на ньому фото, і їх потім неможливо відшукати в мережі.

Одна з керівників Market Research Society Д. Фрост повідомила, що третина акаунтів у мікроблозі Twitter – закриті для пересічних користувачів. Переглядати стрічку можуть лише обрані. Водночас із тих самих пристроїв реєструються й відкриті акаунти з фейковими анкетами, на яких розміщують інформацію для широкого загалу – різноманітні відео, кумедні картинки, тощо.

«Те, що вони розміщують інформацію у загально доступному місці ще не означає, що вони хочуть публічності», – каже К. Стронг ***(Підлітки кардинально змінюють свою поведінку у соцмережах – дослідження // TCH.ua (http://tsn.ua/nauka_it/pidlitki-kardinalno-zminyuyut-svoyu-povedinku-u-socmerezhah-doslidzhennya-415428.html). – 2015. – 15.03).***

## Маніпулятивні технології

Сепаратистські соціальні медіа розпочали підготовку до нового етапу кампанії «русская весна». Про це на своїй сторінці у Facebook розповів народний депутат А. Левус, передає Еспресо.TV.

Він зазначив, що головний антиукраїнський ресурс – група «Антимайдан» у соцмережі «ВКонтакте» (500 тис.) анонсував активну фазу операції, яка розпочнеться вже через кілька тижнів. Хештег #новаявесна оголошено, як ключовий інформаційно-координаційний орієнтир. Він уже ширится соцмережами.

«Територія на якій діятиме проект – Харків, Одеса, Запоріжжя, Херсон, Миколаїв. Головна ціль – дестабілізація ситуації в Україні та формування "Новоросії" на всьому Південному Сході України.

Ініціатори "новойвесны" зазначають, що діяти відкрито уже не можуть, тому задіють нові форми та гасла для проекту. Мова, очевидно, йде і про теракти, і про соціальні бунти. Все це має на меті стати прикриттям для "зелених чоловічків", роль яких відіграватимуть бойовики ДНР/ЛНР родом зі згаданих областей.

Ускладнює, ситуацію масовий вихід на волю сепаратистів та терористів Південного Сходу у наслідок обміну полоненими. Окрім цього, імовірно, "новаявесна" буде проходити в поєднанні з черговим загостренням на східному фронті», – написав депутат.

«Перші паростки "новойвесны" – кривавий теракт в Харкові, кампанія "Порто – франко" в Одесі, провокації – псевдопротести в Києві», – наголосив А. Левус.

Він нагадав, що минулого року спецслужби Росії задіяли для «русской весни» свої агентурні мережі та проросійські структури. Соціальні мережі відіграли не останню роль в проекті. Хештег #русскаявесна став повноцінним центром концептуального управління та обміну інформації для сепаратистів.

«Рік тому СБУ, МВС і патріотична громадськість дали відсіч сепаратистам і зупинили кремлівську спецоперацію у всіх областях, крім Донбасу. Цього року перед нами нові виклики. Якщо будемо пильними та єдиними – переможемо», – зазначив А. Левус.

Він також додав, що СБУ блокує доступ до терористичних ресурсів, а також повідомив, що структури Самооборони Майдану відновили патрулювання міст Південного Сходу ***(Росія розпочинає в Україні проект «новая русская весна» // Espreso.tv (http://espreso.tv/news/2015/03/03/rosiya_rozpochynaye_v_ukrayini_proekt_quot novaya_russkaya_vesnaquot). – 2015. – 3.03).***

***

Сторонники «Исламского государства» (ИГ) угрожают расправиться с одним из основателей Twitter Д. Дорси. Последователи террористов мотивируют такие действия постоянной блокировкой их аккаунтов. Об этом

сообщает BuzzFeed со ссылкой на пост на сервисе Justpaste, в котором появились соответствующие угрозы.

«Ваша виртуальная война станет настоящей войной с вами», – говорится в анонимном послании, адресованном основателю Twitter. Эта надпись сопровождается фотографией Д. Дорси, поверх лица которого нарисован прицел ружья.

«Мы говорили вам с самого начала, что это не ваша война, но вы не поняли этого и продолжали закрывать наши аккаунты на Twitter, однако мы всегда возвращались», – цитирует ресурс сообщение. Помимо этого, пост содержит открытые намеки на угрозы смерти, направленные в отношении предпринимателя и сотрудников Twitter.

Представитель компании Д. Проссер сказал ресурсу, что отдел безопасности соцсети совместно с правоохранительными органами уже расследуют достоверность этих угроз.

В середине февраля хакеры из Anonymous взяли на себя ответственность за взлом 800 аккаунтов Twitter сторонников «Исламского государства». По данным организации, владельцы этих страниц имели отношение к террористической группировке.

Twitter, как и видеохостинг YouTube, как правило, оперативно реагирует на появляющиеся видео «Исламского государства» с казнями заложников. Компании удаляют такие посты и блокируют аккаунты, публикующие запрещенную информацию.

Пользовательское соглашение Twitter подразумевает, что компания имеет право ограничивать публикацию постов, содержащих открытые угрозы насилия против других людей. Также запрещено использовать соцсеть в незаконных целях или для неправомерной деятельности ***(Сторонники ИГ пригрозили смертью создателю Twitter // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42623/118/lang,ru/). – 2015. – 3.03).***

***

Нігерійське ісламістське екстремістське угруповання «Боко Харам» розмістило 2 березня у Twitter відео двох обезголовлених чоловіків. Про це повідомила Associated Press.

Назва цього відео, запущеного на його замовлення медійною групою SITE, – «Жнива шпигунів» (Harvest of Spies).

На ньому не показані самі обезголовлення, однак поведінка ісламістів жахає своєю жорстокістю. Відтяті ними голови жертв лежать на грудях закатованих.

Чоловік, якого називають Д. Мухаммедом з міста Бага, спочатку стоїть на колінах перед кількома озброєними бойовиками в масках. Він зізнається, що отримав від поліцейського 5 тис. найрів (25 дол.). Їх він мав відробляти шпигунством і втішатися обіцянкою, що розбагатіє і йому ніколи більше не доведеться поратися на землі.

Другою жертвою є нігерієць М. Авлу.

Дотепер «Боко Харам» розповсюдила лише одне відео публічної страти – обезголовлення захопленого в полон пілота військово-повітряних сил Нігерії

Американська новинна організація звертає увагу на копіювання пропаганди «Ісламської держави в Іраку і Леванті» (ISIS), що здобула сумну славу у світі публічними стратами. Серед її жертв – викрадені американські репортери-фрілансери Д. Фоулі та С. Сотлофф, японський журналіст К. Гото.

Раніше Boko Haram оголосила в соціальних медіа, що збирається присягнути на вірність ISIS.

SITE хизується тим, що для вдосконалення пропаганди запозичив з її відео «деякі елементи», зокрема, зйомку серцебиття та важкого дихання смертників перед стратою.

Наслідуючи своїх «духовних» наставників, засноване 2002 р. екстремістське угруповання «Боко Харам» діє методами терору в найбільшій за чисельністю населення африканській країні. Минулого року вона проголосила створення на підконтрольній їй північно-східній території Нігерії ісламського халіфату із законами шаріату. 2014-го Рада Безпеки ООН визнала «Боко Харам» терористичною організацією ***(Ісламісти «Боко Харам» залякують нігерійців у Твіттері // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/web/social/islamisti_boko_kharam_zalyakuyut_nigeriytsiv_u_tvitteri/). – 2015. – 3.03).***

***

Украина. Стартовые условия и места осечек в информационной войне, – мнение

На первый взгляд, позиции России в Украине были более чем сильны. Этому способствовало несколько факторов:

1. Низкая мобильность населения. Более 77 % украинцев ни разу не выезжали за рубеж. А более 30 % за всю жизнь не покидали границ своей области. Причём в Крыму показатель превышает 47 %, информирует eizvestia.com (http://eizvestia.com/?p=4432105).

2. Как результат низкой мобильности, в Украинском обществе широко распространены негативные стереотипы восприятия жителей других регионов. Контакты между частями страны зачастую были меньшими, чем жителей приграничных территорий с соседними государствами.

3. При этом у украинцев огромное значение (как источник информации) имеет «личный контакт» – то, что рассказывают, друзья, знакомые. По данным исследования, проведённого IRI уже в 2014 г. 40 % жителей страны указало этот способ получения информации как один из основных. При этом во всех регионах, кроме запада страны, «рассказ друга» входит в тройку основных источников, которым люди доверяют.

4. На Юге и Востоке страны широко присутствуют и популярны российские каналы. РТР, ОРТ, НТВ смотрели (и доверяли как источнику

информации) 47 % и 44 % жителей соответственно. Для сравнения, российское ТВ в западной и центральной части страны имело рейтинги имеет 14 % и 16 %.

5. Социальные сети. Украина входила и пока входит в число стран, где российские социальные сети по числу пользователей вне конкуренции. На начало 2014 г. по данным Яндекс в стране было более 7,47 млн аккаунтов «ВКонтакте», 1,57 млн «Одноклассники». Facebook могла похвалиться всего лишь 857 тыс. участников.

Причём картина была одинаковой в большинстве регионов. За исключением Луганской области с достаточно большим охватом сетью «Одноклассники» – она хоть и осталась на втором месте, но имела значительно большее число подписчиков в расчёте на 1 пользователя Интернет. Вторым исключением стала Одесская область, у жителей которой на втором месте Facebook.

На первом этапе информационной атаки действия российской стороны были более чем успешными. Сконцентрированная подача одной и той же темы в СМИ, социальных сетях, комментариях в интернет-изданиях и обычных слухах стала неожиданностью для нового правительства Украины. Этому так же способствовало поведение отдельных украинских каналов, которые изменили тональность после победы Майдана. Замена «чёрного» на «белое» сыграла с ними плохую шутку: значительная часть населения начала воспринимать как достоверную информацию из второго по порядку источника. Коими в южных и восточных областях были российские СМИ ***(Украина. Стартовые условия и места осечек в информационной войне, – мнение // Экономические известия (http://eizvestia.com/?p=4432105). – 2015. – 6.03).***

***

Facebook ужесточит политику по борьбе с фальшивыми аккаунтами. Об этом заявил глава компании М. Цукерберг.

Проблема фальшивых профилей пользователей стала одной из главных для соцсети в последнее время. Главной напастью являются люди, создающие аккаунты от чужого имени. Особенно остро проблема стоит в развивающихся странах, например, в Индии.

Социальная сеть не раскрывает деталей механизма борьбы с угрозой. Одним из главных инструментов должна стать обратная связь с добросовестными пользователями.

На данный момент, согласно пользовательскому соглашению, никто не может создавать аккаунт от чужого имени. Впрочем, пользователи могут давать разрешение на создание аккаунтов от своего имени. Также социальная сеть просит юзеров не создавать более одного профиля.

Количество фальшивых профилей в Facebook составляет 2 %, по данным самой компании. Многие наблюдатели отмечают, что реальная цифра может быть куда выше. Facebook не единственная интернет-компания,

испытывающая подобные проблемы. Twitter также недавно ужесточил борьбу с фальшивыми пользователями.

В компании очень серьёзно относятся к проблеме фальшивых профилей, заявил глава социальной сети. М. Цукерберг не раз отмечал, что это сильно вредит репутации компании ***(Facebook поборется с фальшивыми аккаунтами // InternetUA (http://internetua.com/Facebook-poboretsya-s-falshivimi-akkauntami). – 2015. – 9.03).***

***

З терористами в контакті. Коли погрожують дітям

Минулого тижня в обласному управлінні СБУ двічі збиралися силовики, освітяни й представники батьків школярів. Обговорювали одне – інформаційну безпеку дітей. Приводом став просто кричущий випадок, коли восьмикласниці зі Снятинщини через повідомлення «ВКонтакте» терористи надіслали відео з погрозами.

Свого часу учні Джурівської школи, що в Снятинському районі, писали листи підтримки до наших військових, відправили їх напередодні свята Миколая. Хлопці передачу отримали, подякували і навіть вислали школі прапор. У наших реаліях – уже цілком традиційна картина. Так роблять тисячі дітей по всій Україні. Але далі ці листи на покинутому блокпості під Чернухіним Луганської області знайшли терористи. І вирішили дітей полякати – записали демонстративний ролик, пише Репортер.

На розгромленому блокпості огрядний дядько звертається до 13-річної дівчинки Х. Мондяк, листа якої тримає у руках.

«Твої захисники, ніби захисники, ми їх прикопали тут, недалеко. Твій учитель у школі змусив тебе написати цей лист, то плюнь в нього і скажи: дядьку, ти говориш неправду. Україна окупована і окупували її не російські війська, а Америка».

Це ще м’який переказ – лексика того «повідомлення» відверто зневажлива й хамська. Далі показують розбитий блокпост і листи інших дітей, де навіть вказані номери їхніх телефонів.

На саму дівчинку вийшли через соцмережі. Потім на її адресу посипалися такі ж образливі коментарі від прихильників окупантів. Дитина, звісно, перелякалася і, цілком логічно – з того «ВКонтакте» видалилася. У школі зчинився переполох, але вчителям все ж таки вдалося пояснити дітям, що цей ролик якраз і робився для залякування. Тож діти й далі збираються писати листи в АТО.

Та сам випадок знову порушив питання інформаційної безпеки дітей. На жаль, він не єдиний, хоч і найбільш кричущий. На цій нараді в СБУ пролунало: є випадки, коли терористи знаходять у соцмережах дітей, які постять патріотичні речі, і переписуються з ними. Та й уся російська пропаганда і просто фейки (придумані новинки), які є в Інтернеті, цілком доступні для наших дітей. І з цим треба щось робити.

Усі прекрасно розуміють, що заборонити дітям доступ до цих сайтів і соцмереж просто нереально. Керівник обласного СБУ М. Найдич так і заявив – служба не хоче і не може цього зробити. Єдиний варіант – пояснити, переконати.

У Івано-Франківську запускають інформаційну кампанію, головним завданням якої є відвернути дітей від російських соцмереж – «ВКонтакте», «Одноклассники», «Мой мир@mail.ru». Або хоча б, щоб вони не вказувати там свої особисті дані – справжні імена, телефони, адреси, де навчаються тощо. Що будуть робити? Уже оголошений конкурс серед франківських школярів на кращий мультимедійний проект, спрямований проти російських соцмереж. Також готують відеоролики на екранах у центрі міста, будуть зустрічі із самими учнями, класними керівниками, батьками. Далі вся схема має запрацювати по районах.

Ніхто не каже, що захистити дітей буде просто.

«Вберегти практично неможливо, – говорить заступник начальника міського управління освіти С. Уварова. – От на сайті Міносвіти вже давно висить інформація для батьків про інтернет-безпеку. Там радять ставити паролі на комп'ютер, контролювати час дитини в Інтернеті і т. д. Але це малодієве. Нині є ті ж телефони, планшети, інтернет-клуби – доступ не обмежити. Єдиний варіант – навчити їх поводитися там правильно».

С. Уварова доводить: колись, у дитинстві, нас батьки вчили – ніколи нікуди не йти з незнайомцями, не відкривати двері чужим, коли ти один вдома… Нині ми вийшли на інший рівень – і так само дитина має бути навчена не приймати чужих у друзі в Інтернеті, не виставляти у соцмережах особисту інформацію, не вступати в дискусію з чужими.

