# СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

*Огляд інтернет-ресурсів*
*(9–22.09)*

**2013 № 17**

# Соціальні мережі
## як чинник інформаційної безпеки

**Інформаційно-аналітичний бюлетень**
**Додаток до журналу «Україна: події, факти, коментарі»**
Огляд інтернет-ресурсів
(9–22.09)
№ 17

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

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

**Редакційна колегія:**
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць



Київ 2013

# ЗМІСТ

# РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Российская социальная сеть «ВКонтакте» планирует в среднесрочной перспективе укрепить свои позиции в Перу, где у нее уже есть 30 тыс. пользователей, чтобы в конечном счете обогнать в этой южноамериканской стране Facebook, пишет «Обозреватель» (http://tech.obozrevatel.com/news/98157-vkontakte-reshila-obognat-facebook-po-podpischikam-v-peru.htm).

Об этом заявил в Лиме заместитель генерального директора «ВКонтакте» И. Перекопский.

«Наша цель – достигнуть первого миллиона пользователей (в Перу), а затем нам будет гораздо проще удвоить и даже в пять раз увеличить их число, обойдя, таким образом, поклонников Facebook», – приводит РИА Новости слова И. Перекопского.

По словам представителя «ВКонтакте» в Перу и Латинской Америке Ф. Гонсалеса, к сентябрю 2014 г. компания планирует увеличить число подписчиков до 500 тыс. человек, а в 2015 г. их число в Перу должно составить уже 2 млн. Таким образом, именно эта страна должна стать отправной точкой для экспансии «ВКонтакте» в Латинской Америке.

Напомним, соцсеть «ВКонтакте» вошла в десятку мировых социальных сетей в мае этого года. Соцсеть заняла в майском рейтинге девятое место с показателем 79,4 млн пользователей, что составило 5 % от мировой аудитории соцсетей.

Первое место рейтинга заняла соцсеть Facebook с числом уникальных пользователей 834,8 млн. Доля соцсети в мировой аудитории составила 53 % ***(«ВКонтакте» решила обогнать Facebook по подписчикам в Перу // Обозреватель (http://tech.obozrevatel.com/news/98157-vkontakte-reshila-obognat-facebook-po-podpischikam-v-peru.htm). – 2013. – 7.09).***

***

9 серпня Instagram оголосив, що місячна спільнота активних користувачів соцмережі збільшилася до 150 млн користувачів.

Причому 50 млн людей почали активно користуватися Instagram протягом останніх шести місяців. Спільнота інстаграмщиків стала також більш глобальною – більш ніж 60 % користувачів соцмережі перебувають за межами США.

Чи це документування протестів у Єгипті, чи це подорож через усю територію США, чи це фото домашніх тваринок – спільнота користувачів, вважає команда Instagram, продовжує дивувати нас щодня креативністю, жагою до пригод та неповторним баченням світу ***(Активна місячна аудиторія Instagram сягнула 150 млн користувачів // Watcher (http://watcher.com.ua/2013/09/09/aktyvna-misyachna-audytoriya-instagram-syahnula-150-mln-korystuvachiv/). – 2013. – 9.09).***

***

Facebook предложит пользователям соцсети добавлять на свои страницы информацию о своем профессиональном опыте. Соответствующий блок появится в настройках личной информации, рядом с разделом «Образование и работа», сообщает TheNextWeb. Таким образом, Facebook может составить серьезную конкуренцию LinkedIn.

Заполняя раздел «Профессиональные навыки», пользователи фактически очерчивают сферу своих профессиональных интересов и таким образом тегируют свою страницу по профессиональному признаку; это значит, что работодатели смогут искать подходящих кандидатов прямо в социальной сети.

Ни для кого не секрет, что уже сегодня многие рекрутеры пользуются Facebook для поиска и проверки кандидатов. Хотя соцсеть не ориентирована на поиск работы и сотрудников, она содержит большое количество разноплановой информации о каждом из своих пользователей и потому может помочь составить более полное впечатление о человеке, чем профессиональные сети, такие как LinkedIn.

Вообще-то, это уже не первый шаг Facebook в направлении социального рекрутинга. Около года назад компания объявила о создании на базе соцсети платформы по поиску работы в сотрудничестве с Министерством труда США. Сообщалось, что в отдельном разделе Facebook будут агрегироваться более 1,7 млн вакансий от BranchOut, JobVite и Monsters.com. Приложение было запущено в ноябре 2012 г.

Сегодняшняя новость, уже подтвержденная представителями компании, означает, что Facebook продолжает активную работу в этом направлении. Похоже, LinkedIn стоит всерьез опасаться: с выходом игрока уровня Facebook на этот рынок расстановка сил на нем может кардинально измениться ***(Facebook составит конкуренцию LinkedIn // InternetUA (http://internetua.com/Facebook-sostavit-konkurenciua-LinkedIn). – 2013. – 10.09).***

***

Компания «TNS Россия» опубликовала рейтинг видеоресурсов Рунета. Первую строчку занимает YouTube, за ним следуют соцсеть «ВКонтакте» и сайт «Яндекса». Исследовательская компания также определила самые посещаемые онлайн-кинотеатры, специализирующиеся на показе исключительно видеоконтента. Эксперты полагают, что их аудитория будет расти в связи с принятием антипиратского закона в России.

По месячному охвату аудитории ожидаемо лидирует видеохостинг YouTube, чья посещаемость за июнь 2013 г. составила более 24,5 млн человек. У сети «ВКонтакте» – 19,7 млн человек, а у «Яндекса» – 15,1 млн человек.

Среди легальных онлайн-кинотеатров первое и второе место по количеству пользователей, смотревших видео, занимают Tvigle.ru и

Videomore.ru (6,5 млн и 4,2 млн человек). На третьем месте – видеоконтент Zoomby.ru (3,6 млн человек).

Лидером по месячному охвату аудитории среди онлайн-кинотеатров стал Zoomby.ru (8,9 млн зрителей), затем идут ivi.ru (7,5 млн человек) и Megogo.net (3,7 млн человек).

Согласно данным TNS Web Index за июль 2013 г., в целом около 84 % пользователей Рунета в возрасте от 12 до 64 лет посещают сайты с онлайн-видео. Более популярны только поисковые системы (94 %), социальные сети (94 %) и почтовые сервисы (86 %). При этом по среднему количеству времени в день, проводимом на сайтах, онлайн-видеопорталы находятся на втором месте (16 мин.) после социальных сетей (41 мин.). Торренты использует 37 % аудитории Рунета ***(YouTube стал самым популярным в Рунете сайтом для просмотра видео // Минфин (http://minfin.com.ua/2013/09/10/806884/). – 2013. – 10.09).***

***

Ежедневная аудитория социальной сети «ВКонтакте» превысила 50 млн человек. Об этом 10 сентября сообщил основатель соцсети П. Дуров, передает Лента.ру.

По словам П. Дурова, суточная посещаемость «ВКонтакте» в понедельник, 9 сентября, составила 50,9 млн пользователей. «”ВКонтакте” – не только самая популярная, но и самая быстрорастущая социальная сеть в СНГ», – написал в посте на своей странице П. Дуров. В августе 2012 г., согласно данным TNS Global, средняя суточная аудитория «ВКонтакте» была почти в два раза меньше (порядка 22 млн человек).

Слова П. Дурова подтверждаются статистическими данными и результатами соцопросов. О лидерстве «ВКонтакте» среди российских соцсетей говорит, к примеру, рейтинг, составленный TNS в июле 2013 г., а также рейтинг ComScore, согласно которому «ВКонтакте» по числу уникальных пользователей опережает своего главного конкурента – «Одноклассники» – примерно на 10 млн.

Единственным опросом, показавшим обратную статистику, стал опрос, проведенный «Левада-центром». Его участники назвали самой популярной российской социальной сетью «Одноклассники». О том, что они посещают ресурс, тогда заявили 76 % респондентов. Пользователями «ВКонтакте» назвали себя 58 % опрошенных. По данным comScore, ежедневная аудитория «Одноклассники» в июле 2013 г. составляла примерно 30 млн человек.

Социальная сеть «ВКонтакте» была запущена в 2006 г. и на сегодняшний день является одним из самых посещаемых ресурсов Рунета. В рейтинге российского сегмента сети, составляемом компанией Alexa, «ВКонтакте» уступает по посещаемости лишь «Яндексу» ***(Суточная аудитория «ВКонтакте» превысила 50 миллионов человек // IT Expert (http://itexpert.in.ua/rubrikator/item/29666-sutochnaya-auditoriya-vkontakte-prevysila-50-millionov-chelovek.html). – 2013. – 11.09).***

***

Facebook запустив великі зображення для розшарених лінків. Відтепер Facebook рекомендує og:image size 1200x627px, мінімальний розмір – 560x292px.

Тобто зображення, яке підтягується до лінка, займає усю ширину стрічки новин. Над зображенням відображається текст, уведений безпосередньо у Facebook при публікації лінка, під зображенням – заголовок та лід публікації.

Коли великі зображення стануть доступними для всіх наразі невідомо. Можливо, із цим нововведенням відпаде потреба (і мода) розшарювати лінки шляхом публікування фото і додавання цього лінка як опис до нього ***(Facebook істотно збільшив розмір зображень для розшарених лінків // Watcher (http://watcher.com.ua/2013/09/11/facebook-istotno-zbilshyv-rozmir-zobrazhen-dlya-rozsharenyh-linkiv/). – 2013. – 11.09).***

***

Google+ інтегрує логін через акаунт у соцмережі до Програми авторства Google. Тепер можна залогінитися до якогось сервісу (наприклад, WordPress.com) через Google+ акаунт і опубліковані вами на сервісі статті будуть автоматично пов'язані із вашим Google+ профілем.

Така інтеграція дасть можливість відображати вашу профільну інформацію в екосистемі Google. Наприклад, вже тепер люди можуть бачити ваше ім'я, профільне зображення та/або лінк на ваш Google+ профіль коли ваш контент з'являється у пошуковій видачі.

Ця інтеграція наразі тестується на двох майданчиках – WordPress та Typepad, невдовзі вона запрацює на About.com, WikiHow, Examiner. У результаті тестування такої інтеграції на сайтах різного типу її зможуть поширити на усі сайти, які використовують логін через Google+ акаунт.

У результаті ви, як автор, можете бачити пошукову аналітику для вашого контенту, виділити свій контент у пошуковій видачі та дати можливість людям знайти через вас як автора інші ваші публікації. Крім того, якщо вам це важливо, ви зможете отримати більше фоловерів у Google+.

Раніше Програма авторства Google дозволяла приєднати ваш Google+ профіль з контентом, який ви створюєте, лише в ручному режимі – або через підтвердження електронної скриньки в тому ж домені або через розміщення підтверджувального коду на відповідному сайті ***(Google+ інтегрує логін через акаунт у соцмережі до Програми авторства Google // Watcher (http://watcher.com.ua/2013/09/12/google-intehruye-lohin-cherez-ekaunt-u-sotsmerezhi-do-prohramy-avtorstva-google/). – 2013. – 12.09).***

***

В веб-версии социальной сети Google+ появились инструменты для редактирования загруженных пользователями фотографий. Об этом сообщил на своей личной странице сотрудник Google Д. Хафтел.

Чтобы внести корректировки в снимок, нужно открыть фотографию и нажать кнопку «Изменить». Пользователи могут менять яркость, контраст и насыщенность всей фотографии или выбранной области, повышать резкость, вращать и обрезать снимок и применять к нему цветовые эффекты.

В основе редактора лежат разработки компании Nik Software, которую Google купила в сентябре 2012 г. Технологии Nik Software также используются в мобильных фоторедакторах Snapseed и – с марта 2013 г. – в приложениях Google+ для платформ Android и iOS.

Фоторедактор в веб-версии Google+ работает только в браузерах Chrome. Google объясняет это тем, что инструменты для редактирования фото созданы с применением технологии Native Client, предназначенной для запуска в браузере нативного кода. Технологию не поддерживают другие обозреватели.

Ранее, в мае 2013 г., Google включила в состав Google+ инструмент Auto Enhance. Он автоматически улучшает качество фотографий, размещаемых пользователями в социальной сети ***(В соцсеть Google+ встроили фоторедактор // InternetUA (http://internetua.com/v-socset-Google--vstroili-fotoredaktor). – 2013. – 13.09).***

***

Сервис микроблогов Twitter вводит новый фильтр, с помощью которого авторизованные пользователи, в том числе знаменитости, смогут отсеять спам и ответы незнакомых людей, сообщается в блоге Twitter.

Упоминания пользователя в сети Twitter будут с помощью фильтра разделены на категории «Отфильтрованы» и «Авторизованные». В первую категорию попадут все упоминания за исключением спама. Во вторую же – только ответы и упоминания других авторизованных пользователей Twitter.

Таким образом, знаменитости, чьи записи в Twitter получают сотни комментариев и упоминаний от незнакомых людей, получат возможность общаться в сети только со своими друзьями, которые также имеют авторизованные аккаунты.

По словам создателей, фильтр находится на стадии разработки, в том числе готовится мобильная версия.

Для Twitter, который получает значительный доход от рекламы, выгодно наличие в сети аккаунтов знаменитостей, на которые подписаны тысячи обычных пользователей ***(Новый фильтр Twitter позволит «звездам» общаться друг с другом // InternetUA (http://internetua.com/novii-filtr-Twitter-pozvolit--zvezdam--obsxatsya-drug-s-drugom). – 2013. – 15.09).***

***

Компанія Facebook заявила про можливість зниження вартості інтернет-підключення у 100 разів. Соціальна мережа хоче збільшити ефективність передачі даних. Про це повідомляється в офіційному блозі адміністрації.

Команда Facebook планує розробити нові технології стиснення і передачі даних. Трафік можна збільшити на 500 % без додаткових витрат за рахунок існуючих серверів. Адміністрація соцмережі впевнена, що збільшення трафіку дасть можливість підключитися до Інтернету кожному власникові мобільного телефону.

Компанія буде вести розробки в межах проекту Internet.org. У ньому також візьмуть участь компанії Ericsson, MediaTek, Nokia, Opera, Qualcomm і Samsung. Розробники планують домогтися поставлених цілей протягом 5–10 років.

Нині соцмережею користується 1 млрд населення Землі. За підрахунками експертів, всього доступ до Інтернету мають 2,7 млрд осіб ***(Facebook обіцяє знизити вартість підключення до інтернету у 100 разів // iPress.ua (http://ipress.ua/news/facebook_obitsyaie_znyzyty_vartist_pidklyuchennya_do_internetu_u_100_raziv_28336.html). – 2013. – 17.09).***

***

Социальной сетью Facebook пользуется уже больше половины мировой аудитории Интернета. Но самыми быстрыми темпами растет число посетителей сервисов Pinterest и Tumblr, передает vedomosti.ru.

Более 50 % активной аудитории Интернета в мире пользуется социальной сетью Facebook – такая статистика приводится в отчете инвестбанка Citi со ссылкой на данные GlobalWebIndex. Доля Google+ среди активной аудитории – 26 %, видеохостинга YouTube (принадлежит Google) – 25 %, Twitter – 22 %, китайской Sina Welbo – 21 %.

Но по темпам роста аудитории лидируют другие социальные сервисы. На первом месте здесь Pinterest, чьи пользователи размещают в своих профилях изображения и собирают из них тематические коллекции. По данным GlobalWebIndex за II квартал 2013 г., на которые ссылается Citi, аудитория Pinterest за год возросла более чем на 80 %. По оценке другой аналитической компании – Semiocast, в июле 2013 г. она достигала 70 млн пользователей.

Высокие темпы роста Pinterest объясняются эффектом низкой базы – сервис работает всего три года, говорит предправления «Финама» В. Кочетков. Это одна из немногих новых соцсетей, рассчитанных на специфическую хипстерскую аудиторию, куда пришли крупные бренды. Теперь эти бренды генерируют для Pinterest новую аудиторию, включая в свои глобальные рекламные кампании ссылки на собственные страницы в этой соцсети, продолжает он. Тем не менее, по данным Socialbakers, рекламодатели предпочитают все-таки крупные соцсети Facebook, YouTube, Twitter и LinkedIn.

На втором месте по темпам роста аудитории – сервис микроблогов Tumblr, недавно приобретенный Yahoo! за 1,1 млрд дол. Его аудитория выросла за год более чем на 74 % – в июле, по данным comScore, она составила 38,37 млн пользователей. Twitter четвертый по темпам роста

аудитории, он уступает индонезийской соцсети Mig33. По данным GlobalWebIndex, за год аудитория Twitter увеличилась более чем на 40 % и составила, по собственным данным Twitter, более 200 млн пользователей.

По количеству активных пользователей лидируют Facebook, Twitter, Google+, Pinterest и LinkedIn, следует из отчета Citi. У Facebook самая большая активная база – 62 % от всей ее аудитории. Доля активных пользователей Twitter – 49 %, Google+ – 44 %, Pinterest и LinkedIn – по 39 %. Facebook и Twitter – состоявшиеся проекты, ими пользуется множество известных людей, которые в том числе и поддерживают высокую активность в этих сетях, объясняет В. Кочетков. А высокую активность пользователей Google+ он связывает больше с интеграцией всех сервисов Google: например, если человек делает фотографию с помощью смартфона под управлением операционной системы Google Android, она может быть автоматически опубликована и в Google+.

В данных Citi и GlobalWebIndex фигурируют и российские социальные сети – «ВКонтакте» и «Одноклассники». «ВКонтакте» оказалась на восьмом месте по темпам роста аудитории, обогнав Facebook (занявшую девятое место). За год аудитория крупнейшей российской соцсети увеличилась почти на 20 %. «Одноклассники», напротив, потеряли около 15 % мировой аудитории. Представитель Mail.ru Group (контролирует «Одноклассники») К. Чабаненко с этими данными не согласна – аудитория обеих соцсетей росла, причем «Одноклассники» весь год обгоняли «ВКонтакте» по темпам роста. В самом деле, по данным comScore, во II квартале 2013 г. аудитория «ВКонтакте» возросла к аналогичному периоду 2012 г. на 11,43 %, а «Одноклассников» – на 20,32 % ***(Соцсетью Facebook пользуется больше половины пользователей Интернета // IT Expert (http://itexpert.in.ua/rubrikator/item/29918-sotssetyu-facebook-polzuetsya-bolshe-poloviny-polzovatelej-interneta.html). – 2013. – 19.09).***

***

Видеохостинг YouTube анонсировал новую функцию, которая позволит смотреть загруженные заранее видео без подключения к Интернету, пишет «Обозреватель» (http://tech.obozrevatel.com/news/17560-youtube-mozhno-budet-smotret-offline.htm).

Как говорится в посте, возможность смотреть видео offline будет доступна только для пользователей мобильных приложений YouTube.

Функция офлайн-просмотра, по словам представителей видеохостинга, станет доступна в ноябре 2013 г. ***(YouTube можно будет смотреть offline // Обозреватель (http://tech.obozrevatel.com/news/17560-youtube-mozhno-budet-smotret-offline.htm). – 2013. – 18.09).***

# СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Кабинет министров Ирана в полном составе завел себе страницы в социальной сети Facebook, несмотря на запрет данного сервиса в стране, пишет «Обозреватель» (http://tech.obozrevatel.com/news/87569-ministryi-irana-zaregistrirovalis-na-facebook.htm).

Кроме этого, в Facebook появилась страница администрации иранского президента.

Эксперты полагают, что данный шаг может свидетельствовать о готовности иранского правительства в скором времени снять ограничения на использование Интернета в стране.

Иранские власти ввели запрет на пользование Facebook после массовых беспорядков в 2009 г., когда противники переизбранного президентом М. Ахмадинежада использовали эту соцсеть для организации своих сторонников.

Напомним, летом этого года власти Ирана объявили об открытии национального сервиса электронной почты. Каждому жителю страны был выделен собственный адрес электронной почты. Управляет ресурсом почтовая служба Ирана ***(Министры Ирана зарегистрировались на Facebook // Обозреватель (http://tech.obozrevatel.com/news/87569-ministryi-irana-zaregistrirovalis-na-facebook.htm). – 2013. – 9.09).***

***

У американского космического агентства NASA появился официальный аккаунт в Instagram. Об этом сообщила пресс-секретарь агентства Л. Уорли.

По слова Л. Уорли, NASA постоянно стремится к расширению собственного присутствия в социальных сетях. Ранее страницы NASA уже были созданы в Facebook, Twitter, YouTube, Foursquare и Google+. «Мы постоянно ищем новые способы рассказать людям удивительную историю исследований и открытий NASA и нам не терпится поделиться с пользователями Instagram нашими лучшими фотографиями, сделанными на земле и из космоса», – сказала Л. Уорли.

Первая фотография (снимок Земли из космоса, сделанный с борта Apollo 11 в 1969 г.) была размещена в аккаунте 6 сентября 2013 г. За несколько дней подписчиками аккаунта стали более 80 тыс. пользователей Instagram.

