СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(13–24.07)

2015 № 13

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(13–24.07)
№ 13

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

Відповідальний редактор
Л. Чуприна, канд. наук із соц. комунікацій

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ 4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 11
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 14
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 20
Інформаційно-психологічний вплив мережевого спілкування на особистість 20
Маніпулятивні технології 21
Зарубіжні спецслужби і технології «соціального контролю» 23
Проблема захисту даних. DDOS та вірусні атаки 28

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Как утверждают сотрудники украинского штаба «ВКонтакте», больше всего материально состоявшихся соотечественников зарегистрированы именно у них – такие данные обнародовала компания Factum Group Ukraine, пишет AIN.UA (http://ain.ua/2015/07/13/591248)

Исследование традиционно проводилось с помощью медиапанели интернет-пользователей Opinion Software Media. Как оказалось, «ВКонтакте» лидирует в Украине по количеству пользователей с полным достатком. Более того, по общему количеству пользователей сайт также обошел конкурентов – в июне десктопная аудитория «ВКонтакте» превысила 12 млн человек. При этом в «Одноклассниках» насчитали 8,3 млн украинцев, а в Facebook – 6,3 млн.

Что касается уровня достатка, то он довольно низкий по Украине в целом, но если смотреть в разрезе аудитории соцсетей, то во «ВКонтакте» «сидит» в полтора раза больше богатых граждан нашей страны – людей с полным достатком и имеющих возможность покупать дорогие вещи.

Также в украинском штабе не прекращают развенчивать миф о «школоте» во «ВКонтакте». По данным исследования, более 70 % посетителей «ВКонтакте» – люди в возрасте старше 25 лет. «Вопреки заблуждениям некоторых медиаэкспертов, в каждом из регионов Украины мы сохраняем лидерство, а наша аудитория – это не только учащиеся, рабочие и домохозяйки, но и руководители со специалистами», – прокомментировал пресс-секретарь «ВКонтакте» в Украине В. Леготкин.

Напомним, исследования в рамках проекта Opinion Software Media проводятся с помощью специального программного обеспечения, установленного на домашние и рабочие компьютеры украинских пользователей от 15 лет, с возможностью осуществлять мониторинг всех посещаемых ими интернет-ресурсов, как национальных, так и зарубежных ***(Самые богатые здесь: «ВКонтакте» отчиталась о достатке украинских пользователей // AIN.UA (http://ain.ua/2015/07/13/591248). – 2015. – 13.07).***

***

Facebook ведет тестирование собственного виртуального помощника, который в чем-то должен составить конкуренцию Siri, Cortana и Google Now. Об этом пишет The Information.

В настоящее время проект проходит под кодовым названием Moneypenny – именно так зовут одного из вымышленных персонажей в романах и фильмах о Джеймсе Бонде. Однако не факт, что на момент релиза сервис будет называться так же.

Moneypenny был создан для того, чтоб позволить пользователям мессенджера Facebook подыскивать наиболее привлекательные предложения, связанные с товарами и сервисами. Moneypenny в работе отчасти полагается на

человеческие ресурсы. Судя по всему, речь идёт о некой гибридной технологии, которая позволяет осуществлять поиск и фильтрацию данных автоматически и при поддержке операторов-людей. Как это будет выглядеть на практике, пока не совсем ясно.

Ассистент должен помочь Facebook обеспечить монетизацию Facebook Messenger, пользовательская база которого сегодня насчитывает 700 млн человек.

На какой стадии находится проект и что еще сможет предложить пользователям Moneypenny, пока неизвестно ***(Facebook работает над собственным виртуальным помощником // InternetUA (http://internetua.com/Facebook-rabotaet-nad-sobstvennim-virtualnim-pomosxnikom). – 2015. – 15.07).***

***

Согласно данным исследования, проведенного компанией Locowise в мае этого года, популярный фотохостинг Instagram продолжает наращивать количество органических фолловеров и органическую вовлеченность гораздо более высокими темпами, чем его собственник Facebook.

Эксперты из Locowise изучали 2500 профайлов в Instagram в течение месяца (май 2015 г.) и выдали следующую информацию:

– число органических фолловеров (то есть естественных последователей, а не подвергшихся влиянию вирусности поста) увеличилось в среднем на 1,48 % по сравнению с 0,2 % на Facebook;

– бренды создали в среднем 2,41 поста в день;

– 91,77 % всего контента составили фотографии;

– только 8,23 % от всего контента составили видеоролики, но они собрали 11,6 % всех комментариев;

– средняя органическая вовлеченность одного поста составила 2,61 % от аудитории сервиса против 0,55 % – у Facebook;

– фотографии привлекли 2,69 % тотального числа пользователей, видео – 1,47 %;

– 97,2 % всех интеракций вовлечения составили «сердца» ***(Средний органический рост у «Инстаграма» выше, чем у «Фейсбука» // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/sredniy_organicheskiy_rost_u_instagrama_vyshe_chem_u_feysbuka). – 2015. – 17.07).***

***

Пользователи заметили, что Twitter тестирует новый раздел «Похожие видео» (Related Videos) для неавторизированных пользователей веб-версии сервиса. Об этом сообщает searchengines.ru

Новый раздел расположен справа на странице твитов или профиля участника социальной сети. Видевшие тестируемый функционал пользователи заметили, что некоторые из предлагаемых в нём твитов были занесены в избранное в ранее просмотренных ими профилях. Иногда рекомендованные

видео относились к пользователю, чей твит или профиль был просмотрен ранее.

В новый раздел попадают видео YouTube, нативные видео и анимированные GIF-изображения. Ролики из Periscope и Vine, похоже, не являются частью этого эксперимента.

Пресс-служба Twitter подтвердила факт проведения тестирования: «Мы продолжаем экспериментировать с опытом наших неавторизированных пользователей, размещая похожие видео рядом с твитами на странице» ***(Twitter тестирует новый раздел Related Videos // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44048/118/lang,ru/). – 2015. – 20.07).***

***

Шістдесят три відсотки американських користувачів розглядають Facebook та Twitter як джерело новин. Про це свідчать результати дослідження Pew Research Center, яке демонструє, для яких інформаційних потреб аудиторія використовує Facebook і Twitter.

Матеріали дослідження опубліковані на сайті Pew Research Center.

Автори констатують, що частина американців, які використовують Twitter і Facebook як новинний ресурс, продовжує збільшуватися. Це відбувається, у першу чергу, за рахунок постійних користувачів, які натрапляють на новини в соцмережі, а не через долучення нових людей до порталів.

У доповіді зазначається, що більшість зареєстрованих у Twitter (63 %) та Facebook (63 %) використовують ці платформи як джерело новин про події. Цей показник помітно зріс порівняно з 2013 р., коли близько половини користувачів (52 % у Twitter і 47 % у Facebook) казали, що використовують соціальні платформи для отримання новин.

«Хоча обидві соцмережі мають однаковий відсоток людей, які отримують новини з цих сайтів, є значна відмінність в потенціалі "новинної потужності" соцмереж», – ідеться на сайті. Наприклад, частка користувачів, які підписані на оновлення останніх новин у Twitter, чи не вдвічі більша за тих, хто робить те саме у Facebook (59 % проти 31 %). Це підтверджує версію, що Twitter має великий потенціал для висвітлення гарячих новин та подій у реальному часі.

Збільшення частини користувачів, які отримують новини із соцмереж, помітно чи не в кожній демографічній групі. Наприклад, використання Twitter як новинного порталу підвищилося як серед людей молодше 35 років (з 55 % до 67 %), так і тих, хто старше 35 (з 47 % до 59 %). А у Facebook показники підвищилися як серед чоловіків (з 44 % до 61 %), так і серед жінок (з 49 % до 65 %) ***(63 % американських користувачів розглядають Facebook та Twitter як джерело новин // MediaSapiens (http://osvita.mediasapiens.ua/mediaprosvita/research/63_amerikanskikh_koristuvachiv_rozglyadayut_facebook_ta_twitter_yak_dzherelo_novin/). – 2015. – 17.07).***

***

Twitter запустил функционал Summary Cards в приложениях для iOS и Android. Теперь ссылки на сайты в мобильных твитах будут отображаться в виде информационных карточек, по типу Facebook. Нововведение призвано дать пользователям лучшее представление о контенте веб-сайта, прежде чем они перейдут по ссылке.

Summary Card – один из видов Twitter Cards, позволяющих встраивать контент из сайта в твиты. Он представляет собой стандартную карточку с заголовком, описанием и изображением.

Твиты отдельных издателей, включающие крупное изображение и несколько строчек вступительного текста наряду со ссылкой, первыми заметили сотрудники BuzzFeed. Теперь представители сервиса микроблогов подтвердили внедрение этого функционала ***(Twitter изменил способ отображения ссылок в мобильных твитах // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_izmenil_sposob_otobrazheniya_ssylok_v_mobilnyh_tvitah). – 2015. – 20.07).***

***

Социальная сеть «ВКонтакте» порадовала своих пользователей и выпустила приложение для обработки и публикации фотографий Snapster. При этом руководство компании позиционирует его как первый мобильный продукт соцсети, существующий отдельно.

Несмотря на независимость Snapster, фотоприложение вплотную интегрировано с сервисами «ВКонтакте». И благодаря этому пользователи могут как размещать фотографии, так и видеть активность своих друзей.

Приложение умеет не только редактировать фотографии, но и размещать их в «ВКонтакте», Twitter, Facebook и Instagram. Помимо этого в нем предусмотрена еще и такая полезная функция, как таймер самоуничтожения, позволяющий настроить время просмотра снимка.

Приложение Snapster уже можно найти в магазинах приложений Google Play Market и Apple App Store, где оно доступно для скачивания совершенно бесплатно ***(ВКонтакте выпустила собственный фоторедактор // IT новости (http://itnovosti.org.ua/2015/07/internet/socialnye-seti/snapster.html). – 2015. – 20.07).***

***

Facebook тестирует отложенный просмотр видео. В популярной социальной сети подтвердили факт эксперимента с функцией «Посмотреть позже» для видеороликов на десктопах.

Маленькая кнопка Watch Later будет появляться в виде наложения в верхнем правом углу видеозаписи при наведении на него курсора и позволит сохранять и просматривать больше интересного видеоконтента, появляющегося в новостной ленте.

Новая опция – очередной шаг Facebook в конкурентной гонке с Google и принадлежащим интернет-гиганту видеохостингом YouTube, который так же предоставляет пользователям возможность отложенного просмотра видеороликов ***(«Фейсбук» тестирует отложенный просмотр видео // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/feysbuk_testiruet_otlozhennyy_prosmotr_video). – 2015. – 21.07).***

***

Засновник Wikipedia Д. Уйелс запустив нову соціальну мережу TPO (The People's Operator), пише Business Insider.

Мережа являє собою віртуальний майданчик, що об'єднує меценатів, охочих пожертвувати гроші на благодійність, і тих, кому, навпаки, потрібна подібна фінансова підтримка. Як зазначає видання, нова мережа «більше походить на Twitter, ніж на Facebook», пише Корреспондент.net (http://ua.korrespondent.net/lifestyle/3542042-zasnovnyk-Wikipedia-zapustyv-novu-sotsialnu-merezhu).

За словами Д. Уйелса, існуючі сучасні соцмережі бачать у своїх користувачів об'єкти продажу рекламодавцям і прибуток, у той час як TPO буде витрачати гроші не на рекламу, а на речі, які дійсно хвилюють її користувачів.

Таким чином, нова соціальна мережа повністю відображає ідеї недавно запущеного в США мобільного оператора TPO. Особливістю цього оператора стало спеціальний розподіл коштів. Десять відсотків від усіх оплат за тарифами абоненти жертвують на благодійність.

Варто зазначити, що абоненти можуть самостійно вибирати ту сферу, у яку хочуть пожертвувати гроші.

