СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(27.05–9.06)

2013 № 11

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(27.05–9.06)
№ 11

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

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

Редакційна колегія:
В. Касаткін, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2013

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ 4

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 12

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 19

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 30

Інформаційно-психологічний вплив мережевого спілкування на особистість 30

Маніпулятивні технології 34

Зарубіжні спецслужби і технології «соціального контролю» 39

Проблема захисту даних. DOS та вірусні атаки 52

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Nextdoor – это необычная приватная мобильная социальная сеть, призванная объединить живущих по соседству людей. Приложение позволяет быть в курсе всех событий своего района. Пока сервис доступен лишь в США, но планирует глобальную экспансию.

Nextdoor – это не одна из тех соцсетей, в которую люди выкладывают тонны бесполезной информации. Она конкретна, заточена под повседневные нужды. В Nextdoor можно найти информацию о гаражных распродажах, сдаваемых комнатах и т. д.

На самом деле новое приложение – это всего лишь мобильный аналог сайта Nextdoor. В целом, в нем можно делать примерно то же самое, что и в браузерной версии, только удобнее.

Nextdoor уделяет большое внимание безопасности района. При помощи приложения можно с легкостью поделиться информацией о любой подозрительной активности. Есть также функция, позволяющая передать экстренное сообщение, которое увидят сразу все жители района.

Также приложение позволяет постить большое количество фотографий, относящихся к месту жителя. Снимки в основном будут по делу – к примеру, потерянные кем-то ключи, заблудившаяся собака или хулиганящие подростки. Жители района быстро увидят фотографии и смогут отреагировать.

«Представьте, что у вас сотни камер, доступных вашему взгляду в любой момент. У каждого ведь есть смартфон», – отметил Н. Толиа, глава проекта. В настоящее время приложение можно бесплатно скачать из App Store. Версии для Android пока что нет, однако разработчики обещают выпустить ее в ближайшее время ***(Nextdoor: соцсеть для соседей // InternetUA (http://internetua.com/Nextdoor--socset-dlya-sosedei). – 2013. – 27.05).***

***

Инструмент для создания видеороликов с эффектом замедленного движения slow-motion появился на видеохостинге YouTube, сообщает Обозреватель (http://tech.obozrevatel.com/news/15469-youtube-nauchili-zamedlyat-videoroliki.htm).

Инструмент получил название «Замедление». Он позволяет «затормозить» скорость движения объектов в кадре в два, в четыре или в восемь раз, создавая иллюзию медленного течения времени.

Чтобы применить эффект «Замедление» к ролику, загруженному на YouTube, нужно открыть редактор видео и нажать кнопку с изображением черепахи.

Обычно для получения эффекта slow-motion используется ускоренная киносъемка. Она ведется на камеру, способную снимать более 24 кадров в секунду, но фильм проецируется со стандартной частотой кадров ***(YouTube***

научили замедлять видеоролики // Обозреватель (http://tech.obozrevatel.com/news/15469-youtube-nauchili-zamedlyat-videoroliki.htm). – 2013. – 29.05).

***

Газета The Wall Street Journal запустит деловую социальную сеть WSJ Profile. Об этом сообщило издание The Times.

Представители компании Dow Jones, владеющей газетой, описали WSJ Profile как «соцсеть для людей со схожими взглядами». По их словам, сеть будет напоминать финансовый форум. Пользователи смогут размещать в своих профилях информацию об опыте работы и образовании, а также писать друг другу сообщения.

Точная дата запуска WSJ Profile пока не известна, но сообщается, что сеть заработает в июне 2013 г. Также неизвестно, в каких странах будет доступна соцсеть.

В марте The Wall Street Journal запустил интернет-приложение WSJ Portfolio, с помощью которого пользователь может управлять своим инвестиционным портфелем. Издание TheNextWeb сообщает, что у этого приложения появится интеграция с WSJ Profile.

The Wall Street Journal и владеющая им компания Dow Jones принадлежат медиакорпорации Р. Мердока News Corporation. Последней ранее принадлежала другая соцсеть – MySpace, которую корпорация купила в 2005 г. за 580 млн дол. В 2011 г. MySpace была продана за 35 млн дол. Р. Мердок впоследствии назвал покупку соцсети «огромной ошибкой» ***(The Wall Street Journal откроет собственную социальную сеть // Utro.ua (http://www.utro.ua/ru/ekonomika/the_wall_street_journal_otkroet_sobstvennuyu_sotsialnuyu_set1370031264). – 2013. – 1.06).***

***

Социальная сеть Facebook начала помечать подлинные страницы знаменитостей. Об этом сообщается 29 мая в пресс-релизе Facebook.

Возле имен знаменитостей появится голубая «галочка», которая будет свидетельствовать о подлинности страницы. Процедуру верификации, отмечает Facebook, пройдут звезды, журналисты, чиновники и популярные компании, на которых подписано большое количество пользователей.

«Галочки» будут появляться у знаменитостей постепенно. На момент написания заметки процедуру верификации прошли, к примеру, певица С. Гомез, основатель техноблога TechCrunch М. Аррингтон и премьер-министр России Д. Медведев.

Как отмечает TechCrunch, Facebook запустил процесс верификации аккаунтов еще в феврале 2013 г. Владельцы некоторых страниц получали предложение подтвердить свою личность, прислав электронную версию своих документов. Но тогда подтвержденные аккаунты внешне никак не отличались от обычных.

Facebook ввела функцию верификации аккаунтов пользователей позже других популярных соцсетей. «Галочки» на популярных страницах уже ставят Twitter, Google+, «ВКонтакте» и «Одноклассники» ***(Facebook научился определять подлинные страницы знаменитостей // Подробности.UA (http://podrobnosti.ua/internet/2013/05/30/907910.html). – 2013. – 30.05).***

***

Щодня понад 2 млн користувачів соцмережі «Одноклассники» вибирають локальну, не російську, мову для спілкування й розваг. Одною з найпопулярніших є українська. Нею щодня користується 650 тис. українців – 122 тис. через мобільні пристрої та 530 тис. – на лептопах та стаціонарних комп'ютерах ***(Мінченко О. В Одноклассниках 650 тисяч користувачів щодня вибирають українську версію // Watcher (http://watcher.com.ua/2013/05/31/v-odnoklassnykah-650-tysyach-korystuvachiv-schodnya-vybyrayut-ukrayinsku-versiyu/). – 2013. – 31.05).***

***

LiveJournal розпочав бета-тестування проекту «ЖЖ на мапі». Суть проекту в тому, що будь-які публікації, пов'язані з якимись конкретними координатами, наносяться на мапу – через яку здійснюється навігація.