Треба розуміти, каже вона, що зараз маємо потужну інформаційну війну. Чим можна захистити дітей? Навчити їх розпізнавати брехню. Для прикладу демонструє ролик за 2012 р. з російського телеканалу про 1 вересня у Львові, який був присвячений УПА.

«Наші вчителі історії не могли додивитися його до кінця! – говорить С. Уварова. – Але дітям можна проілюструвати явні викривлення фактів – і коли була створена УПА, і про те, що на суді в Нюрнберзі про наших повстанців навіть не було мови. Діти старших класів це вже знають. І ми націлюємо вчителів показувати це і розвінчувати будь-який фейк лише фактами. Треба навчити дітей шукати факти з перевірених джерел, а висновки вони нехай роблять самі».

Також важливо пояснити їм, що є засадничі принципи життя нашої держави, які під сумнів ставити не можна.

«Що територіальна цілісність України має бути недоторканною, бо боротьба за переділ уже поділеного світу стала першою причиною двох світових воєн, які призвели до страшних наслідків», – наголошує С. Уварова.

Пояснення в школах, на білбордах, через рекламу – це, звісно, добре. Але чи прислухається до них саме ваша дитина? Ви колись питали у неї, що вона переглядає в Інтернеті та з ким спілкується у соцмережах? Напевно, вже

пора ***(З терористами у контакті. Коли погрожують дітям // Бліц-інфо (http://www.blitz.if.ua/news/z-terorystamy-u-kontakti-koly-pogrozhuyut-dityam.html). – 2015. – 13.03).***

***

Самым популярным каналом связи среди террористов и диверсантов являются российские социальные сети.

Боевики из незаконного военного формирования т. н. «Русской православной армии» (РПА) планировали взорвать в Херсоне офисы двух украинских общественно-политических организаций с помощью почти 3 кг пластида. Об этом сообщил пресс-центр СБУ.

Преступление готовилось через российские социальные сети. Это уже стало устоявшейся практикой террористов и диверсантов, таким образом вербуются и наемники для участия в незаконных военных формированиях на востоке Украины.

«Курьера», который должен был доставить взрывчатку в Херсон, задержали в Одессе. Им оказался гражданин Украины, 1963 г. р., уроженец Донецка, который с 2000 г. проживает в Одессе. У него была изъята сумка со взрывчаткой ***(Донецкий одессит готовил два теракта в Херсоне // Лица (http://www.litsa.com.ua/show/a/20899). – 2015. – 9.03).***

***

Прихильники терористичного угруповання «Ісламська держава» (ІД) створили свою соціальну мережу – Caliphate book. Про це повідомляє агентство Рейтер.

Це сталося після того, як акаунти терористичного угруповання в інших соціальних мережах були заблоковані.

За даними агентства, через день після своєї появи сайт 5elafabook.com виявився недоступним, тому поки невідомо, хто його створив і скільки користувачів там зареєструвалося.

Назва сайту походить від арабського слова khilafa, що означає халіфат. Поєднання «kh» в арабській мові позначають цифрою 5.

Сайт перекладено сімома мовами: голландською, англійською, іспанською, португальською, турецькою, індонезійською і яванською. При цьому арабською він недоступний.

На сторінці ресурсу повідомляється, що він тимчасово призупинив свою діяльність для того, щоб «захистити інформацію про користувачів і забезпечити їх безпеку».

«Сайт 5elafabook.com незалежний, нас не спонсують бойовики ІД. Ми хочемо показати всьому світу, що ми не тільки ходимо зі зброєю в руках і живемо в печерах, як вони це уявляють. Ми розвиваємося разом зі світом і хочемо, щоб цей розвиток був ісламським», – ідеться на сайті.

Ісламісти використовують соціальні мережі переважно для вербування нових бойовиків і обміну інформацією. Крім того, вони викладають у мережу відео зі стратами заручників.

Терористичне угруповання «Ісламська держава», що має зв'язки з «Аль-Каїдою», на початку червня захопило значну частину територій Сирії та Іраку. Екстремісти оголосили про створення на захоплених територіях «ісламського халіфату». США, які очолюють міжнародну коаліцію проти ісламістів, 8 серпня почали військові дії проти екстремістів в Іраку. У вересні вони приступили до завдання повітряних ударів по цілях ІД у Сирії ***(Прихильники «Ісламської держави» створили аналог Facebook // LB.ua (http://ukr.lb.ua/news/2015/03/10/298027_prihilniki_islamskoi_derzhavi.html). – 2015. – 10.03).***

***

Бойцы невидимого фронта. Как украинцы воюют с российскими ботами в интернете

Куратор «Информационных войск» А. Барабошко рассказал, как за тысячу долларов создать армию правдолюбов, чем российские боты отличаются от украинских патриотов, а промывка мозгов – от контрпропаганды, пишет Marketing Media Review (http://mmr.ua/news/id/bojcy-nevidimogo-fronta-kak-ukraincy-vojujut-s-rossijskimi-botami-v-internete-43555/).

А. Барабошко поначалу скептически отнёсся к созданию Министерства информационной политики. Однако прежде чем начать критиковать главу ведомства Ю. Стеця, решил ему написать, предложив свои услуги, так как хотел быть чем-то полезным. Министр ответил. А. Барабошко познакомился с людьми из его команды. Спустя какое-то время ему предложили пост советника.

«Я сказал, что мне больше подходят непубличные форматы работы, но если надо, я не против. Потом запустился сайт министерства, я нашёл себя в списке четырёх советников министра. Реакция была такой же, как и у остальных: ого!» – говорит А. Барабошко.

Последние несколько лет А. Барабошко работал в медиапроектах. «Фактически я занимался информационными войнами, только в украинской политике», – отмечает он.

А. Барабошко предполагает, что информационные войска со временем смогут не только защищаться, но и навязывать проукраинскую позицию в сети. Задача бойцов – доносить правдивую информацию о происходящих в стране событиях. Советник министра признаёт, что, как ни крути, речь идёт о промывке мозгов, но при этом подчёркивает, что Украине приходится защищаться.

Волонтёрская идея

Кто автор идеи создания информационных войск?

– Авторы идеи – ребята-волонтёры, которые работают в этой сфере. Они пришли к министру в середине января и предложили её реализовать. Министру она понравилась, он поддержал, какие-то минимальные деньги им дали. Хотя мне кажется, что было бы правильнее делать это именно как волонтёрский проект, тогда можно было бы развернуться. Например, было задание зайти на Lifenews и там нормально откомментить новости. Куча людей сорвалась, Lifenews отключил комментарии. Но со стороны государства такие шаги не очень корректны.

Я так понял, что этот проект практически не финансируется государством.

– Да. Это небольшие деньги. Точные цифры не назову, но речь идёт примерно о тысяче долларов.

Как это работает?

– Есть сайт. Нужно заполнить форму. Не требуется каких-то особых персональных данных: можно зарегистрироваться под своим именем или никнеймом. Потом на твою почту приходят письма с актуальными заданиями. Например, как только появляются сведения о расследовании трагедии с боингом, россияне наполняют эфир своими статьями. В них приводятся всевозможные фантастические аргументы, доказывающие, что виновата Украина. Есть потребность разбавлять эфир достоверной информацией.

Где вы её берёте?

– Из разных источников. Это мониторинги ОБСЕ, ссылки на какие-то официальные украинские ресурсы, на авторитетные источники в зарубежных медиа и т. д. Эти источники сложно назвать стопроцентно достоверными, но они однозначно более авторитетны, чем российская пресса.

Кто вступает в войска?

– Большая часть (а это более 35 тыс.) зарегистрировалась в первый же день, далее регистрируются не так динамично. Аудитория разношёрстная, в том числе много россиян. Там проходят целые мобилизационные кампании, всякие «антимайданы» предлагают регистрироваться на сайте информвойск, чтобы получать информацию. И это с самого начала закладывалось в идею распространения достоверной информации. Нам на руку, если её будут читать российские пользователи. Они её получают, делают скриншоты, размещают в пабликах, пусть и снабжают ироничными комментариями – «секретные задания», «интернет-войска».

Тут главное количество. Это могут быть и школьники, и домохозяйки, и интернет-специалисты. Каждый прочтёт нашу рассылку. Если увидит, что ему ничего не подходит, не пересекается с его мировоззрением, он её проигнорирует. Но какая-то часть отреагирует. Этот проект нацелен на максимально широкую аудиторию. Министерство сейчас запускает и другие проекты с разным уровнем публичности, там уже набирают группы специалистов. В частности, начались разработки психологических атак.

Собираетесь ли вы с помощью своей армии проводить психологические операции, направленные на противника? То есть информировать о том, что происходит в российском обществе?

– Так и хотим сделать. Мы анализировали события, проблемные российские регионы. Там есть огромные проблемы, которые замалчиваются в российских медиа. С помощью наших войск мы планируем их осветить.

Боты и люди

С помощью армии ботов Россия воздействует на сознание граждан. Насколько этично использовать подобные методы даже для достижения благих целей?

– Сложно сказать. Можно это назвать донесением правды, но всё равно это промывка мозгов, как бы ты это не подавал… Я думаю, с нашей стороны это будет адекватным шагом в ответ. У нас страна в таких условиях, что нам нужно защищаться.

Вы учите людей воевать на информационном фронте, причём они это делают бесплатно. Не боишься, что эти люди переметнутся на сторону противника, если им за это будут платить?

– В информационные войска вступают патриоты. Там нет секретной информации. Вся она в открытом доступе, просто мы её систематизируем. Мне кажется, в этом нет проблемы.

Думаю, одна из задач Мининформполитики – вместе с правоохранительными органами пресекать работу теневых штабов, где работают люди, создающие бот-аккаунты. Милиции лучше бы сейчас направить силы на борьбу с ними вместо того, чтобы ходить с проверками по интернет-магазинам.

Как действует Россия на информационном фронте?

– Было время, когда российские оппозиционеры явно побеждали в Интернете. Потом кремлёвские технологи поняли, что им тоже нужно присутствовать в сети, и из года в год наращивали своё влияние. Сейчас у них десятки тысяч ботов – виртуальных аккаунтов.

В Интернете можно найти отчёты о том, сколько людей было в этом задействовано, сколько они получали. Но Украине эта система не подходит, потому что общество не готово тратить большие деньги на такие цели. К тому же у нас не получится повторить эту систему. Коммуникация с людьми более эффективна.

Правильно ли я понимаю, что со стороны России в сети работают боты, а с украинской – реальные люди?

– Однозначно. И с нашей стороны людям не кидают типовой шаблон того, что они должны написать. Им дают информацию, а они уже решают, будет с их стороны корректным это написать или нет. У нас нет речи о создании армии ботов. Идёт речь об активной коммуникации и координации граждан.

Идея создания информационных войск вызывает скепсис у многих, в том числе у специалистов. Как собираетесь его преодолеть?

– Общество находится в состоянии недоверия ко всем и всему. Люди привыкли не доверять. Скепсис можно побороть, только показывая работу и результат. Прошла неделя, и уже видно, что тональность меняется, люди говорят: давайте пробовать. Если проект себя не оправдает, думаю, его свернут.

Какая-то отдача от него уже чувствуется?

– В прошлые выходные все российские СМИ говорили про эти интернет-войска. Много скриншотов в Интернете, чувствуется, что тональность людей по отношению к Министерству информационной политики частично изменилась. Люди увидели: что-то начали делать, а этого все давно ждали.

Я, честно говоря, сам не был уверен, что это даст какой-то результат, однако очевидно, что он есть. Люди, которые используются Россией в распространении лжи, сейчас вынуждены бороться с нашими интернет-войсками, с этими донкихотовскими мельницами. Это круто.

Шансы на победу

Россия пока доминирует на этом фронте. Как ты оцениваешь шансы переломить ситуацию?

– Россия в основном очень круто была представлена в Twitter. «ВКонтакте» тоже есть какие-то паблики, но аудитория не очень интересуется политикой. Facebook в России не так распространён: у Варламова меньше аудитория, чем у украинских политических блогеров. И вообще кластер российского Facebook не очень оброс социальным капиталом. В Twitter они выглядели гораздо ярче.

Ещё год назад у меня была мечта, что украинцы смогут противостоять там россиянам. Сейчас в «топе» русскоязычного Twitter половина украинцев. На прошлой неделе П. Порошенко был на первом месте по количеству ретвитов и фолловеров. В соцсетях есть многотысячные паблики. Они начинают координироваться. Если кто-то из топовых украинских пользователей начинает разгонять истерию, люди сразу обращают внимание и дают оценку – это истерия. Самоцензурой это не назовёшь, но саморегуляцией можно.

Что нужно, чтобы побеждать?

– У нас много крутых людей – журналисты, эксперты, которые работают на каждых выборах. Раньше они работали на свои штабы, устраивая информационные войны между собой. У каждого были свои интересы. Сейчас нужно объединиться.

Во время глубокого политического кризиса власть должна активно общаться с обществом, как это делал Т. Рузвельт. Сегодня это начинает делать П. Порошенко, но так должны поступать все госорганы. Пояснять непопулярные решения. Например, сейчас все камни летят в сторону главы Нацбанка Н. Гонтаревой. Появление адекватного спикера сняло бы много вопросов. Н. Гонтарева работала бы, а с журналистами общался бы другой человек. На днях меня ребята просили напомнить Генпрокуратуре, что они

не представлены в Twitter и Facebook, почему мы должны обо всём узнавать непонятно от кого? ***(Бойцы невидимого фронта. Как украинцы воюют с российскими ботами в Интернете // Marketing Media Review (http://mmr.ua/news/id/bojcy-nevidimogo-fronta-kak-ukraincy-vojujut-s-rossijskimi-botami-v-internete-43555/). – 2015. – 13.03).***

***

У соцмережах – у групах, які підтримують проросійських сепаратистів – і у деяких чеських медіа поширюють фото, де люди стоять на колінах перед колоною автомобілів. Мовляв, в Україні так мусять вітатись із «Правим сектором», або ж з так званими «поліцаями Автомайдану». Спростування такого фотофейку не забарилось.

У соціальних мережах у групах «Антимайдан» і «Новоросія» активно поширюють фото, на якому люди стоять на колінах, а повз них проїжджають машини з українськими прапорами.

«Ось вони, раби! В Україні, зокрема у місті Львові, коли поряд проїжджають "поліцаї Автомайдану" або ж "Правий сектор", потрібно вийти з машини, встати на коліна і зняти капелюха! Вам це нічого не нагадує? Скачіть і далі, вам ще чоботи вилизувати», – розповідають під зображенням автори в соцмережах.

Імовірно, саме із соцмереж такий фотофейк підхопили й іноземні медіа, пише «Радіо Свобода» публікуючи, зокрема, новину, про «нову українську демократію» з гаслами «всі на коліна». Саме публікація з таким зображенням з'явилась на одному з чеських порталів.

Фото демонструють у контексті ритуалу, який порівнюють з ритуалом терористичних організацій, коли громадяни мусять знімати капелюхи перед кортежем терористів. Пишуть, буцімто такий ритуал був «удосконалений бандерівцями». І заявляють, що на телебаченні такого не покажуть.