Також перераховувати чверть від усього прибутку на благодійність пообіцяв і сам оператор. Компанія TPO є спільним проектом французької компанії Orange і німецької Deutsche Telekom ***(Засновник Wikipedia запустив нову соціальну мережу // Корреспондент.net (http://ua.korrespondent.net/lifestyle/3542042-zasnovnyk-Wikipedia-zapustyv-novu-sotsialnu-merezhu). – 2015. – 21.07).***

***

Facebook запустила новые инструменты для издателей видеоконтента – обновлённый загрузчик видео и библиотеку Video Library. Об этом пишет searchengines.ru

Новый функционал призван дать издателям видеоконтента Facebook больший контроль над их материалами. В ближайшие недели он будет запущен для всех.

Обновлённая система загрузки видео получила переработанный процесс загрузки и новые опции дистрибуции контента, такие как возможность сделать видео скрытым и установить запрет на встраивание ролика на сторонние сайты.

Скрытый видеоролик доступен для просмотра только, если пользователь перейдёт на него по прямой ссылке. Как и в YouTube, эти видео нельзя найти через поиск.

Другие опции контроля, которые получили издатели видеоконтента, включают возможность ограничить зрительскую аудиторию видеоролика по возрасту и полу с помощью более точечных настроек приватности, помимо доступных ранее языка и местоположения.

Также можно установить срок, после которого видео будет удалено. При этом статистика по нему сохранится. Кроме того, ролики можно публиковать прямо на вкладку «Видео» на публичной странице и не размещать их в новостной ленте или хронике.

Наконец, видеоиздатели могут ограничить шеринг видеороликов в социальных сетях.

Facebook также запустила новую видеобиблиотеку, чтобы облегчить издателям управление видеоконтентом. Теперь им доступно как массовое редактирование роликов, так и внесение правок на уровне отдельных видео. Администраторы публичных страниц могут зайти в Video Library через вкладку Publishing Tools на странице.

Другие возможности новой библиотеки включают редактирование метаданных видео после его загрузки. Например, добавление субтитров или изменение изображения превью. Также можно искать и фильтровать результаты поиска по названию, описанию и другим опциям ***(Facebook дал издателям видеоконтента больший контроль над дистрибуцией и просмотрами видео // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44078/118/lang,ru/). – 2015. – 22.07).***

***

Кому соцсеть для программистов? Тернопольскую Devbattles.com заполонили индусы и американцы.

LinkedIn, подвинься! В эпоху технократов приходит время для еще более нишевых проектов. Так подумали тернопольские айтишники и запустили профессиональную социальную сеть для программистов Devbattles.com. На сегодня в ней зарегистрированы и активно общаются тысячи разработчиков, IT-рекрутеров, инженеров и просто интересующихся не только из Украины, но и со всех уголков Земли, пишет AIN.UA (http://ain.ua/2015/07/22/592968).

Команда из четверых тернопольчан во главе с основателями В. Любомиром (CEO) и А. Бережником (CTO) начала работать над проектом с июня 2014 г., а уже в декабре запустилась английская версия сайта. Цель преследовали амбициозную: создать многофункциональный сервис, а вокруг него IT-коммьюнити, члены которого будут делиться опытом и самосовершенствоваться, общаться друг с другом и развивать собственный бизнес.

Сегодня на Devbattles.com зарегистрировано 138 компаний и более 10 тыс. IT-профессионалов из 184 стран мира. Причем украинцы даже не в большинстве (18,7 %), первое место у наших соотечественников отвоевали пользователи из Индии (19,6 %). На третьем месте США (11,2 %). Есть также представители Португалии (6 %), Канады (4,7 %), Пакистана (3,8 %), Израиля (3,7 %), Филиппин (2,9 %), сравнительно немного россиян (2,8 %) и индонезийцев (2 %). Менее 2 % регистраций из Бразилии, Англии, Малайзии, Италии, Германии, Турции, Туниса, Доминиканской Республики и др.

Зато на «доске почета» в основном украинцы.

Функционал ресурса включает:

– регистрацию профиля программиста;

– регистрацию профиля компании;

– профессиональное резюме для разработчиков;

– размещение вакансий, помощь в поиске команды проекта или персонала компании;

– обсуждение задач программирования, чат;

– персональный блог и блог от имени компании;

– соревнования между программистами по языкам программирования, онлайн-турниры по кодингу.

Таким образом, на площадке можно не только знакомиться и общаться на профессиональные темы, но также устраивать игровые турниры и даже искать работу.

В разделе Sandbox (песочница), который служит блог-площадкой для пользователей ресурса, можно найти много полезной информации – новостей и статей о программировании, технических новинках и разных методах реализации конкретных задач.

Зарегистрироваться в сети можно при помощи авторизации через другие социальные сети, в том числе Facebook и «ВКонтакте». Профиль пользователя напоминает структуру социальной сети – здесь есть его имя, фото и сведения о его специализации. Пользователь может формировать свой круг друзей, чтобы видеть в хронике их записи.

Также имеется счет в «местной валюте» под названием DevPoints (DP). Как объяснили AIN.UA в Devbattles.com, это внутренняя оценка активности пользователя, которая используется для повышения рейтинга среди коллег и участия в турнирах (они доступны пользователям свыше 500 DP).

Проект существует почти полтора года и развивается на собственные средства команды. Инвесторов команда не привлекала. Зарабатывает Devbattles.com на размещении рекламы, вакансий и резюме, а также покупке валюты и пока умудряется выходить в ноль.

Своими конкурентами команда называет LinkedIn и более нишевые Stackoverflow и CodeProject. Впрочем, тернопольчане уверены в собственных силах. «Мы обеспечиваем рост внутренних метрик еженедельно примерно на 8 %, используя только собственные ресурсы для продвижения проекта. Основные задачи на сегодня: усовершенствовать продукт, схему его

монетизации и выработать механизм, чтобы обеспечить быстрорастущее professional community», – рассказали AIN.UA представители сервиса. В дальнейшем они планируют привлечь инвестиции ***(Кому соцсеть для программистов? Тернопольскую Devbattles.com заполонили индусы и американцы // AIN.UA (http://ain.ua/2015/07/22/592968). – 2015. – 22.07).***

***

Корпорация Google объявила о том, что с 1 августа 2015 г. обслуживание сервиса Google+ Photos будет прекращено. Взамен пользователям предлагают переходить на безлимитный сервис Google Photos, который работает с облаком Google Drive.

Отключение сервиса начнётся с версии для Android-устройств, после чего придёт очередь веб-версии и iOS-приложения. Представители Google поясняют своё решение желанием упростить работу с персональными фотографиями.

Весь существующий в Google+ Photos фотоархив не будет потерян – его автоматически перенесут в новый сервис Google Photos, представленный в мае этого года.

Пользователям уже сейчас рекомендуется начать установку нового приложения и заранее приступить к переходу на него. Отметим, что в Google Photos фотографии и видео хранятся совершенно бесплатно.

После установки нового приложения фотографии и видео будут автоматически загружены и сохранены в облаке в оригинальном разрешении, с ограничениями на максимальное качество – для фото до 16 Мп, для видео до 1080p.

Если пользователю захочется хранить материалы в более высоком разрешении, можно будет использовать хранилище своей учётной записи Google, которое предлагает 15ГБ свободного пространства. ***(С 1 августа Google отключает Google+ Photos и переводит файлы в новый сервис // Блог Imena.UA (http://www.imena.ua/blog/google-plus-photos-end/). – 2015. – 21.07).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Налайкали: топ-20 украинцев по количеству подписчиков в Facebook

В самой популярной социальной сети в мире Facebook зарегистрированы миллионы украинцев. Но также там есть официальные страницы первых лиц государства, политиков и чиновников, пишет «Обозреватель» (http://tech.obozrevatel.com/news/53481-nalajkali-top-20-ukraintsev-po-kolichestvu-podpischikov-v-facebook.htm).

Издание «НВ» собрало воедино первую двадцатку самых читаемых украинцев по количеству подписчиков.

Первым в списке стоит экс-президент Грузии, а сейчас глава Одесской облгосадминистрации М. Саакашвили. Количество его читателей составляет 581,3 тыс.

На втором месте украинский руфер Григорий Mustang Wanted – 423,2 тыс. подписчиков.

Президент Украины П. Порошенко с количеством фолловеров в 367,7 тыс. занимает третью позицию в рейтинге.

Отметим, что кроме политиков в 20 вошли радиоведущий, шоумен Д. Чекалкин (201 тыс.), телеведущий Д. Карпачев (180 тыс.), блогер и журналист А. Шарий (149 тыс).

Единственная женщина в топ-20 это телеведущая С. Витвицкая с 132 тыс. подписчиками ***(Налайкали: топ-20 украинцев по количеству подписчиков в Facebook // Обозреватель (http://tech.obozrevatel.com/news/53481-nalajkali-top-20-ukraintsev-po-kolichestvu-podpischikov-v-facebook.htm). – 2015. – 13.07).***

***

Дослідники з Bellingcat створили спеціальний акаунт у Twitter, де в режимі реального часу весь день буде публікуватися вся інформація, яка почала з'являтися в мережі із 17 липня 2014 р. – дня краху Боїнга-777.

Про це пише Еспресо.TV із посиланням на Новое Время.

«Ми опублікуємо інформацію, починаючи з того моменту, де люди обговорюють, що бачать, як через місто рухається Бук. Всі ці повідомлення постили рік назад, коли був збитий Боїнг, але тоді люди ще не розуміли і не знали, що відбувається», – розповів один з дослідників Е. Хіггінс.

За його словами, за допомогою цієї Twitter-трансляції буде відтворено хронологію подій трагічного дня з використанням інформації з відкритих джерел.

Повідомлення у Twitter-акаунті MH17 Live публікуються англійською мовою ***(У Twitter з'явився аккаунт з детальною хронікою катастрофи «Боїнга» // Espreso.tv (http://espreso.tv/news/2015/07/17/sogodni_u_twitter_zyavyvsya_akkaunt_z_povnoyu_detalnoyi_khronologiyeyu_pro_katastrofu_boyinga_777). – 2015. – 17.07).***

***

Пользователи соцсети Twitter выступают против закона Верховной Рады об особом статусе Донбасса. В связи с чем создали даже соответствующий хэштег #НетОсобомуСтатусуДонбасса.

Примечательно, что за небольшой период времени он вышел даже на первое место среди хэштегов дня.

Пользователи Twitter используют хэштег, чтобы Верховная Рада не приняла решение о закреплении особого статуса отдельных районов Донецкой и Луганской областей в Конституции Украины ***(Twitter взбунтовался против***

особого статуса Донбасса // Подробности (http://podrobnosti.ua/2047484-polzovateli-twitter-protestujut-protiv-osobogo-statusa-donbassa.html). – 2015. – 16.07).

***

В Україні створено Google Educator Group (Освітню Спільноту Google). Освітні спільноти Google (GEGs) – це об'єднання працівників сфери освіти, де вони навчаються, діляться досвідом з використання веб-технологій у навчальному процесі.

GEG Ukraine створено на основі педагогічної спільноти «Навчаємося з Google», яку заснували освітяни Н. Саражинська, Н. Гущина та А. Букач.

Члени спільноти є активними користувачами Google Apps for Education – системи безкоштовних інструментів, що надають необхідні технології для освіти, і самі прагнуть поширити використання цих сервісів у навчальних закладах України. Окрім використання продуктів Google Apps for Education у навчально-виховному процесі, спільнота також розглядає управлінські аспекти переваг використання цих інструментів. У групі на Google+ та у Facebook освітяни обмінюються новинами та обговорюють дискусійні питання, з'ясовуючи перспективи розвитку навчального закладу через впровадження педагогічних та ІКТ-інновацій.

Заходи спільноти проходять як в очному, так і в дистанційному режимах: у режимі «онлайн» викладачі обговорюють цікаві для них теми і обмінюються спостереженнями, а локальні семінари та інші заходи дають змогу побачитися особисто і ближче познайомитися один з одним. Також на сторінці «Сервіси Google у професійній діяльності вчителя» члени спільноти проводять вебінари, до яких може долучитися кожен охочий.

Освітні співтовариства Google відкриті для всіх: директорів та адміністраторів шкіл, викладачів, учнів та всіх тих, хто використовує продукти Google, щоб навчати інших ***(Розпочала роботу освітня спільнота Google в Україні // Житомирська обласна державна адміністрація (http://oda.zt.gov.ua/rozpochala-robotu-osvitnya-spilnota-google-v-ukraini.html). – 2015. – 22.07).***

***

Парламент Кубы одновременно с открытием ежегодной сессии завел аккаунты в Twitter и Facebook, где публикуются материалы с собраний. Об этом сообщает Associated Press.