Автори вважають, що це має бути дуже зручно під час підготовки до подорожей – дасть змогу знайти контент із перших рук і навіть запитати у автора щось у коментарях. Наприклад, для Чернівців мапа відображає 18 результатів.

Сервіс працює на основі мап від Google, доступні два режими перегляду: звичайна мапа та вигляд із супутника. Кожна точка на мапі має окрему сторінку, яка відображає усі публікації про це місце. До будь-якого місця ви можете додати публікацію про нього, а також відмітити, що вам це місце подобається, що ви тут були чи що хочете туди потрапити. Також ви можете побачити хто тут живе і якщо ви тут живете – вказати це.

Щоб додати якесь місце на мапу, вам потрібно буде авторизувати додаток «LJ Maps Test Application», а потім вказати назву місця та лінк на публікацію про це місце; а також – вказати точку на мапі.

У подальшому планується запустити мобільний додаток для подорожей. Наразі веб-версія проекту містить близько 15 тис. публікацій, прив'язаних до мапи. Але робота над базою локацій та публікаціями про них триває, для цього виділили окрему команду редакторів ***(Костинян М. LiveJournal запускає «ЖЖ на мапі» // Watcher (http://watcher.com.ua/2013/05/29/livejournal-zapuskaye-zhzh-na-mapi/). – 2013. – 29.05).***

***

Сервис микроблогов Twitter сообщает, что с 3 июня видеосервис Vine доступен также пользователям Android, говорится в официальном аккаунте

Twitter, пишет «Обозреватель» (http://tech.obozrevatel.com/news/30265-twitter-zapuskaet-videoservis-vine-dlya-android.htm).

Ранее Vine был доступен только владельцам iPhone. В настоящее время обладатели устройств на Android уже могут загрузить новое приложение на Google Play.

Vine позволяет создавать видеоролики длиной 6 с со звуком с помощью мобильного устройства и делиться ими с друзьями. Twitter купил сервис в октябре 2012 г.

По информации Twitter, видеосервисом пользуются 13 млн человек.

В Android-версии Vine будет функция приближение, которая недоступна для iPhone. В компании обещают, что скоро синхронизируют версии для обеих операционных систем, а кроме того, через несколько недель добавят такие функции, как съемка через фронтальную камеру, поиск, хештэги, а также возможность делиться видео на Facebook ***(Twitter запускает видеосервис Vine для Android // Обозреватель (http://tech.obozrevatel.com/news/30265-twitter-zapuskaet-videoservis-vine-dlya-android.htm). – 2013. – 3.06).***

***

Компания Mail.Ru Group работает над новым функционалом популярного мессенджера ICQ. «Аську» полностью объединят с другим мессенджером, принадлежащим компании, – Mail.Ru Агентом. В результате преобразований новый мессенджер практически превратится в сервис знакомств, сообщает издание Известия.

В частности, здесь можно будет находить в своем городе людей со схожими интересами, а также отправлять платные подарки. Как ожидается, это остановит сокращение аудитории ICQ и позволит монетизировать сервис. За последние три года ежемесячная аудитория ICQ в России уменьшилась вдвое: с 18,5 млн до 8,7 млн человек.

Помимо функционала, позаимствованного у сайтов знакомств, мессенджер приобретет черты соцсетей. Например, пользователи смогут объединяться в группы по интересам. И это тоже отличный способ монетизации: рекламодатели смогут таргетировать рекламу по интересам пользователей.

«В мессенджерах поведение людей отличается от поведения в соцсетях, – комментирует руководитель направления Instant Massaging холдинга Mail.Ru Group И. Ермаков. – Но и здесь может быть полезным объединение в группы по интересам. Например, я пришел на концерт, и мне интересно обсудить его с теми, кто сейчас сидит в том же зале, или с фанатами группы сразу после концерта».

Посмотрим, удастся ли компании вернуть интерес пользователей к некогда весьма популярному сервису. Сегодня пользователи привыкли обмениваться мгновенными сообщениями внутри соцсети. Заинтересует ли их мессенджер с функционалом соцсети? Есть и те, кто убежден, что уже ничто не сможет вернуть «аську» к жизни. Поживем – увидим ***(ICQ станет сервисом***

знакомств // InternetUA (http://internetua.com/ICQ-stanet-servisom-znakomstv). – 2013. – 4.06).

***

Могут ли социальные сети стать блог-платформой

В последнее время наблюдается особая тенденция – блогеры бросают уютные блог-платформы и стэндэлоуны, чтобы перенести свою активность в аккаунты в социальных сетях. Соцсети это, конечно, поощряют – даже появляются каталоги блогеров. Но так ли это удобно, как кажется на первый взгляд?

В соцсетях традиционного типа, к которым можно отнести Facebook и «ВКонтакте», есть особая сущность, «заметки», которая позволяет набивать большое количество текста и даже форматировать его. Заметки действуют как дополнение к обычным постам в профиле, доносящим относительно короткие мысли.

Однако заметками по факту мало кто пользуется, предпочитая стандартные обновления статуса. В Facebook это обусловлено введением таймлайна. Есть признаки того, что Facebook попробует обеспечить себе успех на блоггерском поприще – недавно был приобретён блог-стартап Storylane. Крупнейший социальный сервис может попытаться одолеть Tumblr, отбирающий у него молодую аудиторию. Для этого нужно обновить функцию заметок. На сегодняшний день тот же Tumblr даёт блогерам гораздо больше свободы в выражении мыслей.

Сегодня заметки в Facebook представляют собой жалкое зрелище – есть всего шесть опций форматирования, среди которых изменение стиля текста, создание списков и цитат. Вы можете прикреплять фотографии, но не видео или анимацию – то, что является одной из ключевых ценностей Tumblr. На сегодня этот раздел используют только различные отделы Facebook для больших описаний свеженаписанных фич и уходящие сотрудники для проникновенных прощальных постов. После публикации заметка появляется в ленте новостей, но выглядит очень тускло. В Tumblr каждая запись имеет свою индивидуальность, как и каждый блог.

Что самое главное, раздел с заметками сейчас крайне сложно найти. Facebook следует не только выставить эту кнопку на первый план, но и указывать список заметок прямо в профиле пользователя. Да, на сегодня заметки придерживаются той политики прозрачного упорядочивания, которая помогла в борьбе с извечным хаосом MySpace. Но предоставьте пользователям чуть больше свободы, и они сами пойдут к вам.