Сервис Instagram был запущен в 2010 г. Приложение позволяет делиться в Интернете фотографиями и короткими (до 15 секунд) видеороликами. Каждый месяц сервисом пользуются около 150 млн человек по всему миру ***(У NASA появился аккаунт в Instagram // InternetUA***

***(http://internetua.com/u-NASA-poyavilsya-akkaunt-v-Instagram). – 2013. – 9.09).***

***

Facebook запустив два інструменти, які дадуть змогу великим медіа відслідковувати про що говорять користувачі в режимі реального часу.

Перший – Keyword Insights API, тобто доступ до статистики ключових слів. Ця статистика дасть можливість відслідковувати кількість згадок ключових слів у соцмережі, а також демографічні дані за віком, статтю, локацією та спільнотами, які активно обговорюють теми за цими ключовими словами. Статистика буде доступна за якись заданий період часу. Ці дані будуть анонімними.

Другий інструмент – Public Feed API, доступ до стрічки усіх публічних публікацій у Facebook. Тут будуть доступні публічні публікації від сторінок, а також акаунтів з увімкненою опцією Follow. Ці інструменти вже доступні Buzzfeed, CNN, NBC's Today Show, BSkyB, Slate та Mass Relevance.

Відтепер ці великі медіа можуть інтегрувати Facebook-обговорення до своїх новин через відображення публічних публікацій у режимі реального часу за будь-якою темою. Наприклад, ці медіа завжди можуть оприлюднювати що говорять люди про ті чи інші гарячі новини, звідки ці люди, якого вони віку, скільки їх тощо.

Репрезентативність і доцільність відслідковування цих даних Facebook проілюстрував інфографікою про Facebook і телебачення, яка має показати як активно в соцмережі обговорюють те, що показують по телевізору. Тобто якщо десь щось відбувається цікаве – про це обов'язково говорять у Facebook, і за кількістю обговорень можна судити за важливістю і трендовістю якоїсь теми.

Facebook розпочинає перемовини з іншими партнерськими медіа та маркетинговими розробниками і почне надавати доступ до цих API додатковим партнерам у найближчі кілька тижнів. Також ви можете переглянути документацію для Public Feed API та документацію для Keyword Insights API ***(Facebook відкрив для великих медіа статистику ключових слів у реальному часі // Watcher (http://watcher.com.ua/2013/09/10/facebook-vidkryv-dlya-velykyh-media-statystyku-klyuchovyh-sliv-u-realnomu-chasi/). – 2013. – 10.09).***

***

В соцсети «Одноклассники» появились страницы городов, модераторами которых могут стать пользователи, сообщила Mail.Ru Group.

На страницу своего города пользователи могут перейти, кликнув по названию города, расположенному рядом со своим именем. Сегодня сервис доступен для 13 крупных городов, среди которых Новосибирск, Самара, Рига, Астана, Краснодар, Нижний Новгород, Баку, Минск и Ташкент. Жители этих городов могут опубликовать на их страницах фотографии

интересных мест и местные новости, например, об изменении автобусного маршрута или премьере спектакля.

В настоящее время, по статистике «Одноклассников», в Екатеринбурге в соцсети зарегистрированы более миллиона пользователей, в Ташкенте – более 975 тыс. человек, в Минске – более 715 тыс. ***(Страницы городов появились в «Одноклассниках» // InternetUA (http://internetua.com/stranici-gorodov-poyavilis-v--odnoklassnikah). – 2013. – 12.09).***

***

Є контакт: як місцева влада в Україні опановує соцмережі і чим ділиться в них із громадянами.

Від того часу, як соціальні мережі почали наступ на інтернет-простори країн світу, минуло зовсім небагато років, проте перелік їхніх функціональних можливостей та охоплених ними сфер життя стрімко зростав. Із простої офісної забавки соціальні мережі стали потужною платформою для обміну професійним досвідом, розміщення реклами, згуртування однодумців з усього світу, пошуку роботи, отримання інформації про останні події світу, налагодження необхідних зв'язків, більше того – вони стали сферою діяльності, яка поповнила ринки праці новими професіями. Урешті-решт − кана лом передвиборної агітації, на зміну телебаченню та газетам. Так, приміром, за словами політтехнологів, Б. Обама здобув перемогу на виборах саме завдяки масштабній кампанії у соцмережах. І саме цей потенціал соціальних мереж ще поки недостатньо реалізовано в Україні, як показали минулорічні парламентські вибори. А оскільки наступні вибори, що чекають на українців, стосуватимуться місцевої влади, редакція RegioNews вирішила дізнатися, як очільники областей та міст, а також їхні адміністрації, виходять на контакт із виборцями через соціальні мережі.

Серед українських та й узагалі світових політиків, мабуть, не знайдеш людини, яка б не висловлювала переконання, що народний обранець повинен бути ближчим до свого виборця та усіх громадян, за чий добробут він несе відповідальність. Особливо це завжди стосувалося місцевої влади, результати роботи якої важко представити інакше, ніж вони є. Зазвичай про те, що «назріла необхідність» поспілкуватися з громадою, посадовці згадують, коли на горизонті маячать чергові вибори і водночас починають «ворушитися» конкуренти.

Незважаючи на те, що Україна живе в стані перманентних виборів, депутати полишають свої крісла й приходять нові, кілька разів кардинально змінювався кістяк влади, а виборці відстежили не один політичний шлях своїх обранців, – партійні програми та передвиборні обіцянки не зазнають якихось особливих змін. Як і ті сфери, яким кандидати обіцяють підйом. Саме тому і рівень недовіри до політиків зростає з року в рік, про що свідчать і численні соцопитування, і показники явки на кожних наступних виборах, і слабенькі та нечисленні акції протестного електорату. І стикаючись із використанням тих самих методів та технологій, виборці вже передбачають результат із попереднього гіркого досвіду. Сезонний характер зустрічей із

народом та мінімальних «добрих справ» також вже не викликає жодних сумнівів. І незважаючи на це, методи завоювання електорату в Україні не змінюються, хоча прохолодна реакція на них серед виборців показує, що громадяни виробили стійкий імунітет до підгодовування, голосних гасел, концертів поп-зірок на підтримку кандидатів тощо. Зі свого боку, політтехнологи в Україні наполягають на тому, що ці механізми є дієвими, проте до роботи з ними потрібно докладати набагато більше зусиль, ніж на це спроможна більшість політиків.

Утім, все ж деякі зміни відбуваються серед звичного набору каналів інформації, через які посадовці та депутати намагаються заявити про себе. Так, у минулорічній передвиборній кампанії вперше великі сподівання покладалися на роботу соціальних мереж, щоправда, переважно серед опозиції. Це, по суті, і принесло єдину несподіванку за результатами виборів для більшості політтехнологів – соціальні мережі не спрацювали. Знову ж таки, за словами експертів, через недостатню роботу з ними.

Однак у потенціалі соціальних мереж переконані сьогодні більшість експертів – політтехнологів, піарників, рекламістів, соціологів. Єдине, що ніхто з них не береться точно стверджувати, коли цей потенціал буде реалізовано в Україні. У нинішньому ж вигляді соціальні мережі ще поки слабо виконують функції активізації електорату, натомість допомагають повільно встановлювати хоч якісь більш-менш сталі зв’язки з аудиторією, спостерігати її настрої. Адже, по суті, це єдиний канал інформації, який з однаковою силою притягує до політичної сили чи діяча як палких прихильників, так і запеклих противників, тоді як будь-які канали ЗМІ, чи то газети, чи то телепрограми, формують аудиторію лише з прихильників – тих людей, яких не дратує викладена інформація і вони готові погоджуватися з нею за неможливості розв’язати дискусію чи висловити своє ставлення до предмета обговорення.

Плюсом для будь-якого здобувача народної прихильності при цьому є те, що негативні відгуки, які з’являються на сторінці у соціальній мережі, можна брати до уваги та видаляти, ще й позбавляючи автора можливості знову будь-що коментувати. Тому можна мати абсолютно «позитивну» сторінку, проте паралельно вести для себе облік усіх критичних зауважень.

Як уже було зазначено вище, кампанія у соцмережах до минулорічних парламентських виборів не виправдала покладених на неї сподівань. Проте відмовлятися від цієї схеми ніхто не планує, і очевидно, що до наступних виборів, місцевих, українська влада зміцнить свої позиції у соціальних мережах. Як відбувається цей процес, які обласні державні адміністрації та міські ради, а також хто серед їхніх очільників вже розгортає роботу у «Фейсбуках» та «Твіттерах», і вирішила пересвідчитися редакція. Для цього ми розіслали запити із посиланням на закон про доступ до публічної інформації до відповідних управлінь, а також самостійно вдалися до пошуків у соцмережах.

Отже, за результатами пошуків та відповідями на запити, українська влада на місцях найбільше представлена в мережі Facebook – 40 сторінок

загалом. Удвічі менше сторінок створено в російському «ВКонтакте» – 20. Ще менше – 15 сторінок – існує у мережі Twitter. І лише п’ять акаунтів заведено в мережі Google+.

На думку експертів, поки що сторінки політиків та чиновників у соціальних мережах стають об’єктами пильної уваги насамперед політичних опонентів та журналістів, які бачать для себе багато переваг у такому способі здобувати інформацію. Так, на відміну від решти того, що опубліковано в Інтернеті, пости високопосадовців у соцмережах є інформацією з перших вуст, унікальним та водночас максимально доступним матеріалом. А будь-яка категорична заява чи сміливе висловлювання посадовця в соцмережі можуть відіграти роль інформаційного приводу, роздмухування якого іноді позбавляє журналіста від необхідності самому відшукувати тему і збирати під неї коментарі публічних діячів, пробиваючись через лави прес-служб, офіційних запитів, безкінечних правок і узгоджень. Зі свого боку, полювання журналістів на унікальний та свіжий контент грає на руку власника сторінки у позитивному медіа-висвітленні, оскільки він може порушувати ті теми, які вигідні для нього, його політичної сили чи адміністрації.

Утім, є ще одна причина, пов’язана з діяльністю ЗМІ, яка мотивувала голову уряду закликати чиновників до активної роботи в соцмережах, – бажання скоротити на зібраннях та заходах влади присутність журналістів, яка часто виливається у скандали та акції. Тому всю необхідну інформацію від посадовців співробітники медіа отримуватимуть зі спілкування в соцмережах.

Утім, незважаючи на переваги від такого спілкування й можливості вигідного висвітлення своєї діяльності, велика кількість політиків та місцевих управлінців все ще зволікають з реєстрацією в соцмережах. Що змушує їх втримуватися від такого кроку та яке значення для формування позитивного іміджу відіграють, пояснили RegioNews експерти– президент групи SA Political Communications та голова асоціації зовнішньої реклами України А. Біденко і віце-президент Української PR-Ліги О. Дерев’янко.

А. Біденко: «Відсутність чиновників у соцмережах можна пояснити, по-перше, віковою причиною, а по-друге, тим, що у більшості, мабуть, немає “продвинутих” консультантів, які могли б пояснити переваги використання соцмереж. Крім того, люди в основному користуються соцмережами, як чимось приватним, особливо не поширюючи їх на своє публічне життя. Тільки одиницям вдається поєднувати публічне та приватне, грубо кажучи, розміщувати такі фотографії, за які не буде потім соромно.

Я б не перебільшував значення соцмереж для іміджу, особливо в нашій країні. Але років через десять це буде одним із джерел знань про людей, зокрема й тих, яких ми наймаємо на держслужбу. Тому вже сьогодні необхідно вирощувати експертів, які зможуть, подібно до того, як в 19-му сторіччі людей вчили французької та гарним манерам, навчити правильно користуватися Facebook, Twitter або Instagram».

О. Дерев’янко: «Ми живемо в суспільстві, де чисельність громадян-резидентів тих чи інших соціальних мереж стрімко зростає. Ігнорувати цю

тенденцію влада не має право. Однак усвідомлення потреби у прямому діалозі з громадою не завжди означає перехід до практичних дій.

По-перше, перешкодами є іманентно притаманні чиновництву обережність і відсутність звички звітувати за свої дії, відповідаючи на критику в режимі реального часу. А по-друге, існують випадки, коли краще не мати взагалі інтернет-представництва в соцмережах, ніж перетворити цей сучасний інструмент комунікації у посміховисько – мертвий пропагандистський рупор радянського зразку або недолугу імітацію прозорості та відкритості влади. Не кажучи вже про те, що соціальні мережі громадяни розглядають як таку собі інтерактивну книгу скарг. І відкриваючи на своїй сторінці опцію зворотного зв'язку, чиновники ризикують тим, що будуть одержувати звернення, які не захочуть або об'єктивно не зможуть задовольнити (наприклад, землевідведення у регіонах з високою вартістю ділянок – Крим, Київщина, рекреаційні зони Західної України). Тим самим збільшуючи частку людей, розчарованих діями того чи іншого органу державної влади. А отже, електоральну підтримку діючої владної команди.

Інтернет-спільнота дуже чутлива до фальші і нещадна до її проявів. Тому неадекватно сконфігурована сторінка в соцмережі може завдати більше шкоди, ніж цілковите ігнорування цього сегмента віртуального простору».

− Як наявність або відсутність їх у соцмережах впливає на їхній імідж?

О. Дерев'янко: «Потрібно розмежувати імідж політиків, що займають державні посади, та органів влади, як таких. Для органу влади наявність чи відсутність сторінки важлива, але не надто – бо вона є соцмережевим аналогом офіційного сайту.

Водночас для політика-чиновника вдала комунікація з громадою може стати інструментом зміцнення позицій у владній вертикалі та поліпшення іміджу в очах громадян. При цьому може буде обрана будь-яка стратегія: від створення державницького образу "батька краю" через фамільярний образ "свого хлопця" до майже ексгібіціоністської акцентуації моментів особистого життя. Тут справа смаку – головне, щоб соцмережі не жили окремо від інших репутаційутворюючих активностей.

Але "може" – не означає "буде". Тому що краще нічого не робити, ніж робити не професійно, не враховуючи репутаційних ризиків, які несе інтеграція у світ соцмереж.

На жаль, зараз є не досить розумна тенденція, коли ідеологічні "верхи" у буквальному сенсі примушують місцеві органи влади створювати сторінки у соцмережах, не аналізуючи можливі негативні наслідки. А робота "з під палки" ні до чого доброго ніколи не доводила. Тож я категорично проти соцмережевої "зрівнялівки", процес має відбуватися органічно, послідовно, з забезпеченням балансу всіх "за" та "протии"».

− Більш ніж у половини представників місцевої влади немає сторінок у соцмережах. З чим Ви це пов'язуєте?

О. Дерев'янко: «У більшості випадків – з вищезгаданою обережністю та небажанням власноруч наражатися на неприємності, які неминучі при розмові з народом віч-на-віч. Рідше – з відсутністю ресурсів: організаційних,

фінансових, особистісних (харизми) тощо. І, на жаль, ще рідше – з усвідомленням того, що професійно зробити не можемо, а аби як – не хочемо. Але з урахування останніх примусових тенденцій, ми, імовірно, матимемо можливість вже найближчим часом проаналізувати багато цікавих кейс-сторі про соцмережевий успіх чи соцмережеву ганьбу тих чи інших чиновників».

***

Отже, як бачимо, поки що голови міст та областей не дуже охоче опановують соціальні мережі. Значна частина їх узагалі не має персональних сторінок у жодній з мереж, а більшість зареєстрованих не відзначаються високою активністю. Водночас політтехнологи радять їм не впускати можливість спілкування з громадськістю в режимі реального часу і пророкують велику роль соцмережам у вибудовуванні політичних та виборчих кампаній. А за деякими прогнозами, через кілька років в Україні кандидати матимуть можливість повністю реалізувати успішну передвиборну агітацію та кампанію через соціальні мережі, не вдаючись до старої доброї «гречки» ***(Є контакт: як місцева влада в Україні опановує соцмережі і чим ділиться в них із громадянами // Інформаційне агентство «Регіональні Новини» (http://regionews.ua/node/113018). – 2013. – 12.09).***

***

Председатель Днепропетровского облсовета Е. Удод завел страницу в социальной сети Facebook, сообщает IT Expert со ссылкой на «Укринформ».

«Идея зарегистрироваться в Facebook пришла после того, как появилась потребность общаться и обсуждать свои проекты и идеи с большим количеством людей», – написал на своей странице Е. Удод.

По его мнению, соцсеть позволит большему количеству людей приобщиться к обсуждению и участию в важных социальных проектах, которые реализуются на Днепропетровщине.

Среди первых сообщений Е. Удод разместил подборку фото и информацию о приобретении современной коммунальной техники в рамках проекта «Красивый город».

«Сегодня управлял экскаватором. В работе председателя облсовета иногда есть такие маленькие радости. Передал 10 машин для борьбы со снегом. А до конца года будет больше сотни, от снегоуборщиков до подметальщиков и пылесосов», – добавил он.

Е. Удод стал третьим председателем облсовета, который «прописался» в соцсетях.

Как сообщал Укринформ, среди региональных чиновников свои аккаунты и страницы в соцсетях имеют также восемь председателей облгосадминистраций. Самые активные пользователи – С. Татусяк, М. Вышиванюк и М. Добкин.

Самыми активными пользователями соцсетей среди мэров украинских городов являются городские головы Харькова, Днепропетровска, Одессы,

Львова и Сум. В то же время 12 мэров не имеют страниц в соцсетях ***(Еще один председатель облсовета завел страницу в Facebook // IT Expert (http://itexpert.in.ua/rubrikator/item/29846-eshche-odin-predsedatel-oblsoveta-zavel-stranitsu-v-facebook.html). – 2013. – 17.09).***

***

Симферопольская милиция, благодаря социальным сетям, разыскала родителей потерявшегося ребенка. По сведениям отдела по связям с общественностью Главного управления МВД в Крыму, в милицию пришел горожанин, который рассказал, что видел пятилетнего мальчика, катавшегося на велосипеде без присмотра взрослых.

Мужчина спросил у ребенка, где его родители, на что ребенок ответил, что не знает, так как потерялся. На место приехал сотрудник подразделения милиции по делам детей. Заявлений об исчезновении детей в тот день не поступало. Мальчик помнил свои данные, а также имена родителей, но домашнего адреса или номеров телефонов не знал. Милиционер начал искать родителей ребенка через социальные сети.

Милиционер ввел в информационную базу данные отца ребенка и установив, что он прописан в селе Залесье Симферопольского района, повез мальчика домой. На момент приезда милиционера родители обнаружили исчезновение сына и подняли на его поиски знакомых и соседей, но в милицию не сообщили. В отношении отца ребенка за ненадлежащее выполнение обязанностей по воспитанию ребенка был составлен административный протокол ***(Симферопольский милиционер обнаружил в социальной сети родителей ребенка // УРА-Информ (http://crimea.ura-inform.com/2013/09/18/28414). – 2013. – 18.09).***

***

Американский окружной апелляционный суд постановил 18 сентября, что нажатие кнопки «лайк» на сайте социальной сети Facebook является проявлением свободы слова и поэтому должно защищаться в соответствии с нормой, закрепленной в первой поправке конституции США, пишет «Обозреватель» (http://tech.obozrevatel.com/news/54021-sud-ssha-zaschitil-lajk-na-facebook.htm).

Этим решением суд поддержал иск бывшего заместителя шерифа из штата Вирджиния, который был уволен за то, что «лайкнул» на Facebook страничку конкурента своего шефа на выборах городского шерифа, пишет РИА Новости.

Согласно решению суда, нажатие кнопки «лайк» является «эквивалентом выставления политических символов перед фасадом своего дома», что Верховный суд США считает проявлением свободы слова.

Суд нижестоящей инстанции в прошлом году отказал истцу в удовлетворении его иска, что «лайк» не является в достаточной степени весомым действием, заслуживающим конституционную защиту. При этом

судья, принявший это решение, указал, что действие первой поправки конституции распространяется на сообщения в социальной сети, но в отличие от «лайка» эти сообщения являются «реальными заявлениями».

Представители компании Facebook отреагировали на решение суда, заявив, что они «рады, что суд признал необходимым защищать “лайк” на Facebook первой поправкой конституции».

Напомним, ранее в Германии директора одного из банков уволили с работы за «лайк» в Facebook, который женщина поставила под постом своего мужа, в котором он якобы оскорблял руководство финучреждения ***(Американский суд защитил «лайк» на Facebook // Обозреватель (http://tech.obozrevatel.com/news/54021-sud-ssha-zaschitil-lajk-na-facebook.htm). – 2013. – 19.09).***

***

Около 30 % всего исторически значимого контента исчезает из социальных сетей в течение двух лет. Об этом, со ссылкой на исследование ученых из американского университета в Норфолке, 19 сентября сообщил сайт Techonology Review.

Ученые проанализировали шесть исторически значимых событий, случившихся в период с июня 2009 по март 2012 г. – от получения Б. Обамой Нобелевской премии и египетской революции до выборов в Иране и гражданской войны в Сирии. В результате, удалось установить, что ссылки на сайты и посты в социальных сетях, посвященные этим событиям, в каждом третьем случае выдают ошибку. Как говорится в исследовании, 27 % таких постов либо меняют адрес, по которому они располагаются, либо вообще удаляются из соцсетей.