«Не дивно, що наші ЗМІ не цікавить, як почуваються пересічні українці, які живуть у контрольованій войовничою хунтою державі. І не тільки на окупованих територіях колишньої Луганської та Донецької областей, які досі контролює Київ, але й у центральних і західних регіонах країни, яка розпадається. Повідомлення, які надходять із цих регіонів, часто схожі на ті, що (бачимо) у сучасному Мосулі під владою "Ісламської держави"», – написано на чеському порталі, відомому, серед іншого, матеріалами антєвропейського, антиамериканського і проросійського змісту, на кшталт: «США хочуть війни з Росією за будь-яку ціну. Американські окупаційні підрозділи вже в нас і не ховаються!»)

Знімок, який при цьому публікують, насправді показує, як жителі міста Коломиї засвідчують повагу загиблому під час бойових дій на Сході України землякові Р. Фурику. Люди стоять на колінах перед колоною автомобілів, щоб провести в останню путь свого героя. На підтвердження цього є і відео українських медіа ***(Чеський портал поширює фотофейк про «вітання» з «поліцаями Автомайдану» // Західна інформаційна корпорація***

***(http://zik.ua/ua/news/2015/03/11/cheskyy_portal_poshyryuie_fotofeyk_pro_vitannya_z_politsayamy_avtomaydanu_571343). – 2015. – 11.03).***

***

На своих официальных страницах в социальной сети активисты антиукраинских формирований «Новороссия ХНР» и «Новая Херсонщина» устроили письменные баталии.

Лейтмотив дрязг – ответ на вопрос: кто «настоящий» сепаратист, а кто лишь фейк. Координатор «Новороссия ХНР» называет активистов Новой Херсонщины «укроповскими провокаторами» и просит отписаться от данного паблика.

Чем закончится передел власти? Увидим ***(Херсонские сепаратисты «грызутся» за власть // Kherson.in (http://kherson.in/news/hersonskie_separatisty_gryzutsja_za_vlast). – 2015. – 13.03).***

***

Сепаратисти в Луганську створили власний центр «інформаційних військ»

У Луганську, який перебуває під контролем сепаратистів так званої «ЛНР», був відкритий блогер-центр, який покликаний, як заявляють його засновники, «прорвати інформаційну блокаду» щодо висвітлення подій на контрольованій терористами території Луганської області. Про це інформує сепаратистське видання «Луганский информационный центр».

Як повідомляється, на перші збори блогер-центру, приміщення для якого надало молодіжне інформагентство «Исток», прийшли близько 20 осіб. Керівник центру Д. Кукарський заявив, що адміністраторами в більшості луганських груп у соціальних мережах є не луганчани або луганчани, які проживають не на території «ЛНР». За його словами, через це велика частина інформації – необ'єктивна і «не відповідає нашим реаліям». Він закликав присутніх «прорвати» інформаційну блокаду.

Блогери, за його словами, повинні підключитися до висвітлення будь-яких інформаційних приводів «ЛНР». Д. Кукарський також заявив, що в центрі буде «школа молодого блогера», де навчатимуть початківців. Як «викладачі» виступлять журналісти видання «Луганский информационный центр». Він також додав, що проект блогер-центру базуватиметься на групі в соціальній мережі «ВКонтакте» «Столичный Луганск».

Нагадаємо, 10 березня так звана «рада міністрів» «ЛНР» прийняла постанову «Про обмеження мовлення деяких телеканалів на території ЛНР», якою заборонено мовлення 23 українських телеканалів, а також російського телеканалу «Дождь» ***(Сепаратисти у Луганську створили власний центр «інформаційних військ» // Телекритика (http://www.telekritika.ua/kontekst/2015-03-12/104806). – 2015. – 12.03).***

***

Колишній прокремлівський інтернет-бот розповів, як побудована їх система зсередини

Після вбивства Б. Нємцова кремлівських «ботів», які працюють у коментарях у соцмережах та популярних інтернет-сайтах, терміново переключили з подій в Україні на резонансне вбивство російського опозиціонера.

Про це «Новой газете» розповів колишній найманець пропагандистських військ Олексій, який раніше працював у так званому «лігві тролів», офіс якого розташований у Петербурзі.

«Коли вбили Нємцова, робота кремлеботів змінилася: вони перестали мочити Україну (це їх рутинна щоденна робота) і були перекинуті на вбивство. Якщо ви тоді стежили за новинами, то могли бачити під усіма текстами про вбивство Нємцова сотні, а інколи й тисячі коментарів, де різними словами повторювалися одні й ті ж тези: вбивство – це провокація, Кремль тут ні до чого, це опозиція вбила свого, щоб залучити побільше народу на марш. Плюс брудні жарти з приводу особистого життя убитого. Це був танець на кістках, який триває й досі. Навіть якщо хтось із них і пошкодував щиро про вбитого – робота є робота», – розповів Олексій.

Також він пояснив як працює система зсередини.

Офіс ТОВ «Інтернет-дослідження» розташований у спальному районі Петербурга на вул. Савушкіна. За словами Олексія, єдиним критерієм під час прийому на роботу є питання: як ви ставитеся до чинної влади. Беруть на роботу майже всіх – студентів, колишніх відомих радіоведучих, інвалідів, неформалів, скінхедів, домогосподарок і навіть подружні пари.

Співробітники агентства практично не спілкуються між собою, за найменшу провину штрафують, двері в кабінети мають бути зачиненими, а вікна завішені жалюзями. Так, за одними дверима – люди, які коментують новини, художники малюють карикатури на Навального і Обаму, за іншими – блогери, які критикують Україну, ЄС, Обаму, Навального і російську опозицію в цілому, вихваляють Путіна і міністра оборони С. Шойгу.

Частина співробіників – блогери. Майже всі блогери живуть у Санкт-Петербурзі, свої акаунти створили у 2013 р. Вони не займають високе місце в рейтингу LiveJornal (замовник «бере» їх кількістю), періодично розбавляють «домогосподарчі пости» своїми версіями політичних подій.

Видання публікує приклади завдань для формування громадської думки та пропаганди деяких блогерів, а також перелік нікнеймів ботів, які працюють у рамках петербурзького проекту на Кремль. Детальніше за посиланням ***(Колишній прокремлівський інтернет-бот розповів, як побудована їх система зсередини // UkrainianWatcher (http://watcher.com.ua/2015/03/11/kolyshniy-prokremlivskyy-internet-bot-rozpoviv-yak-pobudovana-yih-systema-zseredyny/). – 2015. – 11.03).***

## Зарубіжні спецслужби і технології «соціального контролю»

Группу «Крым и крымские татары» удалили из популярной российской социальной сети «Одноклассники», передает УНН со ссылкой на Крымскую полевую миссию по правам человека.

Как сообщил глава общины крымских татар в Москве М. Мухтеремов, сначала администрация социальной сети заблокировала, а затем и удалила группу «Крым и крымские татары».

По его данным, численность группы составляла более 14,5 тыс. человек, а была зарегистрирована группа в сети в мае 2008 г.

Правозащитники связывают такие действия с использованием указа главы аннексированного Крыма С. Аксенова «Об утверждении Комплексного плана противодействия терроризму в Республике Крым на 2015–2018 г.», который был издан 30 января. В указе, в частности, запланированы мероприятия по защите интернет-пространства Крыма и блокировке сайтов, содержащих террористические и экстремистские материалы на усмотрение местных органов самоуправления.

Как сообщал MIGnews.com.ua, международное сообщество должно обратить внимание на данные о нарушениях прав крымских татар ***(Группу крымских татар удалили из «Одноклассников» // Mignews.com.ua (http://mignews.com.ua/regiony/krym/5050306.html). – 2015. – 10.03).***

***

Санкт-Петербурзька митрополія Російської православної церкви «не благословила» публічного вираження точки зору священнослужителем Миколою (Савченком) про війну в Україні.

Про це священик написав у своєму блозі.

За його словами, «не благословляється» також дискусія у соціальних мережах на тему подій в Україні.

Священик не повинен виступати на згадану тему в медіа, публічно виражати свою позицію «для уникнення смути та гострих спорів у середовищі громадськості».

«Замість цього мені належить посилити молитви про те, щоб в Україні якомога швидше встановися міцний мир», – написав о. Микола (Савченко).

Він також висловив думку, що цю історію не слід сприймати як заборону оцінки війни як братовбивчої чи закликів до миру. Священик зауважив, що в коментарях до його дописів часто було надто багато нецензурної лексики, а займатися постійним наглядом за численними коментарями у нього не було ні сил, ні бажання.

«У цьому сенсі стан сторінки досить повно відображає стан нашого хворого та розділеного суспільства, де вирують пристрасті і живе ненависть. З часом утворилася група активістів, які взяли собі за мету домогтися мого покарання, як нібито ворожого шпигуна та зрадника Батьківщини», – написав ієрей Микола (Савченко).

Раніше священик зазначав у своїх дописах, що був учасником Маршу миру, виступав за припинення агресії Росії щодо заходу, критикував ворожу пропаганду російських ЗМІ ***(Священика РПЦ «попросили» не писати у своєму блозі про Україну // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/web/social/svyaschenika_rpts_poprosili_ne_pisati_u_svoemu_blogi_pro_ukrainu/). – 2015. – 5.03).***

***

Українські спецслужби затримали двох мешканців Дніпропетровщини, які підозрюються в поширенні через Інтернет закликів до порушення територіальної цілісності України. Про це повідомив у четвер, 5 березня, на щоденному брифінгу речник штабу Антитерористичної операції (АТО) полковник А. Лисенко, передає «Укрінформ».

Як повідомив речник штабу АТО, двоє затриманих мешканців Дніпропетровщини пройшли спеціальну підготовку в тренувальному таборі у російському місті Бєлгороді.

«У Дніпропетровській області затримали двох місцевих мешканців, які підозрюються у створенні інтернет-ресурсів, через які поширювались заклики до насильницької зміни влади та порушення територіальної цілісності України, а також здійснювався збір коштів для бандформувань "ДНР" та "ЛНР"», – повідомив він.

А. Лисенко наголосив, що під час затримання у них вилучено зброю, боєприпаси до неї, а також техніку для конспіративного зв'язку.

Нагадаємо, СБУ затримала громадянина Російської Федерації, якого підозрюють у причетності до збору інформації щодо місць дислокації та переміщення військових формувань, військової техніки й військовослужбовців Збройних сил України в районі населених пунктів Костянтинівка та Дзержинськ (Донецька область). У росіянина контрозвідники СБУ виявили радіотехнічний комплекс, спроможний здійснювати моніторинг радіоефіру та проводити радіосеанси на широкому діапазоні радіочастот, саморобну радіозакладку для здійснення негласного прослуховування, персональний комп'ютер з можливістю віддаленого доступу та керування ним через мережу Інтернет, значну кількість супутникового обладнання, переважна частина якого здійснює прийом російських телеканалів, USB-носії з відеофайлами антиукраїнського спрямування, більшість з яких є матеріалами російського телеканалу LifeNews ***(На Дніпропетровщині затримані місцеві мешканці за підозрою в агітації в Інтернеті на користь «ЛНР»-«ДНР» // Телекритика (http://www.telekritika.ua/pravo/2015-03-05/104576). – 2015. – 5.03).***

***

Начальник Донецкого ГУ МВД Украины В. Аброськин на своей странице в Facebook сообщает, что они собирают материалы на бывших коллег, которые перешли на сторону боевиков.

Террористы и боевики при поддержке предателей из ряда сотрудников областной милиции, пишет В. Аброськин, весной прошлого года начали бандитский захват городов в Донецкой области.

Они собирают материалы на бывших милиционеров, которые сейчас действуют в рядах «полиции ДНР», и направляют их в прокуратуру. Экс-правоохранителей объявляют в розыск и заводят на них уголовные дела.

В. Аброськин на своей странице публикует фотографии тех, кто перешел на сторону противника, и обещает постоянно его обновлять, публикуя имеющуюся в его распоряжении информацию о бывших украинских милиционерах.

Напомним, ранее сообщалось, что боевиками, которые активно обстреливали Дебальцево, разрушая его инфраструктуру и убивая мирных жителей, руководит бывший подполковник милиции в запасе Качура Ольга Сергеевна, которую опознали ее коллеги по тому периоду, когда она еще служила в рядах МВД ***(Аброськин публикует фотографии бывших украинских милиционеров, перешедших на сторону врага // NovostiUA.net (http://novostiua.net/proisshestviya/66098-abroskin-publikuet-fotografii-byvshih-ukrainskih-milicionerov-pereshedshih-na-storonu-vraga.html). – 2015. – 10.03).***

***

Отказ соцсети блокировать страницы «украинских националистов» заставляет российское ведомство подозревать Twitter в распространении экстремистской информации

Роскомнадзор направил в адрес администрации социальной сети Twitter письма с требованием объяснений неприкосновенности аккаунтов с экстремистской информацией, информирует news.eizvestia.com (http://news.eizvestia.com/news_abroad/full/726-roskomnadzor-ne-mozhet-najti-upravu-na-twitter).

Об этом глава ведомства А. Жаров сообщил в среду, 11 марта, в эфире телеканала «Россия 24».

«Так как Twitter также указал, что сознательно не блокирует ресурсы украинских националистов, мы сочли такую ситуацию неприемлемой и направили им письмо с просьбой разъяснить их позицию», – заявил А. Жаров. По его словам, в конце февраля был получен ответ, что запрос рассматривается. В очередном письме от 10 марта Роскомнадзор просил поторопиться с ответом.

А. Жаров отметил, что социальная сеть не удовлетворила ни один из направленных ей российским ведомством 108 запросов. В частности, игнорировались запросы Роскомнадзора на блокировку экстремистской информации и предоставлении сведений о посещаемости российских аккаунтов сети. В то время как от властей США (Twitter является американской компанией) поступило и выполнено около 2,5 тыс. просьб ***(Роскомнадзор не может найти управу на Twitter // Экономические***

***известия (http://news.eizvestia.com/news_abroad/full/726-roskomnadzor-ne-mozhet-najti-upravu-na-twitter). – 2015. – 12.03).***

***

Обновленная версия программного клиента Skype для Windows и Mac осуществляет цензуру передаваемых в переписке гиперссылок на сайты в Интернете. Об этом пишет rg.ru.

По его словам, на проблему ему пожаловались сразу несколько знакомых. Они рассказали о невозможности передать ссылки через чат Skype.

Более подробное изучение проблемы показало, что программный клиент Skype подвергает удалению ссылки на популярный китайский интернет-магазин DX.com. DRek отмечает, что после отправки ссылки какое-то время видны на экране у адресата, однако менее чем через секунду удаляются из переписки. При этом на стороне отправителя ссылки не удаляются.

В ходе исследования также выяснилось, что версии клиента Skype версии 5.5 и ниже не подвергают цензуре отправляемые ссылки. Кроме того, в групповых чатах ссылки пересылаются без проблем. Возможно, клиент отправляет сообщения куда-то на модерацию, предполагает автор поста на Habrahabr.ru.

В комментариях к записи пользователи сообщают, что без приставки «www» ссылки доставляются без каких-либо проблем. Подвергаются ли проверке другие заранее определенные адреса, неизвестно ***(Россияне уличили Skype в цензуре ссылок // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42729/118/lang,ru/). – 2015. – 12.03).***

***

В российских регионах пользователей соцсетей приговаривают к стотысячным штрафам за репосты.

В Кемерово суд обязал блогера С. Калиниченко заплатить штраф в размере 150 тыс. р. за обвинение в «публичных призывах к экстремизму».

