СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(6–19.10)

2014 № 19

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(6–19.10)
№ 19

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

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

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2014

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

На конференции FbStart в Нью-Йорке представители Facebook объявили о запуске кнопки «Мне нравится» для приложений на Android и iOS, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-knopku-mne-nravitsja-dlja-mobilnyh-prilozhenij-41538/).

Т. Крабах, разработчик соцсети, сообщил, что новый функционал даст возможность пользователям лайкать страницы приложений в Facebook или Open Graph объекты внутри этих приложений, а также делиться этими действиями в социальной сети. Кнопка легко синхронизируется с аккаунтом пользователя, за счет чего он может лайкать любой контент в приложении.

Так как аудитория Facebook постепенно «перемещается» на мобильные устройства, нововведение соцсети вполне обосновано – оно поможет поддерживать высокую вовлеченность мобильной аудитории.

Разработчикам приложений настоятельно рекомендуется тестировать расположение кнопки и момент ее показа пользователям, а также страницу приложения в Facebook для максимальной эффективности ***(Facebook запустил кнопку Мне нравится для мобильных приложений // Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-knopku-mne-nravitsja-dlja-mobilnyh-prilozhenij-41538/). – 2014. – 6.10).***

***

Компания Qualcomm готовится запустить новую технологию LTE Direct, которая позволяет совершать звонки и обмениваться сообщениями без получения сигнала от вышек сотовой связи. При использовании данной технологии мобильные устройства способны объединяться в сеть на расстоянии до 500 м, что гораздо больше площади покрытия Wi-Fi и Bluetooth. Возможность совершать звонки на смартфоны в радиусе действия LTE Direct – это минимум, которого можно достичь, применяя данную технологию. Размещённые ретрансляторы по всему городу могут не только усиливать сигнал, но и служить для отправки различных информационных сообщений в радиусе своего действия.

Например, проходя мимо какого-либо магазина вы получите сообщение о скидках или акциях внутри – вариантов использования технологии LTE Direct множество. Без необходимости подключения к сотовой сети вы сможете на небольшом расстоянии звонить, отправлять сообщения и прочее. Компании Facebook и Yahoo уже объявили о своей заинтересованности в возможностях вышеупомянутой технологии. Facebook планирует использовать LTE Direct для взаимодействия пользователей своей социальной сети между собой. В свою очередь, Yahoo ведёт разработку приложения, которое будет отправлять туристам информацию о различных достопримечательностях в городе.

Qualcomm надеется, что первые устройства с поддержкой LTE Direct появятся уже в конце следующего года ***(Qualcomm LTE Direct позволит совершать звонки без подключения к базовым станциям // InternetUA (http://internetua.com/Qualcomm-LTE-Direct-pozvolit-sovershat-zvonki-bez-podkluacseniya-k-bazovim-stanciyam). – 2014. – 6.10).***

***

Компания Twitter в партнерстве с Kantar Media объявила о запуске ТВ-рейтингов в Великобритании. Об этом сообщает searchengines.ru. Нововведение – последний шаг компании в ее мировой стратегии «социального телевидения». Оно позволит измерить то, как пользователи делятся и обсуждают ТВ-программы и релевантный контент в сети Twitter.

Новый сервис будет включать различные метрики, панель управления аналитикой и ТВ-метрику потока данных. Он начнет работу в середине октября.

Изначально ТВ-рейтинг был запущен Twitter в сотрудничестве с исследовательской компанией Nielsen в 2012 г. только на территории США. Новая метрика (Nielsen Twitter TV Rating), основанная на данных Twitter, позволила изучить поведение телевизионных зрителей, пользующихся социальной сетью.

Расширение функционала за пределы США заняло довольно долгое время. Twitter и Kantar впервые объявили о предстоящем сотрудничестве с целью запуска ТВ-рейтингов в Великобритании и Испании больше года назад. Шесть месяцев прошло с того момента, как Twitter объявил, что сделка с Kantar расширит сервис еще на четыре региона – Скандинавы, Россию, некоторые страны Африки и Юго-Восточной Азии.

В настоящее время работают (или начнут работу в ближайшие пару недель) только два рынка из планируемых семи – США и Великобритания.

Социальные ТВ-сервисы Twitter будут построены на базе той же модели, что и сотрудничество с аналитической компанией Nielsen.

«Запуск первых официальных ТВ-метрик для Twitter в Великобритании дает индустрии телевещания понимание уровня вовлеченности аудитории социальной сети в просмотр телевидения», – прокомментировал запуск Э. Браун, руководитель компании мирового уровня и председатель Kantar Media. «Используя ТВ-рейтинги Twitter-Kantar, сотрудники организаций вещания, специалисты по планированию и рекламодатели получат возможность оценить телепередачи и сериалы и более эффективно планировать их продвижение. А продавцы рекламных площадей в СМИ и медиа-баеры с его помощью смогут интегрировать социальные данные в телевизионный компонент их медиа-микса», – добавил он.

Согласно заявлению представителя Kantar, новый инструмент будет сфокусирован на отфильтрованных по географическому признаку данных Twitter в Великобритании и предоставит доступ к метрикам и аналитике, которые ранее не были доступны в этой стране.

Они включают определение соответствия пользователей социальной сети конкретным брендам, каналам и программам; отслеживание количества людей, которые смотрят твиты, относящиеся к отдельным программам; количество показов – сколько раз твит или ретвит был отправлен – для конкретной телепередачи. Другими словами, Kantar измеряет многое из того, что измеряют в Twitter другие, но при этом он способен задать свои параметры для работы с конкретными ТВ-шоу.

Другие возможности будут включать аналитику, включая показатель среднего количества твитов в минуту и наибольший объем твитов в минуту для конкретных программ.

Среди других сервисов, которые будут запущены в середине октября, – панель управления аналитикой Instar Social. Она разработана для вещателей, медиа агентств и рекламодателей и будет включать рейтинговую таблицу топовых программ в Twitter и другие данные.

Редактор TechCrunch И. Лунден считает, что наличие Instar Social наряду с другими инструментами ТВ-аналитики может в будущем привести к тому, что Twitter будет рассматриваться как часть стандартного медиа-микса ***(Twitter запускает ТВ-рейтинги в Великобритании // Media бізнес (http://www.mediabusiness.com.ua/content/view/40868/126/lang,ru/). – 2014. – 6.10).***

***

Компания Facebook работает над приложением, позволяющим пользователям анонимно общаться внутри сети, пишет New York Times со ссылкой на осведомленные источники. Новая программа может выйти в течение ближайших нескольких недель.

Руководителем проекта является менеджер по продукции Facebook Д. Миллер, присоединившийся к Facebook после приобретения стартапа Branch. Д. Миллер и его команда работают над мобильным приложением, которое позволит взаимодействию пользователей без использования своих настоящих имен, рассказали два человека, знакомые с планами компании.

По словам собеседников издания, новинка Facebook даст возможность пользователям использовать несколько псевдонимов для открытого обсуждения различных тем.

Неясными остаются вопросы, как новое приложение будет взаимодействовать с сайтом Facebook и будет ли разрешен анонимный обмен фотографиями.

Издание отмечает, что планы компании демонстрируют иной, экспериментальный, взгляд на вопрос анонимности в Интернете, поскольку главный продукт компании – социальная сеть Facebook является «способом представления своего виртуального образа таким же, как и в реальной жизни», отмечает автор статьи.

Представитель Facebook заявил, что компания не комментирует слухи и спекуляции. Д. Миллер на запрос по электронной почте не ответил.

Ранее Facebook и, в частности, основатель компании, выступали против анонимности в Интернете. М. Цукерберг называл использование такой практики атавизмом и трусостью. В соцсети пользователям не разрешается подписываться ненастоящими именами. М. Цукерберг пояснял, что «Facebook должен показывать то, кем ты являешься на самом деле» и облегчить поиск для своих друзей, что осложнит процесс при использовании не своего имени ***(Facebook выпустит приложение для анонимного общения // Четверта Влада (http://4vlada.net/mass-media/facebook-vypustit-prilozhenie-dlya-anonimnogo-obshcheniya). – 2014. – 8.10).***

***

Приложение Twitter для OS X обогатилось несколькими функциями, ранее доступными для десктопов. В частности, приложение теперь поддерживает возможность размещать несколько фотографий в одном твите.

Как и на других платформах, Twitter для Mac поддерживает обмен до 4 фотографий одновременно. Возможность поделиться несколькими фотографиями была впервые введена в марте 2014 г.

Также реализована возможность просмотра полного варианта изображения, для этого следует кликнуть на его превью.

Кроме того, пользователи Twitter для Mac теперь могут обмениваться фотографиями в приватных сообщениях.

Бесплатное обновление приложения доступно в Mac App Store ***(Twitter для Mac обновил функции поддержки изображений в сообщениях // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_dlya_mac_obnovil_funktsii_podderzhki_izobrazheniy_v_soobscheniyah). – 2014. – 8.10).***

***

Веб-дизайнер Ш. Арифи разработал концепцию редизайна социальной сети Instagram, предполагающую наличие минималистских иконок и показ фотографий пользователей во весь экран.

Чтобы минимизировать беспорядок, основное меню можно увидеть, проведя пальцем вправо по экрану смартфона или нажав на соответствующую иконку. Также пользователи могут увидеть комментарии к своим снимкам, проведя пальцем по экрану влево.

В новостной ленте появятся изображения, загруженное людьми, на чьи обновления пользователь подписан. Они будут поданы в виде фотографий большого размера с миниатюрными иконками, символизирующими лайки и комментарии.

Профиль отображает юзерпик пользователя, его подписчиков и тех, на кого он подписан, а внизу – сделанные им снимки.

Самые популярные фотографии будут размещаться в верху ленты, и пользователь сможет увидеть самые востребованные снимки часа ***(Редизайн***

Instagram: фотографии во весь экран // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/redizayn_instagram_fotografii_vo_ves_ekran). – 2014. – 9.10).

***

Социальная сеть Facebook, 1,3-миллиардная аудитория которой начиналась в основном за счет школьников и студентов, перестала быть местом притяжения тинейджеров. Об этом говорят результаты опроса аналитической фирмы Piper Jaffray, проведенного между весной и осенью 2014 г. За этот период пользование сайтом М. Цукерберга среди молодых людей в возрасте от 13 до 19 лет упало с 72 до 45 %, пишут «Экономические известия» (http://news.eizvestia.com/news_technology/full/266-podrostki-massovo-uhodyat-iz-socseti-facebook).

Другими словами, на вопрос, пользуются ли они Facebook, меньше половины респондентов дали утвердительный ответ. Исход подростков из самой популярной соцсети объясняется увлечением более модными сервисами, такими как Instagram (76 %) или Twitter (59 %), где не зарегистрированы их родители ***(Подростки массово уходят из соцсети Facebook // «Экономические известия» (http://news.eizvestia.com/news_technology/full/266-podrostki-massovo-uhodyat-iz-socseti-facebook). – 2014. – 9.10).***

***

Соцмережа Facebook дозволила додавати стікери, що зображують емоції, в коментарі до записів на профільних сторінках користувачів, пише Корреспондент.net (http://ua.korrespondent.net/tech/technews/3431199-v-Facebook-ziavylasia-mozhlyvist-vstavliaty-stikery-v-komentari).

Відповідна іконка з’явилася в полі для тексту коментаря на Facebook.

Досі значки-стікери, за допомогою яких користувач може швидко описати свою емоційну реакцію, були доступні в особистих повідомленнях і в додатку Messenger, в який Facebook повністю перенесла обмін повідомленнями на мобільних пристроях. Вперше стікери з’явилися на Facebook минулого літа.

Стікери в коментарях працюють за тим же принципом, що і в повідомленнях. Користувач отримує базовий набір смайликів, однак може завантажити додаткові колекції з магазину стікерів Facebook. Поки ці колекції безкоштовні, проте в майбутньому Facebook може зробити їх додатковим джерелом монетизації, подібно до сервісу Viber.

«Думаю, що стікери дадуть можливість відповідати на записи більш забавно, ніж звичайними словами. Ви тепер можете легко висловити свою радість від публікації з хорошими новинами, підтримати друга, який сумує, і висловити безліч інших реакцій», – написав на своїй Facebook-сторінці розробник соцмережі Б. Болдуїн.

Можливо, таким чином Facebook прагне подолати недоліки кнопки Like – користувачі неодноразово критикували її недоречність для реакції на погані новини. Крім тексту та стікерів, користувачі Facebook також можуть вставляти в коментарі фотографії ***(В Facebook з'явилася можливість вставляти стікери в коментарі // Корреспондент.net (http://ua.korrespondent.net/tech/technews/3431199-v-Facebook-ziavylasia-mozhlyvist-vstavliaty-stikery-v-komentari). – 2014. – 14.10).***

***

Возможность узнать, кто просматривал ваш профиль в LinkedIn, появилась довольно давно, но компания расширила ее: теперь пользователи смогут также увидеть, какие их действия привели к просмотру аккаунта другими пользователями. Это может быть, к примеру, обновление данных, или вступление в какую-либо группу.

По словам представителя компании, даже малейшие изменения профиля важны, а знать, что именно повлекло за собой многочисленные посещения, просто необходимо.

К примеру, если юзеру требуется привлечь новых клиентов или бизнес-партнеров, он вступает в группу, где может их найти, а новая функция поможет ему узнать, кто именно из его новых партнеров обратил на него внимание после того, как он вступил в группу ***(LinkedIn позволит узнать, почему ваш аккаунт просматривали // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/linkedin_pozvolit_uznat_pochemu_vash_akkaunt_prosmatrivali). – 2014. – 13.10).***

***

Убийцы Facebook: чего можно ожидать от новой социальной сети Ello

И еще пять сервисов, которым прочат славу «нового Facebook»

В конце сентября любители социальных сетей получили повод радоваться: на просторах Интернета появилась новая социальная платформа Ello, которую в народе уже успели прозвать «антифейсбуком». Эта сеть существовала задолго до ее официальной презентации и создавалась в качестве внутренней сетки для 90 работников онлайн-магазина.

Главное отличие Ello от Facebook в том, что все данные тут абсолютно засекречены, а лента новостей свободна от рекламных объявлений.

По состоянию на сегодня новая сеть выглядит не лучшим образом сайт напоминает скорее платформу для блогов, чем полноценную социальную сеть. Здесь не пополняют фотоальбомы и не обмениваются личными сообщениями, а лишь публикуют записи и комментируют их. Пока в Ello нет ни мобильного приложения, ни возможности пожаловаться на оскорбительную запись. Нет и никакой альтернативы кнопкам «лайк», но это осознанное решение, призванное стимулировать «подлинное общение».

Зато есть функция, отсутствующая у других сервисов: она позволяет разделить всех пользователей на «друзей» и «шум». По умолчанию в ленте

новостей отображаются все записи друзей, а лента для «шума» представляет собой сетку с началами записей, которую можно быстро окинуть взглядом.

«Ello − это бизнес. Как и в App Store, основные сервисы у нас всегда будут бесплатными. Но за совсем небольшие деньги мы намерены продавать приложения, которые пользователям захочется установить в своем аккаунте. Нам уже приходят тысячи запросов с просьбой ввести тот или иной сервис, пусть даже за деньги. Покупать такие вещи за пару долларов – отличный способ поддержать работу социальной сети без рекламы», − рассказала Р. Фукайя, представитель команды Ello, комментируя вопрос о том, как новая социальная сеть собирается зарабатывать деньги.

В Украине эта соцсеть пока остается почти неизвестной. Так что трудно предположить, какое место новинка займет в жизни украинских пользователей Facebook. Кроме того, Forbes вспоминает еще пять социальных сетей, которым прочат славу «нового Facebook».

Secret

Заинтересовать пользователей новой социальной сетью крайне сложно, однако бывают и исключения. Так, в последнее время необыкновенную популярность обрела сеть Secret – она дает возможность полностью анонимно постить короткие сообщения. Пользователи могут публиковать картинки и статусы, не оставляя никаких намеков на то, кому они принадлежат.

Количество установок Secret с Google Play уверенно приближается к отметке в 100 тыс. Этот показатель подтверждает, что анонимная социальная сеть пришлась по душе многим пользователям. Средний балл Secret в Маркете составляет 3,6.

В любой момент в Secret можно удалить все фото, также редактор позволяет закрыть лицо на фотографии. В США эта сеть стала чрезвычайно популярной из-за небывалого слива информации: IT-специалисты, журналисты, блоггеры, маркетологи и пиарщики активно делились секретами о слиянии и поглощении компаний, деталями новых соглашений, слухами о грядущих увольнениях.

Snapchat

Сервис, где все сообщения самоуничтожаются, благодаря чему пользователи чувствуют себя гораздо безопаснее. Главный посыл сервиса – избежать необходимости постоянно оглядываться на общественное мнение и просчитывать последствия своих поступков в Интернете. По словам CEO Snapchat Э. Шпигеля, в сентябре пользователи ежедневно отправляли 350 млн снепов, тогда как в конце прошлого года загруженность сервиса была в 7 раз меньше.

В связи с ростом популярности сети ею начали интересоваться инвесторы и компании, желающие выкупить ее. Сначала цена сервиса была всего 800 млн дол., в настоящее время ее оценивают в 3,6 млрд дол.

Shots of Me

Невероятно популярная сеть среди американских подростков. В ноябре прошлого года американский поп-исполнитель Д. Бибер вложил в Shots of Me 1,1 млн дол., что стало главным толчком к ее развитию.

Идея сети очень проста: чат и селфи фронтальной камерой. «Комментарии под фото невозможны, что позволяет развиваться и не опасаться критики», − рассказывают в команде сети.

Приложение разработала студия Rock Live. Глава компании Д. Шахиди заявил в интервью Tech Crunch, что музыкант Д. Бибер заинтересовался концепцией проекта, потому что другие социальные сети его раздражали. Также разработчики надеются, что со временем Shots of Me вытеснит Instagram, в котором, по словам создателей Shots of Me, можно смотреть только на фото завтраков.

Tinder

Сеть онлайн-знакомств Tinder позволяет очень быстро завести новые знакомства. При регистрации ваше фото берется из Facebook-аккаунта, вся информация тоже черпается именно оттуда. Tinder работает следующим образом: программа показывает фото людей, находящихся неподалеку от вас. После того как вы «лайкнете» фото, появится информация, ответил ли этот пользователь вам взаимностью, если так − между вами открывается чат, и вы можете общаться и познакомиться.

Также приложение пользуется большой популярностью во время проведения крупных спортивных соревнований. Р. Пембакиан, представитель Tinder рассказывает: «В среднем на Tinder пользователь тратит больше часа, примерно 77 мин. И этот показатель вырос почти на 50 % в Бразилии во время проведения Чемпионата мира по футболу. Такое же оживление среди пользователей наша команда наблюдала во время зимних Олимпийских игр в Сочи, некоторым спортсменам даже пришлось удалить свои аккаунты, чтобы сконцентрироваться на спортивных достижениях».

Whisper

Сеть в чем-то напоминает Secret, однако вместо тайн от топ-менеджеров здесь можно прочитать любовные признания и переживания пользователей. Наиболее популярна среди аудитории 18–24 года. Whisper делает акцент на анонимность − отказ от самоидентификации прекрасно коррелирует с трендом, заданным исчезающими сообщениями в Snapchat. Кроме анонимных секретов, у платформы есть возможность личных сообщений, однако за нее придется выложить 6 дол. в месяц.

Именно такая совокупность вирусности и монетизации привлекла внимание инвесторов. По данным AllThingsD, в приложении просматриваются ежемесячно около 2,5 млрд страниц. 40 % пользователей продуцируют контент, а среднее время пребывания в приложении − 30 минут ***(Убийцы Facebook: чего можно ожидать от новой социальной сети Ello // InternetUA (http://internetua.com/ubiici-Facebook--csego-mojno-ojidat-ot-novoi-socialnoi-seti-Ello). – 2014. – 15.10).***

***

Социальная сеть Facebook представила новую функцию Safety Check, созданную для проверки безопасности друзей и родственников во время природных катаклизмов, сообщает The Verge.

Сеть автоматическим определит местонахождение пользователя и если он находится рядом с зоной от зоной стихийного бедствия, ему предложат нажать кнопку «Я в безопасности» для оповещения друзей.

В свою очередь, все адресаты получает автоматически сгенерированное сообщение.

Также пользователи смогут самостоятельно определить, кто из их друзей находится в зоне бедствия.

Глава и основатель Facebook М. Цукерберг представил новую функцию в Японии, которая еще не до конца оправилась от последствий землетрясения и цунами 2011 г.