Причем, как выяснили ученые, чем старше социальная сеть, тем больше важного контента она теряет. Довольно высок также и процент потерь общей информации, не привязанной к тому или иному общественно-политическому событию, – каждый день из соцсетей исчезает примерно 0,02 % такого контента. Таким образом, за год Twitter, Facebook и другие соцсети теряют более семи процентов опубликованной в них информации.

Такие популярные социальные сети, как Twitter и Facebook по мере своего роста все чаще становятся не только средствами общения, но и важными общественно-политическими инструментами. В 2010–2012 гг. соцсети сыграли значительную роль в революционных событиях в Тунисе, Алжире и Египте, став главным средством коммуникации между протестующими и основным источником информации о происходящих событиях. По данным Pew Research, Facebook и Twitter для обсуждения политической ситуации в стране используют около 65 % жителей Египта и Туниса ***(Около 30% исторического контента исчезает из соцсетей за два года // Подробности.UA (http://podrobnosti.ua/internet/2013/09/19/931163.html). – 2013. – 19.09).***

***

Какая польза от Facebook? Можно делать фотографии еды или своих ног, а другие пользователи будут ставить им «лайки». А можно помочь человеку остаться в этом мире – и для этого соцсеть проводит небольшой ликбез.

Сентябрь 2013 г. был объявлен месяцем предотвращения самоубийств, и в его рамках Facebook поместит публичные объявления для пользователей в Канаде, США и Великобритании, которые будут состоять из инфографики, показывающей, как помочь другому человеку, который решил расстаться с жизнью.

По словам директора по безопасности Facebook Д. Салливана, компания предана делу предотвращения самоубийств, соединяя людей с ресурсами и другими людьми, способными помочь в трудной ситуации. Он отметил, что в сети есть специальные инструменты, помогающие выполнить эту задачу.

Д. Салливан напоминает, что пользователи Facebook всегда могут отметить настораживающий пост, сделать поиск по слову «самоубийство» в самой сети, чтобы обнаружить нужные ресурсы, или посетить страницу помощи для того, чтобы получить больше информации ***(Facebook помогает предотвращать самоубийства // InternetUA (http://internetua.com/Facebook-pomogaet-predotvrasxat-samoubiistva). – 2013. – 22.09).***

## БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Сервис микроблогов Twitter объявил о покупке рекламообменной компании MoPub, занимающейся также разработкой и продажей мобильной рекламы, передает «Обозреватель» (http://finance.obozrevatel.com/economy/63827-twitter-sovershil-krupnejshuyu-sdelku-v-svoej-istorii.htm).

Отмечается, что сотрудник этой компании должны заняться усовершенствованием рекламной платформы Twitter и созданием автоматизированной системы покупки рекламы, позволяющей контролировать стоимость и объем рекламного размещения в режиме реального времени.

Эта сделка, по информации The Financial Times, является крупнейшей в истории данной социальной сети. Со ссылкой на источники издание сообщает, что ее сумма могла составить от 300 до 400 млн дол.

MoPub была основана в 2010 г. Площадка MoPub Marketplace, созданная компанией, позволяла клиентам управлять своей рекламой на мобильных платформах iOS и Android, а также покупать друг у друга рекламные размещения на специальном онлайн-аукционе. Через MoPub в сети ежегодно размещалось более 2 млрд рекламных сообщений ***(Twitter совершил крупнейшую сделку в своей истории // Обозреватель***

***(http://finance.obozrevatel.com/economy/63827-twitter-sovershil-krupnejshuyu-sdelku-v-svoej-istorii.htm). – 2013. – 10.09).***

***

Фотосервис Instagram планирует начать продажу рекламы в течение ближайшего года. Об этом со ссылкой на операционного директора Instagram Э. Уайт 8 сентября сообщила газета The Wall Street Journal, передает портал «Лента.ру».

Сервис до сих пор не размещал рекламных постов и не продавал рекламы, однако вскоре пришедшая из Facebook Э. Уайт намеревается изменить текущее положение дел. «В краткосрочной перспективе никакого давления по поводу монетизации мы не испытываем, однако в долгосрочной перспективе мы хотели бы зарабатывать», – сказала Э. Уайт в интервью американскому изданию.

Э. Уайт также сообщила, что за несколько месяцев ежемесячная аудитория Instagram возросла более чем на 15 % и в настоящее время составляет порядка 150 млн пользователей.

В декабре 2012 г. Instagram заявил о внесении в пользовательское соглашение изменений, которые оставляли бы за сетью право использовать изображения и данные пользователей в рекламных целях. Сами авторы изображений при этом, согласно новым правилам, не получали никакой компенсации. После возмущения многих пользователей сервиса подобными изменениями основатель Instagram К. Систром извинился за вызвавший бурную реакцию пункт соглашения и обещал исправить ошибку ***(Instagram в течение года начнет продавать рекламу // IT Expert (http://itexpert.in.ua/rubrikator/item/29589-instagram-v-techenie-goda-nachnet-prodavat-reklamu.html). – 2013. – 9.09).***

***

Facebook не готов предоставить возможность для видеорекламы, о которой компания говорит маркетологам на протяжении года. Но компания планирует определить влияние видеорекламы в новостной ленте пользователей.

В ближайшем времени небольшие группы пользователей Android в США смогут смотреть видео, которые будут автоматически запускаться в ленте новостей. Пользователям нужно просто кликнуть на видео, активировать звук – и видео откроется на их телефонах в полноэкранном формате. Тем не менее, видео, которые публикуются на страницах брендов, не будут загружаться автоматически, даже для тех, кто по своему желанию подписан на страницу.

Если компании покупают видеопост для показа на своей странице, пользователи всё равно должны будут кликнуть на play и запустить видео.

Цель Facebook – получить больше данных и усовершенствовать опыт использования видеорекламы, исследуя, как потребители взаимодействуют с некоммерческими видео.

Встроенные ссылки с YouTube или Vimeo не будут автоматически запускаться в отличие от видео из приложений SocialCam, Cinemagram, Snapshot и CameraAwesome, которые напрямую загружены на Facebook.

В отличие от рекламных видео, видео пользователей не будет ограничено только 15 с. Оно будет обрезано до 20 мин., как в случае с существующими видео на Facebook ***(Facebook тестирует автоматическое воспроизведение видео // Marketing Media Review (http://mmr.ua/news/id/facebook-testiruet-avtomaticheskoe-vosproizvedenie-video-36123). – 2013. – 13.09).***

***

Оставить страницу в социальной сети закрытой или дать возможность пользователям размещать на ней то, что они хотят? Каждый бренд решает для себя эту проблему самостоятельно. Компания Social Bakers провела исследование, цель которого – выяснить, как влияет на вовлеченность то обстоятельство, закрыта стена в сообществе или открыта.

Для сравнения были выбраны 50 страниц авиакомпаний с большим количеством фанов. Данная отрасль была выбрана по той причине, что ее подписчики в соцсетях ведут себя довольно активно. Они не только взаимодействуют с контентом, который постят администраторы сообществ, задают вопросы в службу поддержки, но и создают собственные посты, где делятся впечатлениями от путешествий. Так что же происходит, если стена на странице бренда закрыта и пользователи не могут опубликовать свой пост или задать вопрос?

Для закрытых стен уровень вовлеченности оказывается немного выше! НО: само взаимодействие с контентом оставляет желать лучшего.

Объясняется это простым фактом. Так как фаны не имеют возможности задать свои вопросы, оставив их на стене, они задают их в комментариях к постам администраторов. Тематика поста не имеет в данном случае никакого значения. В итоге тема разговора может уходить совершенно в другом направлении от темы публикации бренда.

Другое дело, когда стена открыта. У фанов нет необходимости рассказывать о своих проблемах в комментариях, поэтому все их внимание направлено на контент.

Закрытая стена в нашей практике скорее исключение – социальные сети нужны бренду для взаимодействия с аудиторией, а не отгораживания от нее, говорит Ю. Степанов, менеджер по работе в социальных медиа Dr. JUNG (в составе DEFA). Даже если клиент очень опасается критики в свой адрес, то премодерация (все посты от пользователей по умолчанию скрываются и раскрываются администратором вручную) или оперативная постмодерация решают эту проблему гораздо эффективнее.

Полностью открытая стена, когда пользовательский контент отображается в хронике наравне с контентом бренда, тоже не лучший вариант. Нарушается визуальное единство таймлайна и продуманный порядок чередования тематик, то есть теряется некая общая логика

повествования. Поэтому чаще всего мы рекомендуем такую настройку открытой стены, в которой пользовательские посты показываются в специально отведенном для этого поле в верхней части таймлайна ***(Закрытая стена в Facebook vs. открытая. Что лучше для вовлечения? // Marketing Media Review (http://mmr.ua/news/id/zakrytaja-stena-v-facebook-vs-otkrytaja-chto-luchshe-dlja-vovlechenija-36103). – 2013. – 12.09).***

***

Акції найбільшої у світі соцмережі Facebook уперше з моменту первинного публічного розміщення пробили позначку в 45 дол. і сягнули історичного рекорду в 45,09 дол. 11 вересня. Про це говорять дані біржі NASDAQ, пише digit.ru.

Facebook провела IPO на американській біржі NASDAQ 18 травня 2012 р. за ціною 38 дол. за акцію. Торгуватися вони почали на рівні 42 дол. – майже на 11 % вище ціни розміщення.

На торгах NASDAQ 11 вересня акції соцмережі доходили в ціні до 45,09 дол. – історичного для компанії рекорду – перш ніж закритися на рівні 45,04 дол., на 3,3 % вище попереднього дня. Ринкова капіталізація компанії оцінюється в 109,7 млрд дол.

24 липня Facebook повідомила про зростання продажів мобільної реклами на 75 % у II кварталі. З того часу акції Facebook додали понад 70 % у вартості.

Експерти очікують, що глава компанії М. Цукерберг найближчим часом оголосить про запуск формату відеореклами, а також про початок розміщення реклами на фотосервісі Instagram ***(Акції Facebook вперше після публічного розміщення сягнули історичного рекорду // iPress.ua (http://ipress.ua/news/aktsii_facebook_vpershe_pislya_publichnogo_rozmishchennya_syagnuly_istorychnogo_rekordu_27966.html). – 2013. – 12.09).***

***

Сервис микроблогов Twitter Inc. подал в Комиссию по ценным бумагам и биржам США (SEC) заявку на проведение первичного публичного размещения акций. Сообщение об этом уместилось в 140 символах – компания информировала пользователей о подготовке к выходу на биржу в официальном аккаунте. Материалы, поданные в SEC, пока носят конфиденциальный характер и недоступны к изучению на сайте регулятора. Twitter воспользовался соответствующей опцией нового закона (Jumpstart Our Business Startups Act), позволяющей компаниям с выручкой ниже 1 млрд дол. до поры не раскрывать темпов развития бизнеса и показателей рентабельности.

IPO Twitter – самое ожидаемое размещение в секторе технологий на сегодня. За семь лет существования сервис превратился в одну из самых популярных и влиятельных социальных платформ в мире. Twitter уже аккумулировал аудиторию более чем в 200 млн пользователей, но до сих пор

не сформировал прозрачную и долгосрочную бизнес-модель, как это в свое время сделали Google и Facebook.

Ведущим андеррайтером размещения, по сведениям источников газеты The Wall Street Journal, выступит Goldman Sachs Group, ведутся переговоры и с другими крупными инвестбанками.

Twitter уже оценивается более чем в 9 млрд дол. Исходя из этой стоимости долю в сервисе в 2013 г. приобрела инвесткомпания BlackRock Inc., выкупив пакеты части сотрудников. К дню размещения Twitter может прибавить еще 5 млрд дол. капитализации, прогнозирует Financial Times со ссылкой на источники в инвестиционных кругах Кремниевой долины. Если на IPO Twitter получит оценку в 15 млрд дол., сервис все равно многократно уступит Facebook – в мае 2012 г. соцсеть была оценена рынком более чем в 100 млрд дол. Правда, на возвращение к этой планке у компании М. Цукерберга ушло почти полтора года – лишь на на сегодняшний день бумаги Facebook установили новый рекорд стоимости и пока стабильно торгуются выше цены IPO. Когда на конференции М. Цукербергу задали вопрос, какой совет он может дать Twitter накануне IPO, тот ответил шуткой: «Я последний человек, у которого вам стоит интересоваться мнением о гладком размещении».

Twitter под руководством гендиректора Д. Костоло двигался в направлении рынка последние три года. Ключевой задачей менеджмента было без ущерба для невероятной популярности сервиса превратить его в прибыльный бизнес и сделать по-настоящему привлекательным для рекламодателей. Благодаря множеству нововведений, в том числе так называемым promoted tweets – рекламным сообщениям, появляющимся на видных местах в лентах пользователей, компания в 2013 г. заработает порядка 583 млн дол., прогнозируют аналитики EMarketer. В 2014 г. показатель возрастет до 950 млн дол., в 2015 г. – перевалит за отметку в 1,3 млрд дол., полагают эксперты. Для сравнения: выручка Google в прошлом году составила 50,2 млрд дол., Facebook –5,1 млрд дол., Yahoo – 5 млрд дол. В мае 2013 г. департамент корпоративного развития Twitter возглавила известный инвестбанкир С. Гейлор, во время работы в Morgan Stanley участвовавшая в подготовке IPO Facebook и LinkedIn.

Когда детали бизнеса Twitter станут доступны широкой публике, остается неясным. Закон JOBS Act, позволивший сервису «тайно» проинформировать SEC о своих намерениях, оставляет претендентам на IPO возможность отказаться от планов выхода на биржу в случае, если те не обнаружат на рынке достаточного интереса. Раскрыты же документы могут быть не позднее чем за 21 день до начала roadshow, в рамках которого компании проводят встречи с потенциальными инвесторами и определяются с прайсингом акций

Если IPO случится скоро (до конца 2013 г.), Twitter впишется в рыночную тенденцию этого года – по подсчетам Dealogic, число размещений в 2013 г. перевалит за 200 и окажется максимальным с докризисного 2007 г. При этом в среднем компания, проводящая размещение, дорожает более чем

на 13 % в первый день торгов, что говорит о позитивном настрое инвесторов, заключают аналитики.

Twitter за все время своего существования привлек свыше 1 млрд дол. вложений. Среди инвесторов компании присутствуют ведущие фонды Кремниевой долины – Charles River Ventures, Benchmark, Insight Venture Partners, Andreessen Horowitz и Kleiner Perkins Caufield & Byers. На более поздних стадиях в проект вошли такие известные игроки, как российский миллиардер Ю. Мильнер и компания T. Rowe Price Group.

За день до появления новости о подаче заявки в SEC на частных площадках бумаги Twitter торговались в диапазоне 26–28 дол. за штуку – это означает стоимость всей компании в 13,7–14,4 млрд дол., рассказал FT один из владельцев доли в сервисе. По его мнению, у Twitter уже есть четкая модель получения выручки, в будущем способная сделать проект прибыльным и принести дивиденды акционерам. В самой компании о выходе бизнеса «в плюс» по состоянию на сегодня не сообщали ни разу.

Сервис появился на свет в марте 2006 г. с подачи Д. Дорси, который на сегодня остается председателем совета директоров Twitter. Изначально Twitter был побочным продуктом подкастинговой компании Odeo, основанной бывшим менеджером Google Э. Уильямсом. Э. Уильямс и Д. Дорси при активной поддержке дизайнера Б. Стоуна смогли заложить фундамент сервиса, справившись с дефицитом инфраструктуры и галопирующим ростом аудитории, пока в октябре 2010 г. на пост гендиректора не пришел Д. Костоло, сосредоточивший оперативное управление проектом в своих руках ***(Первый после Facebook: Twitter подал заявку на проведение IPO // InternetUA (http://internetua.com/pervii-posle-Facebook--Twitter-podal-zayavku-na-provedenie-IPO). – 2013. – 16.09).***

***

Исследование: компании продолжают увеличивать рекламные расходы в Facebook

За 15 месяцев Facebook превратился из экспериментального канала, куда маркетологи не сильно хотели инвестировать деньги, в полноценную структуру, где компании продолжают активно увеличивать расходы. К такому выводу пришли после проведенного в августе голосования 1200 подписчиков AdAge совместно с RBC Capital Markets, уже третьего подобного исследования, начиная с июня 2012 г.

Количество респондентов, которые отметили, что используют Facebook в качестве источника для маркетинга, составляет примерно 80 %. Активность включает присутствие в Facebook, создание контента и слушание, о чем говорят в социальных сетях. Правда, количество тех, кто публикует свою рекламу на Facebook, резко увеличилось за последние 15 месяцев.

Примерно 74 % респондентов отметили, что их бюджет Facebook включает расходы на рекламу, которые неуклонно росли с 62 % января 2012 г. и 52 % в июне 2012 г. Последний опрос включал респондентов, которые идентифицировали себя как маркетологи или клиенты (26 %),

сотрудники рекламного агентства (30 %) и остальные сотрудники медиакомпании.

Процентный рост маркетологов, которые действительно покупают рекламу, определяет чистый показатель дополнительного рекламного дохода, который приходит с Facebook, отметил аналитик RBC Capital М. Магони. «Эти маркетологи также отметили, что ROI в Facebook улучшились за шесть месяцев».

М. Магони также указывает, что 43 % респондентов отметили, что их финансовые показатели на Facebook существенно или «в некоторой степени» улучшились за последние шесть месяцев. (Примерно 48 % сказали, что ничего не изменилось, и 9 % отметили, что положение ухудшилось).

Отвечая на вопрос, какие шесть рекламных онлайн сайтов можно выделить по степени важности, Facebook оказался на втором месте после Google.

Значимость мобильных приложений

Около 75 % респондентов также отметили, что маркетинг в мобильных приложениях Facebook очень важный, в прошлом году их количество составляло 67 %.

Любопытно, что большинство респондентов – 38 % – отметили, ROI мобильной и десктопной рекламы оцениваются примерно одинаково (35 % – за мобильную рекламу, 27 – за десктопную). Размывание границ между мобильной и десктопной рекламой является ключевым фактором роста прибыли Facebook, поскольку всё больше рекламщиков покупают ленту новостей.

Рост бюджета

Следует обратить внимание, что примерно 56 % участников опроса сказали, что ожидают рост бюджета рекламы Facebook на следующий год. И всего лишь 18 % используют биржу Facebook. Согласно утверждению директора по производственным вопросам Ш. Сандстберг, эта биржа всего лишь малая часть всего рекламного дохода Facebook.

И последнее, 64 % респондентов отметили, что они покупают рекламу в Facebook напрямую с социальной сети. Это хоть и доказывает способность самообслуживания Facebook, но в то же время показывает, что растущая область маркетинга находится за рамками традиционных структур рекламных агентств.

Остальные респонденты сказали, что они совершают покупки через услуги рекламных агентств или разработчиков рекламных технологий – соответственно 22 и 14 %. Тем не менее, важно отметить, что бюджет 41 % респондентов составляет примерно 500 тыс. дол., поэтому у них может быть недостаточно ресурсов для услуг агентства ***(Исследование: компании продолжают увеличивать рекламные расходы в Facebook // Marketing Media Review (http://mmr.ua/news/id/issledovanie-kompanii-prodolzhajut-uvelichivat-reklamnye-rashody-v-facebook-36153). – 2013. – 16.09).***

***

Вслед за другими социальными сетями ресурс Pinterest тоже вступил на тропу коммерциализации. Компания начинает программу тестирования «продвигаемых понов» или Promoted Pins, в которой сам ресурс и автор загруженной в сеть фотографии или рисунка смогут зарабатывать деньги на циркуляции контента.

Генеральный директор Pinterest Б. Силберман в сообщении для пользователей сети сообщил, что соцсеть будет экспериментировать с промоутингом небольшого числа пинов в поисковых результатах и категорийных лентах Pinterest. «К примеру, пин Darth Vader будет выдаваться пользователями, которые ищут данные о костюмах на Хэллоуин, – говорит он. – Пока за это никто ничего платить не будет, мы только пробуем работу такой системы и хотим понять, как все это будет устроено. Да, вы сейчас, вероятно, подумали – ну вот, здорово, появится реклама. Но этого не будет. Мы решили, что баннеров тут не будет».

Он также отметил, что будущее Pinterest – это прибыль, по крайней мере, в глобальной перспективе. Как и другие сервисы, Pinterest начал как настольная соцсеть, сфокусированная на пользовательской базе, но за последнее время компания обновила внешний вид, добавила новые возможности и создала мобильную стратегию. Б. Силберманн говорит, что продвигаемый контент – это лишь один из элементов коммерциализации, последуют и другие, но в любом случае, CEO компании обещает «ауккуратную» коммерциализацию.

«Никаких всплывающих баннеров, никаких дополнений. Вы всегда будете понимать, что здесь платное, а что – нет», – говорит он ***(Соцсеть Pinterset начала коммерциализацию // InternetUA (http://internetua.com/socset-Pinterset-nacsala-kommercializaciua). – 2013. – 21.09).***

# СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

## Інформаційно-психологічний вплив мережевого спілкування на особистість

Доктор Т. Месерви из Университета Бригама Янга (штат Юта, США) создал компьютерную программу, которая позволяет определить, лжёт ли ваш онлайн-собеседник, или пишет правду.