Пользователь Twitter сделал в 2013 г. ретвит фотографии с текстом «Бросить ходить на митинги и начать действовать». От себя С. Калиниченко добавил «Я ни к чему не призываю, я просто делюсь фотографией».

Своей вины блогер не признает, пишет «Новая газета».

11 марта похожее дело рассматривали в суде города Иваново. Активистку Е. Красикову приговорили к штрафу в 100 тыс. р.

Дело против Е. Красиковой открыли весной 2014 г. за репост в соцсети «ВКонтакте». Активистка отправила к себе на стену публикацию «Обращение украинцев к народам России».

В суде заявили, что в публикации был призыв к насильственному изменению основ конституционного права РФ.

Однако Е. Красикова заявляет, что сделала репост для того, чтобы обсудить его, а не призывать к чему-то. «Я не соглашалась с авторами текста и не собиралась никого ни к чему призывать, как утверждает гособвинитель», – сказала девушка.

По словам активистки, все обвинения строятся на показаниях «секретных свидетелей». Они не являются надежными, ведь один из таких свидетелей утверждал, что познакомился с Е. Красиковой на протестной акции в 2012 г. Однако девушка начала посещать такие мероприятия только с 2013 г.

Активистка находится на шестом месяце беременности, поэтому суд дал ей рассрочку с выплатой штрафа в три года ***(Свободомыслие в сети стало опасным для россиян // Четверта Влада (http://4vlada.net/v-mire/makkein-raskritikoval-pozitsiyu-shtainmaiera-po-ukraine). – 2015. – 12.03).***

***

«Роскомнагляд» з листопада 2012 р. промоніторив понад 165 тис. підозрілих інтернет-ресурсів і заблокував близько 6,5 тис. сайтів.

Про це в ефірі телеканалу Росія 24 заявив голова відомства О. Жаров, пише ВВС Україна.

О. Жаров сказав, ці сайти не виконали вимоги відомства з видалення незаконної інформації ***(У Росії заблокували майже 6,5 тисячі сайтів, що відмовились від співпраці з владою // Західна інформаційна корпорація (http://zik.ua/ua/news/2015/03/12/u_rosii_zablokuvaly_mayzhe_65_tysyachi_saytiv_shcho_vidmovylys_vid_spivpratsi_z_vladoyu_571602). – 2015. – 12.03).***

***

«Репортери без кордонів» розблоковують сайти, заборонені в країнах-«ворогах Інтернету»

Міжнародна медійна організація розблокувала доступ до дев'яти новинних сайтів, заборонених в 11 країнах.

«Репортери без кордонів» (RSF) роз'яснили подробиці своєї міжнародної акції «Паралельна свобода» (CollateralFreedom).

Її мета – приборкати цензуру в мережі, зробити заблоковані сайти доступними для користувачів.

Щоб обійти їхнє блокування урядами-порушниками прав людини, «Репортери» використовують технологію «дзеркального відображення». Вони дублюють заборонені сайти й розміщують їхні копії на серверах інтернет-гігантів, таких як Amazon, Microsoft і Google.

В 11 країнах, що входять до числа «ворогів Інтернету», їхні сервери блокують. Це обходиться надто високою економічною та політичною ціною. Десять щойно створених дзеркальних сайтів RSF, як стверджує медіа-організація, практично захищені від цензури.

«Репортери» орендують широкоформатну пропускну смугу. Чим більше користувачів мережі відвідуватимуть дзеркальні сайти, тим у ширших масштабах користуватимуться нею.

RSF звертається до інтернет-користувачів із проханням оплачувати додаткові пропускні спроможності широкоформатної смуги з тим, щоб дзеркальні сайти були доступними якомога довше.

Медіа-організація пропонує всім охочим долучитися до своєї акції, розміщуючи список дзеркальних сайтів у соціальних мережах із хештегом #CollateralFreedom.

«Репортери без кордонів» публікують цей список:

1. Заблокований у Росії сайт Grani.ru відтепер доступний за адресою: https://gr1.global.ssl.fastly.net/

2. Заблокований у Казахстані, Узбекистані й Туркменістані сайт Fergananews.com нині доступний за адресою: https://fg1.global.ssl.fastly.net/

3. Заблокований у Китаї сайт The Tibet Post International доступний за адресою: https://tp1.global.ssl.fastly.net/

4. Заблокований у В'єтнамі сайт Dan Lam Bao доступний за адресою https://dlb1.global.ssl.fastly.net/

5. Заблокований у Китаї сайт Mingjing News, доступний за адресою: https://mn1.global.ssl.fastly.net/news/main.html

6. Заблокований на Кубі сайт Hablemos Press, доступний за адресою: https://hp1.global.ssl.fastly.net/

7. Заблокований в Ірані сайт Gooya News доступний за адресою: https://gn1.global.ssl.fastly.net/

8. Заблокований в ОАЄ сайт Gulf Centre for Human Rights доступний за адресою: https://gc1.global.ssl.fastly.net/

9. Заблокований у Бахрейні та у Саудівській Аравії сайт Bahrain Mirror, доступний за електронною адресою: https://bahrainmirror.global.ssl.fastly.net/

Партнером RSF у здійсненні операції Collateral Freedom є неурядова організація китайських активістів GreatFire, яка вже створила дзеркальні сайти для Deutsche Welle, Google та China Digital Times.

«Репортери без кордонів» привертають увагу до того, що інструменти й технології GreatFire безкоштовно доступні в Інтернеті для тих, хто користується ними для боротьби з онлайн-цензурою ***(«Репортери без кордонів» розблоковують сайти, заборонені у країнах-«ворогах Інтернету» // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/web/online_media/reporteri_bez_kordoniv_rozblokovuyut_sayti_zaboroneni_u_krainakhvorogakh_internetu/). – 2015. – 12.03).***

***

Активисты общественной организации «Кампания за детство, свободное от рекламы» ополчились на говорящую куклу Барби.

Красотка Барби, которая умеет записывать и передавать по Интернету речь ребёнка, не только фиксирует высказанные мысли и переживания детей,

но и может пересылать полученную информацию их родителям по электронной почте.

Однако активисты обеспокоены тем, что с помощью Барби производитель игрушки (компания Mattel) будет в курсе озвученных детских пожеланий, которые могут использоваться в маркетинговых и других целях. Защитники прав детей уже направили петицию против выпуска продукта.

Отметим, что говорящая Барби при нажатии на пряжку пояса начинает задавать вопросы и с помощью встроенного микрофона записывает ответы ребенка. Данные в зашифрованном виде отправляются на серверы, где обрабатываются специальным ПО для распознавания речи. Обработав речь, программа даёт кукле команду ответить соответствующим образом. Связь со Всемирной паутиной игрушка поддерживает через беспроводное Wi-Fi подключение.

Кстати, об играх. Министерство обороны Швеции выпустило компьютерную игру, при помощи которой вербует новобранцев в ряды вооружённых сил. Через игру отбираются пользователи, которые умеют работать в команде ***(Активисты выступают против говорящей Барби, шпионящей за детьми // Блог Imena.UA (http://www.imena.ua/blog/shut-down-hello-barbie/). – 2015. – 13.03).***

***

СБУ выявила около 600 антиукраинских групп в социальных сетях. Об этом во время брифинга по результатам противодействия международной киберпреступности сообщил начальник Департамента контрразведки в сфере информационной безопасности СБУ В. Найда.

«СБУ выявила около 600 антиукраинских групп в социальных сетях. В частности, в “Вконтакте” и “Одноклассники”. Менее распространено российскими спецслужбами использование Facebook. Около 80 % подобных групп были созданы и администрируются с территории РФ или “ДНР” и “ЛНР”» , – сообщил В. Найда.

По его словам, ярким примером является группа «Антимайдан».

«Группа “Антимайдан” сейчас насчитывает 27 администраторов. Большинство из них это граждане России», – добавил он ***(СБУ выявила около 600 антиукраинских групп в соцсетях // InternetUA (http://internetua.com/sbu-viyavila-okolo-600-antiukrainskih-grupp-v-socsetyah). – 2015. – 14.03).***

***

Создатели «Википедии» подали в суд на АНБ и Минюст США из-за слежки за своими пользователями.

Некоммерческий фонд Wikimedia Foundation, управляющий интернет-энциклопедией «Википедия», подал в суд на АНБ (Агентство национальной безопасности) и Министерство юстиции США из-за правительственной

программы слежки за интернет-пользователями. Об этом сообщается в официальном блоге фонда.

Wikimedia Foundation отмечает, что добивается прекращения программы массового наблюдения «в целях защиты прав наших пользователей по всему миру». Причиной в фонде считают превышение АНБ полномочий, установленных принятым в 2008 г. Законом «О контроле деятельности служб внешней разведки» (Foreign Intelligence Surveillance Act Amendments Act, FAA).

Wikimedia утверждает, что слежка велась не только за потенциальными экстремистами, но и за гражданами США, среди которых, вероятно, есть и пользователи «Википедии». Это является нарушением первой поправки конституции США, гарантирующей свободу слова и собрания, а также четвёртой поправки, защищающей от незаконных обысков, говорится в сообщении фонда.

По словам представителей Wikimedia, на одном из слайдов презентации АНБ, опубликованной Э. Сноуденом, «Википедия» перечислена как цель для прослушки вместе с проектами вроде Gmail, Facebook и CNN.com. Что именно могло интересовать спецслужбы на ресурсе, где обсуждения и контент публикуются в открытом доступе, в фонде не уточнили, однако заметили, что часть пользователей «Википедии» предпочитает работать анонимно, а угроза слежки может отпугнуть эту аудиторию от проекта.

Мы подаём иск сегодня от имени наших читателей и редакторов. Наблюдение разрушает основные принципы Интернета: открытое пространство для сотрудничества и экспериментов, место, свободное от страха.

В суде фонд и восемь других организаций, включая Amnesty International и Human Rights Watch, будет представлять Американский союз защиты гражданских свобод (ACLU). Основатель «Википедии» Д. Уэйлс и гендиректор Wikimedia Foundation Л. Третиков также выступили с колонкой в газете The New York Times.

В Wikimedia начали обсуждать с ACLU возможность подачи иска еще в 2014 г. Причиной послужили сведения о слежке АНБ за перепиской в Интернете, раскрытые Э. Сноуденом летом 2013 г. ***(Создатели «Википедии» подали в суд на АНБ и Минюст США из-за слежки за своими пользователями // InternetUA (http://internetua.com/sozdateli--vikipedii--podali-v-sud-na-anb-i-minuast-ssha-iz-za-slejki-za-svoimi-polzovatelyami). – 2015. – 10.03).***

***

Евросоюз почистит соцсети от экстремизма

Уже 1 июля начнет свою работу отдел проверок интернет-контента Евросоюза Главной задачей его является пресечение распространения в социальных сетях пропаганды экстремизма. Ведомство получило право

читать подозрительные сообщения, проверять содержимое сайтов и ограничивать доступ к ним. Однако сообщается, что слежка за пользователями мессенджеров на данном этапе пока что исключена.

Несколько ранее, агентство Евросоюза, которое имеет дело с судебными органами (Евроюст), сообщило о необходимости разработки законопроекта, который позволил бы читать переписку в Skype и Viber. Это необходимо для того, чтобы детально наблюдать за деятельностью радикально настроенных граждан, которые вернулись в Европу из стран Ближнего Востока. Но правозащитники уверены, что такого рода меры могут применяться только в случае крайней необходимости ***(Евросоюз почистит соцсети от экстремизма // Age Of Comp (http://ageofcomp.info/chudesa-nauki/32065-evrosoyuz-pochistit-socseti-ot-yekstremizma.html). – 2015. – 14.03).***

## Проблема захисту даних. DDOS та вірусні атаки

Как защитить себя от кражи данных?

Защита данных – ключевая позиция для многих людей. У некоторых в смартфонах хранится деловая информация, цена которой составляет заоблачные гонорары и сделки, а некоторым просто очень важны фотографии как воспоминания лучших годов жизни. В последнее время, когда Э. Сноуден рассекретил данные АНБ, пользователи стали всё чаще задумываться о защите своих данных. И совсем недавно Т. Кук заявил, что властям нужно найти ту грань между безопасностью и неприкосновенностью персональных данных.

Сегодня всё чаще различные хакерские группировки и некоторые секретные службы Западных стран пытаются завладеть личной информацией пользователей, включая даже данные их кредитных карт, личные фотографии и контакты. Однако сильно не пугайтесь, у вас есть шанс защитить свои данные с помощью шифрования диска, которое впервые появилось в Android 3.0. До этого всё это работало очень медленно, устройство при включенном шифровании постоянно зависало, так как это напрямую влияет на скорость записи и чтения данных. Впрочем, в Android 5.0, как известно, этот показатель увеличили в разы, что позволило избавиться от проблем в производительности, теперь вы не заметите лагов и прочих неприятных вещей, однако, конечно, без шифрования девайс будет работать в любом случае быстрее.

Для его работы вам обязательно стоит придумать пароль из шести или более символов, которым вы сможете разблокировать ваш девайс, без пароля в окне блокировки вы не сможете включить функцию шифрования диска.

Следующий момент – это отключение шифрования, реализовать которое у вас выйдет только путем сброса всех настроек, то есть вы получите полностью чистый Android без какой-либо информации. Шифрование данных в Android 5.0 распространяется только на внутреннюю память,

однако сторонние производители могут включить в прошивку возможность шифрования и SD-карты.

Для включения шифрования вам нужно:

– перейти в «Настройки»;

– открыть вкладку «Безопасность»;

– перейти в пункт «Шифрование» и выбрать вкладку «Зашифровать данные».

Перед этим ваш девайс должен быть заряжен более чем на 80 %. Можно использовать и просто пароль на экране блокировки, но тогда вы не сможете защитить данные в случае, если злоумышленник попытается обойти защиту через USB-кабель путем подключения девайса к компьютеру, а вот в случае с шифрованием у него ничего не выйдет, так как при подключении к ПК все данные будут зашифрованы. В теории, если это хакер мирового масштаба, он сможет обойти криптоключ, но это лишь в теории ***(Как защитить себя от кражи данных? // InternetUA (http://internetua.com/kak-zasxitit-sebya-ot-kraji-dannih). – 2015. – 2.03).***

***

Эксперты по борьбе с компьютерными вирусами предупредили пользователей Интернета о новой хакерской угрозе, маскирующейся под официальную почтовую рассылку Microsoft. После перехода на сайт, внешне похожий на веб-представительство компании, компьютер пользователя заражается троянской программой.

Как сообщили в пресс-службе компании Eset, атака ориентирована, в первую очередь, на корпоративных пользователей. Им на электронную почту приходят письма, якобы, от сайта Microsoft Volume Licensing Service Center (VLSC). В письме к адресату обращаются по имени и фамилии, и сообщают ему о предоставлении прав администратора для работы с корпоративными лицензиями.

«Получателям поддельных писем предлагается перейти по ссылкам, которые ведут на веб-сайты, размещенные на скомпрометированном сервере. Дизайн страниц вредоносных площадок имитирует оригинальный контент узла Microsoft VLSC. При переходе на персональные компьютеры пользователей загружается “троян”», – рассказали в компании.