«Наши инженеры в Японии сделали первый шаг к созданию сервиса для улучшения поиска людей после катастрофы», заявила Н. Глейт, вице-президент по управлению продуктами Facebook.

Тесты Safety Check оказались успешными, опция будет доступна в обычной и мобильной версиях Facebook ***(Facebook поможет людям во время стихийных бедствий // Версии.com (http://versii.com/news/314334/). – 2014. – 16.10).***

***

В приложениях сервиса микроблоггов Twitter добавлена новая опция для проигрывания музыки внутри твитов Audio Card. Эта новая возможность Twitter сделана в виде встроенного в твит плеера, в котором показана информация об исполнителе, песне и обложка альбома, в общем, как на обычном плеере. Специалисты компании Twitter сделали возможным прикреплять к сообщениям пользователей музыкальные файлы и подкасты.

В блоге компании Twitter сообщается, что скоро пользователи смогут добавлять к твитам аудиоконтент из iTunes или SoundCloud.Сегодня Twitter объявил, что теперь вы можете слушать музыку и подкасты непосредственно в ленте на Android и iOS устройствах, передает News-software.

Новые карточки позволяют публиковать в Twitter любой аудиоконтент, хранящийся на сервисе SoundCloud или в каталоге iTunes. Она позволит пользователям сервиса слушать аудиозаписи прямо из ленты Twitter на мобильных устройствах под управлением операционных систем iOS и Android. Даже если пользователь будет смотреть ленту новостей внутри приложения, то треки все-равно будут продолжать играть.

В ближайшие недели новый аудио функционал будет доступен всем, кто имеет профиль на SoundCloud. Теперь пользователи смогут добавить к своим твитам любой аудиоконтент из SoundCloud или iTunes. SoundCloud стал первым партнером Twitter в этом начинании, в дальнейшем в

приложение будут интегрированы плееры других музыкальных сервисов ***(Twitter замахнулся на ВКонтакте: теперь и внутри твитов можно слушать музику // InternetUA (http://internetua.com/Twitter-zamahnulsya-na-vkontakte--teper-i-vnutri-tvitov-mojno-slushat-muziku). – 2014. – 18.10).***

***

Украинские программисты запустили социальную сеть для любителей футбола Footplayer. С ее помощью футболисты-любители могут находить себе партнеров для игр, организовывать матчи и турниры, а также следить за результатами своих друзей. Создатель соцсети – киевский программист А. Стегно. Он рассказал AIN.UA, что вместе со своими друзьями решил запустить сайт, чтобы сэкономить время на организацию матчей. «Как правило, у людей уходит много времени на созвоны, поиск полей и недостающих игроков. Наш сайт облегчает эти задачи и мы считаем, что он реально нужен обществу», – сказал он (http://ain.ua/2014/10/17/545686).

Специально регистрироваться на сайте не надо – там можно авторизизоваться через Facebook, Gmail или «ВКонтакте». Вскоре на ресурсе появится возможность создавать команды, отслеживать игровое время и «лайкать» успехи своих друзей. Кроме того, друзья планируют собираться не только не выходных, но и играть в будние дни ***(Киевляне запустили социальную сеть для любителей футбола // AIN.UA (http://ain.ua/2014/10/17/545686). – 2014. – 17.10).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Украинские пользователи уже жаловались на то, что администрация Facebook предвзято относится к политическим конфликтам: наказывает украинских активистов и попустительски относится к россиянам. Пока одни пишут письмо М. Цукербергу, другие берут дело в свои руки: в украинском сегменте Facebook существует уже несколько закрытых групп пользователей, основная цель которых: банить очевидных «кремлеботов». Корреспонденту AIN.UA удалось пообщаться с организатором одной из таких групп на условиях анонимности (http://ain.ua/2014/10/08/544075).

Основная цель работы таких групп – чистка инфополя и привлечение внимания офиса Facebook (и в частности, украинцев, которые там работают), к проблеме «кремлеботов». «Есть много неглупых людей в Facebook, которые очень неумно стравливают пар, матерятся, но ничего не предпринимают», – объясняет организатор такой группы. – Если этих людей объединить и дать им цель, они хотя бы будут проводить время в соцсетях с пользой». Кстати, «смммщиков» в этих группах мало: по словам собеседника

AIN.UA, они циничные и часто не брезгуют заказами от пророссийских политических сил.

К сожалению, профессиональных троллей и ботов, а также их высокобюджетные группы в Facebook забанить почти нереально, поэтому группа сосредоточилась на «простых целях». Указанная группа работает по такому сценарию: кто-то из участников выносит на обсуждение очередной профиль «кремлебота», приводит доказательства в пользу того, что это именно проплаченный бот, и группа принимает решение. Ботов ищут как правило в комментяриях к постам лидеров мнений и проукраинских ресурсов. «Боты в основном оскорбляют и постят картинки, на которые легко отправить жалобу», – объясняет организатор.

Примерно в половине случаев работа группы увенчивается успехом и Facebook банит бота. Собеседник AIN.UA отмечает интересные особенности в работе администрации социальной сети: по некоторым аккаунтам реакция из офиса почти мгновенная, хотя обычно она занимает от четырех часов до суток. «По ощущениям, есть договор не банить ботов с некоторых IP. Кроме того, мы явно видим по некоторым “ватным” ботам, что реакция почти молниеносная», – рассказывает организатор группы.

Подобных объединений интернет-активистов в украинском сегменте Facebook уже несколько. В такие группы входят самые разные специалисты, включая CEO компаний – это одна из причин, почему такие объединения анонимны и закрыты. Другая причина – в том, что если бы в группу было бы легко попасть, в ней рано или поздно оказался бы SMM-профи, который бы начал ее «раскачивать, объясняет огранизатор группы. «В итоге у всех опускаются руки от внутренних склок, и группа разваливается. Что хуже, разваливается вера в совместную работу и люди в очередной раз уходят. Мы стараемся делать так, чтобы не срабатывало «два украинца, три гетьмана», – говорит он. Всем, кто заинтересовался инициативой, предлагается создавать свои группы с участием доверенных людей, у которых будет время этим заниматься.

Руководитель одной из украинских IT-компаний, которому предлагали присоединиться к группе, называет такое движение полезной инициативой. «Считаю, лучше делать, чем не делать. Никто не знает, насколько это будет эффективно. Как никто не знал, чем все кончится в ноябре 2013 или в 2004 г.», – говорит он. Правда, сам он не смог присоединиться к группе из-за нехватки времени: «За это время я заработаю и перечислю ленег “Крыльям Феникса”. А другие пусть банят ботов. Мы идем параллельными курсами».

Напомним, еще в конце августа участились блокировки проукраинских активистов в Facebook. Их блокируют из-за жалоб, которые оставляют так называемые «кремлевские боты». В одной из закрытых групп украинского Facebook родилась идея написать письмо об этом непосредственно основателю социальной сети М. Цукебергу. В Facebook опровергли обвинения в политической предвзятости специалистов сети ***(Украинцы в***

Facebook объединяются в секретные группы и банят «кремлеботов» // AIN.UA (http://ain.ua/2014/10/08/544075). – 2014. – 8.10).

***

У Гарварді вивчили настрої щодо Євромайдану серед користувачів соцмереж в Україні, Росії, США і Великобританії, пише Корреспондент.net (http://ua.korrespondent.net/world/3429680-u-sotsmerezhakh-ssha-yevromaidan-pidtrymuvaly-bilshe-nizh-v-ukraini).

Користувачі соціальних медіа в США і Великобританії підтримували Євромайдан у Києві активніше, ніж в Україні. Про це свідчать результати дослідження Б. Етлінга з Центру досліджень інтернету і суспільства ім. Беркмана при Гарвардському університеті.

Проаналізувавши такі інтернет-інструменти, як Facebook, Twitter і мережеві форуми на предмет вмісту позитивних, негативних і нейтральних відгуків про події в Києві в період з 21 листопада 2013 р. по 26 лютого 2014 р., з'ясувалося, що в Україні 47 % згадувань про дані події носили схвальний характер.

«Результати показують, що настрої в соціальних медіа в Україні значною мірою були позитивними (47 %), істотна кількість контенту (37 %) була нейтральною, і лише 16 % негативною», – ідеться в доповіді.

Водночас, картина соціальної медіаактивністю в контексті київських подій виявилася більш позитивною у США і Великобританії, ніж в Україні. Там дії активістів Євромайдану підтримували 55 % інтернет-користувачів. Відгуків нейтрального змісту було приблизно в рівній з Україною кількості – 35 %. Негативних висловлювань у бік демонстрантів було всього 10 %.

Дані з Росії продемонстрували, що переважна більшість відгуків носила нейтральний характер – 69 %. Контент позитивного і негативного змісту траплявся набагато рідше – в 16 % і 15 % випадках відповідно.

Результати дослідження ґрунтуються на даних і були отримані за допомогою програмного інструменту Crimson Hexagon, який шляхом спеціальних алгоритмів дає змогу здійснювати моніторинг і аналізувати контент у соціальних медіа за заданими параметрами ***(У соцмережах США Євромайдан підтримували більше, ніж в Україні // Корреспондент.net (http://ua.korrespondent.net/world/3429680-u-sotsmerezhakh-ssha-yevromaidan-pidtrymuvaly-bilshe-nizh-v-ukraini). – 2014. – 9.10).***

***

Лікар анестезіолог Кіровоградського обласного онкодиспансеру та головний позаштатний фахівець департаменту охорони здоров'я Кіровоградської ОДА з паліативної та хоспісної допомоги М. Макаревич вирішив створити групу в мережі Facebook «Хоспіс Кіровоград».

Про це у Facebook повідомив лікар Кіровоградського обласного онкодиспансеру та громадський діяч А. Гардашніков.

До спільноти пропонують максимально долучатися або хворих, що мають доступ до Інтернету та сили, щоб дописувати, або їхніх родичів – писати про те, які в них є проблеми.

«Я також думаю, що там має бути якомога більше лікарів, бізнесменів, журналістів та взагалі небайдужих людей, – пише А. Гардашніков. – Хай буде окремий майданчик для постійного обговорення цієї теми. Якщо не всі проблеми будуть вирішені, то хоч частинка, а може з'являться ідеї та рішення, які зроблять можливим зменшити страждання людей, що йдуть з життя. В багатьох областях навіть нашої країни (не кажу про цивілізований світ) ці страждання набагато зменшують завдяки паліативній медицині. В нашій області цього, чомусь, немає…

Адреса спільноти «Хоспіс Кіровоград»: https://www.facebook.com/groups/1573389259547778 ***(Кіровоградський лікар створив у соцмережі спільноту для невиліковно хворих // Точка доступу (http://dostyp.com.ua/novini/kirovograds-ky-j-likar-stvory-v-u-sotsmerezhi-spil-notu-dlya-nevy-likovno-hvory-h/). – 2014. – 16.10).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Facebook разрабатывает систему денежных переводов. Об этом заявляет студент Стэнфордского университета Э. Од, взломавший код Facebook Messenger, сообщает Engadget.

Студент опубликовал скриншоты и видео, которые доказывают, что в скором времени к приложению можно будет привязать банковскую карту и переводить с нее деньги своим собеседникам. Данные о транзакции не будут видны в ленте новостей.

Представления приложения и официального комментария от компании пока не было. По словам студента, приложение уже готового к использованию, но еще не представлено публике ***(Facebook разрабатывает систему денежных переводов // Утро.UA (http://www.utro.ua/ru/ekonomika/facebook_razrabatyvaet_sistemu_denezhnyh_perevodov1412583576). – 2014. – 6.10).***

***

Компанія Facebook завершила анонсовану в лютому операцію з купівлі мобільного месенджера WhatsApp вартістю 19 млрд дол., пише Корреспондент.net (http://ua.korrespondent.net/business/companies/3428330-Facebook-zakryv-operatsiui-z-kupivli-WhatsApp).

Про це повідомляє The Wall Street Journal. 3 жовтня угоду схвалила Єврокомісія.

Купівля WhatsApp стала найбільшою угодою в індустрії стартапів, перевершивши найбільше до цього придбання Facebook – сервісу Instagram за 1 млрд дол. У квітні угоду схвалила Федеральна торгова комісія США, з єдиною обмовкою про безпеку користувача даних: Facebook не повинен використовувати особисті дані користувачів WhatsApp для таргетованої реклами.

Сервіс WhatsApp налічує близько 450 млн користувачів щомісяця, з них 70 % активні кожен конкретний день. Обсяг повідомлень, які відправляються через WhatsApp, наближається до загального обсягу смс-повідомлень по всьому світу. Також WhatsApp показує впевнене зростання, щодня тут реєструються 1 млн нових користувачів.

Як раніше повідомлялося, поповнювальні цінні папери ще на 3 млрд дол. WhatsApp отримає протягом 4-х років після закриття угоди. Крім того, один із засновників додатку, українець Я. Коум увійде до складу ради директорів Facebook ***(Facebook закрив операцію з купівлі WhatsApp // Корреспондент.net (http://ua.korrespondent.net/business/companies/3428330-Facebook-zakryv-operatsiui-z-kupivli-WhatsApp). – 2014. – 7.10).***

***

Компания Teleperformance, ведущий провайдер аутсорсинговых услуг контакт-центров в мире, провела исследование каналов взаимодействия с потребителями компаний сектора онлайн-торговли. 100 % крупнейших организаций, как в России, так и в мире, присутствуют в социальных сетях, однако полноценный сервис предлагают лишь некоторые. Число подписчиков в социальных сетях российских компаний на несколько порядков меньше мировых лидеров в сфере торговли. Клиенты предпочитают традиционные каналы взаимодействия с брендами – электронную почту и телефон. Социальные сети используются потребителями для размещения отзывов без особой надежды на обратную связь. При этом 68 % клиентов верят отзывам о компаниях в Интернете.

Исследование сектора онлайн-торговли в Бразилии, Франции, Германии, Великобритании и США, показало, что, в среднем, розничные компании предоставляют четыре различных канала для взаимодействия с клиентами. Голосовые каналы коммуникации предлагаются клиентам не всегда. При том, что 100 % компаний предлагают e-mail и социальные сети в качестве каналов для вовлечения клиентов во взаимодействие, только 84 % компаний предоставляют голосовые каналы связи.

По всему миру компании сектора онлайн-торговли ведут работу, в среднем, в шести социальных сетях, Facebook и Twitter – наиболее популярны.

Мировые лидеры ритейла имеют широкую базу подписчиков: согласно данным Центра стратегических исследований одной из крупнейших розничных компаний России Enter, среднее число подписчиков страниц розничных компаний в Facebook в мире составляет 3,1 млн человек,

максимальное количество – 18,6 млн. У Walmart число подписчиков превышает 34 млн. Российские показатели на несколько порядков ниже. Среднее число подписчиков у российских компаний в Facebook составляет 9,2 тыс., максимальное – 36 тыс., во «ВКонтакте» среднее – 49 тыс., максимальное – 242 тыс.

Мировая практика показывает, что, даже несмотря на гигантское количество подписчиков, не все социальные медиа работают как выделенные каналы клиентского обслуживания – клиенты не всегда могут решить свою проблему через социальные сети. Только 32 % компаний в мире ведут аккаунт в Twitter как полноценный канал коммуникации.

Как показал опрос компании Teleperformance, потребители используют социальные медиа для того чтобы выразить свое отношение к сервису компании – «спустить пар» или наоборот, похвалить. Чаще всего они не ожидают от компании решения своей проблемы. Для этого они предпочитают использовать телефон (41 %) или электронную почту (46 %).

При этом, потребители сильно подвержены влиянию как позитивных, так и негативных мнений других клиентов по отношению к брендам – 46 % клиентов используют информацию из социальных сетей принимая решение о покупке (исследование американской маркетинговой компании Razorfish). По данным международной исследовательской компании Nielsen, 68 % опрошенных готовы верить мнениям, опубликованным в Интернете.

«Сложилась парадоксальная ситуация. Компании, имеющие страницы в социальных сетях, часто не используют их как полноценный канал коммуникации. Клиентов либо просят обратиться по телефону или электронной почте, либо, в худшем случае, игнорируют, и удаляют их отзывы. Потребители отвечают компаниям взаимностью и не верят в то, что через социальные сети можно эффективно решить свой вопрос. При этом они доверяют отзывам в Интернете, что отражается на их лояльности к брендам. Учитывая то, какими темпами растет число подписчиков на страницы российских компаний в социальных сетях, онлайн-магазинам нужно срочно предпринять меры для того чтобы наладить эффективную обратную связь с потребителями. Клиенты должны поверить в то, что их проблему можно эффективно решить онлайн. В краткосрочной перспективе это будет способствовать повышению лояльности, а в долгосрочной – и продаж», – прокомментировала С. Смирнова, Операционный директор Teleperformance Russia & Ukraine ***(Страницы крупных компаний в социальных сетях не решают проблем потребителей: исследование Лаборатории Клиентского Опыта Teleperformance «Взаимодействие с потребителями в мультиканальной среде» // Mskit.Ru (http://mskit.ru/news/n173007/). – 2014. – 7.10).***

***

Facebook открыл для бизнеса свою платформу по размещению рекламы в мобильных приложениях Audience Network, анонсированную на

конференции разработчиков f8 в апреле. Платформа позволяет монетизировать мобильные приложения с помощью 1,5 млн активных рекламодателей Facebook. Об этом сообщает searchengines.ru.

«В течение последних нескольких месяцев мы оптимизировали нашу сеть, чтобы повысить производительность, и теперь официально запускаем и расширяем услуги для разработчиков и издателей по всему миру», – говорит представитель Facebook Т. Чен.

Audience Network показывает людям правильные объявления, расширяя таргетинг Facebook на сторонние приложения. Это означает, что объявления совпадают с интересами людей, так же, как это происходит в Facebook.

Существующие рекламодатели смогут расширить свои кампании Facebook на Audience Network одним кликом.

В платформе представлены нативный и баннерный форматы рекламы. Также у клиентов сети есть возможность запускать так называемые Interstitial ads, которые отображаются до того, как пользователь сможет получить доступ к контенту страницы.

По предварительным сведениям, Facebook обещает предоставить клиентам мобильной рекламной сети дополнительные возможности таргетинга. Также, сообщается, что изначально количество показов рекламы будет строго регламентироваться ***(Facebook запускает Audience Network для бизнеса // Media бізнес (http://www.mediabusiness.com.ua/content/view/40905/126/lang,ru/). – 2014. – 8.10).***

***

Готовим бизнес к праздникам: как соблазнить клиента с помощью социальных сетей

Вы уже задумывались, как построить праздничную рекламную кампанию, используя социальные сети? В начале сезона праздников спрос может быть не так уже велик, однако под его конец – пользователи соцсетей становятся настоящими «горящими покупателями». Поэтому стоит заблаговременно позаботиться о том, чтоб на ваших страницах была размещена вся необходимая информация о праздничных предложениях, и сделано это было максимально профессионально и продумано.

Ранее мы уже рассказывали о том, как, как подготовить веб-сайт компании к работе в праздники и поделились некоторыми секретами праздничного Email-маркетинга. В этот раз рассмотрим социальные сети как способ привлечь клиентов в праздничный период.

Опрос, проведенный в прошлом году компанией Crowdtap, показал, что 65 % покупателей в праздничный период используют социальные сети, чтобы найти идеальный подарок. Иногда они – это последний шанс для бизнес, чтобы максимально увеличить продажи и сбыть продукцию, предназначающуюся именно для приобретения в виде подарка.

«Независимо от того, владеете вы огромным гипермаркетом или маленьким бизнесом, праздники – самое время развивать свое онлайн-влияние через социальные сети», – говорит руководитель компании Weaving Influence и эксперт по созданию стратегий в социальном маркетинге Б. Робинсон. Имея значительный опыт работы в этой сфере, зная всю ее подноготную, специфику в разные времена года и при разных условиях рынка, она предложила несколько советов касательно того, как использовать социальные сети, чтобы слушать, контролировать и взаимодействовать с существующими клиентами и привлекать потенциальных.

Научитесь прислушиваться к клиентам и рынку

Хотя многие предприятия заблаговременно создают график обновления страниц в социальных сетях, Б. Робинсон считает, что стоит отходить от принципиальности в этом вопросе и демонстрировать готовность коммуницировать со своими подписчиками вне установленных границ.

«Хотя, конечно, очень заманчивой является возможность изначально запланировать и публиковать рекламные обновления в течение праздничного сезона, вы можете выделиться, прислушиваясь к запросам клиентов и отвечая им на конкретные вопросы», – считает специалист. Такое решение поможет вам избежать навязчивости и даст вашим подписчикам ощущения того, что о них заботятся.