По словам исследователя, собеседник, который любит прерываться на середине фразы и заканчивать её через некоторое время, с весьма высокой вероятностью может оказаться лжецом. Паузу он использует для обдумывания своих слов. Кроме того, лжецы чаще других пишут короткие сообщения и вносят в текст больше правок.

Для подтверждения своей теории Т. Месерви разработал компьютерную программу, способную анализировать онлайн-беседы и отслеживать возможные признаки лжи. Программу опробовали на нескольких тестовых группах пользователей. Каждого из 100 участников эксперимента просили ответить на 30 вопросов. При этом 50 % ответов должны быть лживыми.

Подводя итоги эксперимента, исследователь выяснил, что в среднем ложь отнимает на 10 % больше времени, чем правдивый ответ.

Однако Т. Месерви предупреждает, что если кто-то слишком долго пишет ответное сообщение, нельзя однозначно и категорично утверждать, что он лжёц. Тем не менее, у лжи онлайн есть определённая закономерность, и в будущем это поспособствует созданию более совершенных детекторов лжи ***(Специальная программа подскажет, когда вам пишут неправду в соцсетях // InternetUA (http://internetua.com/specialnaya-programma-podskajet--kogda-vam-pishut-nepravdu-v-socsetyah). – 2013. – 13.09).***

***

Поганий приклад у соцмережах заразливий

«Це перше дослідження, що вивчило, як участь тінейджерів у соціальних мережах впливає на вживання ними алкоголю і тютюну», – говорить доктор Т. Валенте, професор профілактичної медицини з Медичної школи Кека при Університеті Південної Каліфорнії. Дослідники опитували понад 1,5 тис. школярів 10 класів з Лос-Анджелеса в період з жовтня 2010 р. по квітень 2011 р. на предмет їхніх дружніх відносин в онлайні і в реальному житті, а також про частоту користування соцмережами, про тютюнової залежності або вживання алкоголю. Середній вік учасників опитування – 15 років, станом на початок дослідження курили близько 30 % і приблизно половина хоча б раз у житті пробувала алкоголь. Одна третина заявила про те, що серед їхніх друзів є хоча б один курець або питущий. Майже половина всіх школярів відвідувала соцмережі Facebook і Myspace регулярно. При цьому до кінця експерименту кількість користувачів Facebook збільшилася до 75 %, а кількість тих, хто використовує Myspace, знизилася на 13 %. У середньому 34 % учасника заявили, що мають хоча б одного друга в мережі, що розповідає онлайн про веселі вечірки, а 20 % розповіли, що їхні друзі публікують онлайн-фото з вечірок, де вони п’ють і курять. Учені виявили, що підлітки, чиї близькі друзі не приймають алкоголю, частіше мали ризик потрапляння під поганий вплив онлайн-пропаганди.

До того ж автори визнають, що освітній і соціальний статус користувачів Facebook виявився вище, ніж у користувачів Myspace. І друга група користувачів була більш схильна до вживання алкоголю. «Наші докази дають змогу припустити, що поведінка друзів в онлайні – значущий інструмент впливу на однолітків». Нагадаємо, раніше двоє студентів з Массачусетського технологічного інституту розробили ефективний метод відвадити людей від Facebook, які не справляються із залежністю від

соцмережі ***(Поганий приклад у соцмережах заразливий // NewsMe (http://newsme.com.ua/ua/tech/health/1945951). – 3.09).***

***

Чем больше вы уделяете времени популярной сети Facebook, чем больше новостей в ленте вы просматриваете и оставляете различных комментариев к фотографиям и ссылкам, тем несчастнее вы себя чувствуете, сообщает UBR (http://ubr.ua/market/media-market/chem-opasen-facebook-8-faktov-252301).

Новое исследование подтвердило, что люди, часами сидящие у мониторов своих компьютеров, менее удовлетворены своей жизнью. Психологи говорят о негативном влиянии социальных сетей на настроение человека.

Похоже на то, что Facebook, действительно способствует подавленному состоянию своих пользователей. И хотя эта информация официально не подтверждена, об этом свидетельствуют некоторые наблюдения психологов.

О. Ибарра, доктор Мичиганского университета, объясняет негативное влияние социальной сети публичным характером подобных сайтов. Это означает, что люди, у которых складывается по жизни хорошо, через фотографии и другую информацию доносят до знакомых и друзей, как у них всё замечательно. На фоне чужих побед и удач свои проблемы и беды кажутся еще более ощутимыми. И человек может впасть в депрессию или же ощутить себя изгоем. И виной всему предвзятое впечатление, созданное хорошей жизнью других людей.

Психологи утверждают, что отношения, которые происходят в реальной жизни, куда лучше любого виртуального общения, так как обладают рядом существенных преимуществ. Прежде всего правильные взаимоотношения в реальности способствуют хорошему настроению, повышению интеллекта, а также приводят к улучшению процесса принятия решений.

Люди, которые социально более интегрированы, как правило, чаще живут долго и счастливо, чем те, кто просиживает часами в Интернете. По словам О. Ибарра, перечень преимуществ реального общения над виртуальным можно продолжать до бесконечности. Психологический эффект от социальных сетей практически доказан учеными.

Чтобы увидеть, какое влияние социальная сеть оказывает на своих пользователей, был проведен специальный эксперимент. В исследовании приняли участие 80 человек. В течение двух недель психологи наблюдали за ними, регулярно оценивая их уровень удовлетворенности жизнью, подверженности депрессиям, а также ряд других психологических факторов, влияющих на самооценку личности человека.

Предположения психологов подтвердились: Facebook действительно влияет на настроение. Посещение социальной сети может как поднять настроение, так и вогнать человека в депрессию, в зависимости от событий, которые происходили на данный момент в жизни каждого ***(Чем опасен***

***Facebook: 8 фактов // UBR (http://ubr.ua/market/media-market/chem-opasen-facebook-8-faktov-252301). – 2013. – 17.09).***

***

В социальных сетях лучше всего расходятся сообщения, окрашенные эмоциями раздражения и злости. Об этом заявили сотрудники Бейханского университета, пишет «Лента.ру» со ссылкой на блог Technology Review. К таким выводам исследователи пришли на основе анализа популярной в Китае микроблоговой соцсети Weibo.

Также ученые сообщили, что сообщения, окрашенные печалью и отвращением, редко расходятся знакомыми пользователей. При этом гораздо лучше передавалась между пользователями радость. И все же абсолютным победителем оказалась злоба – такие сообщения делали не менее трех переходов от одного узла социального графа до другого. В то же время ученые не могут сказать, связаны ли результаты исследования с особенностями самих эмоций или с тем, что гневные сообщения чаще несут более социально важную информацию ***(Самой заразительной эмоцией в соцсетях стала злость // Весь Харьков (http://all.kharkov.ua/news/other/samoi-zarazitelnoi-emociei-v-socsetiah-stala-zlost-issledovanie.html). – 2013. – 18.09).***

***

Исследователи из Австрии составили коллективный портрет людей, которые решили избавиться от своего аккаунта в социальной сети Facebook. Ученые выяснили, что к этому действию чаще всего, в 48 % случаев, подталкивают опасения за безопасность личных данных. Кроме того, у таких людей оказался несколько выше уровень интернет-зависимости и общей сознательности: подробности исследования приведены в статье для журнала Cyberpsychology, Behavior, and Social Networking.

Ученые из Университета Вены опросили 310 человек, которые недавно удалили свои аккаунты в Facebook, и привлекли для сравнения с ними 321 добровольца, которые были обычными пользователями этой социальной сети. Все участники исследования заполнили ряд опросников, которые должны были рассказать психологам об их характеристиках и мотивах выхода из Facebook.

Выбирая между полнотой опросника и удобством для добровольцев (некоторые опросники требуют более часа на заполнение) специалисты остановились на тесте Mini-IPIP, который выдает оценку по пяти разным параметрам (экстраверсия, сговорчивость, сознательность, невротизм и интеллект). Кроме того, участники заполняли короткий, на 20 вопросов, тест на уровень интернет-зависимости I-AT и тест, призванный оценить обеспокоенность пользователя вопросами безопасности личных данных с вопросами вроде «Закрываете ли вы рукой клавиатуру банкомата при наборе PIN?». Все тесты применялись ранее другими специалистами, поэтому

ученые были избавлены от необходимости дополнительно обосновывать их корректность. Кроме того, добровольцы, ушедшие из сети, заполняли анкету, в которой указывали те причины своего действия, которые сами считали наиболее значимыми.

Когда исследователи сопоставили заполненные пользователями Facebook и теми, кто покинул социальную сеть, опросники, то они обнаружили ряд небольших, но статистически значимых различий. Выяснилось, что совершившие «виртуальный суицид» (такая метафора отражена в заголовке работы психологов) несколько более сознательны и у них в среднем немногим выше уровень интернет-зависимости. В числе причин ухода лидировали опасения за личные данные (48 % опрошенных), общая неудовлетворенность Facebook, раздражение кем-то из имеющих аккаунт друзей и (6,5 %) желание избавиться от патологической зависимости от социальной сети. Авторы исследования отмечают, что покинувшие Facebook обычно больше обеспокоены защитой личной информации и это видно как в тестах, так и в ответах на прямо заданный вопрос о причинах ухода.

Ученые подчеркивают, что их работа позволяет дополнить знания психологов о поведении людей онлайн. Они пишут, что ранее люди с большим уровнем сознательности считались менее подвержены интернет-зависимости, но их выборка продемонстрировала обратный эффект и здесь открывается пространство для новых исследований. Кроме того, покидающие Facebook люди оказались далеко не однородной группой, поэтому явление нельзя свести к одному лишь нежеланию делиться с кем-то своими персональными данными. По мнению австрийских специалистов, дальнейшая работа по изучению покидающих социальные сети людей может помочь в понимании не только общих закономерностей онлайн-поведения, но и онлайн-зависимости ***(Социологи составили портрет покидающих Facebook пользователей // Marketing Media Review (http://mmr.ua/news/id/sociologi-sostavili-portret-pokidajuschih-facebook-polzovatelej-36169). – 2013. – 17.09).***

***

Упродовж місяця понад 11 млн користувачів видалили акаунти з Facebook через діяльність WikiLeaks і викриття Е. Сноудена, який розсекретив факт стеження АНБ через соціальні медіа.

Дослідники пов’язують побоювання за вторгнення в приватне життя з діяльністю WikiLeaks, а також викриттями Е. Сноудена, який розкрив факт стеження Агентства національної безпеки через соціальні медіа ***(Більше 11 млн користувачів покинули Facebook у зв’язку з викриттями Сноудена // iPress.ua (http://ipress.ua/news/bilshe_11_mln_korystuvachiv_pokynuly_facebook_28384.html). – 2013. – 18.09).***

## Маніпулятивні технології

В Украине в два раза увеличилось число мошенников, которые работают через Интернет. Об этом заявил начальник отдела по борьбе с преступлениями в сфере электронной коммерции МВД Украины О. Заворотний, пишет nbnews. «За шесть месяцев текущего года выявлено около 2 тыс. случаев мошенничества в сети Интернет. Это почти столько же, сколько было зафиксировано за весь 2012 г.», – заявил О. Заворотний.

Правоохранитель рассказал, что в сети, как правило, существуют две схемы, по которым действуют преступники. Это якобы предоставление определенных услуг со 100 % предоплатой и финансовые пирамиды. «Пирамиды – наиболее социально опасный вид мошенничества, поскольку он связан с большим количеством пострадавших и со значительными суммами убытков. По статистике, вкладчикам возвращается до 40 % средств, но каждый пострадавший надеется на возврат полной суммы», – отметил О. Заворотний.

В Украине в настоящее время нет закона, который препятствовал работе пирамид, поэтому в милиции советуют интернет-пользователям быть предельно осторожными, а также не вестись на всякого рода предложения от неизвестных лиц ***(В Украине в два раза увеличилось количество интернет-мошенников // InternetUA (http://internetua.com/v-ukraine-v-dva-raza-uvelicsilos-kolicsestvo-internet-moshennikov). – 2013. – 15.09).***

***

Неизвестные продолжают масштабную атаку на сайт «Украинская правда» – самый популярный политический ресурс страны. Об этом в авторской колонке для РИА «Новый регион» пишет И. Самойлов.

...Украинское журналистское сообщество не находит себе места. Буквально за одну неделю появился сайт «Украинская неправда», подпольная «бумажная» версия «Украинской правды», и сайт «Украинская кривда», полностью копирующий дизайн и стиль оригинала. Портал, в последнее десятилетие формирующий информационную политику страны, стал жертвой умелой и дорогой спецоперации, заказчик которой пока остается неизвестным.

Королевство «джинсы»

Правила, по которым живут украинские СМИ, весьма далеки от того, чему учат на первом курсе Института журналистики. Словосочетание «независимая пресса» вызывает в среде профессиональных журналистов лишь горькие улыбки. Причем бичем СМИ стала вовсе не цензура или диктат со стороны собственников. В помойную яму из вранья и замалчивания отечественные издание превратило систематическое размещение заказных материалов или «джинсы», как они называются на журналистском жаргоне.

Печатать чужие новости за деньги сейчас не брезгуют даже солидные печатные издания вроде «Комсомольской правды» или «Сегодня». Что уже говорить об интернет-сайтах, иногда состоящих из одной только «заказухи»,

размещаемой как по инициативе руководства издания, так и приносимой рядовыми журналистами.

В этой отлаженной системе «Украинская правда» всегда стояла особняком. «Джинсу» там размещают лишь в редких случаях. Основным источником заработка УП стало высокое реноме издания. «Пробиться» со своей информацией на сайт – вопрос чести для любого политика или бизнесмена страны. Именно это дало руководителям сайта практически безграничную власть над информпространством.

Однако, увлекшись расследованиями и разоблачениями, УП незаметно для самой себя стала орудием в руках олигархических кланов. Подсадив ведущих журналистов УП на потоки «слива» определенной информации, олигархи активно режиссируют новостями в своих интересах. По слухам, в настоящее время наиболее тесные отношения с «Украинской правдой» имеет глава АП С. Левочкин. В то же время сайт не контролируется до конца ни одной из группировок, что позволяет ему сохранять видимость незаангажированности – «мочить всех без разбора».

То ли еще будет

Очевидно, что опасная «игрушка» утомила слишком многих. Нынешним проблемам ресурса рады и власть, и оппозиция. По крайней мере, ни один из политиков не выступил в поддержку «Правды». Все затаили дыхание и наблюдают за тем, как кто-то по медвежьи неуклюже ломает устоявшееся годами статус-кво. А посмотреть есть на что. У инициаторов атаки на УП достаточно ресурсов, да и за дело они взялись весьма серьезно. Если сайты-клоны рассчитаны исключительно на журналистскую «тусовку», то бумажная версия, да еще и с миллионным тиражом, – заявка на влияние, даже большее чем у настоящей «Украинской правды». А ведь «принт» – это только начало проблем.

По последним данным, сейчас в Киеве начался набор персонала – от журналистов до бухгалтеров в новосозданное информационное агентство «Украинская правда», не имеющее ничего общего с настоящей «Правдой». Вакансии открыто размещены на сайте work.ua. Там же указан и номер свидетельства о регистрации СМИ, что говорит о серьезности намерений «доброжелателей» А. Притулы.

Последняя, кстати, во многом сама облегчила жизнь рейдерам. Мало кто знает, что нынешняя «Украинская правда» это вовсе не СМИ – юридически УП является сайтом частного предприятия. Такой статус был выбран не случайно – он годами позволял обходить формальные требования законодательства, в частности не заботиться о достоверности размещаемой информации. Но, похоже, А. Притула и ее соратники перехитрили сами себя. Защитить свой бренд им теперь будет очень непросто.

Кому выгодно?

В настоящее время можно только строить догадки, кто именно стоит за атакой на УП. Пока звучат совершенно разные предположения – от всесильной «семьи» до окружения лидера «Батьківщини» А. Яценюка.

Однако все они основываются лишь на слухах и предположениях, не подтвержденных никакими доказательствами.

Впрочем одно доказательство уже сейчас можно предъявить. Кто бы не занимался борьбой с УП, он не обошелся без прямой помощи спецслужб. Информация, размещенная на сайтах-клонах, могла быть получена только с использованием арсенала чекистов. Массовый взлом почтовых ящиков, прослушка телефонов, слежка за журналистами и политиками – такие источники информации сами по себе говорят о многом. Также без прикрытия спецслужбы, имеющей разветвленную структуру, невозможно печатать и распространять миллионные тиражи политической газеты. Это знает каждый, кто когда-либо пытался хотя бы расклеить листовки на заборах. Впрочем, роль спецслужбы в этой затее тоже пока до конца не ясна.

Как бы там ни было, долго держать в тайне такое мероприятие его организаторам не удастся. Не исключено также, что вся грязная правда всплывет уже после выборов 2015 г. Но это будет еще нескоро, а вот радикальное переформатирование украинского интернет-пространства начнется с момента первой ссылки на информагентство «Украинская правда» ***(Самойлов И. Неизвестные продолжают масштабную атаку на самый популярный политический интернет-ресурс Украины // Новый регион (http://www.nr2.ru/kiev/459218.html). – 2013. – 10.09).***

***

У Росії можуть заблокувати соціальну мережу Facebook через виявлену там рекламу курильних сумішей, повідомив заступник керівника Федеральної антимонопольної служби (ФАС) РФ А. Кашеваров.

Зазначимо, що в рекламному блоці, розташованому праворуч на сторінці Facebook, 16 вересня з'явилася пропозиція придбати «курильні мікси й ейфорію». Там же зазначені безкоштовний телефонний номер і адреса сайту, на якому пропонується купити «спайс» і «легальні порошки».

Також повідомлялося, що пропозиція є в таких містах, як Москва, Краснодар, Київ та Одеса, причому клієнтам пропонуються «величезні знижки на опт» і постійні акції. Тим часом видання Hopes&Fears повідомляє, що Facebook проведе власне розслідування, як реклама наркотиків з'явилася на сторінках соціальної мережі. Про це розповіла голова Facebook у Росії К. Скоробогатова.

Політика соцмережі забороняє розміщення реклами, яка просуває заборонені на території тієї чи іншої країни товари й послуги. Варто зазначити, що виробництво, продаж і зберігання курильних сумішей заборонено в Росії. Відповідна постанова уряду РФ набрала чинності в січні 2010 р. В Україні курильні суміші були заборонені в кінці весни 2010 р. ***(У Росії можуть закрити Facebook через курильні суміші // Інформаційне агентство «Регіональні Новини» (http://regionews.ua/node/113568). – 2013. – 16.09).***

***

Адміністрація компанії Facebook повідомила Федеральній службі з нагляду у сфері зв'язку, інформаційних технологій і масових комунікацій (Роскомнагляд), що контент, у зв'язку з яким були отримані повідомлення про необхідність видалення забороненої інформації, ліквідовано. Про це повідомляє прес-служба Роскомнагляду. Після перевірки посилання Роскомнагляд повідомив, що всі вимоги служби виконано та ініційовано процедуру виключення відповідного запису з реєстру заборонених сайтів ***(Росія могла заблокувати Facebook через курильні суміші Lenta.Mobus // (http://lenta.mobus.com/news_626939.html). – 2013. – 19.09).***

***

У мережі Facebook була створена фейкова сторінка екс-президента України В. Ющенка. Про це повідомила його прес-служба.

«На сторінці представлена неправдива інформація, у тому числі розміщено фальшивий відеоролик, змонтований з фрагментів передвиборного відео В. Ющенка за 2010 р.», – ідеться у повідомленні.

За інформацією прес-служби, ні вона, ні пан Ющенко не авторизували зміст матеріалів на цій сторінці. «У зв'язку з цим просимо Вас утриматися від поширення і посилання матеріалів, які не можна охарактеризувати інакше як політичну провокацію», – наголошується в заяві ***(Фейк на грані фолу // Свобода слова в Україні (http://svobodaslova.in.ua/news/read/22869). – 2013. – 19.09).***

***

Испанские СМИ выяснили, действительно ли можно узнать, кто посещал персональную страницу в Facebook, сообщает IT Expert.

С этим вопросом издание 20 Minutos обратилось непосредственно к официальным представителям соцсети. Их также спросили о том, не планирует ли сам Facebook ввести подобный сервис.

В Интернете существует множество приложений и «трюков», которые якобы могут определить, кто и когда посещал страницу профиля в Facebook. Впрочем, ни один из этих инструментов не работает, утверждают собеседники издания, передает Noticia.ru.

На протяжении долгого времени руководство Facebook предупреждает, что подобные приложения являются мошенническими и пожаловаться на них можно в самой соцсети. «Большинство этих программ разработано третьими лицами, с которыми Facebook не сотрудничает. В них содержится спам и вирусы, которые ставят под угрозу конфиденциальную информацию о пользователе», – объясняют представители компании. «Никто не может знать, кто посещал Вашу страницу», – добавляют они.