Эксперты пояснили, что вирус хорошо скрывает свою вредоносную активность и самокопируется под другим именем, соответственно, его сложно найти на ПК. Специалисты в очередной раз рекомендовали пользователям не переходить по подозрительным ссылкам ***(Пользователей предупредили о фальшивых письмах от Microsoft // InternetUA (http://internetua.com/polzovatelei-predupredili-o-falshivih-pismah-ot-Microsoft). – 2015. – 1.03).***

***

В сети свирепствует новая версия вредоносной программы OpinionSpy. Вирус нацелен на владельцев персональных компьютеров Apple с операционной системой Mac OS X.

Новая версия вируса, созданного ещё в 2010 г., получила обозначение OpinionSpy.3. Она представляет собой трояна с функциональностью бэкдора. При распространении вирус использует трёхступенчатую схему. Так, на сторонних сайтах появляются с виду безобидные программы, в составе дистрибутивов которых присутствует файл poinstall, запускаемый инсталлятором в процессе установки.

Если в ходе инсталляции пользователь соглашается предоставить данному файлу права администратора, poinstall отправляет на сервер злоумышленников серию POST-запросов, а в ответ получает ссылку для скачивания пакета с расширением .osa.

В процессе установки вирус получает администраторские права и работает в системе с максимальными привилегиями. При этом, если на начальном этапе инсталляции выбрать в окне программы установки вариант «I Disagree», на компьютер будет помещена только программа, которую пользователь скачивал из Интернета без каких-либо дополнительных шпионских компонентов.

Зловред собирает информацию об активности пользователей, посещённых ими сайтах, открываемых вкладках, ссылках и т. д. Кроме того, троян может анализировать трафик, проходящий через сетевую карту ПК, и перехватывать сетевые пакеты, отправляемые программами для мгновенного обмена сообщениями ***(В сети наблюдается эпидемия Мас-вируса OpinionSpy // Блог Imena.UA (http://www.imena.ua/blog/mac-opinionspy/). – 2015. – 2.03).***

***

Злоумышленники используют ПО Komodia в атаках «человек посередине»

Специалисты EFF обнародовали результаты исследования базы данных, собранной при использовании опционального режима Firefox Decentralized SSL Observatory.

Когда в медиа появилась информация о Superfish – рекламном ПО, предустановленном на некоторых системах Lenovo, исполнительный директор компании П. Гортензиус заявил, что программа не представляет никакого риска для пользователей. Однако исследователи безопасности обнаружили свидетельства того, что ПО совсем не так безвредно. Впоследствии Lenovo подтвердила некотрые из этих утверждений.

Выяснилось, что Superfish устанавливает на системе собственный сертификат безопасности, позволяющий перехватывать и расшифровывать конфиденциальные данные пользователя. Другой плагин от Komodia – PrivDog превращает браузер пользователя в программу принимающую

любой HTTPS-сертификат, независимо от того подписан он легитимной цифровой подписью или нет.

Специалисты некоммерческой правозащитной организации Фонд электронных рубежей (Electronic Frontier Foundation, EFF) Д. Бонно и Д. Джиллула опубликовали результаты исследования базы данных, собранной при использовании опционального режима Firefox Decentralized SSL Observatory. Анализ показал, что злоумышленники уже используют программное обеспечение с установленными криптографическими библиотеками Komodia, для осуществления атак «человек посередине».

По словам экспертов, в 1,6 тыс. случаев программное обеспечение от Komodia принимало сертификаты, которые должны были бы быть отклонены. Затрагиваемые домены включали важные веб-сайты, такие как Google (в том числе mail.google.com, accounts.google.com и checkout.google.com), Yahoo (login.yahoo.com), Bing, Windows Live Mail, Amazon, eBay (в том числе checkout.payments.ebay.com), Twitter, Netflix, Mozilla Add-Ons, а также несколько банковских сайтов, сам Decentralized SSL Observatory и даже superfish.com.

Также Decentralized SSL Observatory собрал более 17 тыс. различных сертификатов от пользователей PrivDog. Эксперты отметили, что любой из них мог быть использован при осуществлении атаки «человек посередине», однако определить истинность данного предположения не представляется возможным ***(Злоумышленники используют ПО Komodia в атаках «человек посередине» // InternetUA (http://internetua.com/zloumishlenniki-ispolzuuat-po-Komodia-v-atakah--cselovek-poseredine). – 2015. – 1.03).***

***

Обнаружен способ проведения кибератак посредством дисков Blu-ray

Компьютер под управлением Windows можно атаковать, эксплуатируя уязвимости в проигрывателях дисков, пишет Блог Imena.UA (http://www.imena.ua/blog/abusing-blu-ray-players/).

Целых два способа атаки компьютера через диски Blu-ray обнаружил британский хакер С. Томкинсон. Первый заключается в эксплуатации уязвимости в ПО CyberLink PowerDVD, которое воспроизводит DVD- и Blu-ray-диски на компьютере, и использует Java для создания меню.

Брешь позволяет хакерам обойти ограничения безопасности Windows, в результате чего злоумышленники могут записать на диск произвольные исполняемые файлы и автоматически запускать их.

Второй способ основан на методике получения привилегий суперпользователя для Blu-ray-дисков. Он использует код отладки для запуска с внешнего USB-устройства. Хакер может написать код JavaXlet, который повторяет содержимое TCP-потока на адрес netinf, что позволяет эксплуатировать уязвимость.

Таким образом, на сегодняшний день пользователям лучше не воспроизводить Blu-ray-диски, полученные из ненадёжных источников,

запретить автозапуск со съёмных носителей и не позволять приложениям с дисков получить выход в Интернет.

Ранее Министерство обороны США выложило в сеть программный комплекс для защиты от хакерских атак Dshell ***(Обнаружен способ проведения кибератак посредством дисков Blu-ray // Блог Imena.UA (http://www.imena.ua/blog/abusing-blu-ray-players/). – 2015. – 2.03).***

***

AdaptiveMobile зафиксировала беспрецедентно большую вспышку распространения вредоносных программ через SMS.

Как сообщают исследователи безопасности из компании AdaptiveMobile, им удалось выявить крупную вспышку распространения вредоносного ПО Gazon, инфицирующего Android-устройства посредством SMS. Для распространения вирус использует книгу контактов жертвы и в случае успешного заражения пытается осуществить кражу ваучеров Amazon, а также устанавливает дополнительное вредоносное ПО.

«Атака началась в США, и к 25 февраля вирус все еще активно распространялся, успев заразить несколько тысяч смартфонов в 30 странах мира, – отмечают эксперты. – Инцидент затронул пользователей из Канады, Великобритании, Франции, Индии, Кореи, Мексики, Австралии и Филиппин».

Отдельно эксперты отметили эффективность распространения Gazon через SMS, о чем говорит тот факт, что этот метод используется в 99 % случаев. При этом из статистики других методов заражения следует, что по вредоносным ссылкам в Facebook и в письмах электронной почты перешли порядка 16 тыс. раз ***(Злоумышленники массово заражают Android-устройства // InternetUA (http://internetua.com/zloumishlenniki-massovo-zarajauat-Android-ustroistva). – 2015. – 4.03).***

***

Тысячи NAT-устройств Seagate подвержены критической уязвимости нулевого дня, позволяющей злоумышленникам скомпрометировать систему и получить привилегии суперпользователя. Об этом сообщает исследователь безопасности О. Ривз, который опубликовал детальную информацию о бреши на ресурсе Beyond Binary.

Ривз уведомил производителя об обнаруженной уязвимости еще 7 октября прошлого года, но Seagate до сих пор не выпустила исправление. Более того, компания даже не сообщила, когда брешь будет исправлена и выйдет ли вообще исправление.

NAS-продукты Seagate Business включают в себя веб-приложение, с помощью которого администраторы могут управлять ими. Этот компонент использует устаревшие уязвимые версии PHP (версия 5.2.13 2010 г. выпуска), CodeIgniter (версия 2.1.0 2011 г. выпуска) и Lighttpd (версия 1.4.28 2010 г. выпуска).

Проблема также состоит в том, что ключ шифрования токенов сессий CodeIgniter неуникален. Это значит, что в каждом случае используется один и тот же ключ. Таким образом, вся информация о сессии пользователя записывается в файл cookie перед шифрованием и отправкой пользователю. Более того, взломщик может изменить параметр language в файле cookie и получить возможность загрузить произвольный файл на уязвимое устройство.

Еще одна уязвимость заключается в том, что веб-приложение использует версию Lighttpd, которая работает с привилегиями суперпользователя. Таким образом любые действия хакера будут выполнены с соответствующими привилегиями.

В настоящее время уязвимости не исправлены ***(Seagate подтвердила наличие уязвимостей в Business Storage NAS // InternetUA (http://internetua.com/Seagate-podtverdila-nalicsie-uyazvimostei-v-Business-Storage-NAS). – 2015. – 4.03).***

***

Компания-регистратор доменных имен ICANN обнаружила очередную уязвимость в своих системах. Новая брешь позволяет сторонним пользователям раскрывать определенную конфиденциальную информацию об организациях, желающих приобрести тот или иной домен. Более того, эксплуатация уязвимости позволяла конкурентам, участвующим в gTLD-аукционах, следить друг за другом.

Таким образом, подчеркивают IT-эксперты компании, важные коммерческие данные и техническая информация относительно предстоящего расширения сети Интернет находились под угрозой компрометации. В целях предотвращения вероятных атак ICANN остановила работу уязвимых веб-сервисов.

«При определенных обстоятельствах аутентифицированный пользователь портала способен просмотреть данные, связанные с другими пользователями», – следует из сообщения компании.

Регистратор также отметил, что эта информация включает в себя технические данные о добавлении новых родовых доменов верхнего уровня в корневой DNS, контактную информацию, коммерческие тайны клиентов и т. п. ***(ICANN обнаружила очередную уязвимость в своих сетях // InternetUA (http://internetua.com/ICANN-obnarujila-ocserednuua-uyazvimost-v-svoih-setyah). – 2015. – 4.03).***

***

Специалисты Dr. Web продолжают фиксировать активность вируса Rmnet, несмотря на заявления отдела по борьбе с киберпреступностью полиции Великобритании о прекращении деятельности нескольких крупных управляющих серверов, которые распространяли данный вирус, сообщается в пресс-релизе компании.

Полиция Великобритании совместно с Европейским центром борьбы с киберпреступлениями Европола, специалистам из Германии, Италии и Нидерландов, при участии компаний Symantec, Microsoft, AnubisNetworks и других совместными усилиями заблокировали более 300 доменов, распространяющих вирус, и ликвидировали сеть из более чем 350 тыс. зараженных устройств.

Однако наблюдение Dr. Web за сетями Rmnet показывает, что среднесуточная активность вируса по-прежнему составляет 250–270 тыс. зараженных компьютеров в сутки. Вирус встраивает посторонние элементы в просматриваемые пользователем веб-страницы и может выполнять удаленные команды злоумышленника, что теоретически дает возможность получить доступ к банковской информации жертвы с целью хищения денег со счетов ***(Вирус Rmnet заражает пользователей, несмотря на заверения Европола // InternetUA (http://internetua.com/virus-Rmnet-zarajaet-polzovatelei--nesmotrya-na-zavereniya-evropola). – 2015. – 3.03).***

***

Глобальный эксперимент, проведенный специалистами ИБ-компании Avast, показал, насколько небезопасными могут быть публичные точки доступа Wi-Fi. Эксперты исследовали различные точки доступа в девяти крупных муниципальных районах городов США, Европы и Азии. Для проведения эксперимента они использовали ноутбук с поддержкой Wi-Fi и общедоступное бесплатное приложение, позволяющее проводить мониторинг локального Wi-Fi-трафика на частоте 2,4 ГГц.

В ходе исследования выяснилось, что любой желающий может довольно легко увидеть интернет-активность, поисковые запросы, пароли, видеоматериалы, а также электронные сообщения пользователей.

Специалисты отмечают, что наиболее часто атакам подвергаются жители Азии. Больше половины веб-трафика на этом континенте исходит с сайтов, использующих незащищенный HTTP-протокол, при этом 97 % пользователей подключаются к открытым Wi-Fi-сетям, а в 7 из 10 защищенных паролем маршрутизаторов реализованы слабые методы шифрования, что делает их уязвимыми для взлома.

Ситуация в Европе и США обстоит немного лучше, но и здесь только 20 % пользователей предпринимают какие-либо шаги по усилению защиты своих Wi-Fi-сеансов.

Исследователи выяснили, что значительное количество пользователей просматривают, в основном, незащищенные HTTP-ресурсы. Почти половина интренет-трафика в Азии исходит с таких сайтов, тогда как в США этот показатель составляет одну треть, а в Европе – приблизительно четверть от общего объема европейского трафика.

Незащищенность HTTP-трафика позволила команде Avast просматривать браузерную активность пользователей, в том числе домены и

историю просмотров, поисковые запросы, а также персональные учетные данные, видео, электронную почту и комментарии.

Как отмечают специалисты, большинство исследуемых точек доступа были защищены посредством какой-либо формы шифрования. Тем не менее, зачастую используемые средства защиты были довольно слабы и позволяли с легкостью осуществить взлом. Наименьшее количество слабозашифрованных точек доступа Wi-Fi оказалось в Сан-Франциско и Берлине, в Нью-Йорке и Лондоне число уязвимых точек доступа составило больше половины, а в Азии – три четверти ***(Эксперты раскрыли опасности использования публичных точек доступа Wi-Fi // InternetUA (http://internetua.com/eskperti-raskrili-opasnosti-ispolzovaniya-publicsnih-tocsek-dostupa-Wi-Fi). – 2015. – 4.03).***

***

Злоумышленники до сих пор активно эксплуатируют уязвимости ShellShock и Heartbleed. Данная проблема остается актуальной из-за нежелания компаний устанавливать необходимые обновления. Представители организаций жалуются на то, что обновление виртуальной системы занимает большое количество времени, ресурсов и средств, сообщает издание The Register.

ИБ-эксперты заявляют, что на самом деле, можно оптимизировать процесс обновления виртуальной системы, который значительно сократит затрату времени и средств.

Первое, что рекомендуют специалисты, это необходимость проведения качественного проверенного процесса обновлений, который будет задокументирован с подробными инструкциями о том, как процесс был выполнен и в какой сфере. Документ в дальнейшем может использоваться как шаблон или инструкция для установки нужных исправлений в будущем.

Для выполнения качественной работы потребуются правильные инструменты. На данный момент в продаже появляется все большее число программ обновлений, упрощающих работу специалистов. Использование таких инструментов, как SCCM или Redhat Satellite помогут значительно сократить расходы.

Для работы с различными ОС потребуется определенные программы по обновлениям. Некоторые из таких программ являются совершено бесплатными. В любом случае, приобретение полезных инструментов быстро окупят свою стоимость. Необходимо также помнить о том, что каждая ПО по обновлению и устранению ошибок требует тестирования ***(Злоумышленники активно эксплуатируют уязвимости из-за нежелания компаний устанавливать необходимые обновления // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2015/03/04/patching-for-sanity.html). – 2015. – 4.03).***

***

Эксперты обнаружили новую уязвимость, угрожающую миллионам пользователей мобильных платформ iOS и Android.

Брешь получила название FREACK attack и пока что, как сообщает The Guardian, доказательств использования ее хакерами нет. Однако это не исключает возможности похищения данных в любой момент.