Во «ВКонтакте» тоже есть свои заметки, причём гораздо более мощные. Здесь можно и прикреплять поддерживаемые сайтом медиафайлы, и использовать выравнивание, и применять широкий спектр инструментов форматирования, и даже править исходный вики-код. Раньше, если текст поста превышал какой-то размер, пользователю предлагали перенести свои мысли в

заметку. Сегодня это вовсе необязательно – гораздо проще оставить часть поста и накидать снизу несколько медиафайлов.

Здесь тоже мало кто пользуется заметками: во-первых, выгода этого не совсем очевидна, во-вторых, тоже присутствуют определённые проблемы. Агонию местных «заметок» символично завершил недавний пост бывшего пресс-секретаря «ВКонтакте» В. Цыплухина, который пытался сделать красивую заметку о своём путешествии, но обнаружил на своём блогерском пути немало препятствий.

Если отбросить уродство самопального языка разметки – исходный код с первого взгляда кажется случайным нагромождением знаков пунктуации, – то всё упирается в кривизну его обработки. Заметка, которую вы верстаете долгое время, может внезапно разъехаться самыми неимоверными способами. Одновременно с этим, в сети полно WYSIWYG-редакторов, которые пусть и являются оболочкой HTML-кода, но позволяют быстро и точно форматировать текст без лишних усилий. Ничто не мешает разработчикам «ВКонтакте» накидать набор простейших элементов, которые не скрывают под собой нечто монструозное.

Конечно, текущий вики-парсер горячо любим администраторами групп, которые с его помощью шустро верстают менюшки и прочие вспомогательные страницы. Но не всякий непосвящённый пользователь справится с этим с первого захода – ему и не нужно уметь править код, он привык управляться с кнопками. Победив эту проблему, «ВКонтакте» сможет ещё быстрее привлекать на свою сторону не только адептов Facebook, но и ЖЖ-блогеров, которые уже давно разочаровались в своей платформе, но не знают, куда идти ***(Могут ли социальные сети стать блог-платформой // InternetUA (http://internetua.com/mogut-li-socialnie-seti-stat-blog-platformoi). – 2013. – 2.06).***

***

Популярная в США визуальная соцсеть Pinterest решила пересмотреть ограничения, накладываемые пользовательским соглашением на размещение обнаженной натуры. Единственное требование – чтобы подобное изображение имело художественную ценность.

«Pinterest – это ресурс, помогающий людям раскрыть свои увлечения. Часто люди увлечены искусством, а искусство может оперировать обнаженностью», – отметила компания. В целом, пользователи Pinterest, несмотря на запрет, уже разместили в соцсети немало эротических фотографий. Таким образом, действия Pinterest – это просто ответ на то, что уже происходит.

Pinterest сфокусирована на визуальном контенте – в нее можно отправлять любые встреченные в сети изображения. Это делает ресурс привлекательным местом для интересующихся искусством людей. Запрещать выкладывать обнаженные фото, не имея реальной возможности полностью контролировать этот процесс – не слишком-то правильно. Теперь перед Pinterest встанет задача четко отделить искусство от порнографии, чтобы разработать внятные критерии модерирования контента ***(Соцсеть Pinterest***

хочет разрешить эротику // InternetUA (http://internetua.com/socset-Pinterest-hocset-razreshit-erotiku). – 2013. – 4.06).

***

Исследование Gemius Украина представило топ-20 сайтов Уанета по популярности за апрель 2013 г. Данные построены на базе результатов исследования gemiusAudience.

В пятерке самых популярных сайтов оказались Google.com, Mail.ru, Vk.com, Yandex.ua и Youtube.com. На девятом месте расположилась социальная сеть Facebook.com.

…Всего в апрельской панели представлены около 600 сайтов. Социально-демографический отчет составлен на основе 6597 анкет software-списков и 47 823 анкет cookie-списков. Fusion-панель (смешанная панель) в исследовании gemiusAudience объединяет cookie-панель и software-панель.

Охват – процентное соотношение числа посетителей (реальных пользователей), совершивших, по крайней мере, один просмотр страницы на выбранном сайте за этот временной интервал, к общему числу интернет-пользователей за этот временной интервал ***(Названы самые популярные у украинцев сайты // Версии.com (http://versii.com/news/280240/). – 2013. – 5.06).***

***

WPP и Twitter заключили договор о глобальном стратегическом партнерстве, которое позволит значительно расширить сотрудничество между двумя компаниями. Соглашение предусматривает взаимодействие в области аналитики, использования накопленных данных, медиаинвестиций и социальных платформ.

Подразделения WPP смогут использовать данные Twitter для повышения эффективности кампаний благодаря оптимальному таргетированию и получению информации в режиме реального времени.

Сделка охватывает несколько компаний WPP, в том числе GroupM, Kantar, Wunderman и другие digital агентства. Партнерство приведет к запуску новых продуктов и услуг в области обработки данных и их интеграции между платформами WPP и Twitter, сообщили в компании.

Глава WPP М. Соррелл прокомментировал сделку: «Актуальность Twitter продолжает расти – не только как социальной платформы, но и как окна во внутренний мир потребителя и его поведения в реальной жизни. Мы убеждены, что данные Twitter являются ключевым звеном для многих наших дисциплин».

Ранее Twitter заключил рекламную сделку с медиакоммуникационной компанией Starcom MediaVest Group. Основная сфера их сотрудничества – изучение мнения потребителей и влияние соцсети на телесмотрение ***(Twitter и WPP стратегически подружились // МедиаБизнес (http://www.mediabusiness.com.ua/?option=com_content&task=view&id=35260&Itemid=). – 2013. – 7.06).***

***

Девятилетний интернет-гигант Facebook, согласно исследованию компании Pew Research, «обрюзг» и начал терять притягательность для юных пользователей. Тинэйджеры перебегают в молодые мобильные социальные сети, такие как Line и SnapChat, сообщает UBR (http://ubr.ua/ukraine-and-world/events/facebook-perejivaet-krizis-srednego-vozrasta-231776).

Имея 1,1 млрд пользователей, огромный массив данных об их интересах и связях, обширную коллекцию фотографий и онлайн-профилей, служащих для входа на многие другие интернет-сервисы, Facebook в ближнесрочной перспективе вряд ли столкнется с массовой утечкой пользователей.