«Последние обновления в "Хронике" значительно упростили конфигурацию всех личных сведений о пользователе. Раньше риск заключался в том, что некоторые элементы (в особенности фотографии) оставались публичными, так как пользователи не знали, как сделать их приватными», – напоминают представители соцсети. «Программы вроде

“Кто смотрел мой профиль” появляются практически ежедневно, и мы должны опережать всех программистов, которые могут обнаружить недочеты», – рассказывают сотрудники компании. Они также предупреждают, что Facebook не планирует в будущем внедрять подобных функций.

Некоторые из подобных приложений, например Lagsoft, в прошлом пользовались большой популярностью. Программа требовала доступ к профилю, фотографиям, видеозаписям пользователя, запросам о добавлении в друзья и даже запрашивала разрешение на публикацию сведений от его имени. В обмен на это пользователь получал сведения о том, кто посещал его страницу, однако, как выяснилось, она не была достоверной.

Кроме того, в моду вошли и трюки с использованием браузера Chrome. Достаточно было просто посмотреть исходный код страницы в соответствии с видеоинструкцией и получить некий список друзей. Впрочем, он тоже не имел ничего общего со списком посетителей страницы, пишет издание ***(СМИ выяснили, можно ли узнать, кто посещал личную страницу в Facebook // IT Expert (http://itexpert.in.ua/rubrikator/item/29888-smi-vyyasnili-mozhno-li-uznat-kto-poseshchal-lichnuyu-stranitsu-v-facebook.html). – 2013. – 18.09).***

***

В Украине появился новый вид афер: мошенники выманивают в социальных сетях откровенные фотографии, а потом шантажируют изображенных на них людей. На днях представители МВД даже выступили с заявлением, что выкладывать на свои странички или передавать в Интернете свои откровенные фотографии стало опасно.

«Этот вид преступлений для Украины – новый. Есть люди, которые специально мониторят соцсети, чтобы найти жертв и обогатиться за их счет. У нас в области был выявлен случай, когда девушка познакомилась в соцсети с парнем, начала с ним переписываться, подружилась с ним, а после начала отправлять ему фото приватного характера, прикрепляя их на своей странице. Через некоторое время парень начал ее шантажировать, требуя перечислять определенные суммы на свой электронный кошелек (иногда за подобное требуют 300–400 дол. – Авт.), а если этого не произойдет, то обещал разместить эти фото на “сайтах для взрослых”», – рассказал «Сегодня» и. о. руководителя отдела по борьбе с кибер-преступностью Хмельницкого областного УМВД О. Дядык. Как добавили в МВД, уже были случаи, когда выявляли таких аферистов, которые шантажировали своих жертв смонтированными с помощью специальных программ фото. При этом шантажисты находят снимки, даже если страничка пользователя закрыта от посторонних. В МВД говорят, что так заработать пытаются как аферисты-одиночки, так и целые группы мошенников.

К счастью, массовости этот вид афер пока не приобрел. «Исключать, что такие случаи есть, я не стану, но в нашей практике такого не было», – сказал нам оперуполномоченный управления по борьбе с кибер-преступностью МВД М. Стришенец. Как выяснила «Сегодня», многие

оперативники МВД, как из центрального аппарата, так и из региональных подразделений, хоть и зарегистрированы в соцсетях под своими настоящими именами, но ни на аватарке, ни в альбомах многих из них нет настоящих фотографий, лишь заставочные картинки ***(Мошенники освоили шантаж с помощью фото из соцсети // Четверта Влада (http://4vlada.net/smi/moshenniki-osvoili-shantazh-s-pomoshchyu-foto-iz-sotsseti). – 2013. – 19.09).***

***

Как отличить обман от просьбы о помощи в соцсетях

Социальные сети становятся похожи на метро – там почти так же часто стали попадаться объявления а-ля «Помогите, умирает 3-летний сын». Блогер С. Мухамедов подробно описал в своем ЖЖ «Оттенки Серого», как распознать мошенническую публикацию в просьбе о помощи в соцсетях. Редакция theRunet решила поделиться инструкцией С. Мухамедова, чтобы видеть в Facebook меньше постов с окровавленными детьми и животными.

Во-первых, пишет С. Мухамедов, нужно обратить внимание на то, указан ли город в сообщении. Чаще всего такие посты о помощи пишутся без указания места. Таким образом, каждый подумает, что дело происходит в его городе, и сообщение заработает больше лайков.

Во-вторых, блогер советует задуматься над содержаниями постов. Как правило, в них отсутствует логика или здравый смысл. Особенно в тех объявлениях, которые связанны с какой-то халявой – бесплатным iPhone, который автор сообщения отдаст бесплатно, потому что ему по ошибке пришло два; бесплатными породистыми щенками, которых собираются утопить.

В-третьих, нужно обращать на наличие деталей в сообщении. Очень многие написаны предельно эмоционально, capskock-ом и красным шрифтом, но не сообщают, например, где произошла беда, какой диагноз у больного и какой номер у больницы, в которой надо сдать кровь.

Все такие сообщения призывают к срочности. Но блогер все же советует пользователям потратить пару минут на проверку информации, прежде чем сделать перепост. В частности, он предлагает ввести номер телефона в поисковике – вполне вероятно, что кто-то из интернет-юзеров уже сообщил о том, что этот номер – мошеннический. Также нужно обращать на дату сообщения, некоторые из них ходят по сети годами и месяцами.

К тому же современные технологии предлагают поиск по картинкам, так что можно залить изображение из заявления в Google и узнать, что оно взято с какого-то сайта ***(Как отличить обман от просьбы о помощи в соцсетях // InternetUA (http://internetua.com/kak-otlicsit-obman-ot-prosbi-o-pomosxi-v-socsetyah). – 2013. – 21.09).***

## Зарубіжні спецслужби і технології «соціального контролю»

Э. Сноуден рассекретил очередные документы о деятельности американской разведки. Согласно переданным бумагам, Агентство национальной безопасности США на протяжении двух десятилетий занимается взломом наиболее популярных методов шифрования и внедрением уязвимостей в популярные интернет-сервисы. В этой программе АНБ помогает шпионить и британская разведка.

Согласно очередной порции документов, переданных Э. Сноуденом журналистам The Guardian и The New York Times, Агентство национальной безопасности США обошло защиту и разрушило те методы шифрования, которые применяются в мировых торговых и банковских системах, защищают конфиденциальные данные (коммерческую тайну и медицинские записи), электронные письма, запросы в поисковых системах, интернет-чаты и телефонные звонки американцев и других граждан по всему миру.

В рамках программы под кодовым названием Bullrun АНБ занимается криптоанализом и применяет его результаты на практике. Согласно рассекреченным документам и служебным запискам чиновников, АНБ использует сверхмощные компьютеры для взлома кодов и сотрудничает с некоторыми технологическими компаниями в США и за рубежом для создания своей «точки входа» в их продукты. Наиболее интенсивные усилия АНБ были сосредоточены на криптозащите в широко применяемых протоколах и технологиях, таких как SSL, VPN и 4G.

В документах подчеркивается, что, так как шифрование иногда бывает очень эффективным, успех АНБ во многом зависит от сотрудничества с интернет-компаниями: добровольного, принудительного (заставляя их сотрудничать с помощью судебных ордеров) или тайного (перехватывая ключи шифрования или внося изменения в их аппаратное обеспечение и ПО). Названия компаний в документах не фигурируют.

Доступ к программе ограничен лишь избранным кругом специалистов разведки, и Э. Сноуден, судя по всему, к ним не принадлежал, однако все же смог раздобыть некоторые документы. В полной мере возможности США по декодированию известны лишь ограниченному кругу ведущих аналитиков из так называемых «Пяти глаз» (Five Eyes): АНБ и его коллегам из Великобритании, Канады, Австралии и Новой Зеландии. На эти зарубежные страны программа Bullrun не распространяется.

Документы АНБ демонстрируют, что ведомство поддерживает внутреннюю базу данных ключей шифрования для конкретных коммерческих продуктов, называемую «Сервис обеспечения ключами» (Key Provisioning Service), которая может автоматически декодировать множество сообщений. Если нужный ключ не найден, запрос уходит в Службу восстановления ключей (Key Recovery Service), которая затем пытается его получить.

Как ключи появляются в ней – окутано тайной. Независимые криптографы говорят, что многие из них собраны со взломанных

компьютерных серверов компаний. АНБ держит свои методы в секрете даже от других государственных ведомств, но «делится» с ними расшифрованными сообщениями, ключи для которых были добыты легально.

Криптографы давно подозревали, что АНБ могло внедрить некоторые уязвимости в стандарт, принятый в 2006 г. Национальным институтом стандартов и технологий, а затем использованный и Международной организацией по стандартизации, которая объединяет членов 163 стран. Рассекреченные заметки чиновников АНБ косвенно подтверждают, что обнаруженная двумя криптографами из Microsoft в 2007 г. уязвимость этого стандарта была разработана АНБ.

Некоторые эксперты, опрошенные NYT, полагают, что Bullrun противоречит другим миссиям АНБ, одна из которых – обеспечение безопасности коммуникаций в Америке. «Риск внедрения backdoor в систему состоит в том, что не только вы можете ее использовать», – отмечает М. Грин, исследователь криптографии в Университете Д. Хопкинса.

Однако даже программы, направленные на защиту коммуникаций американских граждан, разведка часто использует для проекта Bullrun. Например, Центр коммерческих решений АНБ (N.S.A.'s Commercial Solutions Center) часто приглашает разработчиков методов шифрования презентовать свои продукты перед агентством, аргументируя это необходимостью сотрудничества для усиления американской кибер-безопасности. Однако рассекреченные документы подтверждают, что этот же центр в АНБ используется и для налаживания партнерских отношений с некоторыми промышленными компаниями для внедрения backdoor в их продукты.

Примечателен тот факт, что в этот раз в мировом шпионаже оказалась замешана и британская разведка, которая, согласно обнародованным документам, активно сотрудничала с американскими коллегами. «Последние 10 лет АНБ прилагала агрессивные, разноплановые усилия для взлома широко используемых в Интернете технологий шифрования, – говорится в служебной записке, созданной после совещания между АНБ и Центром правительственной связи (Government Communications Headquarters, GCHQ), британским разведывательным ведомством. – Огромное количество зашифрованных данных из Интернета, которые до текущего момента были отброшены, теперь могут использоваться».

За последние три года GCHQ, почти наверняка в сотрудничестве с АНБ, искал способ получить доступ к защищенному трафику популярных интернет-сервисов: Google, Yahoo, Facebook и Hotmail от Microsoft. К 2012 г., согласно рассекреченным документам, GCHQ разработал «новые возможности доступа» к сервисам Google. При этом Google до текущего момента отрицает предоставление доступа какому-либо правительству и утверждает, что нет никаких доказательств нарушения защиты их систем.

Рассекреченные бумаги дают понять, что АНБ считает свою способность дешифровки жизненно необходимой для конкурирования с Россией, Китаем и другими мировыми державами. «В будущем, сверхдержавы будут сломаны

или созданы, основываясь только на силе их криптоаналитических программ, – говорится в документе за 2007 г. – Это цена входного билета США в кибер-пространство с неограниченным доступом».

Примечательно, что название программы Bullrun – отсылка к битве во время Гражданской войны в США. Параллельная программы GCHQ называется Edgehill, в честь первой битвы во время Гражданской войны в Англии в XVII ст.

Начиная с 2000 г., когда шифрование стало постепенно покрывать веб, АНБ инвестировала в Bullrun миллиарды долларов, пишет NYT. Документ, в котором раскрываются детали бюджета американской разведки, подтверждает, что усилия АНБ, прилагаемые к разрушению криптографической защиты, все еще сильны. «Мы инвестируем в инновационные криптоаналитические возможности, чтобы победить в состязании с криптографией и использовать в своих целях интернет-трафик», – написал в бюджетной заявке на текущий год Д. Клеппер, директор АНБ.

Также АНБ тратит более 250 млн дол. в год на смежный проект Sigint Enabling Project, который «активно привлекает отечественные и зарубежные ИТ-компании тайно влиять и/или открыто использовать свои коммерческие продукты в качестве эксплуатационных образцов». Sigint в названии этого проекта – акроним от signals intelligence, то есть радиоэлектронной разведки. В рамках этого проекта АНБ вскоре планирует получить полный доступ к неназванному крупному сервису интернет-звонков и обмена сообщениями, к некому интернет-сервису на Ближнем Востоке и коммуникациям трех иностранных правительств.

Один из информаторов The Times рассказал, что был случай, когда АНБ стало известно о крупном заказе компьютерного оборудования для иностранной разведки. Американский производитель под давлением АНБ согласился внедрить в это оборудование backdoor, после чего техника была отправлена заказчику.

Два десятилетия назад чиновники в США были обеспокоены распространением ПО с замысловатыми методами шифрования, такого как Pretty Good Privacy, разработанного Ф. Циммерманом. Администрация Б. Клинтона в качестве компромиссного решения официально предложила внедрять во все продукты the Clipper Chip, правительственный backdoor, благодаря которому у АНБ всегда будет «ключ» к данным. Это предложение вызвало негативную реакцию у многих политиков. Например, сенатора от Республиканской партии Д. Эшкрофта и сенатора от демократов Д. Керри. Граждане были солидарны, что такая мера не только убьет четвертую поправку к Конституции США, но и выбросит Америку из глобальной технологической эры. К 1996 г. Белый дом сдался, но не АНБ. «Они пошли и все равно это сделали, только никому ничего не сказав. Сегодня они могут мгновенно, тотально вторгаться в частную жизнь с минимумом усилий. Это золотой век в шпионаже», – комментирует П. Кохер, криптограф, который участвовал в разработке протокола SSL ***(Разведка США научилась взламывать популярные методы шифрования // Центр информационной***

***безопасности (http://www.bezpeka.com/ru/news/2013/09/09/us-intelligence.html). – 2013. – 9.09).***

***

Google усилит систему шифров, чтобы противостоять слежке американских спецслужб. Компания намерена зашифровать весь поток информации для того, чтобы Агентству национальной безопасности США и разведывательным службам других стран стало сложнее получать доступ к необходимым данным, пишет The Washington Post.

Более сложные информационные коды полностью не остановят правительственную слежку в Интернете и не окажут никакого влияния на изменение законных оснований такой деятельности. Однако в компании считают, что повсеместное использование технологий шифрования усложнит задачу правительству и хакерам. По словам экспертов, чем сложнее будет правительству расшифровывать информацию, тем разборчивее станут спецслужбы в своих целях и, возможно, будут следить именно за террористами, а не за всеми подряд ***(Google усилит систему шифров, чтобы противостоять слежке американских спецслужб // NewsOboz (http://newsoboz.org/it_tehnologii/google-usilit-sistemu-shifrov-chtoby-protivostoyat-slezhke-amerikanskih-09092013024500). – 2013. – 9.09).***

***

Громадські організації примусили через суд Міністерство юстиції США опублікувати матеріали щодо діяльності Агентства національної безпеки США.

За рішенням суду, що було прийнято за позовом до суду, який був поданий від Міжнародної некомерційної юридичної організації, що спеціалізується на захисті громадянських прав у галузі комп'ютерних і телекомунікаційних технологій EFF (Electronic Frontier Foundation), Міністерство юстиції США розсекретить деякі матеріали щодо діяльності спецслужб ***(Громадські організації примусили через суд Міністерство юстиції США опублікувати матеріали // Державна служба України з питань захисту персональних даних (http://zpd.gov.ua/dszpd/uk/publish/article/62280). – 2013. – 9.09).***

***

Найбільші світові інтернет-компанії звернулися до суду з вимогою дозволити публікацію даних про кількість і характер запитів до них з боку Агентства національної безпеки (АНБ). Свої позови направили Facebook, Yahoo і Google.

Юрисконсульт Yahoo Р. Белл заявив, що уряд США не повинен забороняти IT-компаніям розкривати кількість звернень від спецслужб.

Глава юрслужби Facebook К. Стретч зазначив, що користувачі повинні більше знати про урядові програми.

Раніше декілька десятків ІТ-компаній США звернулися до Б. Обами й членів Конгресу з проханням дати їм можливість публікувати дані про кількість запитів з боку державних агентств.

Раніше повідомлялося, що Google заплатить 8,5 млн дол. за розголошення приватної інформації ***(Facebook, Yahoo і Google просять суд дозволити їм публікувати запити спецслужб США // Голос столиці (http://newsradio.com.ua/2013_09_10/Facebook-Yahoo-Google-prosjat-sud-dozvoliti-m-publ-kuvati-zapiti-specsluzhb-SSHA). – 2013. – 10.09).***

***

В Китае приняли новый закон, который позволяет привлекать граждан к ответственности за клевету. Об этом сообщают «Комментарии».

Ответить по закону за ложную информацию придется в том случае, если озвученное получит широкое распространение в сети. Так, автора ложного сообщения, получившего более 500 репостов, можно будет приговорить к трем годам лишения свободы. Тюремные сроки предусмотрены также для авторов сообщений, собравших более 5 тыс. просмотров.

Китайские власти принятие закона объясняют тем, что люди, идя на поводу у «безответственных слухов», которые распространяются в сети, часто переживают «духовные терзания».

Борьба правительства КНР с распространением клеветы в Интернете началась несколько месяцев назад, вскоре после приход к власти президента С. Цзиньпина. В течение последних недель за распространение ложной информации в сети были допрошены несколько сот человек, часть из которых были впоследствии помещены под стражу.

Одним из самых громких дел стало задержание 27 человек в г. Ухань. В связи с их поимкой было объявлено, что городская полиция «пресекла деятельность преступной группы, распространявшей слухи в сети».

Напомним, что 18 сентября 2012 г. Верховная Рада Украины приняла закон о введение уголовной ответственности за клевету. Документ вызвал волну массового протеста. 2 октября 2012 г. ВР отменила законопроект о клевете ***(Китайские власти будут сажать за ложь в сети // Левый берег (http://society.lb.ua/life/2013/09/09/225192_kitayskie_vlasti_sazhat_lozh.html). – 2013. – 9.09).***

***

Британские ученые разработали компьютерную программу которая, по их словам, может точно отобразить настроение и реакцию жителей страны на события, анализируя эмоциональное содержание сообщений в Twitter.

Программа называется Emotive и может сканировать до 2 тыс. твитов в секунду и оценить их в соответствии с восемью человеческими эмоциями, среди них – гнев, отвращение и счастье.

Команда исследователей из Университета Лафборо отмечает, что Emotive можно использовать во множестве случаев, к примеру программа

может помочь полиции отслеживать угрозы в реальном времени. С помощью Emotive можно будет определить реакцию людей на инициативы правительства.

Ученые добавляют, что также просто Emotive может анализировать твиты 500 млн пользователей сети по всему миру. Об этом сообщает BBC Русская служба ***(Emotive изучит настроение пользователей Twitter // Електронні Вісті (http://elvisti.com/node/130259). – 2013. – 9.09).***

***

Анонимайзер Tor – одна из немногих сетей, которая позволяет интернет-пользователям скрыть свою деятельность от любопытных представителей правительства и других компаний. Однако недавно выяснилось, что Tor не обеспечивает анонимность от шпионажа со стороны АНБ США.

Оказывается, АНБ вместе с Министерством обороны США на 40 % спонсируют развитие проекта Tor. Помимо того, выделением средств также занималось Министерство иностранных дел США и другие правительственные организации. В общей сложности США выделяют около 60 % всех средств, которые предоставляются на развитие анонимайзера. «Представители правительств США и Швеции, которые нас финансируют, хотят удостовериться, что в будущем в Интернете будет существовать анонимность и конфиденциальность», – написал исполнительный директор Tor Э. Дьюмен в письме электронной почты, отправленном пользователям анонимайзера.

Сложившаяся ситуация вызывает определенные опасения, так как финансирование Tor со стороны правительств может позволить им использовать сеть в своих целях. Администрация анонимайзера в свою очередь отмечает, что США не будут давить на нее, так как сами полагаются на ее услуги ***(Американское правительство финансирует проект Tor // InternetUA (http://internetua.com/amerikanskoe-pravitelstvo-finansiruet-proekt-Tor). – 2013. – 10.09).***

***

Університет Джорджа Вашингтона склав еволюцію шпигунських програм США.

Університет Джорджа Вашингтона, який, до речі, також є «кузнею кадрів» американських спецслужб, у рубриці «Електронний архів національної безпеки» опублікував «Справу Сноудена» (National Security Archive Electronic Briefing Book No. 436 // http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436). Він містить документи Білого дому, Управління директора національної розвідки (ODNI), а також безпосередньо АНБ.

Документи висвітлюють такі питання:

– зусилля ODNI та Білого дому для пояснень, виправдовувань і захисту програм електронного стеження;

– кореспонденція між критиками системи електронного шпигунства й посадовими особами держави;

– фактологічні документи АНБ;

– ключові закони й судові рішення щодо електронного шпигунства, враховуючи Верховний суд США й суди іноземних держав;

– документи щодо організації електронного шпигунства й програм, пропозиції щодо збирання масових даних;

– інструкції щодо того, як використовувати Інтернет для шпигунських цілей ***(Університет Джорджа Вашингтона склав еволюцію шпигунських програм США // Державна служба України з питань захисту персональних даних (http://zpd.gov.ua/dszpd/uk/publish/article/62266). – 2013. – 9.09).***

***

У березні цього року громадська організація «Репортери без кордонів» почала формування переліку компаній – «цифрових найманців», які продають державам з авторитарними режимами обладнання для стеження, зокрема за громадянами.