Государственный портал Cubadebate подтвердил подлинность аккаунтов.

Материалы, включающие дополнения, появились на страницах парламента уже на следующий день после собрания. В них, в частности, говорилось о восстановлении отношений США и Кубы. Использование социальных сетей в правительстве довольно необычно для страны, поскольку граждане привыкли наблюдать за выступлениями парламентариев по центральному телевидению. Кроме того, большинство жителей Кубы имеет

ограниченный доступ к Интернету из-за низкой скорости и высокой стоимости ***(У парламента Кубы появились аккаунты в Twitter и Facebook // InternetUA (http://internetua.com/u-parlamenta-kubi-poyavilis-akkaunti-v-Twitter-i-Facebook). – 2015. – 16.07).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Официальное сообщество Live Express «ВКонтакте» объявило о появлении в интернет-магазине ASOS специальной кнопки «Открыть в магазине».

Позже аналогичный функционал появился и в сообществе AliExpress.com.

Мы обратились к представителям социальной сети, чтобы узнать, планируется ли запуск аналогичных кнопок для других сообществ и когда нам этого ожидать.

А. Круглов, Client service director «ВКонтакте», ответил следующее: «Это наши эксперименты с отдельными интернет-магазинами, массово пока не планируем».

А мы пока будем надеяться, что эксперимент окажется удачным, и возможности ecommerce в ВК станут богаче ***(«ВКонтакте» тестирует кнопку «Открыть в магазине» // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/vkontakte_testiruet_knopku_otkryt_v_magazine). – 2015. – 14.07).***

***

Три случая, когда поиск работы в соцсетях может быть эффективным

Поиск работы в соцсетях начинал набирать популярность лет пять назад, когда рекрутеры пытались закрывать вакансии и с их помощью. В настоящее время многие переоценивают этот способ поиска работы, часто он бесполезен. Но Work.ua выделяет три случая, в которых поиск работы в соцсетях все же может дать плоды.

Когда вы узкопрофильный специалист.

Или относитесь к определенной группе профессий. Аудитория соцсетей отличается, и специалистов в них ищут разных.

Так, «ВКонтакте» в основном ищут сотрудников без опыта работы, студентов, работников на сезонные работы. Facebook более ориентирован на творческие вакансии (журналисты, PRщики, маркетологи, руководители среднего звена), «Одноклассники» – на рабочие специальности, а LinkedIn – на IT-специалистов, финансистов, HR-ов и аудиторию Facebook.

Когда у вас прилежные профили в соцсетях.

Не нужно недооценивать влияние соцсетей на карьеру. Ваши профили в соцсетях не должны говорить о двойной жизни, содержать матерщину и

интимные подробности жизни. Впрочем, и отвлекать от работы также не должны.

К слову о «правильности» ведения профилей соцсетей. Хочется обратить внимание на LinkedIn. В силу того, что сеть относительно новая, многие не понимают её преимуществ.

LinkedIn – социальная сеть профессиональных и деловых контактов. Многие рекрутеры ищут с её помощью специалистов по всему миру с нужным набором навыков. Это сеть, в которой зарегистрировано более 332 млн человек со всего мира и собственными страницами представлены более 4 млн компаний.

Поэтому особенно остро вам нужен профиль в LinkedIn, если вы хотите работать в международной компании или пассивно ищите возможности для развития карьеры.

Когда вы занимаетесь нетворкингом как таковым

Нетворкинг – это поиск социального капитала в социальных сетях. Это могут быть друзья и знакомые из жизни, с которыми вы продолжаете общение в сети, а могут быть знакомые, с которыми знакомитесь непосредственно в сети и «дружите» там же ***(3 случая, когда поиск работы в соцсетях может быть эффективным // Днепропетровская Панорама (http://dnpr.com.ua/content/3-sluchaya-kogda-poisk-raboty-v-socsetyah-mozhet-byt-effektivnym). – 2015. – 15.07).***

***

Twitter запустил несколько новых опций для рекламы установки приложений. В их числе – возможность продвигать продукты с помощью видео.

Кроме того, рекламодатели теперь смогут установить приоритет на установки при покупке рекламы: как через оплату на основе цены за установку, так и через назначение ставок при оплате на базе CPC. Компания также сделает доступным большему числу рекламодателей использование таргетинга Twitter для объявлений в партнёрских приложениях.

«Новый функционал объединяет видео и CTA-кнопки, привлекая установки приложений», – заявил вице-президент компании Р. Алфонси.

«Видео в твите – это захватывающий опыт. Оно повышает эффективность рекламы и позволяет маркетологам передать намного больше информации о возможностях приложения потенциальным пользователям».

Нововведения пока находятся в режиме бета-тестирования ***(Twitter добавил видео и новые опции назначения ставок в рекламу установки приложений // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_dobavil_video_i_novye_optsii_naznacheniya_stavok_v_reklamu_ustanovki_prilozheniy). – 2015. – 16.07).***

***

Facebook работает над созданием интернет-магазинов, которые будут размещаться на страницах предприятий и брендов на сайте. Об этом сообщает lookatme.ru.

Магазины на страницах брендов в настоящее время находятся в ранней стадии тестирования, однако в некоторых уже появилась возможность обнаружить и купить товар, не покидая сайта. Всего на сайте пока несколько десятков таких магазинов, однако в Facebook сообщили, что программа будет расширяться. Наиболее заметны магазины в мобильной версии сайта: они размещаются прямо под панелью инструментов и информации о компании.

В Facebook пока не разглашают список компаний, которые участвуют в тестировании новой функции ***(Страницы брендов в Facebook станут магазинами // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44032/118/lang,ru/). – 2015. – 17.07).***

***

Instagram запускает собственную рекламную платформу

Новые форматы рекламы и таргетинга в сервисе будут доступны клиентам осенью, пишет cossa.ru

О планах рассказал директор по маркетинговым операциям Instagram Д. Сквайрс изданию eMarketer: «Последние 18 месяцев мы посвятили развитию платформы для крупных брендов. Следующий логический шаг – обратить внимание на компании всех масштабов. Instagram необходима возможность таргетировать рекламу на более узкие сегменты. Мы хотим предложить клиентам такой инструмент, который поможет им самостоятельно заказывать рекламу и достигать нужных целей».

Пока что Instagram в процессе тестирования форматов, нацеленных на действие пользователей и покупки через API совместно с избранным числом клиентов. Глобально эти инструменты запустятся в начале осени.

В настоящее время компания предлагает видео- и фотоформаты рекламы, а также формат carousel. К этому добавится реклама, побуждающая человека на действие, которое можно совершить прямо из приложения: скачать приложение, купить продукт, зарегистрироваться на сайте ***(Instagram запускает собственную рекламную платформу // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44059/118/lang,ru/). – 2015. – 21.07).***

***

Деньги вместо лайков: как люди получают кредиты в соцсетях.

Рынок взаимного кредитования физлиц (подразумевается самостоятельная выдача гражданами займов друг другу) растет, благодаря появлению многочисленных интернет-сервисов, позволяющих недорого занять

до 300–500 тыс. р. без справок и поручителей в день обращения, пишут «Экономические известия» (http://news.eizvestia.com/news_economy/full/163-dengi-vmesto-lajkov-kak-lyudi-poluchayut-kredity-v-socsetyah).

Сервисы помогают гражданам оценить надежность друг друга, получают за это комиссию, но гарантий, как правило, не дают. В июне платформу для кредитования в социальных сетях запустила компания «Вебтрансфер Финанс», владельцев которой год назад исключили из реестра микрофинансовых организаций, информирует eizvestia.com.

Надежность по аватару

Сайт Webtransfer-finance.com, позиционирующий себя как социальная сеть для выдачи кредитов, заработал в рунете в июне 2014 г. Для регистрации в ней требуется аккаунт в одной из популярных соцсетей – Facebook, Twitter, Google+, «ВКонтакте», «Одноклассниках» и «Моем Мире». С помощью Webtransfer одни пользователи соцсетей могут выдавать кредиты другим пользователям.

Ставку по займу определяет тот, кто хочет дать деньги в кредит, минимальная – 0,1 %. Какую бы ставку ни указал кредитор, свои деньги он вернет: если заемщик окажется ненадежным, его кредит компенсирует гарантийный фонд Webtransfer по ставке 24 % годовых (то есть 0,065 % в сутки), рассказал РБК представитель Webtransfer Europe в России А. Зисин.

Чтобы получить кредит, нужно заполнить форму заявки – выбрать сумму займа, срок и процентную ставку, а затем дождаться встречной заявки потенциального кредитора. Погасить заем можно, пополнив электронный кошелек в личном кабинете и направив деньги на счет кредитора в системе.

По словам А. Зисина, доля невозврата по кредитам составляет 3,5 %. «Мы сотрудничаем с коллекторскими агентствами, но из-за низкого процента невозврата и незначительного размера сумм задолженности обращаться к коллекторам в большинстве случаев не приходится», – уверяет А. Зисин.

Зарегистрироваться в Webtransfer может любой совершеннолетний пользователь. По данным на 30 сентября количество пользователей платформы в мире превысило 600 тыс. человек, половина из них – из России. Сумма сделок на конец сентября составила более 2,9 млн дол., средний срок кредита – 9 дней, а средняя сумма займа – 154 дол. (около 6,1 тыс. р.). Эти данные отображаются в приложении для авторизованных пользователей.

Для оценки кредитоспособности система изучает профиль пользователя в соцсетях: когда он был зарегистрирован, насколько активно используется и т. д. В основном заемщиками становятся студенты и люди с достатком 35–40 тыс. р., которые берут кредит на неделю-полторы, рассказал А. Зисин.

Компания зарабатывает на комиссии, которую берет за ввод и вывод средств, она достигает 2 % в зависимости от платежного сервиса («Яндекс.Деньги», Qiwi и т. д). Также она получает выплаты от партнеров и пользователей за обслуживание счетов.

На запуск соцсети Webtransfer в России компания вложила 5 млн дол., уточнил А. Зисин. Он говорит, что всю прибыль проект собирается тратить на

выход в новые регионы, прежде всего в Китай и Индию ***(Деньги вместо лайков: как люди получают кредиты в соцсетях // Экономические известия (http://news.eizvestia.com/news_economy/full/163-dengi-vmesto-lajkov-kak-lyudi-poluchayut-kredity-v-socsetyah). – 2015. – 21.07).***

***

А. Сенаторов в своей книге «Бизнес в Instagram: От регистрации до первых денег» выбрал пять хорошо зарекомендовавших себя в работе сервисов, решающих различные бизнес-задачи при продвижении в Instagram.

Onlypult (бывший Instapult)

Сервис, разработанный для управления аккаунтами в Instagram, снискал заслуженную популярность среди администраторов. Изначально он назывался Instapult, но социальная сеть была против такого названия.

С помощью сервиса можно загружать изображения и видео в Instagram с компьютера. Весь функционал самой социальной сети, к примеру, добавление фильтров, здесь также доступен. Чем это хорошо? Тем, к примеру, что вам не нужно каждый раз писать со смартфона/планшета описания. Вы можете скопировать нужный текст и сразу «пульнуть» его в сеть вместе с картинкой. Кроме этого, можно сразу с жесткого диска загрузить фото. Напрямую, без облачных сервисов и отправки email со снимком самому себе. Но самая главная ценность Onlypult – в возможности делать отложенный постинг.

Unfollowgram

Unfollowgram – сайт, позволяющий отслеживать, кто отписался от вашей страницы. Вы логинитесь на сайте с помощью социальной сети, а затем указываете свой email. Далее вы попадаете в основное меню сайта, где наибольший интерес как раз представляет функция определения отписавшихся. Сайт подхватывает список ваших подписчиков, и в следующий раз, когда вы просите его показать статистику, он делает это вновь. Таким образом, у него получается два списка подписчиков – тот, что был на момент вашей регистрации, и тот, который получился, когда вы решили воспользоваться сервисом позднее. Unfollowgram их сравнивает и определяет, кого из тех, что были в первом списке, теперь нет.