Б. Робинсон также советует предприятиям всегда держать ухо востро, следить за рынком и своим местом на нем. Она рекомендует использовать аналитические исследования, которые позволят следить за другими брендами, а также проверять ваши социальные каналы несколько раз в день.

Берите на себя инициативу, когда она уместна

Пользователи часто постят информацию о продуктах и услугах, которые вы предлагаете. Не упустите возможность, заприметив их интерес, превратить этих людей в своих клиентов.

Один из вариантов, по мнению Б. Робинсон, таков: чтобы попасть «на радары» покупателей, предприятия должны сохранять результаты поиска, к примеру, в Twitter, для своей отрасли или региона, а затем находить соответствующие твитты и обновления в социальных сетях, регулярно проверяя поток поиска.

Если в сообщениях пользователя, который не является вашим подписчиком, встречается общее название того или иного продукта без указания бренда (но вы понимаете, что речь идет о том виде товара, который вы предлагаете), это может стать толчком сделать клиенту предложение, опередив его интерес к вашему конкуренту. В праздничное время это особо актуально, так как с увеличением спроса растет и количество предложений. Кто первый решится обратиться к потребителю, привлекая его внимание на себя, может стать победителем.

Будьте открытыми и правдивыми

Социальные сети – это не только продвижение продуктов и услуг. Это построение отношений.

Б. Робинсон считает, что предприятия должны «делегировать» конкретного человека, чтобы он лично участвовал в жизни страницы компании в социальных сетях в режиме реального времени каждый день. Одним из способов являются комментарии к впечатлениям или фактам, которыми делятся подписчики или же вопросы к ним.

Во время праздников, предприятия могут активно делиться своими реалиями жизни, чтобы дать клиентам представление о том, как коллектив готовится к праздникам и их отмечает. Можно размещать фотографии, ежедневно рассказывать о событиях и делиться историями из офисной жизни.

Обеспечьте «особую любовь» самым верным клиентам

Хотя в идеале люди становятся подписчиками страниц брендов в социальных сетях, чтобы получать от них последние новости, Б. Робинсон утверждает, что это все же не главная причина их присоединения к такому онлайн-сообществу. По ее мнению, они все же преследуют другую цель – получить особые предложения и скидки. Будьте изобретательны и думайте о неожиданных способах презентации акций и эксклюзивных предложений. Дайте поклонникам и клиентам то, чего они хотят на самом деле, продемонстрировав этим свою признательность и благодарность за их верность ***(Готовим бизнес к праздникам: как соблазнить клиента с помощью социальных сетей // Международная ассоциация успешного бизнеса (http://maub.com.ua/n/v/984). – 2014. – 9.10).***

***

Facebook запустил новый ресурс FBIQ, который поможет брендам и маркетологам с помощью анализа данных и существующих трендов лучше узнать свою аудиторию.

Аудитория будет анализироваться с точки зрения поколений, регионов проживания и устройств, которыми пользуются люди.

На портале будет присутствовать четыре раздела:

«Аналитика по аудиториям» (Peoples Insights), которая позволит понять, как в целом ведут себя потребители в онлайн и офлайн-пространствах, а также выявит их отношение к какому-либо вопросу, теме или предмету;

«Праздники и события» (Holidays & Events) – здесь будет приведена информация о том, как люди отмечают на Facebook различные праздники, мероприятия и важные события;

«Отраслевые исследования» (Industry Research) сосредоточатся на эффективности рекламных кампаний, а также будут включать мнения экспертов на тему успешных кейсов с использованием различных платформ;

«Статистика» (By the Numbers) – в этом разделе можно будет найти самую последнюю статистику от Facebook.

Команда Facebook надеется, что FBIQ станет полезным дополнением к сайту Facebook для бизнеса ***(Facebook запустил ресурс FBIQ в помощь***

брендам и маркетологам // IT Expert (http://itexpert.org.ua/rubrikator/item/38761-facebook-zapustil-resurs-fbiq-v-pomoshch-brendam-i-marketologam.html). – 2014. – 12.10).

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Среди свыше миллиарда пользователей Facebook есть несчетное количество одиноких сердец. Они не становятся такими после некоторого пребывания в социальной сети – они подключаются, будучи уже одинокими, – утверждают исследователи.

В новом исследовании были решено проанализировать связь между человеческим одиночеством и использованием популярной социальной сети. Эта связь действительно существует, но в иной форме, чем считалось ранее.

Исследование показало, что не Facebook делает людей изолированными от реального мира – это Facebook привлекает одиночек. Данные утверждают, что чем более одиноко чувствует себя человек, тем дольше он находится в сети, а не наоборот.

В то же время социально активные личности посещают страницу в Facebook, чтобы дополнить свое чувство сплоченности с обществом.

Под одиночками исследователи понимают людей неуверенных в себе, или со слабой поддержкой окружающих. Такие люди обращаются к социальной сети, чтобы компенсировать недостаток социальных навыков, – говорится в отчете исследования ***(Социальные сети не делают людей более замкнутыми, чем они есть // AmericaRU.com (http://www.americaru.com/news/71157). – 2014. – 14.10).***

***

Каждый третий подросток в Британии, состоящий в отношениях, находит своего партнёра в Интернете, сообщает британская пресса. По результатам исследования, в котором приняли участие более тысячи человек, выяснилось: всего 1 % опрошенных заходят в Интернет, чтобы побродить по сайтам, не имеющим отношения к соцсетям. Все остальные находятся в сильной зависимости от друзей по онлайну. С подробностями – корреспондент радио «Вести ФМ» в Лондоне Е. Балаева:

«Социальные сети – это уже неотъемлемая часть жизни современных подростков. Вот только взрослые порой до конца не могут представить, насколько сильно их дети зависят от онлайн-сообщества. Судя по опросу, который провела британская телерадиокорпорация, каждый третий подросток находит себе партнёра в социальных сетях, чтобы затем встретиться в оффлайне. Каждый четвёртый при этом утверждает, что в онлайне с виртуальными друзьями чувствует себя увереннее и счастливее, чем в реальной жизни, а каждый десятый уверен: друзья с Facebook знают его гораздо лучше, чем обычные».

Доктор Э. Шорт, психолог из Университета Бедфордшира, объясняет: за последние годы люди начали принимать как само собой разумеющееся тот факт, что можно завести дружбу в Интернете. Но нельзя забывать, что познакомиться в Интернете с незнакомым человеком – это как познакомиться и тут же подружиться с незнакомцем в метро или в автобусе. В настоящее время порой даже эксперты по безопасности не могут с уверенностью установить, являются ли достоверными сведения, которые сообщает о себе человек в социальных сетях. И уже тем более это сложно определить 15-летним детям.

Подросткам надо постоянно напоминать: разговорившись с незнакомцем в чате, они, по сути, ничего о нём не знают, а человек может быть совсем другим, нежели чем представляет сам себя в разговоре. Но даже если подросток ведёт себя осторожно с незнакомыми людьми в онлайне, есть другая, не менее важная проблема – зависимость от социальных сетей. Половина опрошенных британских подростков признались: они постоянно держат телефон в руке, чтобы проверять приходящие им сообщения в социальных сетях. Если же они забыли телефон дома, то чувствуют себя неполноценными и постоянно беспокоятся.

Перебороть зависимость в одиночку не получится. Друзья и родные должны объяснить, что в жизни есть много интересного помимо социальных сетей. Если, конечно, смогут сами оторваться от экрана ***(Балаева Е. Соцсеть как наркотик: британские подростки не могут представить жизнь без Интернета // Радиостанция «Вести ФМ» (http://radiovesti.ru/article/show/article_id/150803). – 2014. – 17.10).***

Маніпулятивні технології

В інформаційних війнах, як правило, не буває жертв у звичайному, фізичному сенсі цього слова. Але від цього вони не стають більш гуманними порівняно з війнами реальними. Тут втрати – це зруйновані дружні, культурні і навіть сімейні зв’язки. Тут люди, ще вчора обговорювали якісь абсолютно мирні теми – футбол, театр, дайвінг, кулінарію – як то кажуть, вставте потрібне слово – зациклюються на обговоренні будь-якого конфлікту

і нерідко, опинившись по різні сторони «інформаційних барикад», стають непримиренними суперниками. Якщо не сказати більше.

Україна – Росія. Конфлікт, вже кілька місяців як перейшов у військову стадію. Упереджено освітлюваний засобами масової інформації обох країн, він з самого початку обговорюється в соціальних мережах. І вже там, в соцмережах, на хвилі цього конфлікту з'являються свої лідери думок і зірки Інтернету, створюються і розпадаються групи і союзи. Війна проникла і туди, в Facebook, «ВКонтакте», Twitter та ін.

Коли ж все почалося? А почалося все, мабуть, з Майдану, взимку. Саме тоді з'явився розрив в оцінці подій.

Не всі були готові прийняти цю інформацію. Більшість влаштовувало те, чим федеральні телеканали звично «годували» своїх глядачів. Хоча – чому тут дивуватися: провідні телеканали були поставлені «під рушницю» ще 10–12 років тому.

Думаю, всі пам'ятають про захоплення на початку «нульових» спочатку «Першого каналу», який тоді, здається, ще називався ОРТ, а потім – болісне приєднання до кремлівського пулу багатостраждального НТВ. Але це окрема історія, про неї як-небудь іншим разом...

Отже, більшості росіян все показуване по телевізору подобалося. Меншість же намагалася скласти більш різноманітну картинку і шукала правду. І дещо знаходила в мережі. Адже соціальні мережі – поки – складніше контролювати тим, хто хоче контролювати все і вся. І, якщо в Китаї доступ до Facebook і Twitter закритий, то в Росії це ще не відбулося.

Хоча, з іншого боку, тим, хто вірить в картинку, яку показують по телевізору, складно пояснити, що все не зовсім так, як розповідають Кисельов і Леонтьєв. Їх влаштовує той небагатий набір штампів, які вищезазначені телеведучі та подібні їм застосовують в своїх передачах, де чітко позначені «свої» і «чужі».

Правда їм не потрібна. Точніше, потрібна, але інша. Та, де Радянський Союз був великим, в їх розумінні, державою, яка боялися і ненавиділи в більшості країн решти світу. Їм хочеться і зараз, щоб їх боялися тому, що в їх розумінні, по їх простій пацанській логіці, бояться – значить поважають.

Інша справа – соцмережі.

В них, а, в першу чергу, в Facebook спочатку і суспільство збиралося, як правило, таке, що володіє більш високим рівнем IQ. І, відповідно, багатьом «фейсбучникам» думки лише одного джерела інформації мало, а бажано кілька, щоб скласти власну картинку того, що відбувається, а не ту, що нав'язує той чи інший засіб масової інформації. Якими б благими намірами це ЗМІ не керувалося.

Зрозумівши нескладну істину, що свої інформаційні запити думаюча частина суспільства задовольняє не в контрольованому медіапросторі, а в соцмережах, держава почав перейматися й цією частиною інформаційного світу.

Кишенькові путінські олігархи почали скуповувати всі ті ресурси, до яких дотягувалися їх руки. Але скупити контроль над всім неможливо. Тим більше, якщо подібний ресурс знаходиться поза юрисдикцією російських «рокфеллерів». Так що, Facebook цим людям поки не по зубам. Так само як і Twitter.

А ось прибрати до рук суперпопулярну в Росії, та й не тільки в ній, мережу «ВКонтакте», видавивши з Росії її засновника П. Дурова, у них вийшло. Поки на цьому, як кажуть, серце і заспокоїлося. Якщо не вважати «Одноклассники» та інші соціальні мережі, що потрапили в сферу впливу А. Усманова та Ю. Мільнера – путінських інтернет-бізнесменів.

Словом, для шукаючих правду або щось на неї схоже, www – це те, що треба. Особливо для тих, хто звик порівнювати і аналізувати інформацію з різних джерел. Іноді навіть зовсім різних.

Знову ж, соцмережі самі по собі складно назвати джерелом інформації. Це скоріше якусь подобу Гайд-парку, де люди обмінюються думками. І вже потім пропонують ті джерела інформації, яким довіряють.

Безумовною популярністю серед російськомовних «фейсбучників»-ліберaлів користуються сьогодні не дуже велика кількість інтернет-ресурсів, але зате їх якість знаходиться на цілком високому рівні. Це такі ресурси, як snob.ru і slon.ru. Не намагаючись аналізувати ці інтернет-ЗМІ, можна сказати, що навіть з підбору авторів вони помітно виділяються на тлі багатьох видань. Сюди ж можна віднести Znak.ru і «Ведомости».

Втім, чи варто перераховувати всі гідні уваги інформаційні мережеві ресурси? Їх цілком достатня кількість, щоб скласти наочну і реальну картинку того, що відбувається. Було б бажання знайти! І не залежати від контрольованих людьми з чистими руками, холодними умами і гарячими серцями засобами масової інформації ***(Іванов В. Соцмережі як криве дзеркало ЗМІ, або де шукати правду // РБК-Украина (http://www.rbc.ua/ukr/analytics/show/sotsseti-kak-krivoe-zerkalo-smi-ili-gde-iskat-pravdu-08102014100000). – 2014. – 8.10).***

***

В пророссийских группах социальных сетей активно распространяются примитивные фальшивки, целью которых является разжигание межконфессиональной вражды, дестабилизация и провоцирование социальной напряженности в обществе, передает пресс-служба СБУ.

«СБУ призывает не поддаваться на эту примитивную провокацию, поскольку целью ее разработчиков является спровоцировать противостояние между теми, кто купится на эту ложь, и теми, кто придет на защиту “жертв”», – отметил советник главы СБУ М. Лубкивский.

Лубкивский призвал граждан быть мудрыми и блокировать попытки сеять раздор в обществе. «Будьте мудры, блокируйте такие попытки и сообщайте СБУ», – заявил он.

В пресс-службе также напомнили, что в СБУ работает круглосуточный телефон «горячей линии» 0800501482, на который граждане могут сообщать информацию о такого рода провокации. Такие сведения немедленно проверяться, по результатам проверки будут приняты соответствующие меры ***(СБУ предупреждает об очередной провокации в соцсетях // Новости Донбасса (http://novosti.dn.ua/details/236104/). – 2014. – 13.10).***

***

Через соцмережі з'ясували, що організатори бунту Нацгвардії – ФСБ. Організаторами так званого бунту Нацгвардії, коли кілька сотень солдатів-строковиків прийшли під Адміністрацію Президента вимагати повернення додому, були російські спецслужби.

Це вдалося з'ясувати в тому числі і через соцмережі – одна з головних організаторів, Ю. Харламова, за звичкою засвітила себе у «ВКонтакте». Вона вербувала через мережу солдат та займалась їх психологічною підготовкою. Разом з диверсійними загонами вона також встигла повоювати на сході України, атакуючи позиції української армії.

Ю. Харламова – давня учасниця неофашистських та нацистських рухів Росії, служила в підмосковному десанті, а з вересня почала займатись диверсійною діяльністю в Україні для ФСБ – вела сторінки в соцмережах. Під час «бунту солдатів» вона разом з іншими жінками-спільницями грала роль «матерів та подруг», вимагаючи «дембеля», та напала на журналістів Podrobnosti.ua.

Це вже не перший раз, коли російські найманці викладають в соцмережі докази власної причетності до терору та війни в Україні ***(Через соцмережі з'ясували, що організатори бунту Нацгвардії – ФСБ // UkrainianWatcher (http://watcher.com.ua/2014/10/16/cherez-sotsmerezhi-z-yasuvaly-scho-orhanizatory-buntu-natshvardiyi-fsb/). – 2014. – 16.10).***

***

Twitter зізнався у експериментах та маніпуляціях з твітами

Представники Twitter нарешті розказали, чому показували користувачам твіти, на авторів яких вони не були підписані.

Як повідомляється в офіційному блозі сервісу, останні 2 місяці компанія провела серію експериментів, в рамках яких включала у стрічки користувачів контент від авторів, на яких вони не підписувались. Вперше ЗМІ помітили це в серпні 2014 р. і сприйняли за спам. У Twitter кажуть, що займались покращенням свого сервісу і вирішили провести експерименти з обмеженим відсотком користувачів.

На думку продуктового директора Twitter Т. О'Брайана, існують ситуації, коли користувач може просто пропустити те, що може бути важливим. Компанія застосовувала свою аналітику, щоб визначити, який саме контент варто показати людині. Для прикладу, ним часто слугували пости, які друзі користувача додавали у Обране. Окрім того, якщо

користувач часто оновлював стрічку через мобільні додатки, але не отримував жодного нового твіту, це також було сигналом до того, що він потребує більше контенту ***(Twitter зізнався у експериментах та маніпуляціях з твітами // UkrainianWatcher (http://watcher.com.ua/2014/10/17/twitter-ziznavsya-u-eksperymentah-ta-manipulyatsiyah-z-tvitamy/). – 2014. – 17.10).***

***

Американские эксперты и чиновники шокированы тем, что Запад проигрывает информационную войну из-за «огромной машины наглой пропаганды» В. Путина, которая активно «дезинформирует» не только россиян, но и русскоязычных жителей соседних стран. В ответ США пытаются активно продвигать «альтернативные» источники информации через соцсети и призывают не верить «лживым» российским СМИ, передает Voice of America.

Госдепартамент США крайне обеспокоен попытками Кремля «ограничивать фундаментальные свободы не только для граждан России, но и для граждан соседних стран, которые получают информацию из российских СМИ». Результаты такой «шокирующей» политики уже отчетливо видны не только в региональном, но и в глобальном масштабе, отмечает Voice of America.

«В то время как мы отвлеклись на другие глобальные вызовы в последние несколько лет, президент В. Путин построил огромную машину дезинформации, которая имеет глобальный охват. Мы шокированы ее наглостью, и тем, какое влияние она оказывает на население стран, граничащих с Россией, на русскоязычные меньшинства в этих странах», – заявила Т. Хомяк-Салви, заместитель координатора Бюро международных информационных программ Госдепартамента США.

Она подчеркнула, что Вашингтон стремится «ответить на усиливающийся, все более энергичный поток пропаганды» из Москвы при помощи создания платформы русскоязычных социальных сетей, которые позволят аудитории «получать представление о реальном положении вещей» и самостоятельно принимать решения и формировать оценки на базе альтернативных источников информации.

«Мы используем социальные сети как быстрый способ распространения нашей информации. Конечно, мы помним о том, что аудитория может скептично относиться ко всем государственным источникам информации. Мы не скрываем того факта, что мы представляем Госдепартамент. Нашей целью при этом является введение нашей точки зрения в дискуссию. Мы полностью осознаем, что люди это прочтут и сформируют собственную точку зрения», – приводит комментарий Т. Хомяк-Салви Voice of America.

Накануне в ходе дебатов о судьбе международного вещания в Институте Кеннана в Вашингтоне эксперты и чиновники Госдепартамента

США выразили мнение, что Запад проигрывает России в информационной войне. Эту точку зрения разделяет и президент организации Freedom House Д. Крамер, который также крайне обеспокоен «пропагандой, исходящей из Кремля и подконтрольных ему СМИ», отмечается в статье.

«Они не просто искажают информацию, они пытаются создать свою собственную реальность. Они неверно все интерпретируют, они лгут и представляют ситуацию такой, какой она на самом деле не является. Яркий пример тому – Украина. Когда у вас есть люди, такие как Д. Киселев, которые просто брызжут ненавистью и используют оскорбительную риторику», – подчеркнул Д. Крамер в интервью Voice of America.

Глава Freedom House также заявил, что эти «говорящие головы пропаганды Кремля» не могут считаться журналистами: «Вся их деятельность построена на лжи и имеет очень антизападный и антиамериканский тон. Они не передают новости, не предоставляют объективного анализа. Они просто изрыгают ложь Кремля, что, на мой взгляд, очень опасно» ***(VOA: Госдеп шокирован «наглостью российской дезинформации» // ИноTV (http://russian.rt.com/inotv/2014-10-19/VOA-Gosdep-shokirovan-naglostyu-rossijskoj). – 2014. – 19.10).***

Зарубіжні спецслужби і технології «соціального контролю»

Американська компанія Twitter 7 жовтня подала позов до Федерального суду Каліфорнії на ФБР і міністерство юстиції США щодо захисту права на свободу слова та першої поправки до конституції США.

Компанія, зокрема, має намір домагатися зняття заборони на розкриття інформації про судові запити американських спецслужб.

«Ми вважаємо, що згідно з першою поправкою, ми маємо право відповідати на стурбованість наших користувачів, а також на заяви представників уряду США, надаючи інформацію про масштаби проведеного американським урядом стеження», – заявив віце-президент Twitter Б. Лі.