Незважаючи на відсутність документів, які підтверджують факт зв'язків з авторитарними режимами, як підстави використовують документи, виявлені WikiLeaks.

Перелік таких послуг, які надають «цифрові найманці», є великим: «законне перехоплення», «масовий моніторинг», «реєстрація мережевих даних» тощо.

Один з оприлюднених документів, датований 2011 р., демонструє злагоджену роботу таких компаній, як британська Gamma Group, німецька Desoma і швейцарська Dreamlab, з метою «створення систем телекомунікаційної розвідки для різноманітних телекомунікаційних мереж з урахуванням потреб і побажань клієнта щодо «законного перехоплення, масового перехоплення даних, утримання даних і контролю над трафіком/додатками/протоколом (блокування та обмеження трафіку)». Крім того, також називаються такі компанії, як Cobham, Amees, Digital Barriers, ETL Group, UTIMACO, Telesoft Technologies и Trovicor ***(В березні цього року громадська організація «Репортери без кордонів» почала формування переліку компаній – «ЦИФРОВИХ НАЙМАНЦІВ» // Державна служба України з питань захисту персональних даних (http://zpd.gov.ua/dszpd/uk/publish/article/62217). – 2013. – 6.09).***

***

Действия Э. Сноудена, разоблачившего секретные американские программы ведения слежки, спровоцировали дискуссию о необходимости выбора между защитой личной информации и обеспечением национальной безопасности. Об этом заявил 12 сентября в Вашингтоне директор

национальной разведки США Д. Клэппер. Он выступил на конференции Национального альянса по безопасности.

Д. Клэппер назвал Э. Сноудена «одной из главных угроз» американскому разведывательному сообществу. Директор подчеркнул, что не рассматривает бывшего сотрудника ЦРУ как изобличителя и назвал его поступок вопиющим.

Вместе с тем глава нацразведки оговорился, что подобные дискуссии неизбежно «должны были начаться». «К сожалению, это не произошло раньше. Они еще будут продолжаться», – добавил он. В этой связи Д. Клэппер обратил особое внимание на вопросы подотчетности разведсообщества. «Думаю, мы должны быть более открытыми в том, что делаем, что заставляет нас идти на те или иные шаги и каких результатов добиваемся», – указал он. При этом Д. Клэппер напомнил, что недавно его ведомство «опубликовало 1,8 тыс. страниц постановлений секретного суда, действующего в рамках Закона о наблюдении за иностранной разведкой».

Д. Клэппер также отметил, что разведсообщество США предпринимает дополнительные усилия, чтобы его члены в дальнейшем не смогли пойти по стопам Э. Сноудена. «Мы концентрируемся на предотвращении подобных внутренних угроз», – подчеркнул он.

В числе главных проблем, с которыми сталкиваются разведструктуры США, Д. Клэппер назвал сокращение бюджета его службы и рост числа кибератак ***(Действия Сноудена спровоцировали дискуссию о выборе между защитой личной информации и безопасностью страны – директор нацразведки США // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2013/09/13/snowden-leaks-spark discussion.html). – 2013. – 13.09).***

***

Правительство Индии осуществляет наблюдение за большим количеством индийских интернет-пользователей при помощи систем перехвата, размещенных в международных шлюзах крупных провайдеров. Об этом 9 сентября сообщило издание The Hindu. Согласно данным газеты, Центр развития телематики (Centre for Development of Telematics, C-DOT) развернул системы перехвата и мониторинга (Lawful Intercept and Monitoring, LIM), нарушив тем самым законодательство Индии касательно защиты персональных данных.

Системы LIM полностью принадлежат и управляются правительством и отличаются от подобных систем, используемых индийскими провайдерами мобильной связи, которые должны соответствовать разделу 5 (2) Закона Индии о телеграфе (Indian Telegraph Act and Rule), а также правилу 419 (A) свода законов об ИТ.

Отметим, что в 2006 г. правительство выпустило «Инструкцию по обеспечению конфиденциальности связи», вводящую должность «узловых офицеров», которые должны присутствовать в каждой интернет-компании. Согласно документу, «узловой офицер» должен сотрудничать с

правительством и предоставлять доступ к запрашиваемым им данным. Тем не менее, такая должность есть далеко не у каждого провайдера. В любом случае, системы LIM действуют автономно, без какого-либо сотрудничества с поставщиками интернет-услуг.

Системы LIM, вероятно, устанавливаются между граничным маршрутизатором и корневой сетью и обладают 100-процентным доступом к онлайн-активности 160 млн интернет-пользователей Индии. При этом провайдеры могут даже не догадываться о проводимом мониторинге электронной почты, URL и IP-адресов ***(Правительство Индии осуществляет наблюдение за большим количеством интернет-пользователей // InternetUA (http://internetua.com/pravitelstvo-indii-osusxestvlyaet-nabluadenie-za-bolshim-kolicsestvom-internet-polzovatelei). – 2013. – 9.09).***

***

Продолжается череда публикаций о деятельности Агентства национальной безопасности. На этот раз стало известно, что АНБ, помимо всего прочего, шпионит еще и за финансовыми транзакциями, осуществляемыми через телекоммуникационные каналы и цифровые устройства. Об этом передает немецкий журнал Der Spiegel со ссылкой на документы, полученные от беглого экс-сотрудника ЦРУ Э. Сноудена.

Программа имеет кодовое название «Следуя за деньгами», которая позволяет мониторить поток банковских операций и платежей, совершенных при помощи кредитных карт. Согласно секретным документам, оказавшимся в распоряжении журналистов, программа позволила спецслужбам за 2011 г. собрать порядка 180 млн финансовых записей, большая часть из которых – операции по кредиткам.

Транзакции хранятся в базе данных АНБ, носящей незамысловатое кодовое имя Tracfin. Издание называет как минимум две компании, которые являются приоритетными целями: это Visa, а также SWIFT – Сообщество всемирных межбанковских финансовых телекоммуникаций) – международная межбанковская система передачи информации и совершения платежей, базирующаяся в Бельгии.

Согласно раскрытым документам география слежки охватывала Европу, Африку и Средний Восток, откуда «собирались, анализировались и хранились транзакционные данные по кредитным картам, с фокусировкой на приоритетные географические регионы».

Представитель Visa не сразу отреагировал на запрос о комментарии ситуации, но затем подтвердил изданию Mashable, что возможность вмешаться в сети компании для изъятия определенной информации действительно есть.

Согласно одному из документов спецслужбы Великобритании в лице GCHQ сотрудничали с АНБ в финансовой слежке ***(Сноуден: Спецслужбы США собирали данные о финансовых транзакциях граждан // InternetUA***

***(http://internetua.com/snouden--specslujbi-ssha-sobirali-dannie-o-finansovih-tranzakciyah-grajdan). – 2013. – 16.09).***

***

В Иране доступ к социальной сети Facebook и сервису микроблогов Twitter для пользователей был открыт в результате технической ошибки.

Об этом сообщает информагентство Reuters со ссылкой на правительство Ирана, передает NewsOboz.org со ссылкой на Lenta.ru.

По словам главы иранского госкомитета по контролю за Интернетом А. Хоромабади, сбой в системе фильтрации, открывший доступ к нескольким запрещенным в стране сайтам и социальным сетям, произошел по вине иранских интернет-провайдеров.

«В настоящее время правительство проводит расследование произошедшего и устанавливает компании, ответственные за сбой», – заявил А. Хоромабади.

Напомним, о том, что Facebook и Twitter стали доступны для иранских пользователей стало известно в ночь на вторник, 17 сентября. Об этом сообщили корреспонденты американских изданий The New York Times и The Washington Post в Тегеране, сославшись на сообщения пользователей внутри страны. При этом никаких официальных сообщений о снятии блокировки с сайтов не поступало.

Обратим внимание, что Twitter и Facebook были заблокированы властями Ирана в 2009 г. В 2013 г., после избрания президентом страны Х. Рухани, в Иране заговорили об ослаблении ограничений в интернет-сфере. В частности, в сентябре 2013 г. страницы в Facebook и Twitter завели все члены иранского кабинета министров. Однако никаких конкретных шагов по снятию блокировки для рядовых пользователей до сих пор не предпринималось.

Кроме вышесказанного добавим, что на Ближнем Востоке у соцсетей-представителей западных государств довольно часто возникают проблемы с местными властями. Так, ранее стало известно, что Саудовская Аравия намерена запретить WhatsApp, в том случае, если американская компания не согласится предоставить доступ к своим серверам местным правоохранительным органам. В ОАЭ продвинулись дальше по этому пути, Skype и Viber закрыты в Эмиратах уже год ***(Открытие доступа к Facebook и Twitter в Иране оказалось технической ошибкой // NewsOboz (http://newsoboz.org/it_tehnologii/mnogoletniy-zapret-v-sile-otkrytie-dostupa-k-facebook-i-twitter-17092013140300). – 2013. – 17.09).***

***

Группа американских и китайских граждан обвинила производителя сетевого оборудования Cisco Systems во вступлении в тайный сговор с китайским правительством с целью негласного мониторинга и выявления членов запрещенной в Китае религиозно-политической организации

Фалуньгун. В иске Cisco обвиняется в «прямом нарушении прав человека» и злоупотреблении своими технологиями на рынке сетевого аппаратного обеспечения.

В иске говорится, что в штаб-квартире Cisco в Сан-Хосе разрабатывались и тестировались решения для сбора разведывательных данных и технология безопасности, известная как «Золотой щит». Судебный иск против компании был подан в федеральный суд города Сан-Хосе 19 сентября.

В документе сказано, что компания спроектировала «Золотой щит» таким образом, чтобы технология могла идентифицировать, отслеживать и изолировать представителей Фалуньгун. «Связи Cicso с правительством Китая прямо указывают на нарушение прав человека компанией», – следует из иска.

В иске также говорится, что крупнейший производителей сетевых решений сотрудничал с китайскими партийными властями как минимум с 2011 г. Такое сотрудничество уже привело к нескольким арестам последователей Фалуньгун.

В пресс-службе Cisco заявили, что считают иск безосновательным и бездоказательным ***(Cisco обвиняют в создании шпионских средств для властей Китая // InternetUA (http://internetua.com/Cisco-obvinyauat-v-sozdanii-shpionskih-sredstv-dlya-vlastei-kitaya). – 2013. – 20.09).***

***

Новые документы, переданные Э. Сноуденом немецкому изданию Der Spiegel, говорят о том, что британская разведка GCHQ стояла за взломом IT-систем крупнейшего в Бельгии оператора связи Belgacom, а также за размещение шпионских кодов на серверах оператора. Ранее в этом подозревали американские спецслужбы.

Газета сообщает, что британские разведчики целенаправленно инфицировали компьютеры нескольких сотрудников Belgacom в рамках атаки, известной как Quantum Insert, которая изначально была создана представителями АНБ США, но реализовывалась полностью британцами. Конечной целью атаки было получение доступа к корневым сетевым маршрутизаторам бельгийского оператора, чтобы проводить анализ перехваченного трафика в Интернете и сотовых сетях.

Также в документах, полученных Der Spiegel, говорилось, что британские разведчики интересовались компанией BICS – совместным предприятием Belgacom, Swisscom и южноафриканской MTN, которая занималась оптовыми продажами услуг проводной телефонии другим операторам, в частности в Йемене и Сирии. Кроме того BICS имела доступ к ряду трансконтинентальных интернет-кабелей для передачи трафика.

Сообщается, что в задачи британских разведчиков входило детальное исследование VPN-инфраструктуры Belgacom и BICS, а также проведение атак типа Man in the middle. Напомним, что в начале этой недели Belgacom официально заявила, что ее внутренние системы были скомпрометированы,

однако в компании заявили, что взломщикам не удалось добраться до «инфраструктуры доставки трафика».

Der Spigel отмечает, что по-хорошему Belgacom следовало бы подать в суд на GCHQ, однако скорее всего этого не будет и Бельгия с Великобританией обменяются просто обменяются дипломатическими колкостями на этот счет, так как две страны являются партнерами по НАТО ***(Британская разведка обвиняется во взломе бельгийского оператора Belgacom // InternetUA (http://internetua.com/britanskaya-razvedka-obvinyaetsya-vo-vzlome-belgiiskogo-operatora-Belgacom). – 2013. – 22.09).***

## Проблема захисту даних. DOS та вірусні атаки

Хакерская группа Anonymous опубликовала обращение к США с угрозой начать кибервойну, пишет «Обозреватель» (http://tech.obozrevatel.com/news/31687-hakeryi-anonymous-obyavili-vojnu-ssha.htm).

«Мы объявляем о мобилизации хакеров со всей планеты для принятия участия в боевых действиях против США. Оружие хакера причиняет больше урона боеспособности врага, чем какие-то пули», – заявили Anonymous.

Хакеры пообещали парализовать все средства массовой информации, прекратить работу крупнейших банков США, нанести непоправимый вред всем узлам удаленного управления, таким инфраструктурам как энергетика, водоснабжение и логистика.

«Это война, настоящая война», – подчеркнули хакеры и отметили, что начнется она в день, когда на землю Сирии ступит нога первого американского оккупанта.

Также Anonymous подчеркнули, что уже через неделю после вторжения в Сирию «против оккупантов обрушится вся хакерская мощь планеты». И при этом отметили, что не будут атаковать Пентагон, а полностью уничтожат экономику страны ***(Хакеры Anonymous объявили войну США // Обозреватель (http://tech.obozrevatel.com/news/31687-hakeryi-anonymous-obyavili-vojnu-ssha.htm). – 2013. – 10.09).***

***

Компания ESET предупреждает о появлении сложной вредоносной программы Hesperbot, высокая активность которой зафиксирована в Турции, Чехии, Великобритании и Португалии.

Hesperbot – это комплексный троян, предназначенный для хищения различной информации с компьютера пользователя. Он способен инфицировать мобильные устройства, работающие под управлением операционных систем Android, Symbian и Blackberry.

При распространении Hesperbot злоумышленники применяют целенаправленный фишинг, в зависимости от страны меняя язык рассылаемых сообщений, а также используя различные информационные поводы, актуальные для того или иного региона.

Троян обладает широкими возможностями по краже конфиденциальных данных. В своём арсенале он содержит клавиатурный шпион, модуль для снятия скриншотов рабочего стола и захвата видео, а также может устанавливать скрытное удалённое прокси-соединение.

Hesperbot относится к классу банковских троянов. Распространение вредоносной программы началось в Чехии в августе 2013 г. Для доставки файла угрозы злоумышленники выбрали специальный URL-адрес с доменом, который напоминает веб-сайт чешской почтовой службы www.ceskaposta.net. При этом в фишинговом сообщении говорилось о якобы отправленной пользователем посылке.

Основной целью злоумышленников является получение учётных данных, которые пользователи применяют для входа на свой аккаунт системы онлайн-банкинга ***(Обнаружен сложный банковский троян Hesperbot с мобильным компонентом // InternetUA (http://internetua.com/obnarujen-slojnii-bankovskii-troyan-Hesperbot-s-mobilnim-komponentom). – 2013. – 9.09).***

***

Компания «Доктор Веб» предупредила о широком распространении вредоносной программы BackDoor.Saker.1, обходящей механизм контроля учетных записей пользователей. Основная функция BackDoor.Saker.1 – выполнение поступающих от злоумышленников команд, и, главное, перехват нажимаемых пользователем клавиш (кейлоггинг).

Проникнув на инфицируемый компьютер, троянец запускает на исполнение файл temp.exe, предназначенный для обхода системы контроля учетных записей пользователей (User Accounts Control, UAC). Этот файл извлекает из ресурсов библиотеку для обхода UAC и встраивается в процесс explorer.exe. После этого данная библиотека сохраняется в одной из системных папок. Далее, при запуске системной утилиты Sysprep, эта библиотека запускает вредоносное приложение ps.exe, детектируемое антивирусным ПО Dr.Web как Trojan.MulDrop4.61259. В свою очередь, данный файл сохраняет в другую папку еще одну библиотеку, которую регистрирует в реестре Windows в качестве службы с именем «Net Security Service» и следующим описанием: «keep watch on system security and configuration.if this services is stopped, protoected content might not be down loaded to the device». Именно в этой библиотеке и сосредоточен основной вредоносный функционал бэкдора.

После успешного запуска BackDoor.Saker.1 собирает и передаёт злоумышленникам сведения об инфицируемом компьютере, включая версию Windows, тактовую частоту процессора, объём физической оперативной памяти, имя компьютера, имя пользователя, серийный номер жесткого диска.

Затем троянец создает в одной из системных папок файл, в который записываются нажатия пользователем клавиш на клавиатуре компьютера. После этого бэкдор ожидает ответ от удаленного сервера, в котором могут содержаться следующие команды: перезагрузка, выключение компьютера, самоудаление, запуск отдельного потока для выполнения команды через командный интерпретатор, или для запуска собственного файлового менеджера, который имеет возможность выгружать файлы с машины пользователя, загружать файлы по сети, создавать папки, удалять, перемещать файлы, а также запускать их ***(Новый бэкдор перехватывает вводимые с клавиатуры данные // InternetUA (http://internetua.com/novii-bekdor-perehvativaet-vvodimie-s-klaviaturi-dannie). – 2013. – 10.09).***

***

В Интернете за 800 дол. можно приобрести PHP-сценарий для эффективных DDoS-атак. Этот сценарий использует готовые скомпрометированные серверы и может осуществлять DDoS-атаки четырьмя методами.

Ранее в этом году организация US-CERT выпустила уведомление, в котором сообщила, что в открытом доступе появились рекурсивные DNS-серверы, активно используемые для атаки усиления DNS (DNS amplification attack), очень эффективного метода DDoS-атак.

Нередко проблема состоит в некорректной настройке серверов доменных имен, что позволяет злоумышленнику отправить DNS-запрос, при котором исходный адрес подменяется адресом жертвы. Когда DNS-сервер отправляет ответ, он содержит адрес жертвы. Огромное количество подобных ложных запросов становится причиной конечного отказа в обслуживании.

Возможно, некоторые системные администраторы в США приняли угрозу всерьез и перенастроили собственные серверы таким образом, чтобы предотвратить дальнейшие взломы, однако данный метод атаки сохраняет свою популярность, причем не только на Западе.

Эксперт Webroot Д. Данчев написал в блоге компании о том, что хакеры на специализируемых форумах занимаются продажей и покупкой PHP-сценария, с помощью которого, используя уже готовые скомпрометированные серверы, можно осуществлять DDoS-атаки.

«На текущий момент PHP-сценарий поддерживает четыре типа тактик DDoS, а именно: усиление DNS, подмену SYN, подмену UDP и поддержку HTTP+proxy. Сценарий также действует как централизованный интерфейс управления всех серверов, на которые он был секретно установлен», – заявил эксперт.

Цена сценария сейчас составляет 800 дол., но исследователь отмечает, что когда он выйдет из ранних этапов развития, разработчики повысят цену. Д. Данчев не знает, применяется ли этот сценарий на практике, но уверен, что со временем он найдет своих жертв ***(В интернете за $800 можно приобрести PHP-сценарий для эффективных DDoS-атак // InternetUA***

***(http://internetua.com/v-internete-za--800-mojno-priobresti-PHP-scenarii-dlya-effektivnih-DDoS-atak). – 2013. – 11.09).***

***

Координационный центр национальных доменов .ru и .рф объявил о создании информационного ресурса, позволяющего проверять интернет-сайты на вирусную активность. Об этом, со ссылкой на главу Координационного центра А. Колесникова, 11 сентября сообщил ИТАР-ТАСС.

По словам А. Колесникова, новый ресурс будет собирать всю информацию о вирусной активности в доменных зонах .ru и .рф, а также позволит пользователям в онлайн-режиме получать динамические отчеты об угрозах на том или ином портале.

Располагаться ресурс будет по адресу netoscope.ru. Работу над его созданием совместно с координационным центром ведут такие представители интернет-индустрии, как «Яндекс», Mail.Ru Group, «Лаборатория Касперского» и Ru-Center.

О подготовке проекта к запуску А. Колесников объявил в рамках первого дня начавшейся в Греции Международной конференции администраторов и регистраторов стран СНГ, Центральной и Восточной Европы. Также в рамках конференции планируется обсудить модели дальнейшего развития кириллических доменов верхнего уровня и работу «антипиратского» закона, вступившего в силу 1 августа 2013 г. Международная конференция под эгидой Координационного центра национальных доменов проходит уже в шестой раз ***(Информацию о вирусной активности в Рунете соберут на едином портале // InternetUA (http://internetua.com/informaciua-o-virusnoi-aktivnosti-v-runete-soberut-na-edinom-portale). – 2013. – 12.09).***

***

Федеральная торговая комиссия США (FTC) оценит правомерность запланированных соцсетью Facebook изменений в правилах сервиса и политике в отношении пользовательских данных, сообщает New York Times со ссылкой на представителя регулятора.