В социальной сети Facebook люди на сегодня проводят существенно больше времени, чем на конкурирующих ресурсах, таких как Google, Microsoft или Yahoo. По утверждению исследовательской компании Nielsen Media, число пользователей Facebook, посещающих этот сайт ежедневно, увеличилось до 59,9 % от их общего числа в I квартале, по сравнению с 58,3 % в IV квартале.

Однако многие юные интернет-пользователи, участвовавшие в опросе Pew Research, пожаловались, что их интерес к Facebook затухает из-за возрастающего присутствия взрослых пользователей, захламливающих ресурс скучными постами и оказывающих на подростков психологическое давление.

«Около 70 % юных пользователей Facebook связаны в этой сети со своими родителями, но это вовсе не означает, что они рады такой дружбе. Подростки испытывают волнение относительно того, что любая размещенная ими в Facebook информация может быть проанализирована родственниками, друзьями и коллегами; у 57 % опрошенных подростков возникала ситуация, когда они отказывались от публикации информации из-за опасения, что это плохо отразится на них в будущем», – описывает проблему главный исследователь Pew Research М. Мадден.

По мнению аналитиков, самая опасная угроза бизнесу Facebook исходит от лавины новых приложений для обмена сообщениями и фотографиями. Эти приложения возникают, как грибы после дождя, и отвлекают сотни миллионов пользователей от времяпровождения в Facebook.

Например, японский сервис моментальных сообщений Line за два года существования привлек 140 млн пользователей, а на двухлетнем ресурсе SnapChat, позволяющем отсылать исчезающие через несколько секунд снимки, пользователи ежедневно обмениваются 60 млн фотографий.

Опасения, что Facebook теряет привлекательность для пользователей, отражается на цене акций, которые падают на фоне общего подъема фондовых рынков. Котировки интернет-гиганта за последние пять недель на опустились на 20 % до 23 дол. за акцию. Это на 40 % меньше, чем они стоили в момент выхода Facebook на биржу в мае 2012 г.

Facebook мало преуспел в осуществлении своей амбициозной цели – стать всеобъемлющей платформой, на которой пользователи смогут получить все возможные интернет-услуги от общения до заработка и осуществления покупок.

Facebook нет равных в том, что касается публикации фотографий и дружеского общения. Однако в секторе поиска работы и профессиональных коммуникаций по-прежнему доминирует социальная сеть LinkedIn, а поисковый бизнес сосредоточен в руках Google.

«Если вы стремитесь охватить все, вы теряете свою миссию. Вы пытаетесь заграбастать слишком много, и от этого становитесь обрюзгшим, а люди чувствуют это. Возможно, хорошей идеей будет сконцентрировать усилия на развитии своих ключевых направлений», – комментирует ситуацию бывший исполнительный директор Facebook Н. Якобсон ***(Facebook переживает кризис среднего возраста // UBR (http://ubr.ua/ukraine-and-world/events/facebook-perejivaet-krizis-srednego-vozrasta-231776). – 2013. – 7.06).***

***

Facebook продолжает стремиться заменить собой весь остальной Интернет, и помогают ему в этом сторонние разработчики, создающие все новые полезные инструменты-приложения. В этот раз колокол прозвонил по файлообменникам – при помощи приложения Pipe пользователи соцсети могут передавать друг другу в сообщениях файлы размером до гигабайта.

Бета-тест Pipe стартует уже через несколько дней. Отметим, что передача данных ведется напрямую через P2P-протокол, серверы Facebook при этом не задействуются. Пользоваться сервисом очень просто: достаточно перетащить в окошко нужный файл и выбрать из списка друзей получателя.

«Мы очень упорно работали, чтобы сделать Pipe настолько простым», – утверждает С. Хоссел, создатель приложения. Так как файлы через Pipe передаются напрямую, отправить их можно только если оба пользователя находятся в онлайне. Если один из них не в сети, файлы отправляются в специальное хранилище, размер которого ограничен ста мегабайтами.

Версии для смартфонов у приложения пока что нет. С. Хоссел отметил, что пользователи сначала должны привыкнуть к возможностям Pipe в десктопном варианте, после этого разработчики займутся мобильной версией ***(Pipe для Facebook: брось в друга гигабайтом // InternetUA (http://internetua.com/Pipe-dlya-Facebook--bros-v-druga-gigabaitom). – 2013. – 7.06).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Корпоративная политика 34 % российских компаний запрещает использование соцсетей на рабочем месте, а в 29 % запрещено использовать сервисы микроблогов. Об этом свидетельствует исследование агентства Ipsos, проведенное для компании Microsoft.

Согласно исследованию, проведенному среди почти 10 тыс. сотрудников из 32 стран, в среднем по миру более 30 % компаний ограничивают использование соцсетей на работе, сообщает «Обозреватель» (http://finance.obozrevatel.com/advertising/28743-v-treti-rossijskih-kompanij-sotsseti-dlya-sotrudnikov-zapreschenyi.htm).

Таким образом, российские тенденции в этой сфере совпадают с общемировыми. По словам сотрудников российских компаний, основными причинами ограничения доступа к соцсетям являются риски, связанные с информационной безопасностью, снижением продуктивности работы и потери данных.

В то же время сотрудники часто используют социальные ресурсы для решения деловых задач. Около 40 % респондентов по всему миру считают, что соцсети способствуют более эффективному взаимодействию с коллегами, а 31 % сотрудников готов тратить на рабочее использование этих сервисов собственные деньги. В России семь из 10 специалистов отмечают рост продуктивности работы от использования соцсетей. Однако около 43 % говорят, что в их компаниях преимущества социальных сервисов недооценены.

«Инструменты для создания корпоративных соцсетей позволяют повысить уровень вовлеченности сотрудников в рабочий процесс, что, в частности, сокращает текучку кадров, а также позволяет руководству получать информацию со всех концов организации», – говорит Н. Прянишников, президент Microsoft в России.

Контроль использования соцсетей сотрудниками становится одним из трендов среди работодателей. В прошлом году ряд западных СМИ сообщал о росте числа требований на собеседованиях в США логинов и паролей от Facebook-аккаунтов. Работодатели хотели проверить, какого рода контент соискатель загружает в свой Facebook-аккаунт. Крупные компании, включая Apple, Microsoft, уже увольняли сотрудников за некорректные публикации в социальных онлайн-ресурсах ***(В трети российских компаний соцсети для сотрудников запрещены // Обозреватель (http://finance.obozrevatel.com/advertising/28743-v-treti-rossijskih-kompanij-sotsseti-dlya-sotrudnikov-zapreschenyi.htm). – 2013. – 28.05).***

***

Французская полиция прекратит искать пропавших людей из-за социальных сетей

После Первой мировой войны французская полиция открыла программу «Поиск в интересах семьи», в рамках которой производился поиск потерявшихся родственников с целью объединить семьи, члены которых потерялись. Теперь эта программа закрывается, и виноваты в этом социальные сети.