Websta (ранее известный, как Webstagram)

Позволяет просматривать ленту, комментировать, ставить лайки, подписываться на страницы и многое другое с экрана компьютера. По сути это полноценный веб-клиент Instagram. Единственное, чего он не может делать, так это публиковать материалы. Зато здесь можно создать галерею снимков для вашего сайта. Это просто код, который вы встраиваете в ваш ресурс (по принципу виджетов социальных сетей).

В итоге на вашем ресурсе появляется полноценная самообновляющаяся галерея, которая показывает пользователям, зашедшим на сайт, как хорошо у вас в Instagram.

Websta, как и Unfollowgram, бесплатна, есть русскоязычный интерфейс.

Iconosquare (бывший Statigram)

Так как сам Instagram по большому счету не предоставляет статистических данных, встает вопрос о том, где их брать. Этот сервис и является ответом. Здесь, конечно, нет детальной информации, но все же немало полезных сведений о своих аккаунтах вы получить сможете. Например, наиболее популярные по лайкам посты за все время существования страницы.

Также сервис предоставляет собственные коэффициенты. Среди них – Love rate. Это рейтинг «лайкания» вашими подписчиками. Он показывает, сколько в среднем лайков ставит каждый ваш фоловер. По аналогии существуют также Talk rate и Spread rate, которые отображают отношение комментариев к количеству пользователей и процент лайков (от общего их числа), полученных от юзеров, которые вашими подписчиками не являются, соответственно. И все это лишь часть функций, возможности сервиса гораздо шире.

Instaport

На сегодняшний день Instaport – это, пожалуй, наиболее удобный способ скачать фотографии из Instagram себе на сайт. Вы авторизуетесь с помощью Instagram, указываете параметры загрузки, и файлы скачиваются на ваш диск. Есть возможность задать определенные временные интервалы (к примеру, хочу скачать все, что публиковалось в декабре). Кроме этого, вам предложат скачать кадры, которые опубликованы не на вашей странице, но которые вы лайкали. Либо вообще можно «слить» себе все, что имеет определенный хештег (не более 500 изображений). На стадии бета-версии находится загрузка видео ***(5 сайтов, которые помогают в работе с «Инстаграмом» // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/5_saytov_kotorye_pomogayut_v_rabote_s_instagramom). – 2015. – 23.07).***

***

Twitter разрешил таргетироваться на аудитории ивентов. Соцсеть запустила новый продукт для маркетологов (event targeting), чтобы помочь брендам таргетировать пользователей во время оффлайн ивентов, таких как Церемонии награждения «Оскар» или Супекубок. Теперь у брендов есть доступ к календарю с главными событиями и к данным об их аудитории и ее активностям в прошлом. Раньше рекламодателям вручную приходилось анализировать события с использованием определенных хэшетгов. Новый инструмент не только показывает все хэштеги мероприятия, но и хэштеги знаменитостей, которые примут в нем участие. Новый продукт функционирует отдельно от ранее разрабатываемой платформы Project Lightning, но, по словам компании, в дальнейшем между ними возможна «синергия» ***(Twitter разрешил таргетироваться на аудитории ивентов // Marketing Media Review (http://mmr.ua/show/twitter_razreshil_targetirovatysya_na_auditorii_iventov). – 2015. – 23.07).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Ученые рассказали о влиянии соцсетей на внешний вид

Группа американских ученых провела онлайн-исследование, направленное на анализ поведения девушек в социальных сетях и их оценки собственной привлекательности. Результаты исследования будут опубликованы в научном журнале The Journal of Adolescent Health.

Всего в эксперименте участвовало 128 студенток из различных высших учебных заведений США. В качестве единой исследуемой сети был выбран Facebook.

Как отмечает один из соавторов работы доктор философии из Школы медицины при Университете Северной Каролины С. Зервас, исследователи хотели разобраться, что движет молодыми девушками при публикации своих фотографий в сети.

Хотят ли они просто поделиться моментом из жизни с друзьями и фолловерами или же хотят понять, как они выглядят в сравнении с остальными.

В результате выяснилось, что при публикации в Facebook большинство студентов не было склонно относиться к своим фото критично или придирчиво.

Судя по ответам, данным студентками на вопросы об отношении к своему внешнем виду, привязанности к соцсети и вкусовых предпочтениях в пище, большинство не относится критично ни к своей фигуре, ни к рациону.

По словам ученых, в данном случае социальные сети выполняют роль своеобразного «костыля», поддерживающего самооценку молодых девушек посредством внимания, лайков и перепостов.

Однако это тенденция действует только до той поры, пока человек не начинает сравнивать себя с кем-то в соцсетях ***(Ученые рассказали о влиянии соцсетей на внешний вид // Утро.UA (http://www.utro.ua/ru/zhizn/uchenye_rasskazali_o_vliyanii_sotssetey_na_vneshniy_vid1437640112). – 2015. – 23.07).***

***

Новое исследование показало, дети, которые тратят более двух часов в день на Facebook, Twitter или Instagram, имеют повышенный риск развития нарушений психического здоровья, высокого психологического стресса и даже появления суицидальных мыслей.

«Наши результаты являются важным сигналом для родителей, что нужно следить за тем, сколько ваши дети проводят в социальных сетях, а также подчеркивают необходимость увеличения количества услуг на этих сайтах для

поддержки психического здоровья», – заявили исследователи Hugues Sampasa-Kanyinga и Rosamund Lewis из организации Ottawa Public Health в Канаде.

Они проанализировали данные о школьниках, учащихся в 7–12 классах, принимавших участие в обследовании состояния здоровья Ontario Student Drug Use and Health Survey.

Почти 25 % школьников сообщили, что они ежедневно проводят в социальных сетях более двух часов.

«Поскольку подростки постоянно находятся на сайтах, то это идеальное место для общественного здравоохранения и поставщиков услуг для того, чтобы связаться с этой уязвимой группой населения и обеспечить укрепление их здоровья», – сказала Бренда Вайдерхолд (Brenda K. Wiederhold) из Интерактивного медиа института (Interactive Media Institute) в Сан-Диего.

Исследование было опубликовано в журнале Cyberpsychology, Behaviour, and Social Networking ***(Соцсети негативно влияют на память у детей // Newsland (http://newsland.com/news/detail/id/1579057/). – 2015. – 23.07).***

Маніпулятивні технології

Офіційний Twitter РНБО зламали представники «Правого сектору». Про це вони написали на цьому ж Twitter, інформує Телеканал новини «24» (http://24tv.ua/news/showNews.do?twitter_rnbo_zlamav_praviy_sektor_i_visunuv_tam_svoyi_vimogi&objectId=592904&tag=ukrayina).

Організація також висунула свої вимоги. Вони вимагають звільнити генерала А. Тарана, який начебто «кришує» контрабанду в АТО, затримати міліціонерів, які віддали наказ на відкриття вогню в Мукачевому, арештувати М. Ланьо і В. Медведчука та вже традиційне – відставку міністра А. Авакова.

У РНБО сподіваються, що незабаром відновлять контроль над своєю сторінкою в цій соцмережі. Звернення про злам уже повідомили правоохоронні органи ***(Twitter РНБО зламав «Правий сектор» і висунув там свої вимоги // Телеканал новини «24» (http://24tv.ua/news/showNews.do?twitter_rnbo_zlamav_praviy_sektor_i_visunuv_tam_svoyi_vimogi&objectId=592904&tag=ukrayina). – 2015. – 13.07).***

***

«Правый сектор» самовольно выводит бойцов из зоны АТО. Дать происходящему правовую оценку потребовал П. Порошенко. Такая новость в Twitter Администрации Президента наделала много шума.

Но все оказалось фейком, аккаунт взломали неизвестные, сообщили в пресс-службе. Инцидент, мол, без внимания не оставят. Взломщиков уже разыскивают.

«Принимаются все необходимые меры для того, чтобы защитить официальные государственные сайты. У нас есть предыдущее информация, но

мы ее будем оглашать, когда завершится расследование», – объяснила пресс-секретарь Службы безопасности Украины Е. Гитлянская.

Что-то странное происходило и на странице в Twitter главы МВД. Там появилась новость о том, что министерство готовит пакет документов в Верховную Раду. Будут лишать депутатской неприкосновенности лидера «Правого сектора» Д. Яроша.

Такая же информация размещена и на персональном сайте министра. Но тут же за А. Авакова вступился А. Геращенко, как всегда, в Facebook. Уверяет – это провокация и происки российских спецслужб.

Потом сообщения и вовсе исчезли из блога. А позже А. Аваков на всех своих ресурсах написал, что к Д. Ярошу относится хорошо, несмотря на то что сам Д. Ярош выступает за его отставку.

В настоящее время аккаунты и Администрации Президента, и главы МВД уже в порядке. Починили довольно быстро ***(Твиттер Авакова взломали спецслужбы России // Подробности (http://podrobnosti.ua/2047060-tvitter-avakova-vzlomali-spetssluzhby-rossii.html). – 2015. – 14.07).***

***

Британський студент Л. Александер опублікував результати свого розслідування: як у всесвітній павутині створюється глобальна мережа прокремлівських сайтів.

Використовуючи доступне програмне забезпечення та електронні ресурси, Л. Александер виявив мережу прокремлівських сайтів, створених однією структурою, повідомляє Радіо Свобода.

Через акаунт Google Analytics під унікальним індексом «UA» Л. Александер вийшов на мережу сайтів, які очорнюють Захід і Україну, а також пропагують РФ та В. Путіна.

Почавши досліджувати сайт вштабе.рф, Л. Александер вийшов на сім інших сайтів, які управляються однією і тією ж людиною або організацією.

Серед них – whoswho.com.ua, який має своєю метою генерувати компрометуючу інформацію про українських офіційних осіб, у той же час представляючи себе як нібито український проект.

Інший подібний сайт Zanogu.com – сховище мемів, багато з яких мають явно виражений антизахідний характер.

Схожий ресурс – yapatriot.ru, який являє собою спробу дискредитувати російських опозиційних діячів, – просуває антиамериканські і «проасадівські» погляди на події в Сирії.

Найбільш вражаючим виявилося присутність у цьому списку Material Evidence, інтернет-сайту, присвяченого пересувній фотовиставці, організованій з безсумнівною участю прокремлівських сил.

З цього списку сайт news-region.ru був також пов’язаний із другим акаунтом у Google Analytics: UA-53159797. Цей акаунт, у свою чергу, асоційований з іншою групою, яка налічує 19 прокремлівських сайтів.

Подальше дослідження цих інтернет-сторінок виявило ще три акаунти в Analytics і додаткові сайти, пов'язані з ними.

Таким чином студент вийшов на більш ніж 30 сайтів кремлівської пропаганди, які управляються однією структурою. Також Л. Александер виявив сайти, які перебувають на стадії створення.

Крім сайтів Л. Александер зміг виявити реальних людей, які стоять за кремлівськими сайтами. За даними дослідження, М. Подгорний стоїть за створенням мережі прокремлівських сайтів ***(Студент розкрив кремлівську мережу сайтів пропаганди // INSIDER (http://www.theinsider.ua/politics/55a89d8c09511/). – 2015. – 17.07).***

***

В соцсетях появился новый вид киднеппинга, злоумышленники похищают фотографии чужих детей и выдают их за своих. Об этом сообщает news.com.au.

Псевдо-«мамы» и «папы» уже даже создали свою некую субкультуру виртуальных киднепперов, к фотографиям они добавляют хэштег #babyrp.

Так, например, в Далласе мама Д. Паттерсон и ее дочь стали недавними жертвами такого похищения. Незнакомец из Нью-Йорка опубликовал фото 4-х летней малышки Паттерсон в Facebook и подписал их так: «Моя дочурка разобьет сердца вашим сыновьям» и «Девичья версия меня».

Под другой фотографией, где девочка изображена в кроватке, злоумышленник оставил комментарий «А вот как она выглядит утром, говорит папочка перестань».

В итоге Д. Паттерсон сделала скриншоты этих публикаций и опубликовала их у себя с комментарием «Это моя дочь. Повсюду на этой странице. Это пугает».