Опасность поджидает в первую очередь тех, кто использует встроенные интернет-браузеры. По словам специалистов, злоумышленники могут вклиниться в обмен данными между устройством и открываемым сайтом и похитить либо изменить сведения.

Уязвимость, по мнению исследователей, вызвана прежде всего слабым шифрованием. Производители программного обеспечения вынуждены использовать устаревшие 512-битные ключи из-за американского законодательства, запрещающего применять более совершенную кодировку в случае, если продукт продается за рубежом.

Эксперт по компьютерной безопасности Университета Мичигана З. Дурумерич пояснил, что по данным на 3 марта из 14 млн исследованных сайтов 36 % «пропускают» эту брешь. В списке как малоизвестные, так и популярные ресурсы, в числе которых несколько зарубежных СМИ, так называемые «скидочные» сайты, страницы платежных систем, гостиниц и даже государственных ведомств ***(Выявлена уязвимость, угрожающая миллионам пользователей iOS и Android // InternetUA (http://internetua.com/viyavlena-uyazvimost--ugrojauasxaya-millionam-polzovatelei-iOS-i-Android). – 2015. – 5.03).***

***

Киберпреступники выпустили модифицированную версию набора эксплоитов Angler, который теперь способен эксплуатировать уязвимость в Internet Explorer, исправленную в октябре прошлого года. Об этом сообщает исследователь FireEye Д. Касэльден.

Речь идет об уязвимости использования после высвобождения, исправленной в бюллетене безопасности MS14-056. Он устраняет в целом 14 брешей в Internet Explorer. По словам Д. Касэльдена, уязвимость недавно была добавлена в набор Angler, включающий в себя эксплоиты для Internet Explorer, Adobe Flash Player и Microsoft Silverlight.

«Недавно в Angler появилась модифицированная версия эксплоита от k33nteam, нацеленного на уже исправленную уязвимость. Интересно, что это первый случай, когда злоумышленники начали атаковать Internet Explorer после введения новой технологии защиты от атак использования после высвобождения MEMPROTECT. Это показывает, что авторы Angler до сих пор заинтересованы в осуществлении атак на IE», – пишет специалист.

Недавно исследователи компании Websense заявили, что считают Angler наиболее сложным набором эксплоитов из числа используемых киберпреступниками на сегодняшний день. Angler включает в себя ряд

технологий по предотвращению обнаружения, включая выявление антивирусного и виртуализационного ПО, а также добавление зашифрованного пэйлоада ***(Набор эксплоитов Angler стал способен взламывать Internet Explorer // InternetUA (http://internetua.com/nabor-eksploitov-Angler-stal-sposoben-vzlamivat-Internet-Explorer). – 2015. – 4.03).***

***

Начальник управления транспорта А. Вербицкая запретила своим подчиненным пользоваться российской почтой и информационными сайтами.

Об этом «Херсонским вестям» сообщают источники в городском совете.

Так, А. Вербицкая издала приказ о том, что ее подчиненные не могу использовать для служебного пользования почтовые ящики и публичные сервисы, размещенные на иностранных ресурсах в зоне домена RU.

К тому же, в приказе указано, что он издается с целью предотвращения утечки служебной информации ***(Начальник управления транспорта запретила своим подчиненным пользоваться российской почтой и сайтами // Херсонские Вести (http://visti.ks.ua/novosti/politika/18691-nachalnik-upravleniya-transporta-zapretila-svoim-podchinennym-polzovatsya-rossiyskoy-pochtoy-i-saytami.html). – 2015. – 5.03).***

***

Безопасность маршрутизаторов для дома и малого бизнеса вызывает серьезные опасения у разнообразных ИБ-экспертов, сообщает издание The Register. С завидной регулярностью появляются все новые эксплоиты для сетевых девайсов, позволяя злоумышленникам использовать миллионы устройств для нелегальной активности.

Большинство уязвимостей существуют из-за беспечности разработчиков. К примеру, огромное количество маршрутизаторов имеют неизменяемые учетные данные, в связи с чем хакеры могут скомпрометировать практически каждое устройство.

Прекрасным примером последствий взлома стал платный DDoS-сервис Lizard Stresser, созданный хакерской группировкой Lizard Squad. По уверению разработчиков, он функционирует на основе сотен тысяч взломанных маршрутизаторов, которые по команде с C&C-сервера перегружали целевые сайты.

Еще год назад исследователи из Team Cymru предупреждали, что неизвестная хакерская группировка взламывала примерно по 300 тыс. роутеров в неделю, изменяя настройки DNS-серверов на вредоносные. Компрометация сетевых устройств осуществлялась с помощью самораспространяемого червя, который с помощью эксплуатации известных уязвимостей, осуществления CSRF-атак и брутфорса паролей к консолям администратора получал доступ к маршрутизаторам.

Одной из наиболее опасных уязвимостей в прошлом году стала Misfortune Cookie, обнаруженная компанией Check Point Security. Эксплуатируя эту брешь, хакеры могли взломать более 12 млн маршрутизаторов таких производителей, как Linksys, Huawei, ZTE, D-Link, TP-Link и прочих. Получив доступ к роутерам, злоумышленники могли изменять любые настройки устройства.

В октябре исследователи Rapid7 также обнаружили уязвимость, позволяющую скомпрометировать не менее 1,2 млн роутеров. Она заключалась в некорректной конфигурации NAT-PMP и позволяла злоумышленникам следить за внутренним трафиком жертв ***(Эксперты предупреждают об огромном количестве уязвимостей в маршрутизаторах // InternetUA (http://internetua.com/eksperti-preduprejdauat-ob-ogromnom-kolicsestve-uyazvimostei-v-marshrutizatorah). – 2015. – 6.03).***

***

Хакеры нашли способ обманывать биометрический сканер радужной оболочки глаза, используя фотографии высокой чёткости, пишет Блог Imena.UA (http://www.imena.ua/blog/clone-eyes-using-google-images/).

Представители известного хакерского клуба Chaos Computer Club сумели обойти проверку в сканере Panasonic Authenticam BM-ET200, специально взятом для тестирования. Этот сканер уже снят с производства, но до сих пор много где используется.

По словам хакеров, подходящая фотография должна быть яркой, большой и детализированной. Для обмана сканера достаточно фотографии радужной оболочки с диаметром от 75 пикселей – в идеале должно быть видно больше 75 % изображения радужной оболочки. Печатать фотографию следует на принтере с разрешением 1200 dpi.

Для проверки своей методики хакеры использовали обнаруженные в Интернете фотографии глав государств высокого разрешения. Например, избирательный плакат А. Меркель высокого разрешения с диаметром радужной оболочки глаз 175 пикселов.

Напомним, ранее инженеры исследовательской компании SRLabs легко обошли сканер отпечатков пальцев, который призван идентифицировать владельца смартфона Samsung Galaxy S5, при помощи копии отпечатка и тонера ***(Биометрию опять скомпрометировали: хакеры обманули сканер сетчатки глаза фотографией // Блог Imena.UA (http://www.imena.ua/blog/clone-eyes-using-google-images/). – 2015. – 6.03).***

***

Исследователи обнаружили новую разновидность троянов для PoS-терминалов

Эксперты ИБ-компании Trend Micro обнаружили и проанализировали новую разновидность троянов для PoS-терминалов, получившую название

PwnPOS. По мнению специалистов, этот вид вредоносов существует с 2013 г., возможно даже ранее. Тем не менее, выявить его удалось только сейчас. Исследователи Trend Micro поясняют, что PwnPOS – один из тех безукоризненных образцов вредоносного ПО, которые могут оставаться незамеченными на протяжении многих лет благодаря своей простой, но, вместе с тем, продуманной конструкции.

Вредонос состоит из дух модулей: RAM-скрепера и двоичного кода, ответственного за эксфильтрацию данных. В то время как RAM-скрепер остается неизменным, компонент эксфильтрции данных претерпел несколько изменений. Эти факты позволяют предположить, что у трояна есть два различных автора.

Подобно другим банковским вредоносам, PwnPOS регистрирует все активные процессы, осуществляет поиск данных кредитных карт и сохраняет их в отдельном файле, который затем сжимает и зашифровывает. Впоследствии файл в виде электронного письма отправляется на определенный почтовый адрес.

Троян остается незамеченным благодаря способности добавлять и убирать себя из списка сервисов, при необходимости загружать и удалять файлы, маскировать вредоносные файлы под самые обычные и скрывать их в директории %SYSTEM$, а также хранить похищенные данные в .dat-файле, размещенном в директории %SystemRoot %\system32.

Эксперты зафиксировали случаи использования PwnPOS совместно с другими вредоносами для PoS-терминалов, такими как BlackPOS и Alina. В основном они затрагивали небольшие и средние предприятия Японии, Австралии, Индии, США, Канады, а также Германии и Румынии, использующие машины под управлением 32-битных версий Windows XP или Windows 7 ***(Исследователи обнаружили новую разновидность троянов для PoS-терминалов // InternetUA (http://internetua.com/issledovateli-obnarujili-novuua-raznovidnost-troyanov-dlya-PoS-terminalov). – 2015. – 9.03).***

***

В 2014 г. учетные записи 34 % пользователей устройств под управлением Android подверглись взлому. Об этом рассказали эксперты «Лаборатории Касперского» и аналитического агентства B2B International.

Совместное исследование компаний показало, что с вредоносными программами в течение года сталкивались 41 % пользователей смартфонов и 50 % пользователей планшетов на Android. Самой распространённой целью злоумышленников остаётся доступ к финансовой информации. Среди обладателей смартфонов с такими угрозами сталкивались 32 % респондентов, доля пользователей планшетов – 37 %.

Несмотря на это многие пользователи очень беспечно относятся к защите информации. Около половины Android-устройств в России не защищены антивирусными программами, говорится в исследовании. На 26 % смартфонов нет даже пароля. Доля планшетов без пароля – 18 %.

При этом многие пользователи продолжают хранить на незащищённых «гуглофонах» важную информацию. Около 10 % незащищённых устройств содержат финансовую информацию – PIN-коды, пароли платёжных систем и т. д.

Почта легкомысленных пользователей также представляет собой легкую добычу. Личную переписку на устройствах без пароля хранят 30 % владельцев, рабочую – 15 %. Ещё 8 % признаются в небезопасном хранении данных, не предназначенных для третьих лиц.

Серьёзной проблемой остаётся низкая осведомлённость пользователей в сфере мобильной безопасности. 38 % опрошенных признались, что не знают о существовании мобильных киберпреступлений. Пятая часть пользователей относится к ним равнодушно.

Android продолжает оставаться лакомым кусочком для хакеров со всего мира. Ранее «Лаборатория Касперского» уже сообщала, что 99 % вредоносного программного обеспечения нацелено на Android. Число атак на подобные устройства почти утроилось за последний год ***(В 2014 году был взломан каждый третий пользователь Android // InternetUA (http://internetua.com/v-2014-godu-bil-vzloman-kajdii-tretii-polzovatel-Android). – 2015. – 9.03).***

***

По всей видимости, мнение о том, что после скандала с Lenovo производители могут одуматься и перестать досаждать пользователям разными надоедливыми и ненужными им приложениями, было слишком оптимистичным. Кажется, в погоне за прибылью компании не слишком волнуют безопасность пользовательских данных и удобство работы с устройством. Сначала появилась новость о компании Oracle и её технологии Java, а теперь имеются сведения о том, что другой китайский производитель, Xiaomi, снова отличился предустановленными на флагманский смартфон Mi4 LTE вредоносными приложениями.

Слово «снова» упомянуто потому, что в прошлом году аппараты Xiaomi уже уличили в сборе пользовательских данных и их отправке на серверы в Китай. Это открытие нисколько не смутило Xiaomi и в новом флагмане вместо одного приложения сомнительной ценности появилось сразу шесть.

Об этом сообщает располагающаяся в Сан-Франциско занимающаяся мобильной безопасностью компания Bluebox. Среди таких приложений три выделены особо: Yt Service, PhoneGuardService и AppStats. Первое относится к категории adware и отображает на устройстве рекламу. Однако это лишь меньшее из зол – второе признано трояном и таит в себе большую угрозу. PhoneGuardService даёт возможность взломать устройство, а AppStats отнесли к категории Riskware.

Также исследователи говорят, что Mi4 открыт для семи значительных Android-уязвимостей. Поскольку аппарат является рутированным

(взломанным для более глубокого доступа пользователя к его настройкам), опасность возрастает ещё больше. Напомним, что Xiaomi использует не сертифицированную Google версию Android с прошивкой MIUI ***(На смартфоне Xiaomi Mi4 нашли шесть вредоносных приложений // InternetUA (http://internetua.com/na-smartfone-Xiaomi-Mi4-nashli-shest-vredonosnih-prilojenii). – 2015. – 9.03).***

***

ИБ-компания Black Lotus опубликовала исследование, наглядно показывающее разительное несоответствие между пониманием интернет-провайдерами потенциальной опасности DDoS-атак и их готовностью к отражению кибернападений.

Эксперты провели опрос среди 120 компаний, как крупных, так и небольших. Согласно полученным результатам, почти все участники (92 %) использовали какие-либо формы защиты от DDoS-атак, однако не смогли остановить их до того, как был нанесен ущерб. По признанию большей части респондентов, подобные инциденты стали причиной увеличения их операционных расходов, при этом более 35 % опрошенных отметили, что еженедельно подвергаются одной или более атак.

Как следует из результатов исследования, 61 % интернет-провайдеров признают, что DDoS-атаки являются значительной угрозой для их бизнеса. Нужно заметить, только 16 % респондентов сообщили, что редко или никогда не подвергались DDoS-атакам. В случае совершения атаки, 34 % компаний удаляют целевой клиент, тогда как 52 % временно добавляют нулевой маршрут в таблицу марштирутизации (Null route) или блокируют проблемный клиент.

По словам руководителя отдела безопасности Black Lotus Ш. Марка, и длительные, и короткие DDoS-атаки могут привести к значительному сокращению доходов и потере клиентуры. Компаниям следует понимать, что на сегодняшний день реализация средств защиты от подобных атак уже не просто роскошь, а необходимость. Благодаря наличию мощных и легкодоступных инструментов, многочисленных уязвимых точек в Интернете и развитию зависимости от Сети, DDoS-атаки продолжат увеличивать свою масштабность и сложность. Предприятия должны научиться воспринимать DDoS-атаки как вероятность, а не простую случайность, подчеркнул Ш. Марк ***(Несмотря на установленные средства защиты интернет-провайдеры не могут предотвратить DDoS-атаки // InternetUA (http://internetua.com/nesmotrya-na-ustanovlennie-sredstva-zasxiti-internet-provaideri-ne-mogut-predotvratit-DDoS-ataki). – 2015. – 9.03).***

***

DNS-провайдер OpenDNS представил новый алгоритм NLPRank, который умеет выявлять фишинговые кампании и продвинутые APT-угрозы, анализируя лингвистические паттерны в DNS-трафике. Другими словами, по

названиям запрашиваемых доменов и по изменению таких запросов со временем.

Аббревиатура NLP в названии означает технику обработки естественного языка (natural language processing). Подобные алгоритмы чаще используют в дата-майнинге и боинформатике, так что применение их для DNS-трафика в сфере информационной безопасности – что-то новенькое.