Как говорят во французской полиции, причина всему то, что современные технологии лучше справляются с этой задачей, чем власти. В XX в. у полиции

были лучшие источники информации во всей стране. Наилучшим местом для поиска данных о человеке были государственные архивы.

Сейчас социальные сети и Интернет вообще позволяют гражданам самим найти любую информацию практически о ком угодно. У современного пользователя сети есть больше возможностей для обнаружения потерянного родственника, чем у всей полиции век назад.

Впрочем, французская полиция не отказывается от поиска пропавших людей вообще. Граждане, находящиеся в опасности – такие, как жертвы преступлений или потерянные дети, подпадают под другую процедуру ***(Французская полиция прекратит искать пропавших людей из-за социальных сетей // InternetUA (http://internetua.com/francuzskaya-policiya-prekratit-iskat-propavshih-luadei-iz-za-socialnih-setei). – 2013. – 28.05).***

***

Тысячи пользователей Интернета выразили протест против сексистских высказываний и изображений, публикуемых в социальной сети Facebook.

Кампания под названием FBrape направлена против позитивного освещения в сети темы сексуального насилия и эксплуатации женщин.

В ее поддержку высказались более 50 тыс. пользователей; около 5 тыс. направили по электронной почте письма в адрес компаний и производителей, которые, как утверждают авторы, публикуют рекламные объявления оскорбительного содержания.

В числе таких компаний называют столь известные как Sky, American Express и Dove.

«Нажать Отдельная онлайн петиция» собрала более 220 тыс. подписей.

Администрация Facebook выпустила специальное заявление, в котором говорится, что компания делает все возможное для скорейшего удаления дискриминационных материалов.

Волна возмущения

Акция протеста организована 40 женскими правозащитными организациями и частными лицами.

В открытом письме, направленном в Facebook, они требуют принятия немедленных и действенных мер против использования темы насилия в этой социальной сети.

В письме приводятся примеры таких злоупотреблений: например, группа в сети Facebook под названием «Вот почему индийских девушек насилуют», а также множество загруженных фотографий, изображающих подвергшихся насилию женщин.

Одна из них изображает женщину, лежащую на полу под лестницей, а подпись гласит: «в другой раз не беременей».

Л. Бэйтс, основатель сайта Everyday Sexism (Повседневный сексизм), участвующего в сборе подписей под сетевой петицией, говорит, что кампания протеста родилась на почве возмущения большого числа женщин, которые жаловались на подобные материалы, а затем связывались с ней.

«Facebook действительно много делает для борьбы с антисемитизмом, например, но когда дело доходит до фотографий насилуемых женщин, ее модераторы просто не считают их проявлениями ненависти, – говорит она. – Многие женщины из-за этого отказываются пользоваться этой сетью».

По ее словам, она согласна с тем, что в социальной сети, подписчиками которой являются полтора миллиарда человек, трудно модерировать все материалы, однако она призывает обратить внимание на эту проблему.

Серьезный подход

Представители компании Dove, под брендом которой выпускается продукция по уходу за лицом и телом, сказали, что очень расстроены в связи с обвинениями в сексизме.

В то же время и Dove, и Facebook утверждают, что все изображения, на которые поступили жалобы, удалены с сайта.

«Dove подходит к этому вопросу очень серьезно и не потворствует деятельности, которая намеренно оскорбляет других людей», – заявил глава отдела по связям с общественностью С. Брайт.

Об этом же в интервью Би-би-си сказал и представитель социальной сети. «На Facebook нет места для разжигания ненависти или сообщений с угрозами или подстрекательством к насилию. Мы не потерпим вредоносных материалов», – говорится в заявлении.

Однако, как говорит представитель соцсети, отнюдь не все материалы, показавшиеся некоторым пользователям «вульгарными и неприятными», на самом деле нарушают политику Facebook ***(Кампанию против сексизма в Facebook поддержали тысячи // InternetUA (http://internetua.com/kampaniua-protiv-seksizma-v-Facebook-podderjali-tisyacsi). – 2013. – 29.05).***

***

Facebook признал, что системы распознавания и удаления оскорбительного контента в социальной сети не выполняют своей задачи.

Признание было опубликовано после того, как на социальную сеть надавили феминистские группы, протестовавшие против страниц в Facebook, где пропагандируется насилие над женщинами… Руководство Facebook заявляет, что пересмотрит свои системы распознавания и удаления оскорбительного контента и тренинга сотрудников, а также установит более тесные связи с активными женскими группами и другими объединениями ***(Facebook признает, что плохо отслеживает оскорбительный контент // Версии.com (http://versii.com/news/279785/). – 2013. – 30.05).***

***

В Казахстане представили проект концепции кадровой политики, касающийся правоохранительных органов, сообщает Tengrinews. Содержание проекта было изложено на круглом столе в Генеральной прокуратуре.

Среди прочего концепция предусматривает «определение нравственных качеств» кандидатов. Для этого предлагается учитывать их поведение в

социальных сетях, а также рекомендации от третьих лиц и другие источники информации. «То есть у нас должна быть цельная картина образа жизни человека», – отметил заместитель генерального прокурора Ж. Асанов.

В концепции также предусмотрено использование полиграфа. Напомним, что парламент Казахстана уже принял поправки в законодательство, которые делают обязательной проверку на детекторе лжи при поступлении на работу в правоохранительные органы.

В 2012 г. в Казахстане была проведена внеочередная аттестация сотрудников правоохранительных органов. Она включала в себя нормативы по боевой и физической подготовке, проверку на знание законодательства Республики, а также тест на логическое мышление и собеседование у психологов.

Всего, как сообщили в конце года в президентской администрации, ее не прошли около 16 тыс. сотрудников. Некоторые из них были рекомендованы к увольнению, другие – к понижению в должности или переводу в другие службы. Среди руководящих работников аттестацию, как отмечалось, не прошел каждый пятый.