Наразі Twitter, як і інші мережеві організації, зобов'язані за запитом правоохоронних органів надавати їм закриті дані про користувачів. При цьому відкрито заявляти про сам факт такого запиту їм заборонено. Так, у квітні 2014 р. частково закрили для публікації «звіт про прозорість», направлений Twitter до американського уряду: серед іншого, цей документ містив і відомості про запити з боку органів безпеки.

Раніше з таким запитом до суду звертався інтернет-гігант Google, домагаючись дозволу публікувати статистику про звернення спецслужб до компанії і про пов'язані з цим судові рішення. Цей запит відхилили.

7 лютого цього року керівництво Twitter розкритикувало угоду про розкриття статистики співпраці зі спецслужбами, укладену найбільшими

американськими ІТ-компаніями з урядом країни. Представники Twitter заявили, що домагатимуться від влади права публікації докладнішої статистики запитів з боку розвідувальних відомств. Крім того, в компанії повідомили, що проситимуть владу про право повідомляти про відсутність запитів певного типу.

На початку лютого звіти за запитами спецслужб опублікували відразу кілька великих компаній (Microsoft, Google, Facebook і Yahoo). Оприлюднена статистика містила секретні запити співробітників ФБР та АНБ, схвалені судом на підставі закону «Про контроль за діяльністю служб зовнішньої розвідки» (Foreign Intelligence Surveillance Act, FISA). Проте, звіти складалися лише із загальних цифр. Детальна статистика взаємодії компаній з органами влади (наприклад, кількість запитів того чи іншого типу) не проводилася.

Публікація даних стала можливою на основі домовленостей, досягнутих компаніями з міністерством юстиції США. ІТ-фірми звернулися до відомства з вимогою дозволити розкриття такої інформації після скандалу, викликаного публікацією документів про програму інтернет-стеження АНБ під назвою PRISM. Секретні документи надав пресі екс-співробітник АНБ Е. Сноуден ***(Twitter подав до суду на Вашингтон // LB.ua (http://ukr.lb.ua/news/2014/10/08/281888_twitter_podal_sud_vashington.html). – 2014. – 8.10).***

***

Российских операторов обяжут фильтровать интернет-контент

В конце сентября крупные операторы получили от исполнительного директора Лиги безопасного Интернета (ЛБИ) Д. Давыдова письмо с концепцией поправок в законодательство, рассказали два человека, получивших письмо. Об этом пишет vedomosti.ru.

ЛБИ предлагает поправить два федеральных закона: «О защите детей от информации, причиняющей вред их здоровью и развитию» и «О связи», обязав операторов ввести семантическую фильтрацию интернет-контента по умолчанию. Они должны будут отфильтровывать «информацию, причиняющую вред здоровью и развитию детей, с помощью программно-технических средств», требования к которым должно будет установить правительство, говорится в документе, разработанном ЛБИ. Совершеннолетние абоненты смогут «по личному заявлению» отключить эту фильтрацию, поясняется в документе.

Впервые предложение ввести автоматическую фильтрацию контента в Интернете озвучила этим летом с подачи ЛБИ депутат Е. Мизулина (она входит в попечительский совет лиги). На расширенном заседании комитета Госдумы по вопросам семьи, женщин и детей она предложила, чтобы все провайдеры автоматически блокировали контент, вредный для детей, а чтобы отключить фильтрацию, пользователи подписывали с провайдерами

специальные допсоглашения (предъявив паспорт). Тогда Минкомсвязи поддержало идею депутата и ЛБИ.

Один из федеральных чиновников говорит, что ему пожаловались региональные операторы: ЛБИ разослала им письмо с предложением установить свое программное решение для фильтрации трафика «в связи с предстоящими изменениями в законодательных актах». Он считает недопустимым «законотворчество, которое нацелено на получение экономической выгоды определенной группы людей». Близкий к ЛБИ источник уверяет, что установка и обслуживание этого софта будут бесплатными.

Д. Давыдов подтвердил, что рассылал операторам концепцию поправок в законодательство. А вот предложений по установке программного обеспечения ЛБИ никому не делала, отрицает он. Лига надеется, что предлагаемые поправки будут внесены кем-нибудь из депутатов Госдумы, обеспокоенных темой защиты детей в Интернете, рассказывает Д. Давыдов. По его словам, свои программные решения лига не навязывает – у большинства операторов и так есть техническая возможность фильтровать контент по принципу «родительского контроля». Надо только сделать эту услугу бесплатной для абонентов и работающей по умолчанию, считает Д. Давыдов. Он также добавляет, что по желанию некоторых операторов лига может установить свое программное решение, но, как правило, это делается на бесплатной основе.

«Ведомости» ознакомились с позицией большой тройки операторов, которую те изложили в коллективном письме к ЛБИ. Предложение лиги «неэффективно с точки зрения достижения цели законопроекта, однако его реализация повлечет серьезные материальные затраты как для операторов связи, так и для государства», считают МТС, «Вымпелком» и «Мегафон». Они предупреждают, что реализация предложений ЛБИ потребует установки операторами на своих сетях дорогостоящего аппаратно-программного обеспечения из расчета, что все 100 % абонентов воспользуются услугой семантической фильтрации контента. «Это повлечет для операторов связи серьезные инвестиции (провизорно – сотни миллионов рублей) и текущие расходы. Эти затраты в связи с невозможностью компенсации их за счет пользователя будут переложены на стоимость других услуг связи», – говорится в отзыве операторов. Они также указывают, что сейчас в мире нет оборудования и софта, позволяющих осуществлять семантическую фильтрацию некоторых видов трафика – https, VPN-соединений и проч.

Представители «большой тройки» не комментируют содержание своих отзывов. Однако представитель МТС Д. Солодовников подтверждает, что, по мнению оператора, предложенный ЛБИ вариант фильтрации контента малоэффективен и не сможет в полной мере оградить пользователей от сомнительной информации. Операторы занимаются передачей информации, нелогично передавать им функции фильтрации контента, рассуждает Д. Солодовников. Правильнее, чтобы этим занимались родители ребенка,

заключает он. Представитель «Мегафона» говорит, что «инициатива подлежит внимательному изучению с точки зрения соблюдения конституционных прав граждан». Представитель «Вымпелкома» отказался от комментариев.

Д. Давыдов говорит, что пока не ознакомился с позицией операторов, но на совещании, которое организовывала лига по этому вопросу, «все высказывались положительно», уверяет он. Заместитель директора Российской ассоциации электронных коммуникаций С. Гребенников сказал, что любое ограничение доступа в Интернет всегда воспринимается негативно, в том числе внедрение белых списков, несмотря на псевдозаботу о подрастающем поколении. Внедрение подобным образом белых списков больше напоминает интерес одних групп в ущерб интересу других, заключает он ***(Российских операторов обяжут фильтровать интернет-контент // Media бізнес (http://www.mediabusiness.com.ua/content/view/40888/126/lang,ru/). – 2014. – 7.10).***

***

Пользователи китайского сервиса микроблогов Weibo обходят цензуру и поддерживают протестующих в Гонконге с помощью сатиры, пишет The South China Morning Post. Как напоминает издание, с начала акций Occupy Central вся неофициальная информация об этом движении подвергается цензуре со стороны правительства в Пекине.

Однако некоторым удается обойти эти ограничения, причем используются для этого юмор и ирония, говорится в статье. Например, один из блогеров поинтересовался, что если почти 1,4 млрд жителей материкового Китая процветают благодаря «лучшему в мире обществу», то почему этим процветанием не делятся с 7 млн жителей Гонконга и 23 млн жителей Тайваня, а позволяют им «страдать от капиталистического мира».

Издание также обращает внимание, что в этом году цензура в Weibo установила новый рекорд. По данным представителей Университета Гонконга, количество постов, получить доступ к которым стало невозможно, выросло с начала протестов Occupy Central в пять раз. Встроенный в сервис поисковик по-прежнему не позволял искать по ключевым словам Occupy Central или Student Movement, добавляет издание ***(Пользователи Weibo обходят цензуру и поддерживают Гонконг с помощью сатиры // InternetUA (http://internetua.com/polzovateli-Weibo-obhodyat-cenzuru-i-podderjivauat-gonkong-s-pomosxua-satiri). – 2014. – 7.10).***

***

Как прослушивают Skype

Часто приходиться слышать мнение, что Skype – это такая сверхнадежная программа, трафик которой не могу перехватить и прослушать даже спецслужбы. По мне нию Р. Идова, аналитика компании

SearchInform, последние сыграли заметную роль в распространении этого мифа, который им только на руку. Эксперт попытался разобраться, можно или нет прослушать Skype.

«Для начала хочу сделать небольшое замечание, касающееся любых вопросов о “невзалываемых”, “непрослушиваемых” и т. п. системах. Дело в том, что таких систем в природе не бывает по одной простой причине: то, что придумал один человек, в состоянии “разобрать по кирпичикам” и проанализировать и другой, а раз так, то взлом – только вопрос времени. Учитывая тот факт, что подобный анализ хорошо “параллелится” во времени, вопрос скорости взлома той или иной защиты – это вопрос количества и компетентности специалистов, которые им занимаются. А это, в свою очередь, сводится к стоимости труда этих специалистов. Из этого следует очень простой вывод: задача абсолютно любых систем безопасности – не сделать взлом невозможным, а максимально увеличить его стоимость таким образом, чтобы само обеспечение безопасности из-за своей дороговизны не стало бессмысленным.

Все это следует в обязательном порядке иметь в виду, говоря и о защищенности от прослушивания разговоров по Skype. То есть, в любом случае, если ваш разговор очень интересен, к примеру, госдепартаменту США, то у вас немного шансов на то, что удастся сохранить его в секрете. Впрочем, для большинства людей, не являющихся международными террористами, “защищенность” Skype – это, прежде всего, защищенность от любопытных глаз:

Ближайшего окружения (коллеги, родственники, начальство);

Конкурентов и недоброжелателей;

Коварных хакеров, жертвой которых в сети, как известно, может стать каждый.

Именно с этой точки зрения мы с вами и посмотрим на Skype.

Действительно, прослушать Skype путем анализа трафика не слишком просто. Это так по двум причинам: протокол Skype имеет распределенную структуру (как, например, тот же BitTorrent), также трафик пересылается в зашифрованном виде. Конечно, после того, как самый популярный в мире VoIP-мессенджер купила корпорация Microsoft, были внедрены многие функции, более тесно привязывающие приложение к центральным серверам, и поэтому сегодня уже говорить о том, что Skype – это в чистом виде распределенный протокол, не приходится. Это теоретически упрощает анализ трафика, но на практике это не очень сильно помогает именно прослушивать Skype, в отличие от его блокирования на уровне офиса.

Зашифрован Skype-трафик вполне надежно, причем это касается как голосового трафика, так и текста, а также пересылаемых по Skype файлов. Также достаточно надежно шифруется информация, нужная для аутентификации пользователя, поэтому того, что ваш Skype-аккаунт “уведут”, можно, в принципе, не бояться. На самом деле, даже спецслужбы обычно не слишком утруждают себя анализом Skype-трафика, просто

обращаясь за нужной информацией в Microsoft. Для Китая корпорация, например, вообще выпустила специальную версию, которая не просто собирает информацию о потенциально опасных для властей КНР сообщений, но и осуществляет их цензуру.

С недавних пор, правда, Skype стал разрешать одновременно заходить из-под одного аккаунта с различных устройств, поэтому опасность стали представлять потерянные и украденные смартфоны, планшеты и ноутбуки. Но учитывая тот факт, что на подобных устройствах куда больше интересной для злоумышленников информации (например, пароли от электронных кошельков), можно считать, что в плане прослушивания Skype потеря или кража портативного устройства заметной опасности не представляет.

Впрочем, зашифрованность трафика Skype еще не значит, что его перехват совершенно бесполезен. Все дело в том, что осуществить перехват можно еще до того момента, как данные станут зашифрованными – для этого нужно перехватывать их не в сети, а на самом компьютере пользователя. Сделать это не так уж и трудно: звуковые данные можно перехватывать непосредственно с микрофона, текст – с клавиатуры, а файлы, зная их названия, и вовсе получить легче легкого. Поэтому безопасность Skype заканчивается там же, где она начинается – на компьютере пользователя этой программы.

Чтобы заниматься прослушиванием Skype, не нужно даже каких-то очень специфических решений. Даже в стандартной для Windows программе звукозаписи есть возможность выбрать в качестве входного канала Stereo Mixer, куда поступают все звуки с микрофона. А перехватить нажатия на клавиатуре может какой-нибудь простой клавиатурный шпион, который в два счета находится в Google или Яндексе. Всего два приложения, и у вас – готовая система слежения за Skype-переговорами своих домашних. Конечно, для компьютера кого-нибудь другого потребуются более продвинутые решения, и уже сегодня их, возможно, применяют ваши работодатели – они кровно заинтересованы в том, чтобы сотрудники не тратили оплачиваемое им время на пустые разговоры, не пересылали по Skype корпоративные секреты и не занимались другими непотребствами. Подобные решения называются DLP-системами (от англиикого Data Leakage Prevention – предотвращение утечек данных), и мониторят обычно не только Skype, но и другие важные каналы передачи информации (электронную почту, социальные сети, внешние носители данных и т. д.). Конечно, сегодня на постсоветском пространстве такая система используется только в каждой пятой компании, но нет сомнения в том, что в будущем в любой организации будут максимально тщательно контролировать своих сотрудников.

Считать ли Skype безопасным средством для ведения личных и деловых переговоров в свете всего, что сказано выше? Простого ответа на этот вопрос, к сожалению, быть не может. С одной стороны, разработчики приложения сделали максимум возможного для того, чтобы на этот вопрос можно было ответить утвердительно. С другой стороны, “спасение

утопающих – дело рук самих утопаючих", и поэтому без соблюдения пользователем хотя бы элементарных правил безопасности надеяться на то, что в один прекрасный день на компьютере не появится, к примеру, тот же клавиатурный шпион, не приходится.

То есть, чтобы переговоры по Skype были действительно безопасными, нужно установить и регулярно обновлять хороший антивирус, не обсуждать никакие личные вещи с рабочего компьютера, и не устанавливать никакие "дополнения" к Skype, которые могут предлагать в Интернете – лишь в этом случае можно с уверенностью говорить о том, что перехват ваших разговоров не удастся осуществить никому, кроме спецслужб. Ну, а про них все уже было сказано выше ***(Как прослушивают Скайп // InternetUA (http://internetua.com/kak-proslushivauat-skaip). – 2014. – 8.10).***

***

У Криму почали порушувати кримінальні провадження за пости у соціальних мережах, пише ZAXID.NET (http://zaxid.net/news/showNews.do?krimchanina_suditimut_za_publikatsiyu_ekstremistskogo_tekstu_v_sotsmerezhi&objectId=1325572).

Першим підозрюваним став 30-річний ялтинець, який опублікував пост «екстремістського змісту», повідомляє прес-служба Слідчого комітету РФ по Криму.

«Жителю Ялти інкримінують ч.1 ст.282 КК РФ (збудження ненависті, ворожнечі або приниження людської гідності)», – ідеться у повідомленні.

За даними відомства, 5 серпня підозрюваний розмістив на своїй сторінці у соціальній мережі «інформацію екстремістського характеру».

Що саме він розмістив і у якій соцмережі – не повідомляється ***(Кримчанина судитимуть за публікацію «екстремістського» тексту в соцмережі // ZAXID.NET (http://zaxid.net/news/showNews.do?krimchanina_suditimut_za_publikatsiyu_ekstremistskogo_tekstu_v_sotsmerezhi&objectId=1325572). – 2014. – 9.10).***

***

Багато хто вважає, що захиститися від шпигування та збору персональної інформації у соцмережах можна, якщо ними не користуватися. Однак учені з Університету Цюриха довели, що не обов'язково мати акаунт інтернет-сервісу, аби він збирав інформацію. Соцмережі знають багато персональних даних навіть з високою точністю про тих, хто там не зареєстрований.

Доступу до баз даних таких сайтів, як Facebook або Twitter, учені не мають, тому проводили свої дослідження на одній з перших у світі соцмереж Friendster, яку заснували у 2002 р. Виявилося, що в її архівах містяться відомості про людей, які нею не користувалися. Соцмережа знала їхній вік, подружній стан, роботу, політичні вподобання та іншу персональну інформацію.

Учені пояснюють своє відкриття ефективністю роботи алгоритмів веб-сайтів. Вони, наприклад, з точністю до 60 % можуть передбачити сексуальну орієнтацію людини на основі великих масивів даних. Адже в них містяться так звані «тіньові профілі» – так дослідники називають побічну інформацію, яку розкривають користувачі соцмереж у своїх постах та записах. У них вони можуть обговорювати уподобання друзів та колег, які самі не користуються цим сервісом.

Проблема тіньових профілів вже добре відома, і представники Facebook кажуть, що вони не ведуть їх. Це в 2011 р. підтвердив аудит ірландської комісії захисту даних. Однак соцмережа не приховує, що вона зберігає інформацію про тих, хто нею не користується, тоді, коли власники акаунтів Facebook імпортують свій список контактів. Завдяки цьому, якщо два користувача Facebook мають у контактах людину з поштою bob@mail.com, тоді вона може зібрати про нього іншу інформацію – телефонні номери тощо ***(Соцмережі шпигують за всіма // InternetUA (http://internetua.com/socmerej--shpiguuat-za-vs-ma). – 2014. – 9.10).***

***

В аналітичній статті для CNN «Китай покладається на старі хитрощі для контролю над висвітленням протестів у Гонкогу» китайський медіаексперт Д. Янг аналізує буремні події, що більше тижня домінували у світових ЗМІ.

«Демократичні демонстрації у Гонконгу минулого тижня були на перших шпальтах міжнародних медіа. Вони зображували події як боротьбу між місцевими жителями та потужним, хоч і далеким, авторитарним пекінським господарем у дусі боротьби Давида з Голіафом, – пише професор журналістики Фуданського університету Д. Янг. – Однак подібні заголовки не з'явилися у континентальному Китаї, де більшість газет і телеканалів поховала цю тему».

За словами автора, події у Гонконгу висвітлювалися в основному через реакцію на них у Пекіні, майже без пояснень, що відбулося насправді. Внаслідок цього публікувалися еклектичні матеріали з осудом протестів і деклараціями у редакційних статтях про те, що «керівник Гонконгу (очільник виконавчої влади – MS) Л. Чунґ-Інґа, ніколи не піде у відставку і що такі протести ніколи не поширяться на Китай».

Д. Янг привертає увагу до майже повної відсутності у контрольованих Пекіном медіа фотографій. З погляду ЗМІ яскраві динамічні світлини протестувальників, поліцейських, політиків та самого конфлікту – це «мрія журналістів, що збулася», знахідка для телебачення і як ілюстрація – для друкованих видань. Проте жоден з цих знімків не потрапив до офіційних медіа Китаю, пише він і наголошує: «Це майже напевно відбувалося за прямою вказівкою чиновників з питань пропаганди, стурбованих тим, щоб такі фото не надихнули інших китайців на схожі дії».

Суворі заборони на «запальні» знімки, відзначає Д. Янг, спостерігалися в «одержиму порядком» Пекіні навіть під час прокитайських протестів. Одна із таких заборон була серед головних складових висвітлення гострої територіальної суперечки з Японією, що відбувалася два роки тому. Згадки про масові протести дивним чином були відсутні у всіх китайських повідомленнях для внутрішнього вжитку.

Медіа КНР вдавалися у висвітленні гонконгзького конфлікту і до іншого старого трюку. Ідеться про редакційні статті, які пропонують історичний екскурс із обмеженим контекстом. У даному випадку тон задавала газета КПК «Женьмінь жибао», опублікувавши серію редакційних статей. Їхня ідея та ж сама: протести у Гонконгу незаконні, такі акції ніколи не поширяться на Китай.

Відколи було проголошено КНР, редакційні повчання стали популярним засобом висвітлення офіційних поглядів на гострі теми. Вони широко використовувалися, зокрема, 2010 р., коли у Google виникла гучна суперечка з пекінською владою. Тоді Китай висунув умовою для співпраці цензурування пошуковика. Конфлікт у кінцевому підсумку закінчився тим, що Google змушений був залишити китайський пошуковий ринок, поступившись місцевим конкурентам.

Щоб контролювати тональність повідомлень, Пекін скористався старою випробуваною тактикою використання ключових слів. Цього разу ними стали «незаконно» (коли йшлося про характеристику гонконгзьких демонстрацій) та «згідно із законом» (стосовно дій під час конфлікту в адміністрації Леуна).