В случае фишинговых и APT-атак можно довольно просто понять принцип работы NLPRank. Авторам вредоносных программ требуются хосты, максимально похожие на легитимные домены. При этом трафик к таким хостам резко возрастает после начала атаки, когда тысячи жертв переходят по ссылкам.

NLPRank использует несколько эвристик. Близость между названиями подозрительного и легитимного хостов он вычисляет по количеству операций, которые нужно совершить для преобразования одной последовательности букв в другую (edit-distance). Эта тенденция прослеживается на примере разных атак.

Кроме буквенной близости, анализируются уникальные номера ASN, данные WHOIS, дата регистрации домена, одинаковые фрагменты HTML-кода на страницах разных доменов и прочее.

Всё это позволило эффективно и автоматически выявлять фишинговые домены, несколько примеров которых OpenDNS приводит в своём блоге ***(Распознавание вредоносных доменов по DNS-трафику // InternetUA (http://internetua.com/raspoznavanie-vredonosnih-domenov-po-DNS-trafiku). – 2015. – 9.03).***

***

Платежная система Apple Pay была использована хакерами для кражи миллионов долларов пользователей. Об этом сообщает информагентство «Рейтер».

Для совершения преступлений злоумышленники используют украденные личные данные вместе с детальной информацией банковской карты. Надежность Apple Pay при этом не ставится под сомнение. Преступникам не удалось обойти систему шифрования активации платежей, слабым место в цепочке оказались банки.

Мошенники пользуются уже украденной личной информацией, подключают чужую пластиковую карту к своему смартфону. Далее Apple пересылает зашифрованные данные в банк вместе с информацией об устройстве.

Жертвами подобных махинаций уже стали 11 млн американцев, а убытки исчисляются миллионами долларов. Банки, попавшие в эту «паутину лжи», заявили, что делают сейчас все возможное, чтобы процесс привязки карты к телефону был максимально безопасным.

Большинство банков, работающих с Apple Pay, заявили, что они усилят защищенность процесса привязки карт к сервису. Apple, в свою очередь,

заверила, что сама платежная система остается надежно защищенной ***(При помощи Apple Pay хакеры украли миллионы долларов // InternetUA (http://internetua.com/pri-pomosxi-Apple-Pay-hakeri-ukrali-millioni-dollarov). – 2015. – 8.03).***

***

Издание Help Net Security со ссылкой на ИБ-компанию Bitdefender Labs сообщило о новой спам-кампании по распространению вымогательского ПО Cryptowall. По словам экспертов, вредоносные письма рассылались пользователям по всему миру, в том числе в Великобритании, США, Нидерландах, Швеции, Дании, Австралии и Словакии. Как показал их анализ, связанные со спам-письмами серверы находились в Австралии, Индии, Вьетнаме, США, Испании и Румынии.

Представитель Bitdefender Labs К. Косой отметил, что злоумышленники использовали слегка устаревший, но эффективный способ автоматического выполнения кода на компьютере жертвы и шифрования его содержимого – вредоносное вложение .chm. Косой пояснил, что .chm является расширением файлового формата Compiled HTML, использующегося для доставки пользователям инструкции к ПО.

«Эти CHM-файлы чрезвычайно интерактивны и работают с несколькими технологиями, в том числе с JavaScript, который перенаправляет пользователя по внешнему URL всего лишь при открытии CHM, – отметил эксперт. – Злоумышленники стали использовать CHM-файлы для автоматического запуска вредоносной полезной нагрузки сразу же при открытии файла. В этом есть смысл – чем меньше взаимодействия, тем большая вероятность инфицирования».

Как только жертва открывает вредоносное .chm-вложение, из локации http:// *********/putty.exe в директорию %temp %\natmasla2.exe загружается код, а затем выполняется. Во время процесса открывается окно командной строки ***(Для выполнения вредоносного кода Cryptowall злоумышленники используют CHM-файл // InternetUA (http://internetua.com/dlya-vipolneniya-vredonosnogo-koda-Cryptowall-zloumishlenniki-ispolzuuat-CHM-fail). – 2015. – 8.03).***

***

Торговое представительство США (United States Trade Representative) не стало исключать российские компании Rutracker и соцсеть «ВКонтакте» из пиратского «списка 301». Перечень опубликован на сайте американского ведомства. Об этом пишет tass.ru

Как говорится в заявлении, торрент-трекеры Rutracker.org и Rapidgator.net продолжают способствовать пиратству. Rutracker.org, размещается и управляется из России, и является 17-м по популярности сайтом в стране, по данным Alexa.com. Оба этих сайтов неоднократно вносились «в список 301».

Помимо торрент-трекеров в список вновь была включена крупнейшая российская социальная сеть «ВКонтакте». По мнению американского регулятора, «соцсеть продолжает зарабатывать, предоставляя возможность неавторизованного обмена музыкальным и другим контентом на своем сайте и посредством приложений».

Вместе с тем «ВКонтакте» борется с пиратством, однако масштабы и объемы нарушений авторского права демонстрируют, что еще многое предстоит сделать для получения положительных результатов, отмечается в сообщении.

Сайт находится в пиратском списке с 2011 г., так как его бизнес-модель предполагает возможность несанкционированного добавления и дальнейшего распространения музыки и другого контента – в том числе через связанные с ним приложения.

Ранее «ВКонтакте» обратилась в Торговое представительство США с просьбой не включать компанию в «список 301». Компания объясняла это тем, что присутствие компании в этом списке препятствует выходу на международный рынок капитала. Тогда «ВКонтакте» заявляла, что не имеет технической возможности премодерировать загружаемый контент, а пользователи соглашаются загружать контент, который нарушает чьи-либо права. Кроме того, в социальной сети есть механизм удаления контента по жалобе правообладателя, и внедряется система распознавания аудиофайлов ***(США оставили «ВКонтакте» и Rutracker в списке пиратских сайтов // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42683/118/lang,ru/). – 2015. – 10.03).***

***

Apple закрыла уязвимость Freak в iOS, OS X и Apple TV

Apple выпустила обновление для OS X, которое повышает безопасность Mac и рекомендуется для установки всем пользователям компьютеров. Исправления доступны также для iOS и Apple TV. Данный патч устраняет уязвимость Freak, обнаруженную ранее экспертами компьютерной безопасности.

О критической уязвимости, затрагивающей мобильные устройства на iOS и компьютеры Mac, стало известно в начале марта. «Дыра», названная Freak (от Factoring RSA Export Keys), касается технологий веб-шифрования. Она позволяет злоумышленникам шпионить за коммуникациями пользователей браузера Safari на Mac.

В Apple сразу заявили, что ведут разработку «заплатки», устраняющую уязвимость. Как написала газета The Washington Post, баг делает пользователей уязвимыми при посещении «сотен тысяч сайтов», включая такие крупные госресурсы США, как Whitehouse.gov, NSA.gov и FBI.gov. В настоящее время ни одного случая Freak-атаки пока зафиксировано не было.

Для установки обновления безопасности пользователям Mac нужно зайти в раздел Обновление ПО в главном меню, пользователям iPhone и iPad – установить iOS 8.2, а владельцам телеприставок Apple TV – перейти в раздел Настройки –> Основные –> Обновления.

Отметим, что уязвимость, которая позволяет потенциальному злоумышленнику обойти защиту протоколов шифрования информации SSL/TLS, присутствует и в операционной системе Windows. Microsoft опубликовала уведомление, согласно которому брешь FREAK действительно влияет на безопасность его ОС. Ранее считалось, что она распространяется только на Mac и iOS, а также на встроенный в Android браузер.

Интересно, что в Microsoft пока не приняли решение о том, как будут реагировать на инцидент ***(Apple закрыла уязвимость Freak в iOS, OS X и Apple TV // InternetUA (http://internetua.com/Apple-zakrila-uyazvimost-Freak-v-iOS--OS-X-i-Apple-TV). – 2015. – 10.03).***

***

Apple закрыла еще одну джейлбрейк-уязвимость в iOS 8.2

С релизом финальной версии iOS 8.2 компания Apple закрыла уязвимость MobileStorageMounter, используемую джейлбрейк-инструментом TaiG. Об этом написал в своем микроблоге хакер Comex.

На странице описания дебютировавшего в понедельник обновления Apple указала имена создателей джейлбрейка с благодарностью за обнаружение «дыры» безопасности.

Из описания уязвимости:

«Доступно для iPhone 4s и выше, iPod touch (5-го поколения) и выше, iPad 2 и выше.

Воздействие: вредоносное приложение могло создавать папки в довершенной зоне файловой системы.

Описание: проблема существовала в технологии монтирования диска, что приводило к невозможности удаления папок дискового образа. Проблема была решена с помощью улучшенной обработки ошибок.

CVE-2015-1062 : TaiG Jailbreak Team».

Обновление iOS 8.2 дебютировало в понедельник вечером. В операционной системе появилось новое приложение для смарт-часов Apple Watch, а также исправлен ряд уязвимостей и улучшена стабильность работы приложений. Согласно сопроводительной документации, в сборке исчезли проблемы с навигацией, автокоррекцией текстовых сообщений, синхронизацией музыки и списков воспроизведения. Исправлены ошибки, связанные с работой Siri Eyes Free, iTunes и Bluetooth, а также уязвимость, позволяющая удаленным аудиокнигам вновь появляться на устройстве.

В первых числах марта хакерская группировка TaiGJBreak заявила, что у нее есть все необходимое для «взлома» устройств на операционной системе iOS 8.2. В TaiG тогда рассказали, что «уже подготовили непривязанный

джейлбрейк для iOS 8.2». У хакеров есть в распоряжении необходимые уязвимости для взлома финальной версии операционной системы.

Разработчики планировали выпустить эксплоит сразу после релиза iOS 8.2. Повлияет ли закрытие уязвимости MobileStorageMounter на планы TaiGJBreak, пока неизвестно ***(Apple закрыла еще одну джейлбрейк-уязвимость в iOS 8.2 // InternetUA (http://internetua.com/Apple-zakrila-esxe-odnu-djeilbreik-uyazvimost-v-iOS-8-2). – 2015. – 10.03).***

***

Пользователи мессенджера WhatsApp подверглись очередной атаке. Как сообщили в антивирусной компании ESET, под видом веб-версии приложения распространяется троян.

По электронным адресам киберпреступники рассылают письма с предложением скачать десктопный вариант мессенджера WhatsApp Web, который был выпущен в конце января 2015 г. В сообщениях указывается ссылка, якобы ведущая на официальный сайт WhatsApp. На самом же деле пользователи направляются на другую площадку, где находится инсталляционный файл WhatsAppInstall.exe, под которым скрывается троян-загрузчик Win32/TrojanDownloader.VB.QRM.

В процессе установки на компьютер загружается вредоносная программа, распознаваемая как Win32/Spy.Banker.ABOD – это «шпион», предназначенный для кражи аутентификационных данных онлайн-банкинга.

Установлено, что вирус создан в Бразилии, однако атаки могут осуществляться на пользователей разных стран.

Эксперты напоминают о необходимости игнорировать подозрительные письма, проверять названия сайтов в адресной строке браузера и загрузки программного обеспечения только с официальных ресурсов.

Это не первая попытка злоумышленников атаковать пользователей WhatsApp. В ноябре прошлого года мошенники организовали массовую подписку на платные sms-сервисы ***(Банковские счета пользователей WhatsApp оказались под угрозой // InternetUA (http://internetua.com/bankovskie-scseta-polzovatelei-WhatsApp-okazalis-pod-ugrozoi). – 2015. – 10.03).***

***

Корпорация Microsoft выпустила 14 бюллетеней безопасности, 12 из которых – для семейства операционных систем Windows. В общей сложности обновление призвано устранить 45 уязвимостей и является одним из самых крупных за последнее время, отмечает ZDNet.

Обновление предназначено для Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8 и Windows 8.1, Windows Server 2012 и Windows Server 2012 R2, Windows RT и Windows RT 8.1.

Пять бюллетеней обозначены как «критические». Они служат для устранения уязвимостей, позволяющих злоумышленникам дистанционно выполнить в системе произвольный код. Остальные бюллетени имеют статус «важных». Они устраняют ошибки, позволяющие поднять привелегии в системе или получить доступ к персональным данным.

Один из бюллетеней устраняет 11 уязвимостей в Internet Explorer. Он предназначен для версий браузера с шестой по 11. В свою очередь, бюллетень для Office охватывает версии 2007, 2010 и 2013.

Новое обновление устраняет все уязвимости, находящиеся в списке Google Project Zero на сегодняшний день, пишет ZDNet.

Напомним, что у Microsoft проект Google вызывает раздражение. Google приняла решение публиковать информацию об уязвимостях спустя 90 дней после уведомления разработчика вне зависимости от того, была она устранена к этому времени или нет. В январе Google опубликовала сведения о двух уязвимостях в продуктах Microsoft, чем вызвала ее негодование. Представитель Microsoft Крис Бетс (Chris Betz) заявил в открытом письме, что Google, по всей видимости, не очень волнует тот факт, что хакеры могут использовать эти сведения во вред пользователям ***(Microsoft устранила 45 серьезных «дыр» в обновлении Windows, Office и Internet Explorer // InternetUA (http://internetua.com/Microsoft-ustranila-45-sereznih--dir--v-obnovlenii-Windows--Office-i-Internet-Explorer). – 2015. – 11.03).***

***

ИБ-компания ESET сообщила о новом вымогательском ПО CryptoFortress, подражающем печально известному TorrentLocker. Впервые о шифровальщике стало известно из публикации исследователя, известного под псевдонимом Kafeine. По словам эксперта, уведомление с требованием выкупа и страница для оплаты у CryptoFortress такие же, как TorrentLocker. Тем не менее, проанализировав вредонос, исследователи из ESET определили, что обе программы существенно различаются.

Похоже, что создатели CryptoFortress просто похитили шаблоны HTML и CSS, поскольку вредоносный код и схемы совершенно разные. По данным ESET, между CryptoFortress и TorrentLocker существует ряд различий. К примеру, последняя распространяется через спам-письма, в то время как CryptoFortress – с помощью набора эксплоитов Nuclear Pack.

TorrentLocker соединяется с жестко закодированным C&C-сервером, содержащем страницу с требованием выкупа. В случае с CryptoFortress уведомление встроено в само ПО. Отметим, что требуемая за расшифровку файлов сумма также разнится (CryptoFortress вымогает 1 биткоин). В TorrentLocker использована криптографическая библиотека LibTomCrypt, и шифруется 2 Мб в начале файла, тогда как в CryptoFortress – Microsoft CryptoAPI, и шифруются первые 50 % файла до 5 Мб. Оба шифровальщика требуют выкуп в биткоинах.

Что касается общих черт, то в обеих программах использован 1024-битный ключ шифрования RSA, на чем их схожесть заканчивается ***(Обнаружено вымогательское ПО, подражающее TorrentLocker // InternetUA (http://internetua.com/obnarujeno-vimogatelskoe-po--podrajauasxee-TorrentLocker). – 2015. – 11.03).***

***

Исследователи безопасности из группы Zero, созданной компанией Google для предотвращения атак, совершаемых с использованием ранее неизвестных уязвимостей, продемонстрировали реальность создания рабочих эксплоитов, использующих уязвимость RowHammer, вызванную особенностями работы современных чипов памяти DRAM.