В нынешнем году чистка рядов продолжилась. С начала 2013 г., по данным МВД Казахстана, к дисциплинарной ответственности были привлечены 4,3 тыс. сотрудников, должностей при этом лишились 120 полицейских ***(В Казахстане при наборе в полицию учтут поведение в соцсетях // InternetUA (http://internetua.com/v-kazahstane-pri-nabore-v-policiua-ucstut-povedenie-v-socsetyah). – 2013. – 5.06).***

***

Центральное телевидение КНДР открыло страницу с прямым эфиром в своем англоязычном аккаунте в Facebook, пишет «Обозреватель» (http://tech.obozrevatel.com/news/54093-severokorejskoe-tv-zapustilo-onlajn-veschanie-v-facebook.htm).

Вещание ведется не в постоянном режиме. Прямой эфир включается ежедневно в 17:00 по местному времени. По воскресеньям вещание начинается в 9:00.

Страница действует и на территории Южной Кореи, хотя в стране жестко ограничивают доступ к любым пропагандистским материалам со стороны КНДР. Национальное полицейское управление Республики Корея уже обратилось в Комитет по связи страны с просьбой заблокировать страницу Центрального телевидения КНДР на территории страны. В южнокорейском управлении подчеркивают, что на странице содержатся «материалы, противоречащие национальным интересам».

Стоит отметить, что страница Центрального телевидения Северной Кореи была создана в ноябре 2012 г. До недавнего времени на ней публиковались только фильмы, фотографии и новости в текстовом формате. Затем стали доступны некоторые видеовыпуски новостей в записи ***(Северокорейское ТВ запустило онлайн-вещание в Facebook //***

Обозреватель (http://tech.obozrevatel.com/news/54093-severokorejskoe-tv-zapustilo-onlajn-veschanie-v-facebook.htm). – 2013. – 6.06).

***

Премьер-министру Н. Азарову нравится общаться напрямую с читателями своей Facebook-странице.

«Большую роль в получении никем не фильтрованной информации от граждан и журналистов, в частности, играет постоянное общение Премьера в социальной сети Facebook, на страницу которого подписались почти 29,5 тыс. пользователей», – отметили в ведомстве пресс-службы Кабмина. Об этом со ссылкой на «Украинскую правду» пишет Gazeta.ua.

«Глава правительства по пятницам лично общается со своими респондентами», – заверили в ведомстве и добавили, что все обращения граждан, которые приходят на страницу Н. Азарова, «анализируются, по ним принимаются решения». «Н. Азаров неоднократно заявлял о том, что очень ценит это общение, потому что оно позволяет наладить прямой диалог и получить информацию из первых уст», – добавили в Кабмине.

Кроме того, по случаю Дня журналиста в пресс-службе правительства отметили, что «информация, обнародованная в СМИ, является приоритетной в повседневной работе Премьера». «Именно с помощью журналистских материалов и обращений общественности удается оперативно реагировать на ситуацию, решать насущные проблемы. Особенно это касается критических публикаций», – заявили в Кабмине. «Кабинет Министров абсолютно открыт к критике. Объективная критика и достоверные факты становятся основанием для управленческих решений, которые устраняют недостатки или ошибки. Это правило работы действующего правительства», – заверили в ведомстве.

Согласно информации, с начала 2013 г., по поручению Н. Азарова было подготовлено и направлено в редакции СМИ 739 писем-ответов, информационных сообщений и пресс-релизов.

«Все запросы журналистов в порядке Закона “О доступе к публичной информации” были своевременно рассмотрены», – добавили в Кабмине.

Как известно, со страницы Премьера Н. Азарова в Facebook удаляют неприятные вопросы и блокируют авторов, которые их ставят.

Также Н. Азаров оставил за собой право не отвечать на неприятные ему вопросы на собственной странице в Facebook.

Напомним, ранее интернет-издание Новости Украины – From-UA сообщало о том, что главным «врагом прессы», по версии Независимого медиа-профсоюза Украины и Института массовой информации стал Премьер-министр Украины Н. Азаров. Такие результаты антирейтинга «Враги прессы в Украине-2012» организаторы исследования объявили в День журналиста. Второе и третье места в антирейтинге занимают Президент Украины В. Янукович и министр внутренних дел В. Захарченко ***(Стало известно, чем на самом деле занимается Азаров в «Фейсбуке» // From-UA (http://www.from-ua.com/news/7911c143c1966.html). – 2013. – 7.06).***

***

В Севастополе поздно вечером 4 июня от дома в садоводческом товариществе «Пилот» (Казачья бухта, Маяк 1) угнали автомобиль «Ситроен».

Хозяйка машины пропажу обнаружила утром, но, со слов соседки, вечером в 22:40 ее уже не было на месте. Утром вызвали ГАИ, милицию, обнаружили на месте, где была машина, разбитое стекло.

«Мы заявление написали, по Интернету развесили объявление, в течении дня был один звонок днем, что машину в Балаклаве видели. А вечером позвонила девушка, прочитавшая объявление на городском форуме, и сообщила, что машина стоит на улице Подводников, 6», – рассказала 0692.ua хозяйка «Ситроена» Алина.

Снова вызвали милицию, подъехали по указанному адресу, возле машины никого не было, следователи сняли отпечатки. Из машины пропал новый магнитофон, а также запасной ключ. Кроме того, разбито боковое стекло.

«Спасибо севастопольцам, в беде не бросают, очень много было репостов “ВКонтакте”, статьи на всевозможных форумах, объявления распространяли все кто мог, и мои друзья, и друзья жениха. Когда уже забрала машину, ребята какие-то остановили, попросили показать документы, сказали видели объявление о поиске “ВКонтакте” Вот такая история с хэппи эндом», – говорит девушка ***(Севастопольцы в беде не бросят: после «шума» в соцсетях сразу нашли угнанный «Ситроен» // InternetUA (http://internetua.com/sevastopolci-v-bede-ne-brosyat--posle--shuma--v-socsetyah-srazu-nashli-ugnannii--sitroen). – 2013. – 7.06).***

***

Преподаватель Университета Нью-Мексико эволюционный психолог Д. Миллер, написав сообщение в Twitter, поставил под угрозу всю свою академическую карьеру.

На прошлых выходных ученый написал в своем блоге следующее сообщение: «Уважаемые аспиранты, страдающие от ожирения! Если у вас не хватает силы воли перестать употреблять в пищу углеводы, не хватит ее у вас и на то, чтобы написать диссертацию», – сообщает Inopressa.ru.