Преследовать таких злодеев юридически тяжело, так как их трудно найти и привлечь к правовой ответственности.

В основном, виртуальными киднепперами становятся подростки и молодые женщины, которые хотят поиграть в дочки-матери в сети.

Более того, уже появилось виртуальное агентство по усыновлению, где пользователи могут себе выбрать фотографии по вкусу для создания идеальной семьи ***(Касьяненко С. Милых детей похищают виртуально в соцсетях // Подробности (http://podrobnosti.ua/2048435-detej-v-sotssetjah-pohischajut-virtualno.html). – 2015. – 21.07).***

Зарубіжні спецслужби і технології «соціального контролю»

Министерство образования Саратовской области (Россия) запретило подведомственным учреждениям использовать в работе популярные интернет-сервисы, включая соцсети Twitter, Facebook и Instagram, а также электронную почту Google и сайты на западных доменных именах.

Об этом сообщает Капитал со ссылкой на «Коммерсант».

Так, запрет вводится для «сохранения конфиденциальности служебной информации». Школам и вузам предписано перейти на российские аналоги этих сервисов.

«В целях сохранения конфиденциальности информации, предназначенной для служебного пользования, от утечек запрещается использовать в деятельности учреждений продукты и услуги иностранных интернет-компаний», – говорится в письме Министерства образования Саратовской области, разосланном накануне в школы и вузы.

Также отмечается, что под запрет попало большинство популярных интернет-сервисов: электронная почта от Google, Yahoo, MSN и AOL, соцсети Twitter, Facebook и Instagram, интернет-мессенджер WhatsApp.

Представителям учебных заведений «не рекомендуется» размещать свои страницы и хранилища данных на британских, немецких и украинских сайтах, а также «в доменных зонах .com, .net, .org и им подобных» ***(Студентам и школьникам Саратова перекрыли доступ к Facebook и Twitter // InternetUA (http://internetua.com/studentam-i-shkolnikam-saratova-perekrili-dostup-k-Facebook-i-Twitter). – 2015. – 13.07).***

***

Основанный П. Дуровым мессенджер Telegram заблокирован на серверах, расположенных в нескольких провинциях Китайской Народной Республики. Об этом сообщает Hong Kong Free Press.

Сервера в Пекине, Шэньчжэне, Внутренней Монголии, Хэйлунцзяне и Юньнане не дают доступа к Telegram. Факт блокировки подтверждает база blockedinchina.net.

Материал, обвиняющий Telegram в содействии антиправительственным выступлениям, был опубликован в китайской правительственной газете People’s Daily в воскресенье, 12 июля. По информации издания, мессенджером пользовались китайские адвокаты-правозащитники, чтобы «подготовить нападение на Коммунистическую партию и правительство». В этом признался сотрудник одной из находящихся в Пекине юридических фирм, выступив на национальном телевидении. В своей речи он упомянул функцию Telegram «секретный чат», которая гарантирует, что содержание переписки автоматически самоуничтожается через заданные промежутки времени.

Как пишет Hong Kong Free Press, на сегодняшний день по делу о готовившемся нападении на Компартию и правительство арестованы 23 китайских правозащитника ***(Мессенджер Дурова заблокировали в Китае из-за антиправительственных выступлений // InternetUA (http://internetua.com/messendjer-durova-zablokirovali-v-kitae-iz-za-antipravitelstvennih-vistuplenii). – 2015. – 13.07).***

***

Прокремлевское молодежное движение «Молодая гвардия» предложило блокировать в социальных сетях группы, оскорбляющие россиян. Соответствующее обращение, как передает РИА Новости, активисты направили основателю и гендиректору Facebook М. Цукербергу.

«Нами была собрана подборка групп, которые даже в своих названиях имеют призывы к противоправным действиям. И мы направили письмо М. Цукербергу с просьбой разобраться вообще в работе своей службы поддержки и принять необходимые меры», – подчеркнул представитель движения К. Гринченко.

По его словам, движение не раз получало жалобы от интернет-пользователей на публикации в Facebook, оскорбляющие россиян. Однако обращения в техподдержку, как правило, ничем не заканчивались ***(«Молодая гвардия» попросила Facebook блокировать группы за оскорбления россиян // InUKRNews.Com (http://inukrnews.com/allnews/rossiya/199737-molodaya-gvardiya-poprosila-facebook-blokirovat-gruppy-za-oskorbleniya-rossiyan.html). – 2015. – 13.07).***

***

Сайт Фейсбукпока.рф надає можливість переносити свої акаунти з американської соціальної мережі на російські платформи.

Проект стартував 11 липня. Як повідомляє Jourdom.ru, його заснував рух «Медиагвардия», який виступає за «чистий інтернет».

На думку засновників проекту, «пости, які ображають громадян РФ і закликають до протиправних дій проти них, продовжують не лише існувати у Facebook, але й ігноруються службою підтримки соціальної мережі та скарги на них».

Користувачам пропонується зайти у Facebook, за допомогою порталу зберегти архів із своїми даними і далі обрати один із сайтів – «ВКонтакте», «Одноклассники», LiveJournal та My.Mail.

Лічильник на порталі показує, що наразі більше 14 тис. росіян скористалися послугами проекту ***(Послугами порталу Фейсбукпока.рф вже скористались більше 14 тисяч росіян // MediaSapiens (http://osvita.mediasapiens.ua/web/social/poslugami_portalu_feysbukpokarf_vzhe_skoristalis_bilshe_14_tisyach_rosiyan/). – 2015. – 16.07).***

***

На початку осені в Росії набирає чинності Закон «Про персональні дані». Він змушує міжнародні інтернет-фірми зберігати дані про російських клієнтів на серверах, розташованих тільки у Росії, пише Телеканал новин «24» (http://24tv.ua/mizhnarodni_novini/cherez_noviy_zakon_z_rosiyi_tikaye__google_i_microzoft/n592881) з посиланням на The Washington Times.

Видання зазначає, що це робиться під приводом турботи про приватне життя громадян Росії. Насправді мета – дати уряду доступ до приватного життя і обмежити конкуренцію з боку міжнародних інтернет-компаній.

Кілька західних інтернет-компаній уже прийняли рішення покинути Росію. Microsoft переводить офіс з розробки Skype з Москви до Праги, компанія Adobe повністю припинила діяльність у Росії, а Google зачиняє московський технічний офіс.

Видавництво пише, що поява цього Закону частково викликано параноєю, на підтвердження цитує висловлювання В. Путіна, який упевнений, що Інтернет виник як спецпроект ЦРУ.

У Росії майже 76 млн користувачів Інтернету, і новий закон їм зашкодить. Він забере можливість росіянам використовувати онлайн-служби для купівлі міжнародних квитків, бронювання готелів і навіть для отримання віз. За даними Євроцентру (ECIPE), Закон призведе до падіння ВВП Росії на 5,7 млрд дол. ***(Через новий закон з Росії тікає Google і Microsoft // Телеканал новин «24» (http://24tv.ua/mizhnarodni_novini/cherez_noviy_zakon_z_rosiyi_tikaye__google_i_microzoft/n592881). – 2015. – 13.07).***

***

У Львівській області вперше засудили чоловіка, який через соцмережу «ВКонтакте» закликав до повалення конституційного ладу та захоплення державної влади. Йому призначили один рік умовно, повідомляє zaxid.net

Правоохоронці виявили на його сторінці «ВКонтакте» публікації, у яких він закликав бойкотувати мобілізацію та йти зі зброєю на Київ, щоб знищити П. Порошенка. Крім того, він обіцяв грошову винагороду за «голову голови СБУ В. Наливайченка»...

Усі дописи опубліковані в період з кінця липня минулого року до початку лютого цього року. За його словами, це «суто ідеологічні речі». Такої позиції він притримується і не підтримує чинної влади.

Чоловіка засудили на рік умовно. Такий м’який вирок він отримав тільки через те, що погодився співпрацювати зі слідством та уклав із прокурором угоду про визнання винуватості. Частина 2 ст. 109 КК України, за якою його судили, передбачає більш суворе покарання – до трьох років позбавлення волі. О. Єрошенко розповів, що погоджується з таким вироком та апеляції подавати не буде.

Як розповіла ZAXID.NET журналіст прес-служби прокуратури Львівщини У. Гавришків, це перший випадок у Львівській області в цьому році, коли людину засуджують за заклики до повалення державної влади, опубліковані в соцмережі. Статистики за попередні роки в прокуратурі немає ***(На Львівщині засудили чоловіка за заклики у соцмережі йти війною на Київ // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44011/118/lang,ru/). – 2015. – 16.07).***

***

Балаклавский районный суд Севастополя вынес обвинительный приговор в отношении двоих местных жителей за «разжигание межнациональной розни в социальной сети».

По информации севастопольской прокуратуры, с 12 января 2013 г. по 17 июня 2014 г. севастопольцы 1994 и 1971 годов рождения разместили в соцсети «ВКонтакте» фото, а также аудио- и видеофайлы, направленные на возбуждение ненависти и вражды по признакам национальности и происхождения.

«Они признаны виновными в совершении преступления, предусмотренного ч. 1 ст. 282 Уголовного кодекса РФ (возбуждение ненависти либо вражды по национальному признаку с использованием сети Интернет)», – отметили в пресс-службе надзорного ведомства.

Государственное обвинение по уголовному делу поддерживала прокуратура Балаклавского района.

Согласившись с позицией государственного обвинителя, суд приговорил обвиняемых к исправительным работам сроком на 10 и 6 месяцев соответственно, с удержанием 15 % заработка в доход государства ***(Суд приговорил к исправительным работам двух севастопольцев за «экстремизм» в соцсети // События Крыма (http://www.sobytiya.info/news/15/53882). – 2015. – 16.07).***

***

Чотири роки, але з відстрочкою, отримала волинянка, котра через соціальну мережу «ВКонтакте» закликала до повалення конституційного ладу в Україні.

Про це повідомляють у прес-службі прокуратури Волинської області.

Прокуратура Волинської області підтримала державне обвинувачення в кримінальному провадженні щодо волинянки, яка через мережу Інтернет закликала до насильницького повалення конституційного ладу в Україні.

Як повідомив начальник відділу нагляду за додержанням законів органами СБУ, Державної митної служби та Державної прикордонної служби прокуратури Волинської області Ю. Новосад, ця жінка, зареєструвавши у 2014 р. сторінку в соціальній мережі «ВКонтакте», розповсюджувала матеріали із закликами до зміни меж території та державного кордону України, на порушення порядку, встановленого Конституцією України, а також закликала до насильницької зміни і повалення в Україні конституційного ладу та до захоплення державної влади.

Вироком Володимир-Волинського міського суду її визнано винною й призначено покарання у вигляді чотирьох років позбавлення волі зі встановленням дворічного іспитового строку ***(Волинянку засудили за заклики повалення конституційного ладу в Україні // Інформаційна агенція «Вголос» (http://vgolos.com.ua/news/volynyanku_zasudyly_za_zaklyky_povalennya_konstytutsiynogo_ladu_v_ukraini_186707.html). – 2015. – 21.07).***

***

Турецкие пользователи не могут войти в сеть микроблогов Twitter на территории страны 22 июля, сообщает ria.ru

Ранее суд турецкого города Суруч провинции Шанлыурфа запретил публикацию фото- и видеоматериалов с места теракта, унесшего жизни 32 человек. Страницы сайтов и социальных сетей, на которых ранее были размещены эти материалы, блокируются.

По данным газеты Milliyet, недоступность для турецких пользователей Twitter может быть связана как с запретом на публикацию материалов о теракте, так и с техническими причинами. Официальных заявлений властей по этому поводу пока нет.