Зрештою, відзначає медіаексперт, існує чинник соціальних мереж, що визначає нову гру не тільки для китайського уряду, а й для влади у всьому світі. Можновладці намагаються використовувати цю потужну силу, щоб упливати на громадську думку.

У популярній в Китаї соцмережі WeChat активно використовувалася критика гонконзьких протестувальників. Причому засуджувалося все: від загрози процвітанню території до ворожості щодо материкового Китаю.

Розповіді маловідомих дописувачів, можливо, справжні, висловлює свої міркування автор статті. Але це радше варіація іншої тактики Пекіна – контролю громадської думки в добу Інтернету.

Відомі під зневажливим прізвиськом «напівпартійці» отримують державну платню за те, що удають із себе незалежних коментаторів і засівають Інтернет думками, прихильними до центрального уряду і його поглядів. Водночас останні акції протесту у Гонконгу можуть стати новим викликом керівництву у Пекіні нового покоління активістів, які прагнуть демократії на периферії Китаю, резюмує медіаекперт.

Д. Янг є автором книги «Партійна лінія: як медіа диктують громадську думку у сучасному Китаї», що вийшла друком у всесвітньо відомому видавництві наукової літератури John Wiley&Sons ***(Пекін замовчує «революцію парасольок» у Гонконгу – Дат Янг у статті для CNN //***

«Медіаграмотність» (http://osvita.mediasapiens.ua/material/35267). – 2014. – 8.10).

***

«Міністерство державної безпеки» «ДНР» 9 жовтня оголосило, що «будь-яка діяльність з розповсюдження провокаційної інформації без її повторної перевірки в офіційних джерелах ДНР розцінюється, як дії на користь ворога, що визначатиме відповідну реакцію». Що означає «провокаційна інформація» можна лише здогадуватися, пише radiosvoboda.org

Нещодавно угруповання, яке в Україні визнали терористичним, вже виступило з вимогою заблокувати кілька десятків інтернет-ресурсів. Що про це думають незалежні журналісти на Донбасі та чи заважає звуження інформаційного простору пересічним жителям міста?

У вересні «міністерство інформації та зв'язку» «ДНР» оприлюднило постанову, яка вимагає заблокувати діяльність низки інтернет-ресурсів на території так званої «Донецької народної республіки». Це рішення ухвалили начебто для припинення розпалювання міжнаціональної ворожнечі, а також боротьби з розповсюдженням неправдивої інформації та наклепу. Під заборону потрапили лише ті інтернет-видання, які не ретранслюють позицію російських ЗМІ, та не підтримують сепаратистські течії на Донбасі. Втім, це рішення не викликало бурхливої реакції у місцевої журналістської спільноти – тотальна заборона проукраїнських засобів масової інформації у Донецьку вже стала нормою за останні півроку.

Загальна кількість заборонених ресурсів у «розстрільному» списку – 27. Деякі з них – це видання, які освітлюють ситуацію в цілому в регіоні, але є й такі, що спеціалізуються виключно на конкретних містах, таких як Слов'янськ, Краматорськ, Костянтинівка тощо. Якщо подивитися на ситуацію з боку прихильників «ДНР», то рішення це досить логічне. Зараз начальники Донбасу намагаються перепідпорядкувати усі системи регіону під свої стандарти та потреби. Так було ще навесні з адмінбудівлями, які є осередком усіх нормативних документів, так було і з вищими навчальними закладами та приватними підприємствами, яких тепер будуть ліцензувати саме комітети «ДНР». Питання Інтернету було лише питанням часу.

«Те, що людям відрізають доступ до інформації, я не вважаю правильним. У нас відрізали доступ до українських каналів, а людина має право знати. І знати різні точки зору і сама робити висновки. Якщо вже дійсно все настільки погано в "ДНР", що вони користуються тими методами, проти яких свого часу так активно виступали, це скажемо так... їхній вибір. З рештою місцеві ресурси, які потрапляють в бан – я не вважаю це вірним, бо ті люди, які покинули Слов'янськ і зараз знаходяться у Донецьку, вони повинні знати, що відбувається у них в місті – що з їхніми будинками, що з їхніми родичами, друзями, підприємствами тощо. Звідки людям брати цю

інформацію?» – запитує журналіст «Ділового Слов'янська» П. Палагута, ресурс якого був заборонений.

«Для них є тільки два види гарних журналістів – російські та мертві»

Проте ситуація з мас-медіа ще складніша. Немає таємниці, що одними з найперших об'єктів, до яких завітали озброєнні адепти «Русской весни» стали телецентр та телерадіовежа у Донецьку. Це важливе рішення, якщо враховувати той факт, що переважна більшість громадян міста отримують інформацію саме з телевізора. Тому заборонили національні українські телеканали, які потім замінили російськими, а замість регіональних запустили кілька «республіканських» – «ОплотТВ», «НоворосіяТВ» та «Перший республіканський». Паралельно з цим відбувався процес залякування журналістів – деяких побили, інші побували у полоні.

«Із Донбасу навмисно і дуже жорстко витісняються усі українські ЗМІ. Блокування сайтів на рівні провайдерів стало вже одним з останніх етапів боротьби бойовиків із українськими журналістами. Спочатку донецьких і луганських колег залякували фізичною розправою, підвалами і викраденнями – до журналістів в цій війні "ДНР" відноситься як до бійців-супротивника. Але ми не солдати. Ми видобуваємо і поширюємо інформацію, і жоден об'єктивний донецький журналіст сьогодні не може захистити своє життя і видання, якщо бойовики захочуть його знищити. Тому ЗМІ в Донбасі працюють з підпілля. Звісно, що звертатися у "ДНР" з проханням вирішити цю проблему було б смішно. Для них є тільки два види гарних журналістів – російські та мертві», – розповідає головний редактор одного з заборонених інтернет-видань регіонального рівня. На жаль, ні ім'я журналіста, а ні назву видання з міркувань безпеки назвати неможна – зараз кореспонденти цього ресурсу працюють саме в Донецьку.

Утім, з часом виявилось, що силові методи або зовсім не працюють, або малоефективні. По-перше, працівники інтернет-ЗМІ, які залишились у Донецьку, продовжили свою діяльність, так само звітуючи про події. Наприклад, висвітлювали «парад» військовополонених 24 серпня, який пройшов у центрі Донецька і щорічне свято ковальської справи, яке також не обійшлось без озброєних людей. Захищають себе працівники мас-медіа по різному – хтось ховає посвідчення журналіста і спостерігає за подіями з позиції рядового мешканця, інші залучаються підтримкою впливових міжнародних ЗМІ, які можуть домовитись із керівниками «республіки», треті ж, ризикуючи свободою, отримують акредитацію «ДНР». Працівники «Міністерства інформації та зв'язку», а також їхні колеги з «республіканських правоохоронних органів» банально не можуть впливати на тих журналістів, які знаходяться на контрольованій українськими військами територіях. Тому і з'явилось рішення заблокувати на рівні маршрутизації неугодні ЗМІ.

«Не думаю, що блокування українських інтернет-ресурсів зменшить кількість людей, що підтримують Україну, на території підконтрольної терористам. Вони просто не вірять тій маячні, яку несуть представники, так

званих “ЛНР” і “ДНР”. Єдине, що погано – ці люди не зможуть дізнатися потрібної їм інформації про нові підписані закони, або як отримувати соцвиплати... Моє ставлення до цього негативне, адже вони (“ДНР” і “ЛНР”) позиціонують себе, як демократичне суспільство. А яка демократія, коли будь-яка інше думка викорінюється?» – ділиться враженнями журналіст забороненого ресурсу «Новини Донбасу» В. Февральска.

Як обходити заборону

Більш-менш освічені користувачі мережі розуміють, що навіть така заборона не є особливо життєздатною. Для подолання обмеження є сотні різних засобів, починаючи з «цибулевої маршрутизації» Tor і закінчуючи низкою розширень до традиційних браузерів. Якщо хтось воліє займатися своєї безпекою власноруч – теж добре, до його послуг цілий спектр можливостей проксі-серверів. Для тих же, хто не звик користуватись традиційними методами, чи полюбляють відрізнятись від решти, є дуже хитра і дивна можливість переглянути заборонений сайт за допомогою сервісу Google Translate. І навіть для найбільш ледачих існує мобільний Інтернет, який не в змозі заборонити навіть «ДНР». Питання в іншому – чи потрібна мешканцям Донецька, які опинилися сам на сам з російськими та «республіканськими» новинами, інша думка? Чи заборона декількох «укропських», як їх називають у Донецьку, ресурсів стане достатнім мотивом для дій, які мешканці міста не вживали навіть у мирні часи?

«З приводу заборони деяких сайтів... я вважаю, що це неправильно. Зрештою, ми живемо у цивілізованому світі, і я думаю, що вихід до інформації повинен бути в кожного. Вживати щось з цієї нагоди я поки нічого не збираюся, мені ці сайти не дуже важливі, але все ж вважаю, що це погано», – розповідає донеччанин Артур.

Чи всі розберуться в проксі-серверах?

Очевидно, це не приватна думка – багато хто з мешканців розуміє, що такі рішення не є нормальною практикою, і що насправді «ДНР» зазіхає на їхнє право отримувати ту інформацію, яку вони забажають. Але щось робити збираються лише одиниці. Наприклад, жителька Донецька Марина обурена рішенням заборонити деякі ресурси, але не впевнена, що зможе щось зробити: «Проксі-сервери... Якщо я зможу це якось знайти, то так, я буду намагатися це робити, тому що та інформація, яку вони (“ДНР” – ред.) пропонують і вважають, що мені потрібна, це все одно що промивка мізків».

Зрештою, реакція донецької журналістської спільноти на конкретне обмеження «ДНР» була досить в’ялою – ресурси дали новину, хтось розповів що робити в цій ситуації і на цьому історія нібито закінчилась. Але за конкретною дією насправді ховається ціла тенденція. Спочатку телебачення і радіо, потім інтернет-ЗМІ, наступними, як дехто побоюється, можуть бути соціальні мережі та Інтернет взагалі ***(Як в «ДНР» зачищають інформаційний простір // Медіа бізнес (http://www.mediabusiness.com.ua/content/view/40937/126/lang,ru/). – 2014. – 10.10).***

***

Представители IT-компаний призывают правительство США уменьшить масштабы online-наблюдения.

На встрече за круглым столом, которая прошла в Кремниевой долине в среду, 8 октября, исполнительный директор корпорации Google Э. Шмидт заявил, что online-слежка, которую ведет правительство США, может привести к разрушению экосистемы Интернета, сообщает информагентство France-Presse.

Его мнение поддержали и другие участники дискуссии, в том числе представители Facebook, Microsoft и Dropbox.

В ходе встречи обсуждались вопросы, связанные с экономическими и регулятивными последствиями, вызванными скандалом вокруг online-слежения, которое проводило правительство США. Такие действия властных структур привели к тому, что значительное количество пользователей утратило доверие к компетентности и желанию интернет-компаний сохранять конфиденциальность общения в сети.

Специалисты отмечают, что ограничения свободного перемещения данных в Интернете, которые устанавливают некоторые правительства, может привести к нарушению экосистемы Интернета, который является движущей силой для экономик многих государств, а также предоставляет возможность сотрудничества между собой для людей по всему миру.

Кроме того, IT-компании обеспокоены законодательным требованием некоторых правительств о переносе дата-центров на территории соответствующих государств. По их мнению, такие законы приведут только к потере эффективности работы online.

«Идея о региональном размещении дата-центров идет вразрез с архитектурой Интернета», – подчеркнул генеральный советник Facebook К. Стретч.

Представители IT-компаний призвали правительство США уменьшить масштабы online-наблюдения. А пока этого не произошло, владельцы интернет-ресурсов продолжат усиливать безопасность своих сетей и сервисов ***(Online-слежка может привести к разрушению экосистемы Интернета // InternetUA (http://internetua.com/Online-slejka-mojet-privesti-k-razrusheniua-ekosistemi-interneta). – 2014. – 10.10).***

***

Кабинет Министров предлагает Верховной Раде обязать операторов связи устанавливать на своих сетях оборудование, необходимое для проведения спецслужбами разведочной и контрразведочной деятельности, сообщают «Українські новини».

Об этом говорится в законопроекте Кабинета Министров № 5148 от 9 октября.

Кабмин предлагает Раде внести изменения в ст. 39 закона «О телекоммуникациях» и обязать операторов и провайдеров телекоммуникаций за свой счет устанавливать на своих сетях оборудование, необходимое для осуществления уполномоченными органами контрразведывательных и разведывательных действий, а также для проведения негласных следственных действий.

Операторы должны будут обеспечивать функционирование такого оборудования и в пределах своих возможностей и полномочий способствовать проведению этих действий и не допускать разглашение организационных и тактических приемов их проведения.

Действующая редакция закона обязывает операторов устанавливать оборудование и способствовать только проведению оперативно-розыскных действий правоохранительными органами.

Также Кабмин предлагает в законе «О разведывательных органах Украины» регламентировать определение термина «технические средства разведки» ***(Кабмин предлагает Раде обязать операторов «шпионить» за пользователями // ProIT (http://proit.com.ua/news/gosregulation/2014/10/10/132121.html). – 2014. – 10.10).***

***

Как сайты шпионят за нами?

Как правило, каждый раз, когда вы посещаете веб-сайт, небольшой текстовый файл остается в папке на вашем компьютере. Эти данные называются cookies. Они регистрируют какие сайты вы посещали и когда.

Cookies были разработаны для запоминания паролей и предпочтений, таких как язык, часовой пояс и т. д. С ними использование веб-сайтов стало быстрее, проще и приятнее.

Cookies также позволяют компаниям построить картину того, кто вы и что вы хотите сделать, создавая подробную историю посещенных страниц. Информация высоко ценится рекламодателями, которые используют ее для целевых клиентов. Например, говорят, что вы ищете конкретный набор серег или запонок на Google. Через несколько минут на другом веб-сайте вы можете обнаружить объявления этого продукта или подобные ему.

Как выключить все cookies?

Вы можете полностью отключить cookies через опции интернет-браузера (Internet Explorer, Firefox, Google Chrome и т.д.). Вы также можете удалить cookies, которые уже сохранились на вашем компьютере. Помните, что это затруднит использование некоторых сайтов – вы потеряете данные для входа.

Что еще нужно знать?

Новые технологии стремительно развиваются. Например, появления устройства для «считывания отпечатков пальцев». Ваш браузер попросит нарисовать маленькое изображение на экране, когда вы посещаете веб-сайт,

без вашего ведома. Изображение превратится в число и указывает, какие сайты вы посещали и когда. Режимы «инкогнито» в браузерах не будут этому помехой.

Что насчет других сайтов?

Facebook, в частности, собирает огромное количество информации о своих пользователях. Даже если вы не указали вашу дату рождения, пол, семейное положение и личный адрес, Facebook делает догадки, основанные на том, что вы размещаете, кто ваши друзья, и т. д. Нажмите на размещенную рекламу и выберите «Почему я вижу ее», чтобы увидеть, что сайт думает о вас.

Алгоритмы Google также читают вашу электронную почту, чтобы «нацелить» рекламу. Скажем, вы получаете письмо от друзей, что они планируют посетить Францию. И вы можете начать видеть рекламные объявления для скидок на паромы или полеты при проверке почты ***(Как сайты шпионят за нами? // InternetUA (http://internetua.com/kak-saiti-shpionyat-za-nami). – 2014. – 13.10).***

***

Генеральна прокуратура РФ заблокувала дев'ять блогів LiveJornal, у яких містилися передруки тексту із закликами притягнути до кримінальної відповідальності депутата Ставропольської місцевої думи від партії «Єдина Росія» А. Ширінова.

Про це повідомляє TJournal із посиланням на веб-портал antizapret.info, що займається моніторингом реєстру заборонених сайтів Роскомнагляду.

Було закрито доступ відразу до декількох LiveJornal, що розмістили у себе публікації про ставропольського депутата. Обмеження тривали впродовж тижня, з 5 по 12 жовтня.

Першопочатково резонанс викликав матеріал із заголовком «Айдын, пора назад в тюрьму! О том, как депутат-едросс возглавил ОПГ в Мин. Водах». Його розмістила у LiveJornal користувачка з ім'ям О. Вьольва.

У тексті було описано події, що трапилися після масової бійки в одній із лікарень міста Мінеральні води наприкінці вересня. В результаті конфлікту був убитий 31-річний чоловік на ім'я Анатолій Ларіонов. ЗМІ повідомляли, що причиною бійки був побутовий конфлікт, що розпочався у кафе і продовжився у лікувальному закладі.

Цей інцидент набув великого розголосу у місті, там відбулася низка масових акцій з вимогою затримати винних у трагедії. Водночас Інтернетом почала ширитися інформація про те, що до трагічної події певним чином причетний депутат А. Ширінов. Його звинувачували у «прикриванні» місцевих злочинних угруповань та у «замітанні слідів».

Авторка резонансного запису LiveJornal написала, що А. Ширінов є другом директора приватної охоронної фірми, чиї співробітники і організували вбивство А. Ларіонова в лікарні. Закінчувалася публікація вимогою зняти А. Ширінова із займаних посад та закликом засудити його.

TJournal пише, що звернувся із запитом стосовно масового блокування блогів до Генпрокуратури РФ, однак у відомстві на нього не відповіли ***(Генпрокуратура РФ заблокувала 9 блогів із закликами засудити місцевого депутата // «Медіаграмотність» (http://osvita.mediasapiens.ua/material/35400). – 2014. – 13.10).***

***

Інтернет-користувачів усе частіше турбує питання кібербезпеки та приватності. Особливо сильно люди побоюються стеження через веб-камеру пристрою, свідчать результати дослідження Kaspersky Lab і B2B International.

Питання стеження через веб-камеру турбує 52 % опитаних користувачів. За даними дослідження, більше однієї четвертої користувачів заліплюють чи завішують об'єктив веб-камери на своєму комп'ютері. 5 % заклеюють камери також на на мобільних пристроях.

Водночас дослідження засвідчило, що майже третина користувачів (34 %) досі не знає, що існує така загроза.

Експерти пояснюють, що тривога людей небезпідставна. Зловмисники зламують веб камери з різною метою. Таким чином, наприклад, можна отримати приватні фото для шантажу чи розваги. Крім цього, злам камери дає можливість дістати таємну службову інформацію, викрасти облікові дані до фінансових сервісів та інше.

При цьому опитування показало, що велика частина інтернет-користувачів є безтурботною. Кожен десятий респондент сказав, що записує паролі до онлайн-сервісів на папері або стікерах та зберігає їх поряд із комп'ютером. Сучасні якісні веб-камери дають можливість прочитати подібні записи ***(Кожен четвертий інтернет-користувач заклеює об'єктив веб-камери на пк, побоюючись стеження // MediaSapiens (http://osvita.mediasapiens.ua/material/35421). – 2014. – 13.10).***

***

Рада національної безпеки та оборони могла б стати координуючим органом з моніторингу та протидії порушенням в інформаційній сфері, пише ukrinform.ua.

Про це на засіданні «круглого столу» в Укрінформі «Проблеми державно-громадської протидії антиукраїнській інформаційній війні: де закінчується забезпечення національної безпеки і починається цензура» заявив заступник керівника інформаційно-аналітичного центру РНБО В. Полєвий, повідомляє кореспондент агентства.

«Українське законодавство передбачає обмеження щодо закликів до повалення конституційного ладу, захоплення влади, пропаганди насильства та жорстокості. Насправді в цьому плані немає проблем – ми маємо правову базу для того, щоб певним чином реагувати на порушення в інформаційній сфері. Інша справа, який громадський чи державний орган повинен

здійснювати, наприклад, моніторинг цих порушень, які саме механізми для того, щоб протидіяти цим протиправним діянням», – сказав В. Полєвий.

Він нагадав, що одним з органів, які виконують цю функцію, є Національна експертна комісія України з питань захисту суспільної моралі.

«Вважаємо, що у всій цій діяльності є місце і Раді національної безпеки як координуючого органу у сфері безпеки», – заявив В. Полєвий ***(РНБО хоче координувати боротьбу з пропагандою // Медіа бізнес (http://www.mediabusiness.com.ua/content/view/40964/126/lang,ru/). – 2014. – 14.10).***

***

Более половины россиян одобряют введение цензуры в Интернете. Об этом свидетельствуют данные опроса, проведенного «Левада-центром», пишет lenta.ru.