Сообщение профессора, говорится далее, моментально вызвало бурю недовольства, особенно среди его коллег по научной деятельности и журналистов. Так, издание Wired Magazine вообще провело параллели межу «позорным твитом» Д. Миллера и генетической селекцией, которой занимались нацисты.

Несмотря на то, что Д. Миллер принес извинения за «свой идиотский, импульсивный и основанный исключительно на негативных оценках твит», признался, что «он не отражал его настоящих взглядов, убеждений и ценностей», и скрыл свою страничку в социальной сети, репутация ученого, равно как и его карьера, находятся под угрозой. Руководство университета уже пообещало расследовать инцидент и принять соответствующие меры ***(Профессора могут уволить за шутку в соцсети // InternetUA***

(http://internetua.com/professora-mogut-uvolit-za-shutku-v-socseti). – 2013. – 9.06).

***

Электромобиль, который вместо топлива использует энергию социальных сетей, успешно завершил свое первое путешествие, отъездив 1,5 тыс. км. Он двигался из Канзас-Сити в столицу, Вашингтон.

31 мая группа в составе 17 старшеклассников и восьми наставников покинула Канзас-Сити в Karmann Ghia 1967 г. Машину, которая была в ужасном состоянии, учащиеся отремонтировали и подготовили к поездке сами в рамках развивающей программы Minddrive, которая ориентирована на помощь детям из неблагополучных семей и школьникам, которые склонны постоянно ввязываться в неприятности и нарушать закон.

Самое интересное заключается в том, что детям удалось перенастроить электромотор машины, и та научилась получать «топливо» из весьма необычного источника: социальных сетей. Когда пользователи ставят проекту «лайк» на Facebook, пишут про него или отмечают как понравившееся фото в Instagram, машина получает энергию для движения. За активностью в социальных сетях следит устройство на базе Arduino.

Авторы проекта провели немало бессонных ночей, пытаясь придумать, как «выжать» энергию из социальных СМИ. Когда решение было найдено, команда определила, что будет приносить то или иное количество энергии. Так, новый фолловер в Twitter дает 5 Вт, лайк на Facebook – 1 Вт. Подпись онлайн-петиций дарит сразу 10 Вт, а ретвит или упоминание на Twitter – 3 Вт.

К счастью, поездка прошла успешно, хотя участники и признались, что порядком устали за время путешествия. В Вашингтоне их встретили, как героев. Надеемся, Minddrive поможет этим детям обрести уверенность в своих силах и пойти по верной дороге в своем будущем ***(Первое путешествие машины, работающей на сообщениях из соцсетей, прошло успешно // InternetUA (http://internetua.com/pervoe-puteshestvie-mashini--rabotauasxei-na-soobsxeniyah-iz-socsetei--proshlo-uspeshno). – 2013. – 8.06).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Как сообщает блог Inside Facebook, на днях стало известно о том, что рекламодатели соцсети вскоре получат возможность таргетировать кампании на пользователей, исходя из их текущей активности как на сайте социальной сети, так и в мобильном приложении.

Специальная функция Action specs позволяет создавать описания интеракций пользователей с объектами Open Graph, которые осуществлялись посредством мобильных приложений или веб-приложения социальной сети. Таким образом, Action Specs может быть использована в целях таргетинга объявлений как на пользователя, совершившего определённые действия в Facebook, так и на его друзей. К примеру, можно ориентировать свою

кампанию на группу пользователей, которые недавно прослушали в соцсети новую музыкальную композицию, прокомментировали тот или иной пост, играли в онлайн-игру.

Важно отметить, что новая функция не предоставляет возможность таргетинга, связанную с использованием людьми кнопки Like.

Рекламодатель может отслеживать активность пользователей за 14 прошедших дней. При желании этот интервал можно сократить: к примеру, задать интервал отслеживания действий пользователей за последние три дня.

В настоящее время функционал проходит стадию бета-тестирования ***(Рекламу на Facebook можно таргетировать на основе недавних действий пользователей // Marketing Media Review (http://mmr.ua/news/id/reklamu-na-facebook-mozhno-targetirovat-na-osnove-nedavnih-dejstvij-polzovatelej-34802/). – 2013. – 27.05).***

***

Министерство доходов приглашает пользователей Facebook присоединиться к обсуждению инвестиционного климата, передает корреспондент proIT со ссылкой на пресс-службу Миндоходов.

В социальной сети Facebook открыта специальная страница для формирования повестки дня панельной дискуссии Doing Business in Ukraine, которая состоится 13 июня 2013 г. в рамках Международной бизнес конференции ABC: Ukraine & Partners-2013.

Конференция будет проводиться по инициативе Премьер-министра Украины Н. Азарова 13–15 июня 2013 г. в Киеве. Целью мероприятия является дальнейшее развитие диалога между властью и бизнесом, объединение усилий для поиска путей взаимоприемлемого сотрудничества и преодоления путей негативного влияния глобального экономического кризиса.

Во время дискуссии Doing Business in Ukraine, которой начнется конференция, топ-менеджеры ведущих украинских и иностранных компаний, руководители бизнес-ассоциаций, ведущие украинские и международные эксперты обсудят пути повышения инвестиционной привлекательности Украины. К дискуссии также присоединится министр доходов и сборов Украины А. Клименко.

Пользователи сети Facebook могут уже сегодня задать участникам вопросы для обсуждения, а также высказать свое видение предмета дискуссии.

Как сообщает пресс-служба, наиболее интересные посты и вопросы будут озвучены во время дискуссии. Кроме этого, именно на Facebook-странице накануне и во время мероприятия будут представлены эксклюзивные материалы и комментарии участников и гостей мероприятия.

Уже сегодня пользователи соцсети задают международным экспертам многозначительные вопросы: «Презираете ли вы тех, кто не платит налоги? И если да, как вы тогда общаетесь с украинскими миллиардерами?» ***(Инвестиционный климат Украины обсуждают на Facebook // proIT (http://proit.com.ua/news/internet/2013/05/30/110311.html). – 2013. – 30.05).***

***

Facebook усилит надзор за пользователями из-за ухода рекламодателей

Крупнейшая социальная сеть мира Facebook отреагировала на претензии нескольких крупных рекламодателей, недовольных размещением своей контекстной рекламы по соседству с женоненавистническими постами и с фотографиями женщин, подвергшихся насилию. В последние дни «стало очевидно, что наша система отслеживания и удаления расистской и порочащей информации недостаточно эффективна», заявила соцсеть Facebook и пообещала «немедленно» усовершенствовать подготовку модераторов: реакция на нарушения стандартов общения в соцсети станет более быстрой. Об этом пишут «Ведомости».