По мнению критиков новых правил, среди которых американский сенатор Э. Марки и шесть правозащитных организаций, изменения позволят Facebook передавать любую информацию пользователей без их разрешения третьим сторонам для использования в рекламных целях. Кроме того, новые условия якобы лишат пользователей возможности ограничивать подобное использование своих данных. Компания Facebook, однако, отрицает сам факт какого-либо изменения действующих правил по существу, утверждая, что обновление текста призвано лишь разъяснить пользователям суть действующей политики.

Новую редакцию основных документов, регламентирующих взаимоотношения соцсети и ее пользователей, Facebook обнародовала

29 августа, запланировав ввести ее в действие уже через неделю после публикации, 5 сентября. Однако, как сообщал Digit.ru, Facebook отложила введение новых правил с целью рассмотрения отзывов пользователей.

В действующих правилах, в частности, явно прописано право пользователя ограничивать использование его имени и фотографии в рекламных целях. В новой версии правил это положение удалено, но добавлен пункт, обязывающий Facebook учитывать установленную пользователем аудиторию, имеющую доступ к его контенту. Также, согласно новым правилам, помимо профильной фотографии и имени пользователя в рекламных целях может использоваться любая загруженная им информация.

Федеральная торговая комиссия проверит соответствие нового текста правил соглашению, заключенному между Facebook и регулятором в 2011 г. Это соглашение обязывает соцсеть запрашивать у пользователей разрешение на передачу их данных, осуществляемую в обход установленных пользователями настроек конфиденциальности ***(Новые правила Facebook будут проверены регуляторами США // InternetUA (http://internetua.com/novie-pravila-Facebook-budut-provereni-regulyatorami-ssha). – 2013. – 13.09).***

***

Хакеры пытаются взломать новую iOS 7

Команда хакеров Evad3rs, которой удалось выпустить утилиту для непривязанного джейлбрейка iOS 6, приступила к изучению новой мобильной операционной системы Apple.

Известный хакер Planetbeing сообщил о начале тестирования iOS 7 GM, а также поделился первыми успехами.

«С помощью архивных инструментов удалось выполнить неподписанный код в userland. Теперь у нас есть платформа для получения доступа к ядру», – заявил разработчик.

Это отличные новости для джейлбрейк-сообщества, но не стоит забывать, что сейчас речь идет лишь о подготовительном этапе. Хакерам нужно испробовать существующие инструменты для взлома и разработать новые, чтобы подготовить общедоступную утилиту. Это будет не скоро ***(Хакеры пытаются взломать новую iOS 7 // InternetUA (http://internetua.com/hakeri-pitauatsya-vzlomat-novuua-iOS-7). – 2013. – 15.09).***

***

Если ваше Android-устройство (смарфтон или планшет) когда-нибудь авторизовался в каком-нибудь Wi-Fi-хотспоте, то с большой долей вероятности пароль от хотспота стал известен также и компании Google. Учитывая, как много «андроидов» ходит по миру, можно предположить, что у Google есть доступ практически ко всем запароленным точкам доступа в мире.

По статистике IDC, во II квартале 2013 г. было продано 187 млн устройств, что соответствует 748 млн в год. И это не считая планшетов.

Начиная с версии Android 2.2 операционная система сконфигурирована по умолчанию на автоматический бэкап настроек системы. Для большинства пользователей эта опция кажется полезной, так что почти никто не меняет настройки по умолчанию: кому хочется потом заново конфигурировать десятки и десятки опций? Но мало кто понимает, что среди настроек на серверы Google передаются также пароли от точек доступа в незашифрованном виде, то есть открытым текстом. По крайней мере, в Android 2.3.4 соответствующая настройка называется Back up my settings, Back up my data или Back up current settings and application data, но сам термин Wi-Fi вообще не упоминается. Только в версии Android 4.2 к опции Back up my data описание мелким шрифтом честно сообщает о «резервном копировании настроек приложений, паролей Wi-Fi и других настроек на серверах Google».

Пользователи Android 2.3.4, если они хотят узнать, что конкретно подпадает под резервное копирование и куда сохраняются данные, должны прочитать страницу 374 в «Руководстве пользователя Android».

В случае с устройством Galaxy Nexus и операционной системой Android 4.0 о передаче паролей Wi-Fi говорится на странице 97 «Руководства пользователя Galaxy Nexus».

Нужно понимать, что Google – американская компания, подчиняется местным законам и обязана выдать правоохранительным органам любую личную информацию о пользователе, которая хранится у них на серверах, если получит такой запрос. Так что властям не нужно взламывать шифры WPS, пароль они могут узнать открытым текстом, пишет ComputerWorld ***(Google знает почти все WIFi-пароли в мире // InternetUA (http://internetua.com/Google-znaet-pocsti-vse-WIFi-paroli-v-mire). – 2013. – 16.09).***

***

Для атаки на клиентов электронных платежных систем киберпреступники научились использовать «технологии облаков». Такие данные обнародовала немецкая компания G Data, сообщает Digit.ru.

«На стороне пользователя злоумышленники перехватывают данные платежных операций с помощью вредоносного ПО, а элементы вредоносного кода размещают в “облаке”. Это осложняет анализ атак и создание эффективных инструментов борьбы новой угрозой», – отмечают эксперты.

Обычно для атаки на банковские счета вредоносное ПО использует конфигурационные файлы на компьютере пользователя. Они содержат адреса часто посещаемых сайтов, на которые планируется нападение.

Для размещения вредоносного кода на этих сайтах используются банковские троянцы.

Они помогают хакерам похитить данные доступа и персональную информацию пользователей.

Банковский троян ZeuS размещает не весь вирус на атакуемый сайт, а его часть – в виде Javascript, которая затем загружает из «облака» остальные компоненты вредоносного ПО.

В последнее время появилась усовершенствованная технология атак на клиентов банков, троянец Ciavax.

«От своего предшественника она отличается тем, что не позволяет антивирусным программам определить сайты, которые собираются взломать злоумышленники», – объясняет антивирусный эксперт G Data Т. Зиберт.

Это свидетельствует о росте профессионализма писателей вирусов, отметил он ***(Хакеры атакуют счета с помощью облачных технологий // Utro.ua (http://www.utro.ua/ru/proisshestviya/hakery_atakuyut_scheta_s_pomoshchyu_oblachnyh_tehnologiy1379227308). – 2013. – 16.09).***

***

Сотрудники Университета Райса и специализирующейся на компьютерной безопасности компании RSA разработали систему шифрования, которая позволяет защитить электрокардиостимуляторы от атак хакеров и одновременно не требует сложной системы аутентификации. Подробности системы приводит блог Массачусетского технологического института, передает NewsOboz.org со ссылкой на Lenta.ru.

Система предназначена для вживляемых устройств, которые способны обновляться по беспроводному каналу. В настоящее время такие системы обычно никак не защищены от действия потенциальных хакеров, которые могут отключить кардиостимулятор, заставить его работать в неправильном режиме или тратить заряд впустую.

Чтобы защитить устройство от незаконного проникновения, ученые предлагают проводить аутентификацию на основе сравнения данных о пульсе. При этом устройство будет предоставлять доступ только в том случае, когда собственные данные устройства совпадут с теми, которые транслирует внешняя система, которая предлагает обновление. Таким образом доступ к имплантированному устройству получит только тот, кто сможет находиться в непосредственном контакте с пациентом.

По словам авторов, одним из главных преимуществ такой системы аутентификации является отсутствие каких либо паролей, которые в экстренной ситуации будет сложно вспомнить и относительная простота реализации.

Тем не менее, при должном желании со стороны злоумышленника у него остаются достаточно широкие возможности для незаконного проникновения. Дело в том, что сердечные сокращения, как показали недавние исследования, можно считывать на расстоянии с помощью искусственного усиления незаметной для глаза пульсации крупных сосудов ***(Кардиостимуляторы обзавелись защитой от хакеров // NewsOboz (http://newsoboz.org/mir/kardiostimulyatory-obzavelis-zashchitoy-ot-hakerov-17092013033000). – 2013. – 17.09).***

***

Администратор системы сканирования сайтов Sucuri рассказал о том, что в сети появилась первая программа, которая предоставляет сторонним пользователям доступ к ресурсу, созданная без единой буквы или цифры в коде, пишет imena.ua.

Так, один из западных веб-сайтов недавно взломали при помощи бэкдора, в коде которого не было ни единой буквы или цифры.

Специалисты поясняют, что, поскольку суть программ-бэкдоров в максимальной скрытности, их авторы часто прибегают к необычным методам запутывания кода. Например, первая строчка @$_[]=@!+_ интерпретируется как array(true).

Таким образом, бессмысленный, на первый взгляд, набор символов оказывается опасной программой, которая может предоставить злоумышленнику доступ к тому или иному сайту.

Но когда исследователи разобрали по строчкам обнаруженную на сайте программу, они установили, что она без цифр и букв находится в «режиме ожидания», дожидаясь, когда получит программный аргумент с шифрованной командой для исполнения на сервере.

Только после получения команды бэкдор начинает активную работу. До этого же зловредный код может храниться на сервере годами, будучи невидимым для стандартных на сегодняшний день средств безопасности ***(В сети появился незаметный для защиты вирус без букв и цифр в коде // Версии.com (http://www.versii.com.ua/news/286976/). – 2013. – 17.09).***

***

Издание Forbes подготовило свой рейтинг самых громких киберпреступлений, совершенных в последнее время.

Самым громким преступлением в сфере информационной безопасности, по мнению экспертов издания, стала атака на компанию HBGary Federal. Спровоцировал атаку глава компании, который заявил, что внедрился в хакерскую группу Anonymous и раскрыл ее лидеров. Через сутки Anonymos взломали серверы HBGary Federal и вывесили всю внутреннюю переписку сотрудников – более 71 тыс. сообщений – на файлообменных ресурсах. «HBGary, вы сами навлекли на себя наш гнев. Вы пытались укусить Anonymous за руку и получили пощечину. Вы думали, что конфликт с нами ограничится перебранкой, но теперь вы испытаете на себе всю ярость Anonymous», – заявила группа.

На втором месте оказалась атака Anonymous на платежные системы MasterCard, Visa и Paypal, когда те в конце 2010 г. отказались принимать платежи для сайта WikiLeaks. «Операция “Расплата”. Цель: www.visa.com. Огонь!» – заявили хакеры в Twitter. Ущерб от атаки достиг 5,5 млн дол. В эту сумму включены прямые убытки компаний от простоя, а также затраты на обновление систем безопасности.

Замыкает тройку лидеров атака на Citibank в июне 2011 г. Сначала сообщалось, что в руки злоумышленников попали только имена, номера счетов и контактная информация более 360 тыс. вкладчиков. Позже руководство Citigroup признало, что хакеры похитили 2,7 млн дол. со счетов 3400 клиентов банка. Citibank обещал возместить понесенные клиентами убытки.

На четвертом месте – атака хакеров из Anonymous на сайты турецких государственных учреждений, президента и премьер-министра. Хакеры заявили, что таким образом пытаются поддержать антиправительственные демонстрации.

Пятое место в списке Forbes принадлежит взлому группировкой LulzSec телеканала PBS, который показал фильм WikiSecrets с критикой Д. Ассанжа и его информатора Б. Мэннинга. На главной странице сайта появилось сообщение: «All your base are belong to LulzSec» («Все ваши базы принадлежат LulzSec») и фальшивая история о том, что убитый рэппер Т. Шакур жив и находится в Новой Зеландии.

Номер шесть рейтинга – взлом игровой сети Sony PlayStation Network 17 апреля 2011 г. В результате кибератаки злоумышленники получили имена, адреса и учетные записи пользователей. Под удар попали и реквизиты кредитных карт, которые использовались для оплаты сервисов Sony. Совокупный ущерб, нанесенный компании составил 171 млн дол. В результате взлома произошла утечка личной информации 138 тыс. интернет-пользователей.

На седьмой строчке рейтинга оказалась неудавшаяся атака на Gmail путем кражи паролей, которую пытались осуществить хакеры из китайского города Джинан. В ходе расследования выяснилось, что хакеры пытались получить информацию о чиновниках и китайских активистах.

Восьмое место досталось взлому базы данных сайта американского сената, ответственность за который взяла на себя хакерская группа LulzSec. Свою атаку хакеры назвали «тренировкой перед более серьезным делом». Сразу после этого, 15 июня 2011 г., LulzSec атаковала сайт ЦРУ, заблокировав пользователям к нему доступ.

Замыкает список ряд атак на сайты правительства Египта, осуществленные в 2011 г. группировкой Anonymous в ответ на блокировку президентом Мубараком доступа граждан к соцсетям. В результате действий хакеров пострадали ресурсы Министерства информации, Министерства внутренних дел и Национальной демократической партии Египта ***(Составлен рейтинг наиболее громких кибератак последнего времени // InternetUA (http://internetua.com/sostavlen-reiting-naibolee-gromkih-kiberatak-poslednego-vremeni). – 2013. – 18.09).***

***

Исследователи из компании Symantec подготовили отчет о хорошо организованной группе хакеров из Китая, которая осуществляет нападения в цифровом пространстве на заказ. Объединение под названием Hidden Lynx

чаще всего проводить кампании, связанные с кибершпионажем, который исходит из Китая. В отличие от заявлений других IT-компаний, в Symantec не обвиняют китайское правительство в причастности к этим кибератакам.

В 28-страничном докладе, опубликованном Symantec, Hidden Lynx описывается, как профессиональная организация, которая состоит из 50–100 человек с различными навыками, необходимыми для взлома компьютерных сетей и кражи информации, в том числе корпоративных секретов. Предположительно, именно эта группа хакеров ответственна за проведение операции Aurora, в рамках которой были взломаны сети большого количества американских компаний (Google Inc, Adobe Systems и пр.).

В Symantec заявляют, что участники Hidden Lynx также нацеливались на финансовые организации, которые в большинстве случает располагали информацией о слиянии других предприятий или поглощении одной компании другой. Эта информация подтверждает, что заказчики хакеров были заинтересованы в переговорах о поглощениях и продаже акций.

По словам специалистов Symantec, коммерческие банки от рук Hidden Lynx не пострадали.

Среди вредоносным инструментов, используемых группой хакеров, оказались Trojan Naid и Trojan Moudoor, который похищали данные с инфицированных компьютеров ***(Раскрыта самая яркая и профессиональная хакерская группировка последних лет // InternetUA (http://internetua.com/raskrita-samaya-yarkaya-i-professionalnaya-hakerskaya-gruppirovka-poslednih-let). – 2013. – 19.09).***

***

Исследователи обнаружили вредоносную программу, которая устанавливает сразу несколько модулей на компьютеры своих жертв, «замораживая» деятельность жёсткого диска.

Эксперты из компании Bkav обнаружили и проанализировали так называемый руткит, который скрывает следы присутствия злоумышленника или вредоносной программы в системе.

«Заморозка» жёсткого диска является специфическим механизмом защиты руткита. Вирус запускает несколько модулей, которые исполняют основные функции вредоносного ПО, и способствуют его распространению.

Один из них, PassThru, – это драйвер сетевого модуля, блокирующий или перенаправляющий пользователя на определенные сайты. А модуль Wininite подключается к C&C-серверам и получает от них команды. Один из этих серверов расположен в Китае, а другой – в США.

Наконец, модуль DiskFit каждый раз после перезагрузки компьютера восстанавливает жёсткий диск компьютера до статуса, который был до инфицирования машины.

Кроме того, DiskFit создаёт на компьютере жертвы область для хранения кэшированных данных, в которой хранится информация обо всех операциях, осуществляемых пользователем.

Таким образом, пользователь не может вносить изменения в данные на оригинальном диске.

Каждый раз, когда пользователь проводит перезагрузку компьютера, все его действия на системе удаляются, начиная с создания или загрузки новых документов, и заканчивая установкой программного обеспечения ***(Новый вирус «замораживает» жёсткий диск // InternetUA (http://internetua.com/novii-virus--zamorajivaet--j-stkii-disk). – 2013. – 20.09).***

***

Более трети пользователей, регулярно подключающих свои устройства к публичным точкам доступа Wi-Fi, не принимают каких-либо мер безопасности. Таков итог специального исследования, проведенного по всему миру для «Лаборатории Касперского» летом 2013 г. Между тем для злоумышленников публичные сети Wi-Fi могут стать средством перехвата важных данных пользователя.

В ходе исследования, проведенного аналитическим агентством B2B International, было опрошено 8605 респондентов в возрасте 16+, проживающих в странах Латинской и Северной Америки, Ближнего Востока, Азии, Африки, Европы и России в частности.

Сегодня получить доступ в Интернет просто: помимо сотовых сетей и сетей проводного широкополосного доступа в распоряжении современного пользователя компьютеров и мобильных устройств практически всегда есть хотя бы один хот-спот, через который можно без проблем получить доступ в сеть. Однако ради удобства во многих публичных точках доступа не применяются вообще никакие меры защиты, и большое количество пользователей эта ситуация устраивает. Так, 36 % респондентов в России заявили, что не предпринимают никаких мер предосторожности, когда подключаются к публичным хот-спотам. При этом еще 8 % пользователей ответили, что через публичные точки доступа заходят на сервисы интернет-банкинга и в онлайн-магазины. И только 10 % опрошенных сообщили, что стараются проверять, какой стандарт шифрования используется в случае с конкретной точкой доступа.

Эксперты «Лаборатории Касперского» считают, что прибегать к дополнительной защите при подключении к публичной точке доступа – очень важная мера предосторожности, потому что никогда нельзя с точностью сказать, что делает «тот парень с ноутбуком за соседним столиком в кафе»: проверяет личную почту или просматривает интернет-трафик беспечных пользователей, сидящих вокруг. Атаки типа Man in the middle это позволяют. Точка доступа Wi-Fi является своего рода окном в Интернет для множества подключенных к ней устройств.

Запросы от устройств сначала идут на точку доступа и только потом – к сайту, который намеревается посетить владелец устройства. Если обмен данными между точкой доступа и устройством пользователя не защищен шифрованием, злоумышленник даже не самого высокого ранга сможет перехватить данные, которые пользователь вводит, например, на сайте банка

или интернет-магазина. Более того, такая атака возможна, даже если доступ к хот-споту защищен паролем, а между искомым сайтом и браузером пользователя установлено защищенное https-соединение.

Среди данных, которые могут быть перехвачены злоумышленниками, сообщения в социальных сетях, пароли и логины от аккаунтов в них, а также учетных записей в почте, платежных и банковских системах – все это преступники могут использовать для незаконного обогащения ***(Публичные Wi-Fi-сети – излюбленное «место» хакеров // http://internetua.com/publicsnie-Wi-Fi-seti---izluablennoe--mesto--hakerov). – 2013. – 20.09).***

***

Специалисты компании «Доктор Веб» обнаружили самую крупную в мире бот-сеть из инфицированных мобильных устройств на базе ОС Android. На сегодняшний день известно о более чем 200 тыс. смартфонах, которые были заражены вредоносными программами семейства Android.SmsSend и входят в ее состав. Основной источник заражения в этом случае – принадлежащие злоумышленникам или взломанные интернет-ресурсы.

Наибольшее число инфицированных устройств принадлежит российским пользователям, на втором месте по данному показателю располагается Украина, далее следуют Казахстан и Белоруссия. По предварительным оценкам ущерб, нанесенный пользователям злоумышленниками в результате данного инцидента, может исчисляться многими сотнями тысяч долларов.

Для заражения мобильных устройств и включения их в состав бот-сети злоумышленники использовали несколько вредоносных приложений: среди них новый троянец Android.SmsSend.754.origin, а также вредоносные программы Android.SmsSend.412.origin (известна с марта 2013 г., распространяется под видом мобильного браузера), Android.SmsSend.468.origin (известна с апреля 2013 г.) и маскирующийся под мобильный клиент для социальной сети «Одноклассники» троянец Android.SmsSend.585.origin, известный антивирусному ПО Dr.Web с июня 2013 г.

Троянец Android.SmsSend.754.origin представляет собой apk-приложение с именем Flow_Player.apk. Устанавливаясь в операционной системе, он просит пользователя запустить данную программу с привилегиями администратора устройства – это позволит вредоносному приложению осуществлять управление блокировкой дисплея. Кроме того, Android.SmsSend.754.origin в дальнейшем скрывает свой значок с главного экрана мобильного устройства.

После завершения процедуры установки троянец отправляет злоумышленникам информацию об инфицированном устройстве, включая уникальный идентификатор IMEI, сведения о балансе, код страны, номер телефона жертвы, код оператора, модель мобильного телефона и версию ОС. Затем Android.SmsSend.754.origin ожидает поступления от злоумышленников

соответствующей команды, по которой он может отправить СМС-сообщение с определённым текстом на заданный номер, выполнить СМС-рассылку по списку контактов, открыть заданный URL в браузере или продемонстрировать на экране мобильного устройства сообщение с определённым заголовком и текстом.