Около 54 % опрошенных заявили, что в Интернете «существует множество опасных сайтов и материалов», поэтому цензура необходима. В сентябре 2012 г. такой точки зрения придерживались 63 % респондентов. Считают, что «опасность Интернета переоценивается» и нельзя вводить цензуру 31 % опрошенных. Два года назад в этом были уверены только 19 % россиян. Затруднились ответить на вопрос социологов 16 % россиян.

За введение цензуры в сети чаще выступают женщины (56 % против 50 % среди мужчин) и граждане в возрасте 18–24 лет и 40–54 лет (по 56 %).

При этом 37 % россиян отрицательно отнеслись бы к принятию Госдумой законов, ограничивающих доступ россиян в мировой Интернет. Нейтрально восприняли бы подобную новость 38 % респондентов, 15 % поддержали бы это решение.

Опрос был проведен 26–29 сентября среди 1630 человек старше 18 лет в 46 регионах страны. Статистическая погрешность не превышает 3,4 % ***(Более половины россиян согласились на цензуру в интернете // Медіа бізнес (http://www.mediabusiness.com.ua/content/view/40971/126/lang,ru/). – 2014. – 14.10).***

***

Президент Росії В. Путін підписав закон про обмеження частки іноземних акціонерів у статутному капіталі російських ЗМІ на рівні 20 % і заборону іноземцям виступати засновниками засобів масової інформації в Росії

Відповідний документ опублікований 15 жовтня на офіційному порталі правової інформації. Закон був схвалений Радою Федерації 1 жовтня, пише ТАСС.

З ініціативою внести поправки в російський закон «Про ЗМІ» виступили депутати Держдуми В. Дєньгін (ЛДПР), В. Парахін («Справедлива Росія») і Д. Вороненко (КПРФ). Чинне на той момент законодавство не

обмежувало участь іноземних осіб в друкованих та мережевих виданнях, планка в 50 % була встановлена тільки на частку в телебаченні і радіо.

Норми, що встановлюються документом, будуть введені з 1 січня 2016 р. Власникам ЗМІ дається час до 1 лютого 2017 р. на приведення всієї корпоративної ланцюжка у відповідність із законом, а нові документи про власників і засновників повинні бути передані в Роскомнадзор не пізніше 15 лютого 2017 р. У разі порушення, відомство зобов'язане звернутися до суду для призупинення діяльності ЗМІ.

В тексті закону особливо наголошується, що обмеження на іноземну участь в ЗМІ вводяться, «якщо інше не передбачено міжнародним договором Російської Федерації». Як приклад таких ЗМІ називалися міждержавна телерадіокомпанія «Мир» і телерадіокомпанія Союзної держави Росії і Білорусії ***(Путін підписав закон, через який в Росії залишаться тільки пропагандистські ЗМІ // Espreso.tv (http://espreso.tv/news/2014/10/15/putin_pidpysav_zakon__cherez_yakyy_v_rosiyi_zalyshatsya_tilky_propahandystski_zmi). – 2014. – 15.10).***

***

Американські програмісти розкрили мережу російських хакерів, що роками стежили за чиновниками НАТО, ЄС і України. Їх жертвами, особливо в розпал української кризи, ставали політики, вчені та енергетичні компанії

Російські хакери використовували «дірки» в операційній системі Windows, щоб стежити за іноземними лідерами та організаціями протягом останніх п'яти років. За даними, оприлюдненими компанією з Далласа ISight Partners, об'єктами шпигунства з боку хакерської компанії стали НАТО, українські урядові організації, служби Європейського союзу, енергетичні компанії (особливо польські), компанії телекому та американські наукові організації, повідомляє Gazeta.ru.

За словами фахівців, виявлені «діри» присутні роками в операційних системах, починаючи з Windows Vista.

Цілями хакерського угруповання, якому дали назву піщаного черв'яка (Sandworm), стали як мінімум один американський учений, що спеціалізується на українських питаннях, а також учасники міжнародної конференції з питань зовнішньої безпеки GLOBSEC, яка пройшла в Братиславі за участю лідерів і глав МЗС європейських держав.

«Атака була частиною дворічної російської кампанії, що відбиває зростаючі апетити Росії в плані розвідки за США і ЄС у відповідь на їх дії на Україні і по всьому світу», – пише Bloomberg. В поле зору фахівців iSIGHT Partners російські хакери потрапили в кінці 2013 р., сліди діяльності осередку простежуються з 2009 р. Хакери використовують метод так званого спрямованого фішингу – розсилки шкідливих прикріплених файлів, переважно в форматі PowerPoint.

Варто жертві хакерів відкрити прикладений файл, як система запускає виконуваний файл, що відкриває пролом в безпеці.

Зовсім недавно ці хакери стали застосовувати в своїй роботі поширений для стеження вірус BlackEnergy, який імовірно використовувався влітку 2008 р. під час російсько-грузинського військового конфлікту при кібератаках на грузинські державні інтернет-сайти.

В минулому серпні стеження за хакерами показала, що Sandworm особливо пожвавився, використовуючи фішингові атаки проти кількох українських організацій і як мінімум однієї американської під час саміту НАТО в Уельсі. Повідомляється, що хакери використовували уразливість всіх ОС, серверних операційних систем Windows Server 2008 і 2012, крім XP.

«Ми тут же сповістили постраждалі сторони і наших клієнтів серед безлічі урядових структур і почали працювати з Microsoft з відстеження цієї кампанії і розробці "латок"», – ідеться в повідомленні iSIGHT Partners.

Але програмісти впевнені: незважаючи на те що уразливість існує майже у всіх версіях Windows і становить потенційну загрозу для мільйонів користувачів, аналіз показав, що про «дірки» відомо не багатьом, і проникнення крізь них здійснювалося переважно російським вірусом ***(Російський вірус стежив за чиновниками НАТО, ЄС і України // InternetUA (http://internetua.com/ros-iskii-v-rus-stejiv-za-csinovnikami-nato---s---ukra-ni). – 2014. – 15.10).***

***

Массовая слежка за пользователями Интернета, осуществляемая спецслужбами стран мира, подрывает право на частную жизнь, говорится в материале специального докладчика Организации Объединенных Наций по вопросу защиты прав человека в условиях борьбы с терроризмом Б. Эммерсона.

22-страничный доклад, опубликованный 15 октября, является ответом на разоблачительные материалы, обнародованные в прошлом году бывшим сотрудников АНБ США Э. Сноуденом.

Программы слежки спецслужб, как следует из составленного Б. Эммерсоном документа, «являются прямым вызовом существующим нормам международного права».

«Аргумент о том, что технологии массовой слежки могут внести вклад в предотвращение терактов и преследование их исполнителей, сам по себе не является достаточным оправданием для их использования, если учитывать сферу прав человека», – отмечается в докладе.

Б. Эммерсон отверг также аргумент и о том, что все выкладываемое в Интернете автоматически становится достоянием гласности. «Интернет не является полностью общественным пространством. Он состоит из многих слоев, как частных, так и общедоступных», – говорится в тексте.

«Государства должны пересмотреть внутреннее законодательство, регулирующее современные нормы слежения, чтобы гарантировать соответствие подобных практик международным законам в сфере прав человека», – подчеркивает Б. Эммерсон ***(ООН: Слежка за людьми в***

Интернете противоречит нормам международного права // InternetUA (http://internetua.com/oon--slejka-za-luadmi-v-internete-protivorecsit-normam-mejdunarodnogo-prava). – 2014. – 16.10).

***

Британские власти намерены ужесточить наказание за оскорбления и угрозы в Интернете. Об этом в субботу, 18 октября, сообщил министр юстиции Великобритании К. Грейлинг газете The Mail on Sunday, пишет UBR (http://ubr.ua/ukraine-and-world/world/britaniia-ujestochit-nakazanie-dlia-internet-trollei-311746).

Наказание планируется увеличить с полугода до двух лет тюремного заключения.

К. Грейлинг подчеркнул, что «интернет-тролли – это трусы, которые отравляют нашу жизнь». Он отметил также, что никто не потерпит подобного обращения при личном общении, поэтому таким проявлениям не должно быть места и в социальных сетях.

Министерство юстиции объявило о своем решение после того, как британские СМИ распространили информацию о нескольких случаях жестоких оскорблений в Интернете ***(Британия ужесточит наказание для интернет-троллей // UBR (http://ubr.ua/ukraine-and-world/world/britaniia-ujestochit-nakazanie-dlia-internet-trollei-311746). – 2014. – 19.10).***

***

Директор ФБР Д. Коми хотел бы, чтобы Apple и Google оставляли в мобильных устройствах «бэкдоры» для доступа спецслужб к данным. Внедренное в последних версиях платформ Android и iOS шифрование по умолчанию он считает излишним и мешающим правосудию.

«Правосудие может быть бессильно, если мобильный телефон или жесткий диск будет защищен», – сказал директор ведомства, публично обратившись к таким компаниям, как Apple и Google в Брукингском институте в Вашингтоне.

Д. Коми поделился, что его тревожит отсутствие прописанных в законе правил работы ИТ-компаний, согласно которым они должны были бы оставлять в своих продуктах «бэкдоры» и сообщать о них спецслужбам.

В США существует закон о «Телекоммуникационном содействии правоохранительной системе», согласно которому операторы и производители оборудования связи должны в обязательном порядке предоставлять спецслужбам возможность прослушки телефонных разговоров и перехвата данных в оборудованиях и сервисах.

С 2004 г. это обязаны делать не только операторы и телеком-компании, но и поставщики услуг VoIP, такие как Skype. Коми об этом не упомянул.

Директора ФБР беспокоит стремление крупнейших ИТ-компаний максимально защитить коммуникации своих клиентов. В прошлом месяце стало известно о том, что в iOS 8 шифрование находящихся в памяти

мобильного устройства всех пользовательских данных будет включено по умолчанию.

Аналогичный уровень защиты введен корпорацией Google в ее новой платформе Android 5.0 Lollipop.

Д. Коми говорит, что уважает руководителей Apple и Google. Это «хорошие люди», которые заботятся о пользователях на фоне скандальных открытый, сделанных Э. Сноуденом. Но эти усилия, полное шифрование данных абонентов, могут создать рай для преступников. В конце сентября 2014 г. глава ФБР заявил, что эти усилия «позволят некоторым людям быть над законом».

«Мы не требуем, чтобы производители оставляли нам лазейки, – оправдывается Д. Коми. – Мы ходим входить через парадную дверь, чисто и прозрачно, всецело следуя букве закона». Под буквой закона он подразумевает, помимо прочего, судебные постановления, поясняет CNet.

Эксперты по безопасности отреагировали на заявления Д. Коми критично. По их мнению, Д. Коми не задумывается о том, что такие послабления в итоге сами по себе сыграют на руку злоумышленникам, так как они смогут беспрепятственно входить через те же «двери».

«Ослабление защиты позволит “шпионам иностранных государств и преступникам” получать доступ к данным, как бы Д. Коми не называл лазейки – “бэкдорами” или “парадными дверями”, подчеркнул К. Сойан, старший технолог Американского союза защиты гражданских свобод. «Директор ФБР не говорит о том, какие риски несут бэкдоры, он полностью игнорирует эти риски», – считает М. Блейз, эксперт по криптографии из Пенсильванского университета ***(ФБР потребовало от Apple и Google оставлять «дыры» для доступа спецслужб к данным пользователей // InternetUA (http://internetua.com/fbr-potrebovalo-ot-Apple-i-Google-ostavlyat--diri--dlya-dostupa-specslujb-k-dannim-polzovatelei). – 2014. – 18.10).***

Проблема захисту даних. DDOS та вірусні атаки

Група невідомих хакерів оприлюднила секретні документи з Криму, ДНР та Російської Федерації, які стосуються багатьох подій, що відбуваються зараз в Україні.

“Злив” можна умовно поділити на три частини: в першій містяться документи з Криму після анексії його Росією, в другій – документи терористичної організації ДНР, а в третій – скани паспортів українців з візами в Грецію та інші країни.

Хакери також виклали скани на Lexus кримської помічниці голови ДНР Пушиліна, документи Я. Павленко з кримської Ради. В зливі також є порція документів, які не мають відношення до ситуації в Україні, наприклад еротичні фото жінки заступника міністра енергетики РФ, О. Новака

(Українські хакери виклали в інтернет секретні документи з Криму, ДНР та Росії // UkrainianWatcher (http://watcher.com.ua/2014/10/06/ukrayinski-hakery-vyklaly-v-internet-sekretni-dokumenty-z-krymu-dnr-ta-rosiyi/). – 2014. – 6.10).

***

Сайт «Украинской правды» pravda.com.ua перестал открываться в нескольких популярных браузерах. При попытке зайти на сайт через Google Chrome или Mozilla Firefox пользователь видит предупреждение о возможном заражении компьютера вредоносным ПО. Антивирусная защита браузеров считает, что на сайте издания находится вирус, который ворует личные данные пользователей. Сам «вирус» представляет из себя Javascript-файл с двумя десятками строчек кода. При загрузке страницы «зловред» в фоновом режиме подгружает программный код с сайта pmsaudio.com, который отмечен Google как подозрительны, пишет AIN.UA (http://ain.ua/2014/10/06/543663).

По словам технического директора антивирусной лаборатории Zillya! О. Сыча, скрипт открывает внешнюю ссылку для сбора статистики. Помимо этого, он заменяет рекламные блоки на сайте и это может быть проявлением недобросовестной конкуренции рекламодателей.

Обновлено: сайт заработал в нормальном режиме.

Часть браузеров блокируют сайт Украинской правды из за вирусов ***(Часть браузеров блокируют сайт «Украинской правды» из-за вирусов // AIN.UA (http://ain.ua/2014/10/06/543663). – 2014. – 6.10).***

***

Самым распространенным типом вредоносного программного обеспечения (ПО) для пользователей Android-устройств за период с августа 2013 г. по июль 2014 г. стали троянские программы, рассылающие без ведома владельца устройства SMS-сообщения на платные номера. Об этом говорится в совместном исследовании «Лаборатории Касперского» и Интерпола.

На их долю пришлось 57 % всех срабатываний защитных продуктов «Лаборатории Касперского» для Android-устройств.

На втором месте по распространенности семейство RiskTool (21,5 % инцидентов) – условно легальные программы, которые, тем не менее, могут быть использованы во вредоносных целях (отсылка SMS, передача геолокационных данных и пр). На третьем, с долей 7,4 % – приложения с навязчивой рекламой, отображаемой во всплывающих окнах и уведомлениях в строке состояния.

Всего за период с августа прошлого года по июль 2014 г. защитные продукты компании зарегистрировали более 3,4 млн срабатываний на опасное ПО для мобильных Android-устройств у более одного миллиона пользователей.

По данным компании, с октября прошлого года число атак на Android-устройства стало активно расти. Так, только за первые два квартала 2014 г. аналитики выявили 175,4 тыс. новых уникальных вредоносных программ под Android, что на 18,3 % (или на 32,2 тыс. программ) больше, чем за весь 2013 г.

Основными целями киберпреступников, зарабатывающих на вредоносном ПО для Android, являются пользователи из России, Индии, Казахстана, Вьетнама, Украины и Германии. Аналитики связывают это с распространенностью в указанных странах сервисов оплаты контента и онлайн-услуг с помощью платных SMS-сообщений – для злоумышленников это привлекательный способ монетизации вредоносных атак, поскольку он позволяет анонимно выводить деньги с предоплатных счетов абонентов сотовой связи на сторонние банковские счета ***(SMS-трояны стали самой большой угрозой для Android-пользователей // InternetUA (http://internetua.com/SMS-troyani-stali-samoi-bolshoi-ugrozoi-dlya-Android-polzovatelei). – 2014. – 7.10).***

***

Американский бизнес больше всего страдает от атак китайских хакеров. С таким заявлением выступил директор ФБР Д. Коми.

«В США есть два типа крупных компаний: это те, что уже испытал хакерские атаки китайцев и те, кто не знает о том, что стали жертвами подобных атак», – сказал Д. Коми. Директор ФБР не взялся оценить даже приблизительный ущерб от кибератак, но отметил, что он измеряется миллиардами долларов.

По оценкам американских спецслужб, наиболее частым атакам иностранных хакеров подвергаются защищенные серверы, на которых хранится экономическая и оборонная информация. При этом китайские хакеры остаются лидерами в это области ***(ФБР: Китайские хакеры приносят многомиллиардные убытки бизнесу в США // InternetUA (http://internetua.com/fbr--kitaiskie-hakeri-prinosyat-mnogomilliardnie-ubitki-biznesu-v-ssha). – 2014. – 7.10).***

***

Apple уведомила пользователей Mac об обновлении встроенного механизма защиты от трояна Mac.BackDoor.iWorm. Данный «зловред» позволяет выполнять на инфицированном «маке» широкий набор различных команд, поступивших от злоумышленников. По данным компании «Доктор Веб», свыше 17 тыс. компьютеров Mac инфицированы данным троянцем.

5 октября Apple обновила встроенный механизм защиты в OS X, который теперь успешно идентифицирует и блокирует OSX.iWorm.A и OSX.iWorm.B. Обновление устанавливается на ОС автоматически и запрещает исполнение зараженных файлов при помощи технологии Apple Xprotect. Данная функция, названная в честь файла Xprotect.plist, хранящего

сигнатуры вредоносного ПО, впервые была выпущена в августе 2009 г., одновременно с дебютом Mac OS X 10.6. Используя Xprotect, компания может автоматически блокировать опасные типы файлов.

Наибольшее количество компьютеров-зомби находится в США – там их свыше 4500. 1200 зараженных Mac обнаружено в Великобритании и Канаде. По несколько сотен узлов ботнета удалось найти в Австралии, Бразилии, Испании, Мексике, Нидерландах, и Швеции.

Исследователи отмечают необычный способ работы iWorm – за списком управляющих серверов она отправляется на популярный сайт для гиков Reddit.com. Перечень серверов публикуется в открытом виде в виде комментариев к одной из тем, созданной на форуме.

Заразив Mac, троянская программа способна выполнять различные системные команды, скачивать файлы, передавать на управляющий сервер различную информацию. Цель создания ботнета пока что остается неизвестной. Чаще всего зомби-сети используются для рассылки спама, организации DDoS-атак и других злонамеренных действий ***(Apple заблокировала троян iWorm, заразивший 17 000 компьютеров Mac // InternetUA (http://internetua.com/Apple-zablokirovala-troyan-iWorm--zarazivshii-17-000-kompuaterov-Mac). – 2014. – 6.10).***

***

В ніч на 7 жовтня на сайті Астраханської обласної державної думи невідомі особи розмістили повідомлення про вихід Астраханській області зі складу Росії. Про це повідомляє rbc.ru.

Їхнє повідомлення було опубліковане під заголовком «Звернення надзвичайного комітету». У ньому висувається вимога про вихід регіону зі складу РФ та проголошення «Нижньо-Волзької народної республіки». Написане звернення нібито від імені губернатора Астраханської області, голови обласної держдуми, а також «керівника народного ополчення» І. Стрелкова.

Як розповів ИТАР-ТАСС представник прес-служби Астраханської облдуми В. Маритиненко, сайт, скоріше за все, зламали.

Тривалий час до astroblduma.ru доступу не було. Однак станом на 9:55 робота сайту відновлена ***(На офіційному сайті Астраханської облдуми хакери повідомили про вихід зі складу Росії // «Медіаграмотність» (http://osvita.mediasapiens.ua/material/35219). – 2014. – 7.10).***

***

Количество атак с эксплуатацией ShellShock продолжает увеличиваться: эксперты утверждают, что активно эксплуатируемая уязвимость оболочки Bash, используемой в UNIX-системах, была задействована для атаки на серверы компаний Yahoo, Lycos и WinZip.

Хакерское вторжение на серверы компаний с применением ShellShock было обнаружено Д. Холлом, исследователем безопасности и президентом

консалтинговой фирмы Future South Technologies, о чем он уведомил компании 5 октября этого года. По утверждению эксперта, хакеры, находящиеся на территории Румынии, пытались использовать скомпрометированные серверы Yahoo для взлома игровых серверов компании, ежедневно посещаемых миллионами пользователей. Кроме того, скомпрометированными оказались серверы компании Lycos и платежная система компании-поставщика WinZip.