20 июля в чайном кафе перед культурным центром в Суруче произошел теракт, жертвами которого стали 32 человека и более 100 получили ранения. Бомба взорвалась перед входом в культурный центр, где собрались турецкие курды и члены молодежных организаций, которые готовились отправиться в Сирию для помощи в восстановлении города Кобани, пострадавшего от нападения боевиков террористической организации «Исламского государство» (ИГ). Ответственность за теракт власти возложили на ИГ, которое использовало смертника ***(Сеть микроблогов Twitter недоступна для пользователей в Турции // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44076/118/lang,ru/). – 2015. – 22.07).***

Проблема захисту даних. DDOS та вірусні атаки

Ранее в этом месяце неизвестные активисты разместили в Интернете 400 ГБ данных, похищенных в результате взлома корпоративной сети компании Hacking Team, которая поставляла шпионское ПО спецслужбам различных стран. Похищенная информация включает корпоративные документы, исходные коды и даже, как стало известно, несколько эксплоитов для уязвимостей нулевого дня в Adobe Flash.

Также в архиве содержится электронная переписка, указывающая, что в 2013 г. компания использовала предпочитаемые спамерами техники для «присвоения» адресного пространства, принадлежащего одному из интернет-провайдеров. Делалось это с целью восстановления контроля над шпионской сетью, предположительно организованной для общей оперативной группы итальянской полиции (Raggruppamento operativo speciale), которая была создана для борьбы с организованной преступностью, терроризмом и более сложными видами преступлений.

Как пояснил ИБ-эксперт Б. Кребс, Hacking Team разместила C&C-серверы у хостинг-провайдера Santrex, пользовавшегося популярностью у разнообразных спамеров. Однако Santrex неожиданно отключил свои серверы в связи с внутренними неполадками в сети, из-за которых происходили

постоянные сбои в ее работе. Таким образом, итальянские правоохранители потеряли контроль над своей системой наблюдения и обратились за помощью к Hacking Team.

По данным исследователей из OpenDNS Security Labs, экпертам компании удалось восстановить контроль над принадлежащим Santrex адресным пространством, используя BGP перехват (префиксный перехват или перехват маршрута) для перенаправления трафика и перемещения инфраструктуры.

Довольно часто спамеры «присваивают» адресные пространства, не используемые в течение длительного периода времени. Преступники практически во всеуслышание «объявляют» всему Интернету, что данные адреса находятся во владении принадлежащего им хостинг-сервиса, и в случае отсутствия каких-либо возражений хакеры получают полный контроль над диапазоном IP-адресов ***(Hacking Team использовала BGP перехват для получения контроля над шпионской сетью итальянской полиции // InternetUA (http://internetua.com/Hacking-Team-ispolzovala-BGP-perehvat-dlya-polucseniya-kontrolya-nad-shpionskoi-setua-italyanskoi-policii). – 2015. – 13.07).***

***

В опубликованных в открытом доступе документах компании Hacking Team обнаружены еще две уязвимости нулевого дня в проигрывателе Adobe Flash. Бреши, эксплуатация которых позволяет удаленно захватить контроль над целевой системой, по всей видимости, уже используются злоумышленниками в различных вредоносных кампаниях.

Еще не устраненные программные ошибки, получившие идентификаторы CVE-2015-5122 и CVE-2015-5123, очень похожи на уязвимость нулевого дня, устраненную на прошлой неделе (CVE-2015-5119). Все они затрагивают Flash для операционных систем Windows, Linux и OS X. Обнаружить новые бреши удалось исследователям из FireEye и TrendMicro соответственно.

Отметим, что Hacking Team использовала эти уязвимости в ходе разработки своих шпионских платформ. Эксплоиты к упомянутым брешам продавались правительственным органам Саудовской Аравии, Судана, России и США.

В настоящее время, по данным Adobe, разработчики компании работают над выпуском соответствующих исправлений. Патчи для проигрывателя должны появиться в течение текущей недели ***(В документах Hacking Team найдены экплоиты для двух новых уязвимостей нулевого дня в Flash // InternetUA (http://internetua.com/v-dokumentah-Hacking-Team-naideni-ekploiti-dlya-dvuh-novih-uyazvimostei-nulevogo-dnya-v-Flash). – 2015. – 14.07).***

***

Антивирусная компания Trend Micro проанализировала ряд нападений, проведенных хакерами из Pawn Storm, и выяснила, что злоумышленники

эксплуатируют уязвимость нулевого дня в Java. Для платформы это первая брешь такого рода за последние два года.

Исследователи отмечают, что уже давно ведут мониторинг активности злоумышленников. При этом мотивы преступников, предпочитающих узконаправленные атаки, тесно переплетены с мировой экономикой и политикой.

Сам эксплоит к уязвимости был выявлен благодаря подозрительным URL-адресам, с помощью которых вредоносное ПО заражало целевую систему.

«Упомянутые URL были предназначены для хостинга эксплоита к уязвимости нулевого дня в Java. Аналогичные URL использовались ранее участниками Pawn Storm в ходе атак на компьютеры сотрудников НАТО и американского Белого дома в апреле этого года», – следует из блога антивирусной компании.

Целью текущего нападения также были несколько представителей НАТО и работники неназванных оборонных ведомств США. Вредоносные ссылки были высланы им на адреса электронной почты ***(В Java обнаружена первая за два года уязвимость нулевого дня // InternetUA (http://internetua.com/v-Java-obnarujena-pervaya-za-dva-goda-uyazvimost-nulevogo-dnya). – 2015. – 14.07).***

***

Уязвимость CVE-2014-7952 в механизме резервного копирования и восстановления данных, используемом Android-устройствами, позволяет злоумышленникам получить высокий уровень доступа к мобильному устройству. ИБ-исследователи из Search-Lab сообщили о том, что полное резервное копирование приложения, включая хранящиеся в разделе дынных личные файлы, выполняется по умолчанию, однако приложение можно настроить по-другому путем реализации класса BackupAgent. Об этом сообщает издание Help Net Security.

Диспетчер создания резервных копий, использующий кастомизированный класс BackupAgent, не фильтрует поток данных, возвращаемый приложениями. При выполнении BackupAgent в процессе создания резервной копии появляется возможность без согласия пользователя внедрять в бэкап-архив дополнительные приложения в виде APK-файлов. BackupAgent не нуждается в каких-либо разрешениях от ОС Android.

При восстановлении из резервного архива система устанавливает внедренное в него приложение с повышенными привилегиями. Поскольку приложение входит в состав архива, система считает его аутентичным. Таким образом Android-приложение может установить другое приложение с повышенными привилегиями без разрешения пользователя.

Механизм резервного копирования работает с помощью утилиты Android Debug Bridge, так что все устройства, использующие для резервного копирования и восстановления данную утилиту, подвержены уязвимости.

ИБ-исследователи сообщили об уязвимости разработчикам Android еще в 2014 г., однако брешь до сих пор не была устранена. Представитель Google

заявил, что исправление данной уязвимости не является приоритетным, так как она не влияет на обычную работу Android-устройства. Опасность может исходить тогда, когда пользователь сам загрузит потенциально вредоносное приложение ***(Уязвимость в Android-устройствах позволяет устанавливать вредоносные приложения // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/07/14/Android-flaw.html). – 2015. – 14.07).***

***

После истории с Heartbleed сообщество всерьёз обеспокоилось безопасностью open source программ. Вскоре запустили CII (Core Infrastructure Initiative), инициативу для аудита ключевых свободных программ. Спонсорами выступили все крупнейшие интернет-компании. Теперь Linux Foundation запустила вспомогательный Census Project: перепись системных утилит Linux, чтобы понять, каким из них нужна помощь в первую очередь.

Census Project – это беглый автоматический анализ по нескольким критериям: сколько человек принимали участие в разработке, то есть вносили патчи, за последние 12 месяцев, как много уязвимостей найдено, насколько широко используется программа и насколько она открыта для сетевого доступа. Код проекта Census опубликован на Github.

Максимальный уровень риска присваивается популярным проектам с малым количеством разработчиков, наличием известных проблем безопасности и работающим с сетью.

По мнению авторов проекта, наибольшего внимания специалистов по безопасности требуют вовсе не те проекты, которые изначально перечислены для аудита в рамках проекта CII, а ключевые системные утилиты Linux. Действительно, ведь над популярными проектами работают сотни человек, там всё хорошо изучено, а системные утилиты Linux давно никто не изучал внимательно.

В настоящее время в Census Project проведён анализ 395 проектов. Максимальный рейтинг риска получили утилиты ftp, netcat-traditional, tcpd и whois, получившие 11 из 15 баллов.

Результаты довольно неожиданные. Например, веб-серверу https присвоен рейтинг всего лишь 8, несмотря на большое количество известных багов, выявленные в последние годы. Дело в том, что его аудитом занимается большое количество людей, это повлияло на снижение рейтинга риска ***(Linux Foundation оценила уязвимость системных утилит Linux // InternetUA (http://internetua.com/Linux-Foundation-ocenila-uyazvimost-sistemnih-utilit-Linux). – 2015. – 15.07).***

***

Корпорация Microsoft выпустила ежемесячную порцию обновлений, устранив внушительное количество багов в операционных системах Windows, офисных приложениях, браузере Internet Explorer и различных программных компонентах.

В рамках июльского апдейта редмондский гигант опубликовал 14 бюллетеней безопасности с описанием 58 уязвимостей. Это один из самых крупных пакетов патчей в нынешнем году.

Кумулятивный пакет обновлений для браузера Microsoft (бюллетень MS15-065) содержит 28 «заплаток» для Internet Explorer с 6-й по 11-ю версии. Некоторые «дыры» носят статус критически опасных, позволяя злоумышленникам получить несанкционированный доступ к удалённому компьютеру и выполнить на нём произвольный программный код.

Кроме того, критические уязвимости обнаружены в серверных и клиентских операционных системах Windows (бюллетени MS15-066, MS15-067 и MS15-068). Проблемы, в частности, затрагивают протокол удалённого рабочего стола RDP, средства виртуализации Hyper-V и некоторые другие компоненты.

Оставшиеся бюллетени Microsoft содержат описания уязвимостей, охарактеризованных «важными». С подробным описанием всех выявленных проблем можно ознакомиться на этой странице. Редмондская корпорация рекомендует как можно скорее инсталлировать патчи, поскольку некоторые из «дыр» уже эксплуатируются злоумышленниками при совершении сетевых атак ***(Microsoft устранила более 50 уязвимостей в своих продуктах // InternetUA (http://internetua.com/Microsoft-ustranila-bolee-50-uyazvimostei-v-svoih-produktah). – 2015. – 15.07).***

***

20 июля компания Microsoft выпустила внеплановое обновление MS15-078, устраняющее уязвимость нулевого дня во всех поддерживаемых версиях операционной системы Windows, включая еще не вышедшую Windows 10. Речь идет об очередной бреши, обнаруженной экспертами безопасности в ходе анализа документов итальянского производителя шпионского ПО Hacking Team. Напомним, ранее исследователи уже выявили несколько эксплоитов для уязвимостей нулевого дня, в том числе трех брешей в Adobe Flash Player.

Уязвимость (CVE-2015-2426), обнаруженная экспертом компании FireEye Г. Цзяном и участником Google Project Zero М. Юржиком, существует из-за ошибки в библиотеке Windows Adobe Type Manager Library при обработке OpenType шрифтов. Ее эксплуатация позволяет удаленному пользователю с помощью специально сформированной веб-страницы или файла, содержащего шрифт OpenType, выполнить произвольный код на целевой системе с привилегиями пользователя, запустившего приложение.

Уязвимыми являются следующие версии Microsoft Windows: Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1.

Хотя о бреши стало известно задолго до выхода патча, у Microsoft нет данных об эксплуатации ее злоумышленниками. Тем не менее, в компании указывают, что код эксплоита может быть написан таким образом, что атакующий сможет постоянно эксплуатировать данную уязвимость ***(Microsoft***

выпустила экстренный патч, устраняющий уязвимость нулевого дня в Windows // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/07/21/Microsoft-urgent-update.html). – 2015. – 21.07).

***

Международная антивирусная компания ESET раскрыла вредоносную киберкампанию «Операция Liberpy». Злоумышленники специализировались на краже персональных данных пользователей путем установки в систему программ-кейлоггеров. Ботнет, обнаруженный специалистами ESET, включал более 2000 зараженных устройств.

Для распространения вредоносных программ в рамках «Операции Liberpy» использовались фишинговые сообщения электронной почты, замаскированные под уведомления о почтовой доставке. Письма содержали ссылки на загрузку вредоносного ПО.