Изначально проблема с памятью DRAM скептически оценивалась многими экспертами, которые считали, что проблема ограничена лишь возможностью совершения отказа в обслуживании, а применение уязвимости для проведения более серьёзных атак считалось нереалистичным. Исследователи сумели опровергнуть данное мнение и задействовали уязвимость для совершения реальных атак, имеющих критический уровень опасности. Подготовлено два эксплоита, которые можно использовать в обычных условиях на штатном потребительском оборудовании. Первый эксплоит позволяет организовать выполнение кода с правами ядра системы. Второй вариант атаки даёт возможность обойти sandbox-изоляцию Native Client в браузере Chrome (CVE-2015-0565).

В качестве методов блокирования проявления проблемы, кроме внесения изменений на аппаратном уровне, упоминается ряд обходных путей защиты, которые можно применить на уровне ОС или выпустив обновления BIOS и прошивок. Например, повышение частоты обновления DRAM существенно затрудняет проведение атаки, а использование счётчиков производительности CPU позволяет выявлять факты осуществления атак. В Native Client блокировать уязвимость удалось добавив в систему верификации кода запрет на использование инструкции CLFLUSH.

В отчёте также указывается на важность публичного доведения до всеобщего сведения информации о выявляемых проблемах. Судя по всему производители знали об уязвимости уже давно, о чём свидетельствуют представленные в стандарте LPDDR4 два метода защиты от уязвимости, но не спешили реализовать исправления и не предупредили пользователей, так как считали уязвимость неопасной и влияющей только на стабильность.

Напомним, что в прошлом году группа исследователей обратила внимание на достаточно простой способ проявления эффекта искажения содержимого отдельных битов памяти DRAM – повреждение отдельных битов DRAM-памяти можно инициировать путём цикличного чтения данных из соседних ячеек памяти (простой цикл с чтением содержимого памяти и очисткой кэша). Проблема обусловлена особенностью работы памяти DRAM,

которая формируется как двухмерный массив ячеек, каждая из которых состоит из конденсатора и транзистора.

Состояние сохранённого в ячейке значения определяется тем, заряжен или нет конденсатор. Для поддержания заряда применяется цикл регенерации. При выполнении непрерывного чтения одной и той же области памяти из-за постоянного открытия и закрытия линии WL (Word Line), которая управляет транзисторами доступа, возникают флуктуации напряжения, которые могут привести к аномалии, вызывающей небольшую потерю заряда соседних ячеек. Если интенсивность чтения достаточно большая, то ячейка может потерять достаточно большой объём заряда и очередной цикл регенерации не успеет восстановить его первоначальное состояние, что приведёт к изменению значения сохранённых в ячейке данных ***(Продемонстрировано использование уязвимости в DRAM-памяти для повышения привилегий в системе // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2015/03/11/exploiting-dram-rowhammer-bug.html). – 2015. – 11.03).***

***

SMS-троянец под названием Podec, информация о котором появилась в прессе ранее, известен специалистам «ВКонтакте» на протяжении вот уже двух месяцев. Об этом на своей странице сообщил пресс-секретарь социальной сети Г. Лобушкин.

По его словам, сразу же после обнаружения опасной активности специалисты приняли меры по предотвращению распространения вредоносной программы. В настоящее время Podec уже не распространяется в сети «ВКонтакте», подчеркнул Г. Лобушкин в разговоре с «РГ».

О распространении в популярной соцсети опасного SMS-трояна сообщила «Лаборатория Касперского». По словам экспертов, Podec похищает деньги со счетов владельцев Android-смартфонов, тайно подписывая их на платные сервисы. В компании также отметили, что программа распространяется через группы «ВКонтакте», где пользователям Android предлагается скачать взломанные версии популярных приложений.

В настоящее время в России зарегистрировано 4 тыс. заражений смартфонов Podec, заявили в «Лаборатории Касперского».

«Вирусы придумываются и распространяются постоянно. Несмотря на то, что они распространяются не только через “Вконтакте”, но и другие сети или средства коммуникации, мы как самая популярная площадка в Рунете боремся с их распространением постоянно и предельно эффективно», – прокомментировал ситуацию пресс-секретарь «ВКонтакте» ***(«ВКонтакте» опровергает данные о распространении опасного вируса // InternetUA (http://internetua.com/vkontakte--oprovergaet-dannie-o-rasprostranenii-opasnogo-virusa). – 2015. – 12.03).***

***

Вирусописатели начали использовать уникальные идентификаторы продуктов Windows для понижения шансов на обнаружение вредоносной деятельности. Это становится возможным за счет генерации значений так называемого мьютекса, программного средства синхронизации одновременно выполняющихся потоков, сообщает исследователь из SANS Л. Зельцер.

По его словам, значения мьютекса, позволяющие обнаружить запуск идентичных процессов, использовались вирусом BackOff (предназначен для хищения данных кредитных карт) в течение последних нескольких лет.

Не так давно в открытом доступе появился новый вирус, получивший название TreasureHunter и использующий уже не статические, а динамические значения мьютекса. Среди прочего, это лишает исследователей возможности использовать уже известные «вирусные» значения для быстрого выявления факта компрометации.

Л. Зельцер также подчеркивает, что использование ID продуктов Windows в этих целях является уникальным методом: «Вредоносный код анализирует директории реестра, в том числе HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\DigitalProductId для выявления Windows ID» ***(Обнаружено вредоносное ПО, использующее ID продуктов Windows // InternetUA (http://internetua.com/obnarujeno-vredonosnoe-po--ispolzuuasxee-ID-produktov-Windows). – 2015. – 12.03).***

***

Антивирусные продукты Panda Security из-за сбоя в обновлении приняли за вирус собственные файлы. Некоторые системные администраторы попытались решить проблему с помощью перезагрузки, но это лишь ухудшило ситуацию – на компьютерах пропал доступ в Интернет.

Шесть продуктов испанской антивирусной компании Panda Security, включая Panda Antivirus Pro 2015, Panda Internet Security 2015 и Panda Global Protection 2015, после установки бракованного обновления в среду, 11 марта, обнаружили вирус в собственных файлах – psanmodrep.dll и alertsmanager.dll, – сообщает Register. Представитель компании подтвердил изданию эту информацию.

«Вчера мы выпустили обновление с ошибкой. В результате некоторые файлы программного обеспечения были распознаны движком Panda как вредоносные. Мы отозвали это обновление и выпустили вместо него исправное, добавив в него функцию восстановления файлов, помещенных в карантин по ошибке», – рассказал представитель Panda Security изданию Register.

Как пишет издание, на предприятиях, пользующихся продуктами Panda, вследствие выхода бракованного обновления возникли сложности – некоторые из них стали работать со сбоями, на других пропал доступ в Интернет.

Один из читателей Register рассказал изданию, что проблемы возникли на каждом пятом компьютере в его компании – на 60 из 300. «Panda Antivirus одновременно на десятках компьютерах в пяти различных офисах сообщил об обнаружении вируса в собственных файлах. И если у вас схожая проблема, и вы перезагрузите компьютер, то у вас пропадет доступ в Интернет», – сообщил он.

Представитель Panda Security в разговоре с изданием Register настоятельно рекомендовал пользователям не перезагружать компьютер, так как в этом случае компания не сможет самостоятельно установить исправное обновление и восстановить файлы, помещенные в карантин.

Жалобы на продукты Panda после установки последнего обновления появились и в Twitter. «Мы потеряли 20 компьютеров. Ни за что НЕ ПЕРЕЗАГРУЖАЙТЕ ВАШ КОМПЬЮТЕР», – предупредил пользователь М. Рид, выделив сообщение крупными буквами. «Самый худший антивирус в истории. Он удалил файлы из папки System32. После перезагрузки компьютеры перестали работать», – пожаловался Erroneus ***(Антивирусные продукты Panda Security приняли собственные файлы за вирусы // InternetUA (http://internetua.com/antivirusnie-produkti-Panda-Security-prinyali-sobstvennie-faili-za-virusi). – 2015. – 13.03).***

***

Случайно разглашенными оказались адреса, имена, номера телефонов, а также адреса электронной почты.

В результате неисправной работы программного обеспечения поискового гиганта Google компания случайно обнародовала имена, адреса, адреса электронной почты и номера телефонов, указанные пользователями в процессе регистрации своих веб-сайтов. При этом пользователи отмечали, что желают сохранить эти данные в тайне.

Отметим, что инцидентом была затронута база данных whois, содержащая контактные данные людей, покупавших доменные имена. Исходя из соображений безопасности, и часто за дополнительную плату, они могут потребовать сокрытия своих данных.

Исследователи безопасности в свою очередь подчеркивают, что в ближайшее время пострадавшим пользователям стоит ожидать повышенного внимания со стороны мошенников, специализирующихся на фишинговых атаках.

«В руках злоумышленников окажутся настоящее имя, адрес, наименование соответствующего веб-сайта, номер телефона», – поясняет сотрудник Cisco К. Уильямс. По его словам, этой информации более, чем достаточно, чтобы составить крайне достоверное электронное письмо в вредоносной ссылкой или вложением ***(Из-за ошибки Google в открытый доступ попали персональные данные пользователей // InternetUA (http://internetua.com/iz-za-oshibki-Google-v-otkritii-dostup-popali-personalnie-dannie-polzovatelei). – 2015. – 13.03).***

***

PayPal купит стартап CyActive, разработавший способ предсказания новых вирусов. PayPal намерена сделать свою вторую покупку в Израиле. На этот раз будет приобретена молодая фирма CyActive, специализирующаяся на информационной безопасности.

CyActive разработала очень оригинальную эвристическую технологию. По утверждению компании, технология эта способна предсказывать, какие новые вредоносные программы злоумышленники изобретут в скором будущем. В результате разработчики могут начать работать над средствами защиты заблаговременно, ещё до того, как произойдут первые атаки.

По словам гендиректора CyActive Л. Танкмана, вредоносное ПО всегда производно по отношению к чему-то, даже самые совершенные вирусы имеют общие компоненты с программами предыдущих поколений. «Можно очень чётко видеть… все методы, которые хакеры используют сейчас, и их варианты, которые они могут использовать в будущем. Даже крупные атаки последних лет, такие как Flame, Stuxnet и другие, имеют общее ядро», – сказал Л. Танкман в интервью.

PayPal и CyActive пока не прокомментировали сделку. По информации источника, на который ссылается ZDNet, стоимость покупки составит как минимум 60 млн дол.

В CyActive интересно то, что этому стартапу едва исполнился год, а он уже представляет большой интерес для инвесторов, как израильских, так и международных. Основатели компании являются видными экспертами в области кибербезопасности ***(PayPal купит стартап CyActive, разработавший способ предсказания новых вирусов // InternetUA (http://internetua.com/PayPal-kupit-startap-CyActive--razrabotavshii-sposob-predskazaniya-novih-virusov). – 2015. – 13.03).***

***

Российские вирусы маскируют под официальные документы СБУ.

Служба безопасности Украины обнаружила и заблокировала вредоносное программное обеспечение (ПО), которое разрабатывалось и использовалось спецслужбами Российской Федерации.

Об этом сообщила пресс-служба СБУ в Facebook.

Шпионская программа была предназначена для получения информации с компьютеров, а также поражения сетевого оборудования. Ее рассылали в органы власти и правоохранителям, задействованным в АТО.

Адресату направлялся электронное письмо с вложением «фейковых» официальных документов от якобы СБУ, Госпогранслужбы, МВД или других ведомств. Файл, как правило имел типичное название и не вызывал подозрения, например, «справка об обстановке на государственной границе по состоянию на ...». После открытия такого файла на компьютер загружалась шпионская программа, которая предоставляет удаленный доступ

к содержанию почтового ящика и информации на жестком диске компьютера.

«Установлено, что с телекоммуникационного оборудования, размещенного за пределами Украины, в частности на территории Российской Федерации, рассылались электронные письма на почтовые адреса должностных лиц органов государственной власти и правоохранительных органов», – отметили в СБУ ***(СБУ обнаружила российские шпионские программы на компьютерах госорганов // InternetUA (http://internetua.com/sbu-obnarujila-rossiiskie-shpionskie-programmi-na-kompuaterah-gosorganov). – 2015. – 13.03).***

***

В Facebook по-прежнему присутствуют серьезные уязвимости

Португальский исследователь безопасности Д. Сопас сообщил об обнаружении нескольких уязвимостей в Facebook, которые, по его мнению, могут быть опасными. Эксперту не удалось убедить руководство соцсети в серьезности этих брешей, поэтому он выложил информацию о них в общественный доступ.

По данным Сопаса, одна из уязвимостей позволяет злоумышленнику с помощью инструмента Ads/Tools/Text_Overlay загружать на серверы Facebook исполняемые файлы с любым расширением или использовать их как репозиторий. В качестве доказательства исследователь без каких-либо ограничений загрузил на серверы соцсети ряд файлов, к которым у него есть доступ в любое время, пока он авторизован в своей учетной записи.

Кроме того, Д. Сопас обнаружил несколько уязвимостей, позволяющих злоумышленнику обмануть пользователей, убедив их в том, что они загружают файл (например, вредоносное ПО) якобы из доверенного домена. По мнению эксперта, эта брешь еще более опасная по сравнению с описанной выше, поскольку не требует аутентификации.

Все, что необходимо для успешного осуществления атаки – заставить жертву пройти по ссылке, которая автоматически загружает специально сконфигурированный исполняемый файл .bat, открывающий вредоносную страницу в браузерах IE, Chrome, Opera, Android Browser и Chrome для Android ***(В Facebook по-прежнему присутствуют серьезные уязвимости // InternetUA (http://internetua.com/v-Facebook-po-prejnemu-prisutstvuuat-sereznie-uyazvimosti). – 2015. – 13.03).***

***

Adobe исправила 11 уязвимостей в Flash Player. В число исправленных входят девять уязвимостей, позволяющих злоумышленникам удаленно выполнить код.

В четверг, 12 марта, Adobe выпустила обновления безопасности для Flash Player, исправляющие 11 уязвимостей. Производитель отмечает, что установка патча является приоритетной для Windows, OS X и Linux.

Пользователям и администраторам Adobe Flash Player для Linux Chrome и Internet Explorer, Flash Player Extended Support Release и Flash Player Desktop Runtime также рекомендуется установить обновления.

В число исправленных входят девять уязвимостей, позволяющих злоумышленникам удаленно выполнить код, инфицировать систему вредоносным ПО и, как результат, получить над ней контроль. По состоянию на момент выпуска патча сообщений об эксплуатации этих брешей компания не получала.

Уязвимыми являются версии Adobe Flash Player 16.0.0.305 и ниже, Adobe Flash Player 13.0.0.269 и ниже, а также Adobe Flash Player 11.2.202.442 и ниже ***(Adobe исправила 11 уязвимостей в Flash Player // InternetUA (http://internetua.com/Adobe-ispravila-11-uyazvimostei-v-Flash-Player). – 2015. – 13.03).***

***

13 березня українські хакери зламали низку сайтів терористів. Про це терористи стали повідомляти в другій половині дня. Зокрема, один з головних сайтів терористів «Кіберберкут» був заблокований ***(Українські хакери ламають сайти терористів // ІНФОРМАТОР (http://www.informator.su/ukrajinski-hakery-lamayut-sajty-terorystiv/). – 2015. – 13.03).***