По мнению экспертов, в настоящее время существует 11 типов атак, эксплуатирующих уязвимость ShellShock. И. Ульрих, ведущий специалист института SANS, считает, что атакам предшествует сканирование серверов на наличие уязвимости. В некоторых случаях для получения информации о параметрах системы используется заголовок HTTP User-Agent. К сканированиям прибегают и хакеры, и специалисты по интернет-безопасности, однако, по мнению эксперта, авторизованный поиск уязвимостей через заголовок HTTP User-Agent не отвечает задачам обеспечения безопасности систем: создается возможность доступа к информации, необходимой для создания усовершенствованных версий вредоносного ПО ***(Сайты компаний Yahoo, Lycos и WinZip подверглись хакерским атакам // InternetUA (http://internetua.com/saiti-kompanii-Yahoo--Lycos-i-WinZip-podverglis-hakerskim-atakam). – 2014. – 7.10).***

***

«Лаборатория Касперского» обнародовала результаты расследования серии кибератак, нацеленных на банкоматы по всему миру: при помощи хитроумного вредоносного ПО злоумышленникам удалось похитить миллионы долларов США.

Бэкдор, инфицирующий банкоматы, получил обозначение Tyupkin (по классификации Касперского). Отмечается, что программа работоспособна на банкоматах, производящихся одним из крупнейших игроков рынка. На этих устройствах применяется 32-битная операционная система Windows.

Схема работы злоумышленников делится на две этапа. Сначала они получают физический доступ к банкомату и используют загрузочный диск, чтобы установить бэкдор. После перезапуска системы преступники получают контроль над банкоматом: вредоносная программа активируется и ожидает дальнейших указаний.

Чтобы избежать обнаружения Tyupkin использует несколько приёмов. В частности, программа активна только в определённое время ночью. Кроме того, для каждой сессии используется ключ, генерируемый из выбранного случайным образом числа. Без этого ключа взаимодействие с зараженным банкоматом невозможно.

Второй этап предполагает собственно хищение средств. При вводе правильного кода зловред выводит на экран информацию о количестве денег, доступных в каждой кассете, и позволяет злоумышленнику, имеющему

физический доступ к банкомату, получить 40 купюр из выбранной кассеты. Вставлять какие-либо пластиковые карты при этом не требуется.

В настоящее время вредоносная программа обнаружена в системах банкоматов стран Латинской Америки, Европы и Азии ***(Бэкдор Tyupkin для банкоматов позволил похитить миллионы долларов // InternetUA (http://internetua.com/bekdor-Tyupkin-dlya-bankomatov-pozvolil-pohitit-millioni-dollarov). – 2014. – 8.10).***

***

Сайты, работающие на основе CMS WordPress, часто оказываются скомпрометированными и в дальнейшем используются для рассылки спама и фишинговых писем. Зачастую это происходит из-за использования устаревшей версии популярного CMS или уязвимых плагинов к нему. Об этом пишет специалист компании Sucuri Д. Сид.

В качестве примера Д. Сид привел одно из фишинговых писем, которое он получил на свой ящик электронной почты. В нем предлагалось немедленно перейти по ссылке, чтобы просмотреть важный документ, касающийся «недавних переговоров». Ссылка вела на подставной сайт, имитирующий внешний вид страницы входа Документов Google.

Как сообщает Д. Сид, количество фишинговых страниц в Интернете непрестанно увеличивается. В 2008 г. специалисты Google детектировали примерно 3 тыс. таких страниц в день, в то время как сейчас детектируется более 23 тыс. фишинговых ресурсов ежедневно.

Большинство сайтов, с которых рассылаются фишинговые письма, работали под управлением CMS WordPress. Злоумышленникам удалось скомпрометировать эти ресурсы и разместить подставные веб-страницы в подпапках сайтов. Чаще всего использовались папки wp-includes и wp-content.

В качестве основной причины взлома вначале рассматривалась уязвимая версия WordPress, но оказалось, что большинство скомпрометированных ресурсов использовали последнюю версию CMS (3.9.2 / 4.0). Проблема крылась в устаревших версиях многих плагинов для WordPress, которые были установлены на большинстве взломанных сайтов. Используя SQL-инъекции или удаленное выполнение команд, хакеры могли за несколько минут получить доступ к любому ресурсу, использующему уязвимые плагины ***(Хакеры используют скомпрометированные сайты на WordPress для рассылки фишинговых писем // InternetUA (http://internetua.com/hakeri-ispolzuuat-skomprometirovannie-saiti-na-WordPress-dlya-rassilki-fishingovih-pisem). – 2014. – 8.10).***

***

Около месяца назад стало известно об уязвимости, позволяющей обойти ограничения безопасности в Google Android Browser. По данным исследователей из компании Lookout, занимающейся вопросами

безопасности мобильных систем, в настоящее время уязвимая версия браузера установлена у 45 % ее клиентов. До тех пор, пока не будут выпущены обновления, безопасность пользователей находится под угрозой.

В Lookout сообщили, что наибольшее число уязвимых браузеров, которыми пользуются клиенты компании, зафиксировано в Японии (81 %) и Испании (73 %). Пользователи в этих странах должны получить патчи в первую очередь, однако, похоже, что они до сих пор этого не сделали.

Уязвимость, обнаруженная в прошлом сентябре, присутствует в версии Android 4.3 и ниже. Google заменила браузер на более новый и функциональный Chrome Browser в Android 4.4, поэтому пользователям этой сборки можно не беспокоиться.

Для обеспечения безопасности данных владельцам Android-устройств, на которых установлен уязвимый браузер, рекомендуется предпринять следующие шаги:

• Обновить Android 4.3 до более поздней версии.

• В случае, если в телефоне отсутствует возможность обновления платформы, лучше всего приобрести более новое устройство, в котором уязвимость уже исправлена.

• Загрузить браузер Chrome или Firefox.

• Сделать Chrome или Firefox браузером по умолчанию для перехода по ссылкам ***(Пользователи продолжают работать с уязвимым браузером в Android 4.3 // InternetUA (http://internetua.com/polzovateli-prodoljauat-rabotat-s-uyazvimim-brauzerom-v-Android-4-3). – 2014. – 8.10).***

***

Компания Proofpoint, занимающая вопросами безопасности электронной почты, обнаружила целую инфраструктуру, которая стоит за одним из крупнейших ботнетов, основанном на трояне. В ботнет Qbot (также известен как Qakbot) входят 500 тыс. инфицированных систем. Вредоносному ПО удалось перехватить около 800 тыс. транзакций online-банкинга. Предположительно, более половины (59 %) сессий были перехвачены у клиентов пяти крупнейших банков США.

Исследователи считают, что за атаками стоит группировка русскоговорящих хакеров. Помимо жителей США, учетные данные для online-банкинга также были похищены у клиентов некоторых европейских финорганизаций.

По данным Proofpoint, атаки по типу drive-by-download осуществлялись с помощью скомпрометированных сайтов на базе платформы WordPress. При этом хакеры использовали заранее приобретенный список имен администратора. Злоумышленники загружали вредоносное ПО на легитимные ресурсы с целью заражения посещающих их пользователей. Многие из этих сайтов занимаются новостной рассылкой, поэтому вместе с сообщениями жертвы также получали вредоносное ПО.

Примечательно, что в целях получения прибыли злоумышленники занимались продажей доступа к скомпрометированным системам ***(Эксперты обнаружили новый ботнет, инфицировавший порядка 500 тыс. систем // InternetUA (http://internetua.com/eksperti-obnarujili-novii-botnet--inficirovavshii-poryadka-500-tis--sistem). – 2014. – 8.10).***

***

"Українські кібер-війська" звернулися до Президента України П. Порошенка з вимогою звільнити Міністра оборони Гелетея з посади.

Звернення було зроблене в дуже незвичайний спосіб: хакери знайшли вразливість на сайті Державної служби зайнятості, і за допомогою XSS-втручання розмістили власний текст.

Звернення провисіло на сайті Держзайнятості тривалий час, поки адміністратори ресурсу виявили вразливість та ліквідували "звернення". Це не перший випадок, коли сайти державних органів влади України стають об'єктами для вивчення та злому хакерами: раніше подібні вразливості були помічені на kvs.gov.ua, dcz.gov.ua та kmu.gov.ua ***(Українські кібер-війська звернулися до Петра Порошенка // UkrainianWatcher (http://watcher.com.ua/2014/10/09/ukrayinski-kiber-viyska-zvernulysya-do-petra-poroshenka/). – 2014. – 9.10).***

***

В последние несколько месяцев хакеры развернули полномасштабную фишинговую кампанию против ряда технологических гигантов, включая Microsoft, Apple, Oracle и Adobe. Неизвестные злоумышленники задались целью получить исходные коды их продуктов.

Эксперты по безопасности отмечают, что хакеры сфокусировались на стратегических целях и наиболее уязвимом секторе высоких технологий, пытаясь заполучить исходные коды, обнаружить в них бреши и эксплуатировать для атак на пользователей.

Чтобы выманить у жертв их учётные данные, хакеры используют вредоносные письма и приложения. В последнее время отмечается всплеск фишинговых атак на технологические компании Microsoft, Apple, Adobe и Oracle.

Помимо инъекций вредоносного кода, злоумышленники активно используют и социальную инженерию. Аналитики отмечают, что ежедневно в Сети появляется порядка 160 тыс. вредоносных программ.

Так, во II квартале 2014 г. всего хакерами было создано 15 млн образцов вредоносного ПО. Самыми распространёнными вредоносами остаются трояны – на них приходится 62,8 % всех случаев инфицирования ***(IT-гиганты всё чаще становятся жертвами фишинга, направленного на кражу исходных кодов // Блог Imena.UA (http://www.imena.ua/blog/it-hackers-phishing/). – 2014. – 9.10).***

***

Исследователи ИБ-компании Proofpoint опубликовали отчет о работе русскоязычной хакерской группы, взломавшей 800 тыс. банковских учетных записей в США и Европе. По мнению исследователей, реализация «доли процента» добытой ими информации принесет хакерам многомиллионную прибыль.

У. Хуань из занятой информационной безопасностью компании Proofpoint опубликовал подробный отчет о группировке хакеров Qbot, скрытно получающей доступ к чужим учетным записям в банках.

На пике группировка Qbot контролировала около 500 тыс. ПК, собирая данные о вводе с клавиатуры пользовательских паролей к банковским сервисам.

Полмиллиона зараженных ПК – это не слишком большая ботсеть по нынешним стандартам, однако, исследование, опубликованное исследователем экспертом Proofpoint интересно тем, что описывает сложную тактику авторов этого ботнета, и, кроме того, оно указывает на их русское происхождение.

Гипотеза о русских (русскоязычных) корнях создателей ботнета основана на панели управления Qbot, к которой получили доступ исследователи Proofpoint. На скриншотах, представленных в отчетах Proofpoint, хорошо видны пункты меню и комментарии на правильном русском языке на управляющих страницах ботнета.

По данным исследования, Qbot, которую в Proofpoint также называют Qakbot, была нацелена на атаку систем дистанционного банковского обслуживания американских банков. На США приходится 75 % IP-адресов, на связь с которыми выходили управляющие сервера ботнета, причем 59 % из них принадлежат клиентам пяти крупнейших американских банков. На остальные страны мира приходится лишь четверть подконтрольных ПК.

Интересно, что 52 % ПК, которые удалось заразить Qbot, работают под управлением Windows XP, хотя, как подчеркивают авторы отчета, эта ОС сейчас занимает долю лишь в 20–30 % ПК как в домашних хозяйствах, так и в корпоративном секторе. Поддержка Windows XP была прекращена Microsoft в апреле 2014 г.

Согласно анализу Proofpoint, 82 % успешных заражений Qbot были совершены посредством браузера Internet Explorer.

Атаки на компьютеры потенциальных жертв проводились с сайтов, построенных на движке WordPress. Первоначальный доступ к ним создатели ботнета получили, купив на черном рынке базу админских имен и паролей, после чего внедрили в сайты свой вредоносный код.

При посещении потенциальной жертвой зараженного сайта специальная система управления трафиком анализировала ПК потенциальной жертвы по признакам его IP-адреса, типа браузера, операционной системы, установленного защитного ПО и других критериев.

Таким образом создатели ботнета минимизировали опасность обнаружения их внедренного в сайты вредоносного программного обеспечения.

Большинство зараженных сайтов выполняло регулярные антивирусные сканирования, однако внедренный вредоносный код оставался незамеченым, поскольку атакующие старались использовать эксплойты, не вызывающие реакции у антивирусных программ. По данным У. Хуанья, перед загрузкой вредонсоного кода он проверялся по базе данных Scan4U, агрегирующей данные от десятков антивирусных компаний. Если база узнавала вредоносный код, его меняли на такой, у которого сканирование не вызывало проблем.

Создатели Qbot приняли меры для защиты от антиврусных компаний: если посетитель их сайта был похож на автоматический антивирусный сканер, то система управления трафиком перенаправляла его к незараженной версии сайта. В распоряжении хакеров имелся список IP-адресов, используемых ИБ-компаниями, и любой трафик от них также переадресовывался к «чистым» копиям сайтов. Вследствие этих мер, как пишет У. Хуань, многие владельцы сайтов, с которыми он связывался, не верили, что они атакованы.

Для целей сниффинга (сканирования клавиатурных нажатий при вводе банковского логина и пароля) авторы Qbot использовали целый массив уязвимостей в плагинах PDF, Java, Flash и Internet Explorer, которые выбирались в каждом конкретном случае в зависимости от уникальных особенностей целевой системы. Эксплойты для эксплуатации этих уязвимостей обычно приобретались на черном рынке, и хакеры от них отказывались, когда они становились слишком распространены.

У. Хуань пишет в своем исследовании, что авторы Qbot, просканировав 500 тыс. компьютеров, смогли получить данные примерно о 800 тыс. банковских учетных записях.

По его данным, организованные преступные группировки готовы покупать данные о банковских учетках, исходя из цены 25 тыс. дол. за штуку, и, таким образом, даже если создатели Qbot «продадут на черном рынке долю процента учетных записей, они получат многомиллионную прибыль от своей операции».

Хотя внутренние средства безопасности создателей Qbot были хороши, совершенными их назвать нельзя, говорит У. Хуань и приводит забавную подробность: когда он нашел веб-адрес панели управления ботнетом, обнаружилось, что доступ к ней не требует пароля ***(Русские хакеры провели масштабную операцию по взлому банковских счетов в США и Европе // InternetUA (http://internetua.com/russkie-hakeri-proveli-masshtabnuua-operaciua-po-vzlomu-bankovskih-scsetov-v-ssha-i-evrope). – 2014. – 9.10).***

***

Обнаружена новая уязвимость, открывающая доступ к голосовому помощнику Siri в мобильных устройствах, работающих на платформе iOS 8. Об этом сообщает Н. Гонзалез из WonderHowTo.

Новый, довольно несложный эксплоит позволяет запускать Siri и получать доступ к текстовым сообщениям, электронной почте и учетной записи в Twitter, однако не дает возможности обойти экран блокировки устройства и получить доступ к приложениям. Выполнение следующих действий позволяет обойти экран блокировки устройства:

1. Отключите устройство от беспроводной сети;
2. Задайте Siri вопрос;
3. Извлеките и вновь установите SIM-карту;
4. Нажмите кнопку Siri «Редактировать» и сформулируйте команду «Прочитать все мои сообщения», «Прочитать мою электронную почту», «Отправить пост в Twitter» или «Отправить письмо по электронной почте». Любая из этих команд должна быть создана с помощью функции «редактировать».

На другие команды, например, запустить приложения, Siri не реагирует. Таким образом, уязвимость открывает доступ только к недавно отправленным электронным письмам и сообщениям, а также позволяет отправлять сообщения от имени владельца устройства.

Для того чтобы защитить устройство от действия эксплоита, необходимо отключить Siri на экране блокировки, выполнив следующие функции: Настройки > Touch ID и пароли > Снять галочку с «Siri» в поле «Разрешить доступ при блокировке» ***(Уязвимость в iOS 8 открывает несанкционированный доступ к голосовому помощнику Siri // InternetUA (http://internetua.com/uyazvimost-v-iOS-8-otkrivaet-nesankcionirovannii-dostup-k-golosovomu-pomosxniku-Siri). – 2014. – 9.10).***

***

Глава центра по киберпреступности Европола Т. Эртинг заявил, что в мире имеется всего около сотни, действительно, опасных киберпреступников. Об этом сообщает Русская служба Би-би-си, передает «Донбасс. Комментарии».

Как отметил Т. Эртинг, правоохранительным органам необходимо сосредоточить свое внимание на довольно ограниченной по составу группе одаренных программистов.

«Нам примерно известно, кто они. Если нам удастся их обезвредить, то вся созданная ими система рухнет», – заявил он.

При этом Т. Эртинг признает, что борьба с киберпреступностью остается сложнейшим делом: «Мы пока справляемся, но преступники обладают большими ресурсами, чем мы, и они ничем не связаны. Они руководствуются жадностью и создают зловредные программы со скоростью, за которой мы с трудом поспеваем».

Большая часть таких самых опасных киберпреступников, по словам Е. Эртинга, находятся в русскоязычном мире.

Отношения Европола с российскими правоохранительными органами не всегда были хорошими, но сейчас они улучшаются.

Е. Эртинг рассказал, что недавно побывал в Москве, где принял участие в обсуждении четырех крупных дел в области киберпреступности, и выразил надежду, что теперь там будут произведены аресты и возбуждены уголовные дела.

Такие преступные группы программистов создают и испытывают зловредное ПО, а затем продают их через специальные интернет-форумы.

По словам Т. Эртинга, оттуда программы расходятся по всему миру. Коммерциализация киберпреступности делает поиск преступников все более сложным.

«Нормальным потребителям нужно проявлять осторожность и больше думать о безопасности своих учетных записей в социальных сетях и электронной почте. Если преступникам удается проникнуть в них, они могут причинить много вреда», – предупредил он ***(Глава центра по киберпреступности призывает пользователей соцсетей к бдительности // «Донецк. Комментарии» (http://donbass.comments.ua/news/104482-glava-tsentra-kiberprestupnosti.html). – 2014. – 12.10).***

***

Любители «клубнички» очень рискуют, кликая по ссылкам с заголовками, обещающими показать им что-нибудь эдакое. На этот раз доверчивые пользователи Facebook получили троянца вместо обещанного видео с обнаженной Э. Уотсон, сообщается в блоге Bitdefender Labs.

Мало того, что троян пытается украсть личную информацию, такую как номера телефонов, маркеры приложений и компрометирует пользовательские сессии Facebook. Он еще и подписывает жертву на платные SMS-рассылки.

Если пользователь нажимает на вредоносную ссылку в комментарии Facebook, который обещает показать ему видео обнаженной актрисы, которое якобы «утекло» в сеть, то жертву перенаправляют на фальшивую страницу YouTube, на которой он видит сообщение, где его просят обновить Flash Player, чтобы просмотреть видео. Когда жертва «обновляет плеер», компьютер инфицируется трояном, который исследователи назвали Trojan.JS.Facebook.A.

Обещанное видео так и не отображается, а с аккаунта жертвы рассылается то самое мошенническое сообщение, на которое «клюнул» доверчивый пользователь ***(Троян вместо «обнажёнки»: очередная схема, нацеленная на пользователей Фейсбук // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/10/10/emma-watson-leaked-facebook-video-reveals-trojans-not-nude-pictures.html). – 2014. – 10.10).***

***

Компания Cyberintel раскрыла масштабную преступную компьютерную сеть, осуществлявшую атаки на сотни компаний Германии, Австрии и Швейцарии. Начиная с 2012 г., хакеры использовали подставные компании, зарегистрированные в Великобритании, чтобы атаковать крупные организации и государственные учреждения.

2 сентября Cyberintel раскрыла масштабную киберпреступную сеть, которая атаковала сотни крупных компаний, государственных организаций, исследовательских лабораторий и важных объектов жизнедеятельности в Германии, Австрии, Швейцарии и пресекла возможность атаки на другие европейские страны. Сеть функционировала на протяжении 12 лет, действуя через более чем 800 подставных компаний, зарегистрированных в Великобритании.

Специалисты обнаружили вирус Harkonnen Operation в системе одной из компаний, в процессе внедрения в неё своего программного обеспечения. Жертвой атаки стала крупная немецкая компания, занимающаяся хранением конфиденциальных данных своих клиентов со всего мира. Специалистами были найдены два «трояна», перекачивающих важную информацию, а дальнейшая проверка показала, что домен, с которого осуществлялась атака, был зарегистрирован английской компанией, и что остальные 833 компании, которые являлись подставными, были также зарегистрированы в Великобритании.

На деле, эта атака оказалась только верхушкой международного киберпреступного айсберга. Далее Cyberintel обнаружила следы вируса в системах более 300 компаний в Германии, Австрии и Швейцарии, при этом целью атак были ключевые представители компаний.

Атака представляла собой серию целевых фишинговых атак, и осуществлялась двумя троянскими вирусами, созданными в Германии. Проникая в компьютеры, вирусы создавали каналы для передачи конфиденциальной информации в базу преступной сети.