Эксперты ESET обнаружили несколько версий вредоносной программы, отслеживавших нажатия клавиш и перемещений указателя мыши. Полученные данные отправлялись на удаленный C&C-сервер злоумышленников, который использовался для хранения собранной информации.

Основной компонент вредоносной программы – кейлоггер (клавиатурный шпион). Он написан на языке Python и обнаруживается антивирусными продуктами ESET NOD32 как Python/Spy.Keylogger.G.

Вредоносное ПО поддерживает функцию заражения съемных устройств. Похожий механизм компрометации съемных носителей используют, в частности, программы Win32/Dorkbot, JS/Bondat и VBS/Agent.NDH. При этом директория с файлами вредоносной программы получает атрибут «скрытый», что препятствует ее обнаружению пользователем.

Установлено, что вредоносная кампания была ориентирована на пользователей из стран Латинской Америки. Подавляющее большинство заражений приходится на Венесуэлу, где обнаружено 1953 бота ***(ESET раскрыли операцию кибершпионажа // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/raskryta-ocherednaya-operaciya-kibershp.html). – 2015. – 16.07).***

***

«Лаборатория Касперского» предупреждает о появлении вредоносной программы TeslaCrypt 2.0 – новой версии трояна-шифровальщика, жертвами которого становятся преимущественно любители компьютерных игр.

Первые образцы TeslaCrypt были обнаружены в феврале 2015 г., и с тех пор шифровальщик претерпел несколько изменений. Отличительной особенностью этого зловреда является то, что он заражает типичные игровые файлы, например, файлы сохранений, пользовательских профилей, записанных повторов игр и т. д. За ключ для декодирования данных вымогатели требуют 500 дол. США.

Троян TeslaCrypt 2.0 запрашивает выкуп путём демонстрации своим жертвам HTML-страницы, полностью скопированной у другого широко известного вымогателя – CryptoWall 3.0. Зачем это сделано, не совсем ясно. Возможно, злоумышленники хотели таким образом продемонстрировать серьёзность своих намерений, ведь до сих пор файлы, зашифрованные CryptoWall, не поддаются расшифровке.

Новая версия TeslaCrypt отличается от предшественников существенно улучшенной криптографической схемой, из-за которой в настоящее время расшифровать затронутые файлы не представляется возможным. При каждом заражении TeslaCrypt генерирует новый уникальный адрес Bitcoin и секретный ключ для приёма платежей от конкретного пострадавшего.

TeslaCrypt поражает как обычные носители, подключенные к системе, так и все доступные сетевые файловые ресурсы, даже если они не смонтированы в качестве отдельного диска.

В основном от вымогательств этой программы пострадали пользователи в США и Германии ***(Необычный троян-шифровальщик притворяется другим зловредом // InternetUA (http://internetua.com/neobicsnii-troyan-shifrovalsxik-pritvoryaetsya-drugim-zlovredom). – 2015. – 16.07).***

***

Группа итальянских исследователей предложила три новые техники обфускации, способные обмануть антивирусные сканеры и успешно распространять вредоносные программы методом drive-by. Техники основаны на новых стандартах HTML5, объясняют авторы научной работы. По их мнению, увеличение количества малвари в сети объясняется именно внедрением новых веб-технологий.

Для обфускации используются некоторые программные интерфейсы HTML5, хотя принципиальная схема drive-by остается прежней. На предварительном этапе происходит шифрование зловреда и его размещение на сервере. Как только жертва загружает зараженную страницу, то одновременно скачивает вредоносную программу, которая дешифруется и запускается на исполнение.

Из двух указанных этапов первый остается без изменений. Как и раньше, следует найти подходящий «дырявый» сервер и сделать инъекцию кода.

Второй этап гораздо интереснее. Для доставки зловреда и дешифровки применяются программные интерфейсы HTML5. Именно это позволяет остаться незамеченным для антивирусов, которым пока незнакомы подобные методы.

В научной работе исследователи описывают три инновационных метода обмана антивирусов. Дело в том, что многие антивирусные системы отслеживают стандартные процедуры декодирования или деобфускации. Есть несколько способов избежать обнаружения.

Делегированная подготовка (Delegated Preparation): зловред разбивается на фрагменты в «базе данных», а деобфускация перекладывается на браузер с помощью Web-SQL API или IndexeDB API.

Распределенная подготовка (Distributed Preparation): обычно процедуры деобфускации выглядят безобидно по отдельности, но подозрительно все вместе. Это их свойство используется при распределенной деобфускации, когда зловред разбивается на фрагменты, и они расшифровываются в разных контекстах.

Деобфускация пользователем (User-driven Preparation): разновидность распределенной подготовки, когда расшифровка и исполнение программы размазаны по времени, которое пользователь проводит на зараженной веб-странице. Для внесения элемента случайности действия зловреда инициируются непосредственно действиями пользователя, не подозревающим об этом.

Эксперимент показал, что такая тактика позволяет обмануть большинство систем обнаружения и антивирусных сканеров.

Исследователи призывают разработчиков защитных систем модернизировать свои программы с учетом возможностей HTML5 ***(Распространение зловредов средствами html5 // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/07/17/html5-malware.html). – 2015. – 17.07).***

***

В кэш-файлах сайта WikiLeaks.org были обнаружены содержащие вредоносное ПО документы. Данные документы были скомпрометированы в ходе кибератаки на американскую частную разведывательно-аналитическую компанию Stratfor (Strategic Forecasting) в 2011 г. Напомним, одним из ключевых организаторов атаки на Stratfor был основатель проекта по обучению хакеров HackThisSite активист Д. Хаммонд.

В 2012 г. Д. Хаммонд передал ресурсу WikiLeaks рассекреченный архив электронной почты Stratfor. Д. Ассанж начал распространять данный архив через BitTorrent, а также через прямую ссылку на WikiLeaks. В 2015 г. рассекреченная переписка стала доступной в удобной для поиска базе данных WikiLeaks, в которой также можно найти скомпрометированные документы Sony Pictures и Hacking Team.

К сожалению, никому не удастся до конца изучить документы Stratfor, которые ведут к далекому 2004 г., из-за обнаруженного в файлах вредоносного ПО. Системный администратор Д. Видер, который обнаружил вредоносный код в данных, обеспокоен, что многие журналисты, активисты и исследователи могли инфицировать свои устройства, скачав файлы.

В общей сложности Д. Видер выявил 18 вредоносных программ, большинство из которых содержались в файлах PDF, Excel и Word. Видер оценил вредоносное ПО как крайне опасное и составил список электронных сообщений Stratfor, которых стоит избегать.

Вполне вероятно, что в базе данных WikiLeaks скрывается множество вредоносных документов. В настоящее время представители WikiLeaks не дали никаких конкретных комментариев по этому поводу ***(В базе данных WikiLeaks обнаружено вредоносное ПО // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/07/17/spyware-found-in-WikiLeaks.html). – 2015. – 17.07).***

***

Даже некоторые из самых популярных приложений позволяют предпринимать неограниченное количество попыток авторизации в учетной записи пользователя, а значит не имеют защиты от так называемых атак методом полного перебора. Речь идет о таких распространенных программах для Android и iOS, как SoundCloud, ESPN, CNN, Expedia и Walmart.

Согласно отчету исследователей из AppBugs, проанализировавших 53 распространенных приложения (в общей сложности их скачали 600 млн раз), все разработчики уязвимых продуктов были уведомлены о наличии брешей. При этом независимые эксперты дают 30 дней отсрочки для выпуска обновления, после чего информация о соответствующем приложении публикуется в открытом доступе.

Часть содержащих уязвимые механизмы авторизации программ уже была разглашена, а их полный перечень будет доступен 30 июля. При этом некоторые из разработчиков уже выпустили обновления безопасности для своих платформ (Wunderlist, Dictionary и Pocket).

По заверениям экспертов AppBugs, в большинстве случаев для взлома учетной записи пользователя злоумышленникам требуется от 30 мин. до одного месяца времени ***(Популярные приложения не имеют защиты от брутфорс-атак // InternetUA (http://internetua.com/populyarnie-prilojeniya-ne-imeuat-zasxiti-ot-brutfors-atak). – 2015. – 19.07).***

***

Исследователи ИБ-компании Trend Micro зафиксировали новую вредоносную кампанию, в ходе которой атакующие распространяют новый образец из семейства PoS-троянов GamaPoS при помощи ботнета Andromeda. GamaPoS предназначен для похищения информации кредитных карт из памяти платежных систем.

Как сообщили исследователи, атаки начинаются с рассылки спам-сообщений, которые якобы содержат документацию стандарта PCI DSS (Payment Card Industry Data Security Standard) с требованиями по обеспечению безопасности данных о держателях платежных карт или обновления, необходимые для защиты компьютерных систем от недавно обнаруженного вредоносного ПО MalumPs.

На самом деле в электронном письме находится вложение с вредоносным макросом, который устанавливает бэкдор на инфицированный компьютер под управлением Windows. Этот бэкдор злоумышленники используют для загрузки

GamaPoS, а также других инструментов, при помощи которых могут вручную взломать другие системы в сети целевой организации.

По данным экспертов, подавляющее число случаев инфицирования зарегистрировано в США (85 %). На долю Канады пришлось 2 % инцидентов. На третьем месте находятся Тайвань, Китай и Япония с показателем в 1 %. Целевыми являются компании, предоставляющие услуги по медицинскому обслуживанию на дому, интернет-магазины розничной торговли, а также продавцы бытовой техники, рестораны, кредитные организации и пр. ***(Хакеры используют ботнет Andromeda для распространения нового вредоноса // InternetUA (http://internetua.com/hakeri-ispolzuuat-botnet-Andromeda-dlya-rasprostraneniya-novogo-vredonosa). – 2015. – 19.07).***

***

Компания Corero Network Security провела в рамках конференций RSA Conference 2015 и Infosecurity Europe 2015 исследование мнения профессионалов относительно худших последствий DDoS-нападений.

Согласно опросу, 52 % респондентов заявили, что худшим, к чему может привести DDoS-атака, является потеря доверия клиентов. Следующими по важности признаны недоступность услуг и снижение доходов – так считают 22 % участников исследования.

Четверть опрошенных уверены, что жертвы DDoS-атак в первую очередь страдают от заражения вредоносными программами в ходе хакерской операции. Наконец, 11 % полагают, что нет ничего хуже кражи данных и потери интеллектуальной собственности, которая периодически происходит в ходе нападений.

Интересно, что в 21 % случаев, когда начинается атака, компании узнают о ней после жалоб пользователей, пытающихся получить услуги. Впрочем, 14 % специалистов регистрируют такого рода активность киберпреступников по перебоям в работе собственной инфраструктуры. И такой же процент опрошенных отметил сбой приложений, например, сайта.

К сожалению, менее половины респондентов (46 %) сообщили о возможности заранее замечать признаки еще только надвигающейся угрозы. При этом приблизительно 50 % опрошенных полагаются на традиционную ИТ-инфраструктуру или вовсе опираются на провайдера в деле предотвращения атак. Только 23 % специалистов в области ИБ противостоят нападениям с помощью специальных решений или посредством облачных анти-DDoS-сервисов. Однако порядка 32 % все же подчеркнули, что собираются взять на вооружение такие решения ***(Потеря доверия клиентов – худшее последствие DDoS-атаки // InternetUA (http://internetua.com/poterya-doveriya-klientov---hudshee-posledstvie-DDoS-ataki). – 2015. – 21.07).***

***

Группа хакеров, подозревающихся в атаках на Белый дом и Государственный департамент США и предположительно связанных с Россией,

провели изощренную фишинговую атаку на компьютеры служащих американского военного ведомства, сообщает thedailybeast.com.

По данным внутренней служебной записки военного ведомства, пострадали по крайней мере пять пользователей, однако о хищении данных не сообщается.

Эксперт Пентагона по IT-безопасности М. Адамс в своем Twitter сообщил, что изощренность атаки превышает все фиксирующиеся до этого времени случаи, связанные с этой хакерской группой. Все свободные силы ведомства брошены на устранение последствий атаки ***(Российские хакеры атаковали Пентагон // InternetUA (http://internetua.com/rossiiskie-hakeri-atakovali-pentagon). – 2015. – 20.07).***

***

Злоумышленники используют созданные на JavaScript диалоговые окна для отображения на экранах iPhone и iPad предупреждений о системном сбое. Об этом сообщает ресурс Securitylab.