По сведениям, собранным специалистами, в бот-сеть на сегодняшний день входит более 200 тыс. мобильных устройств, работающих под управлением Google Android, при этом наибольшая их часть (128 458) принадлежит российским пользователям, на втором месте располагается Украина с показателем 39 020 случаев заражения, на третьем – Казахстан: здесь от действий злоумышленников пострадали 21 555 пользователей ***(Обнаружена крупнейшая в мире бот-сеть из 200 000 зараженных устройств // InternetUA (http://internetua.com/obnarujena-krupneishaya-v-mire-bot-set-iz-200-000-zarajennih-ustroistv). – 2013. – 21.09).***

***

Интернет-мошенники используют новый вид вредоносного ПО, заставляющее компьютеры, работающие на Windows, генерировать виртуальную валюту Bitcoin. Вредонос Reveton, обнаруженный исследователями из компании Malwarebytes, блокирует пользователю доступ к компьютеру перед тем, как системы начинают генерировать Bitcoin. Это означает, что для получения прибыли преступникам уже не нужно ждать выплаты «выкупа».

Reveton, использующийся для вымогательства, является широко распространенным вредоносным ПО. Обычно вирус выдвигает пользователю, ставшим его жертвой, ложное обвинение в скачивании контента, защищенного авторским правом или содержащего изображения сцен жестокого обращения с детьми. Далее Reveton требует выплатить штраф за разблокировку компьютера. Оплата, как правило, требуется в виде ваучера от анонимного плательщика через сервисы Ukash или Paysafecard.

Ранее подобное ПО использовалось, в основном, для мелкого мошенничества с продажами поддельных антивирусных решений. Использование его для генерации Bitcoin является новой ступенью в развитии этого вида мошенничества. Так, «зарабатывание» денег путем генерации Bitcoin требует использования графических процессоров и все более сложных алгоритмов.

«Вредонос чаще всего распространяется путем сопутствующих загрузок. По всей видимости, Reveton работает с некоторыми из самых известных на сегодняшний день наборов эксплоитов», – сообщил исследователь из Malwarebytes А. Куджава. Эксперт советует пользователям обновлять браузеры и плагины для защиты от наиболее распространенных видов угроз, в том числе от Reveton ***(Новый вредонос заставляет компьютеры генерировать Bitcoin // InternetUA (http://internetua.com/novii-vredonos-zastavlyaet-kompuateri-generirovat-Bitcoin). – 2013. – 21.09).***

***

Поисковая машина, созданная программистом Д. Мазерли, ищет не веб-страницы, а устройства, подключенные к сети: от радионянь до инженерных систем.

На свое 34-летие М. Гилберт получил ужасный сюрприз от какого-то незнакомца. После того как празднование дня рождения закончилось, житель Хьюстона услышал незнакомый голос в детской, где спала его двухлетняя дочка. «Просыпайся, маленькая шлюшка!» Вбежав в комнату, М. Гилберт обнаружил, что источник звука – радионяня, а человек, получивший контроль над этим устройством, также мог манипулировать видеокамерой. М. Гилберт незамедлительно отключил радионяню, но хакер успел обозвать его дебилом.

Еще за несколько месяцев до скандального события специалисты по безопасности производителя устройства – китайской фирмы Foscam – обнаружили изъяны в программном обеспечении радионяни: хакеры, используя банальное имя пользователя «admin», могли получить удаленный доступ к устройству и взять под контроль передаваемые данные. Foscam исправила недостатки радионяни, но ничего не сообщила покупателям устройств со «старой прошивкой». Когда М. Гилберт проверил свой аккаунт в Foscam, то обнаружил, что хакер внес туда собственное имя пользователя Root и получил возможность подключаться к радионяне в любой момент. Теперь М. Гилберт готовит групповой иск против Foscam. Он смог найти других истцов, благодаря поисковику Shodan. И похоже, что этим же поисковиком воспользовался хакер-извращенец, чтобы найти М. Гилберта.

Shodan – не типичный поисковый сервис. Он не ищет веб-страницы, а прочесывает Интернет в поисках различных устройств, многие из которых запрограммированы на ответ. Поисковик уже находит автомобили, кардиомониторы, системы кондиционирования и освещения в офисных зданиях, установки для очистки сточных вод, системы управления электростанциями, светофоры и глюкометры. Запрос на поиск радионянь модели, как у М. Гилбертов, показывает, что более 40 000 людей используют IP-камеры и могут оказаться легкой добычей для хакеров. Shodan не может похвастаться интерфейсом Google: чтобы найти определенное устройство, вам нужно знать его некоторые характеристики, а результаты выдачи содержат язык интернет-протокола, который может быть не понятен обычному пользователю.

«Google ищет сайты, а я ищу устройства», – объясняет Д. Мазерли, 29-летний программист, выпустивший в 2009 г. Shodan. Он назвал свою систему именем искусственного интеллекта – злодея из видеоигры System Shock: «Хакеры и нерды сразу поймут, о чем речь».

Д. Мазерли надеялся, что Shodan будут использовать такие сетевые гиганты, как Cisco, Juniper и Microsoft, чтобы обыскивать весь мир в поисках продуктов, произведенных их конкурентами. Вместо этого система стала важнейшим инструментом для специалистов по безопасности, ученых,

силовых структур и хакеров. Все они ищут устройства, которые не должны быть подключены к Интернету или могут оказаться уязвимыми для взлома.

Shodan уже использовали для обнаружения видеокамер наблюдения со слабой системой защиты: достаточно набрать их IP-адрес в браузере, чтобы получить возможность подглядывать за тем, что происходит в домах у людей, в офисах полиции, в операционных больниц, в детских садах и даже у наркодилеров. Д. Тентлер, специалист по вопросам безопасности, консультировавший Twitter, создал программу под названием Eagleeye, которая обнаруживает камеры со слабой защитой при помощи Shodan, подключается к ним и делает скриншоты. Д. Тентлер нашел почти миллион уязвимых камер. «Это как крэк для вуайеристов», – говорит он.

После обнаружения «дыр» в программном обеспечении управления зданиями специалист по безопасности Cylance Б. Риос, используя Shodan и еще одну программу, нашел офисы банков, жилые дома и даже штаб-квартиру Google в Австралии, чьи системы безопасности, освещения и кондиционирования мог легко взять под контроль хакер извне. «Прямо сейчас вы можете найти в Интернете около 2 тыс. зданий и получить контроль над ними, достаточно лишь угадать или узнать их IP-адрес», – рассказывает Б. Риос. Ранее в этом году Министерство национальной безопасности США сообщило, что хакеры уже воспользовались слабой защитой и в 2012 г. взломали системы управления отоплением в одном из «правительственных учреждений», сделав температуру там «необычайно теплой».

В отраслевом отчете производителя электроники Ericsson говорится, что к 2020 г. примерно 50 млрд устройств будут иметь подключение к сети и вместе они образуют «Интернет для устройств» (Internet of Things). «Я не думаю, что моя система вызывает страх, – говорит Д. Мазерли. – Куда страшнее то, что электростанции подключены к Интернету».

Поисковик использует freemium-модель. Бесплатный поисковый запрос выдаст вам только десять результатов. Около 10 тыс. пользователей выкладывают до 20 дол. за один запрос, показывающий 10 тыс. результатов. Десятки корпоративных пользователей – это фирмы, занимающиеся компьютерной безопасностью, – платят каждый год пятизначную сумму за доступ ко всей базе данных Д. Мазерли, куда занесено 1,5 млрд устройств, подключенных к сети.

Федералы могут осложнить жизнь Д. Мазерли, если они захотят применить к нему закон о компьютерном мошенничестве, запрещающий несанкционированный доступ к компьютерным системам. «Я даже не пытаюсь получить доступ к серверам и не делаю ничего такого, что можно расценить как взлом», – рассказывает Д. Мазерли.

Конечно, его нужно не преследовать, а наградить за то, что он привлек внимание к невероятно глупым ошибкам, совершенным компаниями, выпускающими гаджеты, и указал на невнимательность пользователей к безопасности приобретаемых продуктов. Все устройства, которые подключаются к сети, должны быть защищены паролями, но большинство

людей забывают об этом, используют слишком простые пароли или пару логин – пароль по умолчанию. В прошлом году анонимный пользователь взял под свой контроль более 400 тыс. подключенных к Интернету устройств, использовав для этого всего лишь четыре пароля по умолчанию. «Все говорят о высококлассных эксплойтах и кибервойнах, – написал этот хакер. – Но четыре простых и глупых пароля для Telnet могут дать вам доступ к сотням тысяч потребителей и к десяткам тысяч промышленных устройств по всему миру».

Д. Мазерли надеется, что создание Shodan обеспечит большую прозрачность и общественное порицание тех компаний, которые продают уязвимые системы, но при этом он не испытывает особого оптимизма. «Хотим мы этого или нет, но все оказывается в Интернете», – говорит Д. Мазерли ***(Google для хакера: поисковик Shodan поможет получить контроль над электростанцией // InternetUA (http://internetua.com/Google-dlya-hakera--poiskovik-Shodan-pomojet-polucsit-kontrol-nad-elektrostanciei). – 2013. – 21.09).***

***

Агентство национальной безопасности США уличили в том, что оно покупало у хакеров уязвимости многих сайтов, позволяющие провести атаку на ресурс.

В Интернете появился контракт, заключённый между Агентством национальной безопасности США и хакерской фирмой VUPEN Security, которая специализируется на продаже эксклюзивных 0day-эксплойтов клиентам из стран НАТО.

Контракт предусматривает, что VUPEN обеспечивает «услуги по эксплойтам и анализу бинарников» для АНБ в течение 12 месяцев.

Репутация VUPEN в хакерской среде отлично известна: в марте 2012 г. они отказались от вознаграждения на конкурсе Pwn2Own за публикацию эксплойта для IE9, решив сохранить его для своих клиентов.

Зачем АНБ покупать уязвимости интернет-сайтов, и намерено ли агентство ими воспользоваться – ещё один интересный вопрос, пока что остающийся без ответа ***(Американская разведка скупает уязвимости сайтов у хакеров // InternetUA (http://internetua.com/amerikanskaya-razvedka-skupaet-uyazvimosti-saitov-u-hakerov). – 2013. – 21.09).***

***

Пользователи сети профессиональных контактов LinkedIn обвинили администрацию ресурса в том, что она ворует электронные адреса из их почтовых ящиков и рассылает приглашения по списку контактов. Об этом в воскресенье, 22 сентября, сообщает агентство Bloomberg.

Иск подан в суд города Сан-Хосе в Калифорнии 17 сентября. Истцы требуют от компании прекратить подобную практику и вернуть прибыль, полученную нечестным путем. Они намерены добиваться рассмотрения дела судом присяжных.

Согласно иску, LinkedIn, заставляя указывать в качестве имени пользователя внешний электронный адрес, получала доступ к адресам в списке контактов пользователя. Затем эти данные использовались, чтобы рассылать приглашения вступить в сеть. При этом пользователи никак не могут остановить этот процесс.

Представитель LinkedIn заявил, что иск является необоснованным и компания намерена доказать его несостоятельность в суде. Администрация никогда не пользуется доступом к электронной почте клиента без его разрешения и не «притворяется» пользователем, чтобы проникнуть в чужие почтовые ящики, подчеркнули в LinkedIn.

Между тем, одна из истиц иска заявила Bloomberg, что LinkedIn разослал от ее имени не менее 3000 приглашений вступить в профессиональную соцсеть, причем использовались не только непосредственные адресаты писем, но и те, кому направлялась копия. Другой пользователь рассказал, что он якобы пригласил пообщаться в LinkedIn людей, с которыми не разговаривал почти десять лет, в том числе нескольких бывших подруг, чьи контакты забыл удалить.

Как указывают истцы, частью стратегии LinkedIn является «обеспечение вирусного роста клиентской базы». По данным самой соцсети, в нее уже вступили более 238 млн профессионалов со всего мира. В мае 2011 г. LinkedIn, запущенная в 2003 г., провела первичное размещение акций (IPO). По итогам последних торгов на Нью-йоркской бирже, акции компании упали на 2,1 % ***(Пользователи обвинили LinkedIn в краже адресов электронной почты // InternetUA (http://internetua.com/polzovateli-obvinili-LinkedIn-v-kraje-adresov-elektronnoi-pocsti). – 2013. – 22.09).***

***

В последнее время вопросы информационной безопасности все чаще беспокоят пользователей компьютеров, мобильных устройств, сервисов. Нельзя сказать, что многим так уж важно сохранять тайну сетевой активности – не у всех есть страшные секреты – но неприятно осознавать, что где-то там, в секретных помещениях, гигантские сервера не переставая отслеживают каждое действие.

После международного скандала из-за публикации Э. Сноуденом данных о проекте PRISM, общественность не на шутку разволновалась, насколько надежно компании хранят большие и маленькие секреты, которые им доверяют. С одной стороны все обещают шифрование надежными алгоритмами, конфиденциальность и безопасность, но с другой – откуда нам знать, как это реализовано на практике? Насколько тесны взаимоотношения спецслужб и технологических гигантов?

Компания Apple неоднократно уверяла, что сообщения, отправляемые через iMessage, надежно защищены. Ни у кого, кроме отправителя и получателя нет возможности превратить зашифрованный поток нулей и единиц в осмысленный текст. После заявлений Э. Сноудена о тотальной прослушке представители компании выступили с очередным заявлением о

безопасности фирменной технологии общения – сообщения невозможно перехватить между абонентами, так что нечего беспокоиться. Но вчера появилось опровержение. Известные хакеры GG и Pod2G анонсировали доклад об уязвимости в работе iMessage, которая позволяет перехватывать сообщения пользователей. Иными словами у Apple есть техническая возможность предоставлять спецслужбам доступ к переписке владельцев мобильных устройств и компьютеров. Пользуется ли она этой возможностью? Не известно.

Для перехвата сообщений используется MITM-атака, когда криптоаналитик становится промежуточным звеном в переписке – незаметно читает и видоизменяет сообщения, которыми обмениваются корреспонденты. Это не опровергает заявления Apple, что сообщения шифруются по принципу «end-to-end» и не могут быть расшифрованы, но в общение двух людей может вклиниться третья сторона, которая будет получателем, ретранслирующим сообщения от собеседника к собеседнику. Нельзя сказать, что эта уязвимость была специально оставлена программистами Купертино, но и полностью исключать эту возможность не стоит. Для взлома iMessage MITM-атакой нужны очень хорошие специалисты и оборудование, которое есть в распоряжении Apple и крупных организаций, например, Агентства национальной безопасности.

В октябре на докладе хакеры собираются рассказать подробности о технологии взлома в надежде, что в Apple прислушаются к их словам и сделают защиту сообщений еще надежней. Не только для пользователей, но в интересах компании. На Apple могут вновь обрушиться иски от разгневанных пользователей, которые верили в заявления об абсолютной защищенности iMessage ***(Безопасность iMessage – миф // InternetUA (http://internetua.com/bezopasnost-iMessage---mif). – 2013. – 22.09).***

***

Корпорация Symantec сообщила об использовании злоумышленниками в направленных атаках новой уязвимости нулевого дня в браузере Internet Explorer. Данная уязвимость до сих пор остается открытой, и злоумышленники, которые ее эксплуатируют, могут запускать на компьютерах жертв собственный вредоносный код.

Как рассказали CNews в компании, 17 сентября корпорация Microsoft сообщила о новой уязвимости нулевого дня браузера Internet Explorer (CVE-2013-3893). В сообщении говорится, что уязвимость может приводить к повреждению памяти, позволяя злоумышленникам запускать собственный вредоносный код. В ходе атаки пользователей заставляют открыть веб-страницу, эксплуатирующую уязвимость, при помощи Internet Explorer. Согласно заявлению Microsoft, на данный момент уязвимость была использована только в небольшом числе направленных атак.

Пока исправление данной уязвимости находится в разработке, Microsoft предоставила временный инструмент ее устранения. Для защиты от этой угрозы Symantec добавила в свои продукты следующие технологии

детектирования: в антивирусный модуль – Bloodhound.Exploit.513; в систему обнаружения вторжений (IPS) – Web Attack: Microsoft Internet Explorer CVE-2013-3893, Web Attack: MSIE Memory Corruption CVE-2013-3893 3.

«Направленные атаки год от года становятся все более популярными. По данным ежегодного отчета Symantec об угрозах интернет-безопасности в 2012 г., их объем за год вырос больше, чем на 40 %. Это означает, что злоумышленники ищут все новые способы проникать в системы своих жертв, в том числе с помощью уязвимостей нулевого дня, – подчеркнул О. Шабуров, руководитель направления информационной безопасности Symantec. – Согласно тому же отчету, количество обнаруженных уязвимостей нулевого дня за год увеличилось на 6 %, поэтому пользователям нужно тщательно выбирать средства защиты и постоянно обновлять свое программное обеспечение» ***(Новая уязвимость нулевого дня Internet Explorer используется в направленных атаках // InternetUA (http://internetua.com/novaya-uyazvimost-nulevogo-dnya-Internet-Explorer-ispolzuetsya-v-napravlennih-atakah). – 2013. – 22.09).***

***

На коммерческие компании приходилось 67 % всех утечек в мире по итогам первого полугодия 2013 г., за год этот показатель увеличился на 19 п. п., сообщила 19 сентября на международной конференции генеральный директор ГК InfoWatch Н. Касперская.

Доля утечек информации из государственных учреждений выросла незначительно и составила по итогам первого полугодия текущего года 30 %. Н. Касперская напомнила, что речь идет о публичных утечках, ставших достоянием СМИ – это примерно 1–5 % от всех утечек в мире, поскольку многие, но не все страны обязаны по закону сообщать об утечках конфиденциальной информации. Как ранее сообщал Digit.ru, всего за первое полугодие текущего года эксперты InfoWatch зафиксировали 496 утечек, что на 18 % больше прошлогоднего показателя.

По ее словам, еще год назад эксперты компании зафиксировали снижение доли персональных данных в общей картине утечек информации (89,4 %), однако в первом полугодии наблюдался рост таких утечек, показатель вырос до 93,8 %. На утечки, связанные с коммерческой тайной, приходится 3,4 %, с гостайной – 2,6 %.

Доля злонамеренных (когда человек осознает негативные последствия своих действий) утечек в общей структуре выросла незначительно и составила 46 % против 43 % годом ранее, а вот доля случайных утечек выросла на 8 п. п. – до 45 %. По-прежнему большее число утечек конфиденциальной информации происходит из-за кражи/потери оборудования – 29,2 %, на утечки информации на бумажных носителях приходится 25,4 %, через сеть информация утекает примерно в 11,7 % случаев. При этом Касперская отметила, что доля «новых» каналов – мобильные устройства – пока остается незначительной.

По данным экспертов InfoWatch, за первое полугодие 2013 г. в мире скомпрометировано более 258 млн записей, в том числе финансовые данные, номера полисов социального страхования, медицинская информация, иные персональные данные ***(Утечки информации в 67 % случаев происходят из коммерческих компаний // InternetUA (http://internetua.com/utecski-informacii-v-67--slucsaev-proishodyat-iz-kommercseskih-kompanii). – 2013. – 22.09).***

***

Специалисты из Университета Массачусетса разработали метод взлома внутреннего криптографического механизма микропроцессоров способом, который не оставляет следов для обнаружения взлома имеющимися методами, даже под электронными микроскопами. Теоретически производители процессоров могут оставлять в них лазейки, которые позволят выполнять какие-либо действия без ведома пользователя. Хотя это и трудно осуществимо, поскольку затронет процессы обработки данных, характеристики производительности и стабильность работы, всё же такие медоты возможны. Единственной реальной возможностью проверки таких процессоров является их визуальный осмотр на микроуровне.

Теперь и его может оказаться недостаточно. Например, генератор случайных чисел в процессорах Intel может быть модифицирован так, что это невозможно отследить – за счёт изменения используемых в транзисторах примесей. Примеси включаются в кристаллическую структуру материала, из которого изготавливаются транзисторы, и играют важную роль в процессе их правильного функционирования и придания им нужных свойств. Незначительное изменение примесей на определённых участках может незаметно изменить поведение генератора случайных чисел. Например, можно получать постоянные от блока, который должен генерировать переменные.

Обычно шансы на успех хакерской атаки против генератора случайных чисел Intel составляют 1/2128, но в случае с модифицированным блоком они становятся равны 1/2n, где n – разрядность констант, выбираемая создателем трояна. Чипы Intel содержат механизм самопроверки, призванный фиксировать криптографические манипуляции, но по словам исследователей, такие модификации обнаружить он не способен, как и прочие существующие методы. Сложность увеличивает тот факт, что криптографический блок изолирован от остальных аппаратных частей – это призвано затруднить взлом, но затрудняет и проверку. Остаётся только надеяться, что такие открытия подтолкнут Intel к поиску путей создания более достоверных механизмов самопроверки ***(Исследователи нашли новый низкоуровневый метод взлома процессоров // InternetUA (http://internetua.com/issledovateli-nashli-novii-nizkourovnevii-metod-vzloma-processorov). – 2013. – 22.09).***