«Пользуясь тем, что требования, установленные в Великобритании для приобретения SSL-сертификатов безопасности, были не слишком жёсткими, злоумышленники открывали подставные компании, чтобы те имитировали законные веб-сервисы», говорит Д. Гэд, компания Elite Cyber Solutions. «Немецкие хакеры, являвшиеся частью сети, полностью контролировали заражённые компьютеры и осуществляли шпионаж оставаясь незамеченными много лет».

Проведённый экспертный анализ позволил отследить злоумышленников по оставленным в Интернете следам, и обнаружить лиц, стоявших за этой атакой. Cyberintel передала имеющуюся информацию своему клиенту, который привлёк к расследованию немецкую полицию.

«На данный момент, мы знаем о масштабах вируса Harkonnen Operation, но вред, нанесённый вирусом организациям, включающий в себя потерю важных данных и доходов, а также утечек информации связанной с

сотрудниками компаний и их клиентами несоизмерим», – добавил Д. Гэд ***(Эксперты обнаружили хакерскую сеть Harkonnen // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/10/10/Harkonnen.html). – 2014. – 10.10).***

***

Хакеры из группы Anonymous начали кибервойну с Китаем, сообщает издание The South China Morning Post. При этом начать они решили с сайта зоны свободной торговли Нинбо и портала для поиска работы администрации округа Чансин провинции Чжэцзян, на котором размещаются вакансии и резюме.

Всего обнародованы сотни электронных адресов, телефонов и имен пользователей. При этом непонятно, почему пострадали именно эти сайты. Ни администрация провинции Чжэцзян, ни дирекция Нинбо, ни центральные министерства произошедщее никак не комментируют. Более того, эксперты не уверены, что атака на правительственные ресурсы действительно является делом рук Anonymous – не исключено, что ее осуществила отдельная группа хакеров, действующих по собственной инициативе, информирует news.eizvestia.com (http://news.eizvestia.com/news_technology/full/878-hakery-iz-anonymous-nachali-kibervojnu).

2 октября хакеры из Anonymous заявили о своей солидарности с протестующими Гонконга, заблокировали несколько городских сайтов и пообещали, что нападению подвергнутся еще несколько десятков ресурсов, принадлежащих как администрации Гонконга, так и властям КНР ***(Хакеры из Anonymous начали кибервойну // «Экономические известия» (ttp://news.eizvestia.com/news_technology/full/878-hakery-iz-anonymous-nachali-kibervojnu). – 2014. – 13.10).***

***

Командование армии Израиля планирует существенно уменьшить уязвимость страны к хакерским атакам. Предполагается, что новые меры превратят Израиль в главный оплот кибербезопасности в мире.

Такую инициативу, помимо военных, уже поддержал Премьер-министр страны Б. Нетаньяху, который назвал Интернет новой линией фронта для любого из государств.

Предполагается, что Израиль инвестирует средства в компании, которые занимаются разработкой систем защиты от хакерских атак.

Будет запущен мощный образовательный проект для молодых борцов с преступностью в сети. В рамках данного проекта израильское правительство создаст программы обучения в 100 учебных учреждениях страны.

Кроме того, в Израиле будут созданы тематические внешкольные мероприятия, включая тренировочные лагери.

После обучения молодые специалисты будут проходить обязательную службу в киберподразделениях израильской армии, разрабатывая системы защиты Израиля от хакерских ударов.

Через 3–4 года службы молодые люди смогут организовывать собственные компании, разрабатывающие методику противостояния хакерам.

Следует уточнить, что на сегодняшний день Израиль является вторым в мире экспортером программного обеспечения после США. В стране существует 200 частных компаний, которые разрабатывают, преимущественно, системы защиты.

В 2013 году программисты из Университета им. Бен-Гуриона, Израиль, разработали спам-фильтр, который способен, в прямом смысле, понимать, о чём идёт речь в очередном электронном письме ***(Израиль превратится в главную опору кибербезопасности в мире // Блог Imena.UA (http://www.imena.ua/blog/diplomacy-defense/). – 2014. – 10.10).***

***

Невідомі хакери заявили, що викрали близько семи мільйонів логінів та паролів користувачів хмарнового сервісу зберігання даних Dropbox. Водночас представники компанії кажуть, що витік інформації не є загрозливим, оскільки викрадена інформація вже недійсна.

Як повідомляє The Next Web, файл із паролями до акаунтів Dropbox був опублікований на сайті Pastebin. У документі міститься 400 електронних адрес, імовірно, користувачів Dropbox. В ньому також поряд із кожною адресою зазначене таємне слово.

При цьому хакери заявляють, що надані в цьому документі дані є лише невеличкою частинкою того, що вони отримали унаслідок зламу. За їхніми словами, вкрадено паролі від 6937081 акаунту. Зловмисники також пообіцяли викласти решту конфіденційної інформації в обмін на пожертви у біткоїнах.

Водночас користувачі ресурсу Reddit, що помітили витік інформації одними із перших, пишуть, що інформація може бути достовірною. Одному із користувачів Reddit вдалося зайти у чужий акаунт, скориставшись опублікованою хакерами інформацією.

Dropbox натомість заявляє, що сервіс не зламували, а персональні дані були викрадені через сторонні сайти ***(Хакери заявили про викрадення майже семи мільйонів паролів до Dropbox // Osvita.MediaSapiens (http://osvita.mediasapiens.ua/material/35436). – 2014. – 14.10).***

***

Специалисты международной антивирусной компании ESET (Словакия) обнаружили новые следы активности известной киберпреступной группы Sednit. Теперь хакеры используют новый набор эксплойтов для распространения вредоносных программ.

В течение последних пяти лет жертвами группы Sednit стали различные организации преимущественно из Восточной Европы. Хакеры распространяли вредоносное ПО среди корпоративных пользователей с помощью фишинговых сообщений электронной почты. Письма содержали вложенные файлы Microsoft Word с распространенными эксплойтами, которые использовались для автоматической установки других вредоносных программ.

«Недавно мы столкнулись со случаем компрометации легитимных финансовых сайтов. Веб-страницы содержали вредоносный объект, который перенаправлял посетителей на набор эксплойтов. На базе наших собственных исследований и информации, предоставленной нам группой аналитиков из Google Security Team, мы установили причастность Sednit к данной атаке. Если ранее группа специализировалась только на рассылке фишинговых сообщений с вредоносными вложениями, то теперь хакеры меняют стратегию», – комментирует Д. Калвет, вирусный аналитик ESET.

Специалисты компании ESET проанализировали вредоносное содержимое, размещенное группой Sednit на сайте крупного финансового учреждения из Польши. Было обнаружено, что в одном из исследуемых объектов используется URL-адрес, очень похожий на адрес авторитетного новостного ресурса о военной промышленности. Вредоносные объекты перенаправляли пользователей на набор эксплойтов, устанавливающих на компьютеры троян Win32/Agent.WLF.

В последние годы комплекты вредоносных программ – наборы эксплойтов – все чаще используются киберпреступниками. Они предназначены для операций финансового мошенничества, рассылки спама, майнинга биткоинов и кражи конфиденциальных данных пользователей. Схема кибератак, используемая Sednit, известна под общим названием «watering hole». Она предполагает компрометацию злоумышленниками известного веб-ресурса, что приводит к многочисленным заражениям пользователей ***(Группа хакеров Sednit атакует финансовые учреждения // InternetUA (http://internetua.com/gruppa-hakerov-Sednit-atakuet-finansovie-ucsrejdeniya). – 2014. – 13.10).***

***

В мережу потрапила майже сотня тисяч зображень, які користувачі Snapchat пересилали одне одному. Це відбулося після кількаденних чуток про можливий витік інформації, повідомляє Mashable.

Видання зазначає, що загрози були недаремними. У неділю збірка майже із 98 тис. файлів із фото та відео (загальним обсягом більше 13 гігабайт) були опубліковані на The Pirate Bay. Імовірно, ці зображення належали користувачам сервісу Snapchat.

Це відбулося через добу після того, як невідома особа, імовірно злодій, заявила, що змінила свою думку та не буде публікувати викрадені фотографії. Дані були зібрані за допомогою сайту snapsaved.com, який дає

змогу користувачам відкривати свої фото не лише їх мобільного додатка, але й з комп'ютера.

Напередодні представники Snapsaved підтвердили, що їхній сайт був зламаний. Однак вони повідомили, що витік складає лише 500 мегабайтів. Після того, як стало відомо про проблему, керівництво ресурсу вирішило повністю видалити сайт та його базу даних. Вони також зазначили, що за допомогою викрадених знімків неможливо відтворити базу з пошуком за іменами.

Вперше інформація про витік інформації з'явилася 10 жовтня. Тоді користувачі сайту 4chan заявили, що мають у своєму розпорядженні тисячі викрадених фотографій та планують опублікувати їх у мережі.

Mashable зазначає, що користувачі Reddit очікували на появу в злитому архіві багатьох оголених фотографій. Натомість один із користувачів, який детально ознайомився із архівом, помітив, що більшість файлів є «сміттям» на кшталт селфі, мемів, пейзажів та домашніх тварин ***(У мережу потрапили 98 тисяч фотографій та відео користувачів сервісу Snapchat // «Медіаграмотність» (http://osvita.mediasapiens.ua/material/35438). – 2014. – 14.10).***

***

Как выяснилось, в утечке виноват сайт Snapsaved.com. Его владельцы написали в Facebook, что сайт был взломан, и с него было украдено по крайней мере 500 мегабайт данных. Как только им стало известно о хакерской атаке, сайт был отключен, а его база данных перенесена в другое место. Большая часть «пострадавших» – жители Швеции, Норвегии и США. Доступа к личным данным пользователей (адресам электронной почты, никам, местоположению и т. п.) злоумышленники не получили. Владельцы Snapsaved.com принесли извинение и заявили, что не хотели, чтобы пользователям Snapchat был причинен вред ***(Найден сервис, виновный в утечке фотографий из Snapchat // InternetUA (http://internetua.com/naiden-servis--vinovnii-v-utecske-fotografii-iz-Snapchat). – 2014. – 14.10).***

***

Государственная служба специальной связи и защиты информации создала оперативную группу по вопросам реагирования на компьютерные инциденты с целью предупреждения нарушений безопасности информации.

Как сообщает Цензор.НЕТ со ссылкой на сайт Службы, в состав координационного центра войдут представители Госспецсвязи, СБУ, МВД, Службы внешней разведки, Министерства обороны, Генштаба ВСУ, Генпрокуратры и Национальной комиссии, осуществляющей государственное регулирование в сфере связи и информатизации. Кроме того, в деятельности центра будут участвовать представители двух десятков ведущих операторов и провайдеров телекоммуникаций, а также общественных организаций ИнАУ, Телас и Киевского отделения ISACA.

В задачи оперативной группы по борьбе с кибератаками входят: скорейшая отработка компьютерных инцидентов, информация о которых поступила в команду реагирования на компьютерные чрезвычайные ситуации CERT-UA; координация сил и средств, направленных на предотвращение нарушений безопасности информации в информационно-телекоммуникационных системах; обсуждение и наработки действенных механизмов обеспечения кибербезопасности путем консультаций экспертов компаний и организаций. Также будет осуществляться информирование общественности о хакерских атаках и их ликвидации.

Создание координационного центра по кибератакам является первым шагом к созданию межведомственного Национального центра киберзащиты и противодействия киберугрозам, что предусмотрено Указом Президента Украины от 24 сентября 2014 г. «О решении Совета национальной безопасности и обороны Украины» от 28 августа 2014 г. «О неотложных мерах по защите Украины и укреплению ее обороноспособности» ***(В Украине создана группа реагирования на киберугрозы // InternetUA (http://internetua.com/v-ukraine-sozdana-gruppa-reagirovaniya-na-kiberugrozi). – 2014. – 15.10).***

***

Небрежность создателей вредоносного ПО позволит предсказать будущие модификации уже существующих вредоносных программ. Начинающая израильская компания CyActive занимается созданием новой технологии, которая позволит разработчикам спрогнозировать возможные модификации эксплоитов и тем самым разработать метод смягчения будущей хакерской атаки.

По словам главного исполнительного директора CyActive Л. Танкмана, вредоносное ПО (так же как и легитимное) довольно часто является деривативным. Даже в усовершенствованных атаках базовые компоненты остаются неизменными, что позволяет четко увидеть методы, которые злоумышленники используют сейчас и предсказать модификации, которые с наибольшей вероятностью будут использованы в будущем.

Этот феномен подтверждают хакерские атаки, нацеленные на торговую сеть Target, которые были совершены в декабре прошлого года. В ходе атак на PoS-терминалы ритейлера злоумышленники использовали вредоносную программу BlackPoS, также известную как Kaptoxa. В результате атаки скомпрометированными оказались данные кредитных карт миллионов пользователей. Похожей атаке подверглась еще одна крупнейшая американская торговая сеть Home Depot. В ходе нападения преступники использовали слегка модифицированную версию вредоносного ПО, которая состояла из фрагментов кодов других программ. Специалисты сравнили обе вредоносные программы и обнаружили огромное количество сходных компонентов и операций.

Л. Танкман уверен, что при возможности анализа исходной программы, специалистам CyActive наверняка бы удалось спрогнозировать новую версию BlackPoS. Как отметил глава компании, новая технология позволяет в течение 20 минут предсказать 10 тыс. вариантов конкретной вредоносной программы и тем самым создать эффективные средства защиты от них.

Несмотря на то, что новая технология в настоящее время находится в разработке, в ней уже заинтересованы промышленные предприятия, в частности компания Siemens, которая является главным инвестором компании CyActive ***(Небрежность создателей вредоносного ПО позволяет предсказать его будущие версии // InternetUA (http://internetua.com/nebrejnost-sozdatelei-vredonosnogo-po-pozvolyaet-predskazat-ego-budusxie-versii). – 2014. – 15.10).***

***

Высокоорганизованная хакерская группировка Hurricane Panda, находящаяся, по всей видимости, в Китае и атакующая компании с крупной инфраструктурой, использовала в своих нападениях эксплоит к уязвимости нулевого дня в продуктах Microsoft. При этом длительность нападения составила более 5 месяцев. По данным исследователей из CrowdStrike, первая обнаруженная ими атака была произведена еще весной этого года.

Эксперты также отмечают, что изначально образец вируса был выявлен на машине под управлением 64-битной Windows Server 2008 R2. С его помощью удалось выяснить, что нападение начинается с компрометации веб-сервера и последующего выполнения вредоносных сценариев Chopper. Последние позволяют злоумышленникам повысить свои привилегии, для чего также используется инструмент Local Privilege Escalation, эксплуатирующий недавно выявленную уязвимость нулевого дня. В конечном итоге атакующие получают привилегии SYSTEM и создают новый процесс с аналогичными правами доступа, с помощью которого осуществляется сбор конфиденциальных данных.

«Хакеры часто используют обнародованные уязвимости повышения привилегий, чтобы получить административный доступ, но настоящие уязвимости нулевого дня применяются довольно редко и потому это нападение вызывает особый интерес», – пояснили исследователи ***(Хакеры из Hurricane Panda эксплуатировали уязвимость нулевого дня в течение 5 месяцев // InternetUA (http://internetua.com/hakeri-iz-Hurricane-Panda-ekspluatirovali-uyazvimost-nulevogo-dnya-v-tecsenie-5-mesyacev). – 2014. – 15.10).***

***

Несколько специалистов в области IT-безопасности продемонстрировали на конференции Black Hat Europe метод, позволяющий спрятать вирус в графический файл с расширением .PNG, а затем упаковать его вместе с просмотрщиком в файл .APK для ОС Android. После запуска

приложения и открытия графического файла на мобильном устройстве создается еще один установочный файл.

Именно его злоумышленники могут применять для кражи личных данных пользователя: текстовых сообщений, фото, списка контактов или иной информации. Во время презентации мобильная ОС уведомила о том, что некое ПО (распакованное из графического файла) требует дополнительных привилегий. Однако, по словам инженеров, используя метод DexClassLoader, подобное сообщение можно скрыть, и жертва не узнает о вторжении.

Также разработчики сообщили о некоторых других предпринятых шагах, которые требуются для того, чтобы скрыть от системы вредоносный файл и позволить Android выполнить его.

Подобный тип вторжения работает на версии Android 4.4.2, однако Google уведомлена о существующей уязвимости ***(Хакеры нашли способ прятать Android-вирусы в картинках // InternetUA (http://internetua.com/hakeri-nashli-sposob-pryatat-Android-virusi-v-kartinkah). – 2014. – 18.10).***

***

Администрация Президента констатирует, что сайт Президента регулярно подвергается хакерским атакам.

Об этом в интервью Українським Новинам сказал заместитель главы Администрации Д. Шимкив, передает Цензор.НЕТ.

«Каждую неделю я получаю отчет от Государственной службы спецсвязи о кибератаках, постоянно идет отражение атак. Но не будем же мы каждый день публиковать сообщения о том, что нас атакуют. Ну атакуют, службы работают, отражают атаки, каждый день практически. Есть отчеты и графики, на которых отображается степень атак. Когда это переходит определенный порог – подключаются уже специалисты другого уровня», – сообщил он.

Вместе с тем Д. Шимкив подчеркнул, что в Администрации знают о проблемах, которые возникают в работе сайта в связи с этими атаками, и учитывают возникающие сложности ***(АП пожаловалась на регулярные хакерские атаки на сайт Президента // InternetUA (http://internetua.com/ap-pojalovalas-na-regulyarnie-hakerskie-ataki-na-sait-prezidenta). – 2014. – 18.10).***

***

Исследователи из Google обнаружили новую уязвимость в веб-браузерах и программном обеспечении для интернет-серверов, которая позволяет хакерам получать контроль над атакуемой системой, сообщает Reuters.

Ошибка в популярном протоколе шифрования SSL 3.0 получила название Poodle (Padding oracle on downloaded legacy encryption). Благодаря

этой уязвимости злоумышленники могут похитить любые личные данные: пароли для электронной почты, системы интернет-банкинга, страницы в социальных сетях. Получение информации хакерами становится возможной благодаря краже файлов cookies, которые создаются браузером и содержат личные данные.

В этом году специалисты уже выявили несколько глобальных интернет-уязвимостей, затрагивающих множество интернет-серверов и обычных персональных компьютеров. Две наиболее опасные из них получили названия Heartbleed и Shellock. С их помощью хакер получает полный контроль над атакуемой системой.

Разработчики софта ищут способы борьбы с Poodle. Например, Mozilla, выпускающая браузер Firefox, отключит SSL 3.0 в новой версии веб-обозревателя, а в Google планируют избавиться от этого протокола шифрования во всем клиентском ПО ***(Google: «Пудель» делает веб-браузеры уязвимыми для хакеров // InternetUA (http://internetua.com/Google---pudel--delaet-veb-brauzeri-uyazvimimi-dlya-hakerov). – 2014. – 18.10).***

***

Единая система коммуникаций Binder является основной целью для любого вредоносного программного обеспечения (ПО), разрабатываемого для системы Android. Об этом говорится в сообщении компании Check Point Software Technologies.

Механизм Binder встроен в систему коммуникаций Android Inter-process Communication (IPC). Компания изучила архитектуру операционной системы Android и выявила возможность кражи информации, которая хранится или находится в процессе передачи при помощи механизма обработки сообщений Binder.

В стандартных операционных системах процессы работают с десятками элементов системного оборудования: жестким диском, адаптером дисплея, сетевой картой и т. д. Однако в связи с особенностями архитектуры ОС Android тот или иной процесс может выполнить те же задачи, контролируя все взаимодействия приложений через Binder. Таким образом, через Binder могут быть перехвачены такие важные данные, как результат клавиатурного ввода, информация из приложений, например, банковских транзакций, и содержимое SMS-сообщений.

По словам А. Разумова, руководителя группы консультантов по безопасности Check Point Software Technologies, в результате исследования было выявлено слабое звено в IPC на устройствах Android, которое делает Binder новой целью атак мобильного вредоносного ПО.

«Важнейшим преимуществом Binder для злоумышленников является недостаточная осведомленность пользователей о том, какие данные пересылаются через IPC. Без соответствующей системы многоуровневой защиты киберпреступники могут перехватить коммуникации на устройстве Android через Binder, обходя все меры безопасности, применяемые

отдельными приложениями на устройстве», – отметил Разумов ***(Найдена главная «дыра» в безопасности Android // InternetUA (http://internetua.com/naidena-glavnaya--dira--v-bezopasnosti-Android). – 2014. – 17.10).***