Как выяснили эксперты финской компании F-Secure, сообщение о сбое iOS является разновидностью мошенничества, при которой злоумышленники выдают себя за операторов технической поддержки. Преступная схема направлена на владельцев iPhone и iPad в США и Великобритании. При поиске в браузере на устройствах жертв появляются всплывающие окна с сообщением о системном сбое и предложением позвонить в техподдержку для устранения проблемы.

Деятельность злоумышленников использует особенности работы стандартного iOS-браузера Safari. Преступники требуют, чтобы жертва позвонила на линию поддержки и заплатила от 19 до 80 дол. для устранения проблемы. В Великобритании эта цифра составляла 20 фунтов стерлингов.

Схема выглядит следующим образом. Пользователь получает сообщение: «Предупреждение!! Системный сбой iOS!!. Из-за приложения от стороннего разработчика на вашем устройстве произошел сбой iOS. Обратитесь в поддержку для устранения проблемы». Отображаемое на дисплее устройства предупреждение содержит контактные номера телефона. Пользователям в Великобритании, позвонившим на линию поддержки, сообщают, что на их устройстве есть вредоносное ПО, похищающее данные. Для устранения проблемы операторы требуют данные о кредитной карте.

Служба техподдержки Apple предлагают следующий способ блокировки всплывающих предупреждений:

– включить на устройстве Авиарежим.

– очистить данные Safari: Настройки > Safari > Очистить историю;

– выйти из авиарежима.

По словам экспертов F-Secure, предупреждение, появляющееся в виде всплывающего окна, является диалоговым окном, созданным на JavaScript. Наиболее быстрым способом устранить проблему будет отключение JavaScript в Safari, хотя такое решение негативно скажется на легитимных сайтах.

Попав на вредоносный сайт через браузер Chrome для Windows, во всплывающем окне появится опция «Предотвратить появление дополнительных диалогов на этой странице». Эта опция доступна в текущих версиях Chrome и Firefox для Windows и не доступна в Internet Explorer и Safari. Выбор указанной функции позволит пользователю прервать цепь сообщений ***(Пользователи iPhone и iPad стали жертвами мобильного мошенничества // InternetUA (http://internetua.com/polzovateli-iPhone-i-iPad-stali-jertvami-mobilnogo-moshennicsestva). – 2015. – 21.07).***

***

Два американских программиста смогли через Интернет подключиться к бортовому компьютеру Jeep Cherokee. Они запускали и выключали двигатель, управляли работой стеклоочистителей, омывателя и радио, вывели из строя тормозную систему. За рулем автомобиля находился журналист Wired, он не пострадал, пишет издание.

В качестве хакеров выступили сотрудник Twitter Ч. Миллер, ранее работавший в Агентстве национальной безопасности США, и специалист по компьютерной безопасности К. Валасек. Целью шоу было продемонстрировать уязвимость современных автомобилей перед кибервзломщиками.

Тест проходил на парковке хайвея близ Сент-Луиса. Хакеры находились на расстоянии нескольких километров от машины и с легкостью проникли в ее систему управления. «Сотни, тысячи машин на дорогах не имеют достаточной защиты», – констатировал Ч. Миллер ***(Хакеры удаленно отключили тормоза Jeep Cherokee // InternetUA (http://internetua.com/hakeri-udalenno-otkluacsili-tormoza-Jeep-Cherokee). – 2015. – 22.07).***

***

Количество известных вирусным аналитикам вредоносных программ, предназначенных для демонстрации пользователям Интернета назойливой рекламы, увеличивается день ото дня.

В июле 2015 г. специалисты компании «Доктор Веб» обнаружили несколько подобных троянцев, один из которых, получивший наименование Trojan.Ormes.186, встраивает рекламу в просматриваемые жертвой веб-страницы с использованием технологии веб-инжектов.

Вредоносная программа Trojan.Ormes.186 представляет собой расширение для браузера Mozilla Firefox, состоящее из трех файлов, написанных на языке JavaScript. Один из этих файлов зашифрован и предназначен для демонстрации различного рода рекламы, а два других встраивают его в открываемые в окне браузера веб-страницы непосредственно на компьютере жертвы: подобная технология называется веб-инжектом.

Основной код троянца расположен в зашифрованном файле и именно он реализует основные функции Trojan.Ormes.186 по встраиванию постороннего содержимого в веб-страницы. В теле вредоносной программы содержится список, состоящий из порядка 200 адресов интернет-ресурсов, при обращении к

которым Trojan.Ormes.186 выполняет веб-инжекты. Среди них – различные сайты для поиска и размещения вакансий, а также адреса популярных поисковых систем и социальных сетей.

В коде троянца предусмотрена специальная функция, предположительно реализующая возможность автоматической эмуляции щелчка мышью на различных элементах веб-страниц с целью подтверждения подписок для абонентов мобильных операторов «Мегафон» и «Билайн». Кроме того, при открытии в окне браузера сайтов «Яндекс», YouTube, а также социальных сетей «ВКонтакте», «Одноклассники» и Facebook Trojan.Ormes.186 загружает с удаленного сайта и выполняет соответствующий сценарий, который через цепочку редиректов перенаправляет жертву на сайты различных файлообменных систем, использующих для монетизации платные подписки. В процессе работы с популярными поисковыми системами троянец также встраивает в страницы с отображаемыми в результате обработки запроса ссылками рекламные баннеры. В страницы социальной сети Facebook данная вредоносная программа внедряет скрытый элемент iframe (с целью установки внутренних переменных, необходимых для работы троянца), благодаря чему Trojan.Ormes.186 может автоматически устанавливать отметку Like («мне нравится») ряду веб-сайтов из специального списка.

Среди других возможностей Trojan.Ormes.186 следует отметить функцию автоматического входа на сайты онлайн-казино, список которых также имеется в теле вредоносной программы. Если сайт содержит предложение об установке приложения для социальных сетей, троянец выполняет автоматическое перенаправление пользователя на страницу такого приложения. Отслеживая открытие подобных страниц, Trojan.Ormes.186 эмулирует щелчок мышью по ссылке, разрешающей установку, – в результате приложение инсталлируется фактически без участия пользователя ***(Рекламный троянец осуществляет веб-инжекты // ITnews (http://itnews.com.ua/news/77673-reklamnyj-troyanets-osushhestvlyaet-veb-inzhekty). – 2015. – 23.07).***

***

Мошенники взламывают страницы пользователей с целью наживы, пишет 5692.com.ua (http://www.5692.com.ua/news/899088).

Пользователи социальной сети «ВКонтакте» подвергаются атакам мошенников. Злоумышленники взламывают страницу и от имени пользователя рассылают сообщения с просьбой о помощи или с просьбой «положить деньги на модем».

Всем, кому пришли сообщения подобного содержания, вызывающие подозрение, не стоит реагировать на них. Также необходимо как можно быстрее предупредить об этом друга, чья страница была взломана, чтобы тот предпринял необходимые меры безопасности.

Пользователю, чья страница пострадала от взлома, рекомендовано привязать страницу к номеру своего мобильного телефона, а также регулярно проверять компьютер с помощью антивирусной программы. Помимо этого,

стоит подобрать надежный пароль и периодически его менять. О взломе страницы необходимо сообщить в техподдержку. Активность своей страницы можете проследить в истории активности ***(В Днепродзержинске обнаружена схема мошенничества в социальных сетях // 5692.com.ua – Сайт города Днепродзержинска (http://www.5692.com.ua/news/899088). – 2015. – 22.07).***

***

Вирусные аналитики компании «Доктор Веб» исследовали новый образец троянца-бэкдора, представляющего опасность для операционных систем семейства Linux.

По задумке авторов этой вредоносной программы она должна обладать чрезвычайно широким и мощным набором возможностей, однако на текущий момент далеко не все ее функции работают соответствующим образом.

Данный бэкдор, получивший наименование Linux.BackDoor.Dklkt.1, имеет предположительно китайское происхождение. По всей видимости, разработчики изначально пытались заложить в него довольно обширный набор функций – менеджера файловой системы, троянца для проведения DDoS-атак, прокси-сервера и т. д., однако на практике далеко не все эти возможности реализованы в полной мере. Более того: исходные компоненты бэкдора были созданы с учетом кроссплатформенности, то есть таким образом, чтобы исполняемый файл можно было собрать как для архитектуры Linux, так и для Windows. Однако, поскольку разработчики отнеслись к этой задаче не слишком ответственно, в дизассемблированном коде троянца встречаются и вовсе нелепые конструкции, не имеющие к Linux никакого отношения.

При запуске Linux.BackDoor.Dklkt.1 проверяет наличие в папке, из которой он был запущен, конфигурационного файла, содержащего необходимые для его работы параметры. В этом файле задаются три адреса управляющих серверов бэкдора, однако используется им только один, в то время как два других являются резервными. Конфигурационный файл зашифрован с использованием алгоритма Base64. При запуске Linux.BackDoor.Dklkt.1 пытается зарегистрироваться на атакованном компьютере в качестве демона (системной службы), а если это не удается, бэкдор прекращает свою работу.

После успешного запуска троянец формирует и отсылает на управляющий сервер пакет с информацией об инфицированной системе, при этом весь трафик обмена данными между бэкдором и удаленным командным центром сжимается с использованием алгоритма LZO и шифруется алгоритмом Blowfish. Каждый пакет также снабжается контрольной суммой исходных данных для определения целостности полученной информации на принимающей стороне.

После этого Linux.BackDoor.Dklkt.1 переходит в режим ожидания входящих команд, среди которых следует отметить директивы начала DDoS-атаки, запуска SOCKS proxy-сервера, запуска указанного в пришедшей команде приложения, перезагрузки или выключения компьютера. Все остальные

команды Linux.BackDoor.Dklkt.1 либо игнорирует, либо обрабатывает некорректно. Троянец способен выполнять следующие типы DDoS-атак:

SYN Flood
HTTP Flood (POST/GET запросы)
ICMP Flood
TCP Flood
UDP Flood

Сигнатура этого бэкдора добавлена в вирусные базы Dr.Web, поэтому пользователи Антивируса Dr.Web для Linux защищены от действия данной вредоносной программы ***(Обнаружен новый бэкдор для Linux // ITnews (http://itnews.com.ua/news/77680-obnaruzhen-novyj-bekdor-dlya-linux). – 2015. – 23.07).***

***

Компьютерные атаки вскоре смогут стать причиной человеческих смертей

Сотрудничество между государственным и частным сектором в сфере компьютерной безопасности неуклонно расширяется с каждым днем и, по мнению работающих с критической инфраструктурой IT-экспертов, у обоих сторон есть острая необходимость в развитии такого взаимодействия. Об этом заявили участники опроса совместно проведенного представителями Aspen Institute и Intel Security.

Согласно документу, эволюция угроз информационной безопасности приобретает характер снежной лавины, которая в скором времени может достигнуть точки, потенциально ведущей к человеческим жертвам. Вместе с тем, по мнению 86 % IT-экспертов, связанных с критической инфраструктурой, взаимная поддержка бизнеса и правительства является ключом к обеспечению достойной защиты от совершенствующихся киберпреступников.

Интересно также, что в течение последних трех лет большинство специалистов отмечали улучшение общего положения дел в сфере информационной безопасности. Оценивая уровень безопасности собственных организаций в ретроспективе, 50 % опрошенных сообщили, что три года назад он был «очень или чрезвычайно» низок. В настоящее время таковыми собственные компании считают 27 % IT-экспертов.

Еще одним тревожным показателем является то, что за прошедших три года почти девять из десяти (89 %) специалистов сталкивались как минимум с одним успешным нападением на администрируемые ими системы, которые были признаны надежными ***(Компьютерные атаки вскоре смогут стать причиной человеческих смертей // InternetUA (http://internetua.com/kompuaternie-ataki-vskore-smogut-stat-pricsinoi-cselovecseskih-smertei). – 2015. – 23.07).***