Несколько рекламодателей, включая автоконцерн Nissan и крупнейший интернет-банк Великобритании Nationwide, свернули рекламные кампании на Facebook. Причиной стали рекламные баннеры, размещенные рядом с постами сомнительного содержания. Скриншоты подобных страниц появились на сайтах защитников прав женщин и быстро распространились в Twitter вместе с призывом добиться от компаний отзыва рекламы. Опрошенные Financial Times рекламодатели сомневаются, что ужесточение цензуры принесет достаточный эффект: по их мнению, Facebook стоило бы найти технический способ исключить появление рекламы на страницах с оскорбительным содержанием.

В I квартале 2013 г. выручка Facebook возросла на 38 % к уровню годичной давности (до 1,46 млрд дол.), в том числе основная статья доходов – заработки от размещения рекламы – на 43 % (до 1,25 млрд дол.).

На рынке контекстной рекламы, тематически привязанной к запросам пользователя, случаи отказа рекламодателя от сотрудничества с интернет-площадкой по причине размещенного на ней нежелательного контента крайне редки, говорит гендиректор рекламного агентства iContext М. Черницкая. В случае с медийной рекламой проблемы несовместимости могут возникать, признает гендиректор AdWatch А. Чернышов, но существует отлаженная технология их решения: система управления рекламой может заранее отсеять страницы, на которых баннер появляться не должен ***(Facebook усилит надзор за пользователями из-за ухода рекламодателей // IT Expert (http://itexpert.in.ua/rubrikator/item/26595-facebook-usilit-nadzor-za-polzovatelyami-iz-za-ukhoda-reklamodatelej.html). – 2013. – 30.05).***

***

Генеральный директор Twitter Д. Костоло говорит, что телевизионные компании – это ценные партнеры для сервиса микроблогов, и Twitter намерена инвестировать в них соответствующим образом.

«Twitter – это социальное дополнение телевидения. Мы приняли решение активно инвестировать в эту область. Есть несколько областей, в которых мы можем успешно сотрудничать с вещательными компаниями», – сказал Д. Костоло на конференции AllThingsD в Калифорнии.

Напомним, что ранее Twitter заявила, что намерена к 2014 г. довести свою выручку до 1 млрд дол. В рамках реализации этой программы компания уже добавила поддержку видео, а в начале мая сообщила о начале партнерства с НБА и медиа-компаниями ESPN и Walt Disney.

Одновременно с этим сервис микроблогов сообщил о намерении инвестировать в развитие систем безопасности для пользователей. Напомним, что за последние пару недель Twitter стал объектом критики после того, как хакеры один за одним взламывали Twitter-ленты ряда резонансных пользователей, в частности таких как Associated Press, Sky News и др. На прошлой неделе компания реализовала систему двухфакторной аутентификации, однако и она уже успела собрать порцию критики.

«Пока в сфере безопасности мы не движемся так быстро, как это необходимо и как нам самим того хотелось бы», – признался он. Кроме того, Д. Костоло еще раз заметил, что первичное размещение акций Twitter пока отошло на второй план и не является основным приоритетом для организации. «Сейчас мы стараемся сделать хороший и полезный сервис, работая на рынке, а размещение акций на данный момент не значится в числе наших первейших приоритетов», – говорит он.

Напомним, что на сегодня аналитики оценивают капитализацию Twitter примерно в 10 млрд дол. ***(Twitter намерена инвестировать в телевизионные компании // Marketing Media Review (http://mmr.ua/news/id/twitter-namerena-investirovat-v-televizionnye-kompanii-34847/). – 2013. – 30.05).***

***

Количество твитов о финансовых «пузырях» выросло в 170 раз за полгода

Число сообщений со словом bubble (англ. – пузырь) в социальной сети Twitter увеличилось со 168 до 29,6 тыс. за последние шесть месяцев. Об этом твиттер-аналитик и предприниматель П. Хоутин написал в своей статье для MarketWatch.

По его словам, такой рост может свидетельствовать об обеспокоенности пользователей относительно перегрева фондового рынка. Вместе с тем определенная часть твитов – просто перепечатка сообщений из СМИ, которые активно тиражируют слухи о надувании «пузыря».

П. Хоутин известен как основатель первого в мире и пока единственного хедж-фонда, в котором планировалось принимать инвестиционные решения на основе анализа сообщений в Twitter. Предприниматель основал фонд Derwent Capital Markets объемом в 40 млн дол., однако идея не нашла поддержки у инвесторов, и компания закрылась через месяц, не обеспечив необходимый приток финансов.

П. Хоутин написал в своей статье для MarketWatch, что решил проанализировать количество твитов о финансовых «пузырях» в связи с тем, что в последние месяцы появилось много слухов на эту тему.

Инвесторы подозревают, что американский рынок акций «перегрелся», так как индексы в первой половине этого года достигли многолетних

максимумов. В частности, в начале февраля Dow Jones впервые с 2007 г. превысил 14 тыс. пунктов, а индикатор S&P 500 преодолел пятилетний максимум в конце марта.

Аналитики используют для сбора информации не только социальные сети. В конце апреля Т. Прейс, Х. Моат, Ю. Стенли опубликовали статью, в которой связали количество поисковых запросов в Google с экономическими ожиданиями пользователей сети.

Ученые выяснили, что рост запросов на экономическую тематику свидетельствует об обеспокоенности пользователей относительно состояния экономики, а значит, в скором времени индексы будут падать. Соответственно, считают авторы статьи, снижение количества таких запросов свидетельствует о том, что в ближайшее время фондовые индексы будут расти ***(Количество твитов о финансовых «пузырях» выросло в 170 раз за полгода // InternetUA (http://internetua.com/kolicsestvo-tvitov-o-finansovih--puziryah--viroslo-v-170-raz-za-polgoda). – 2013. – 31.05).***

***

После нескольких месяцев переговоров социальная сеть Facebook отказалась от покупки израильского стартапа Waze, сообщает All Things Digital со ссылкой на осведомленные источники.

Ранее сообщалось, что Facebook была готова предложить за Waze 1 млрд дол.

По информации источников, сторонам не удалось договориться по некоторым пунктам. Яблоком раздора также стало то, что команда Waze отказалась переезжать в штаб-квартиру Facebook в Калифорнии.

Помимо Facebook, в переговорах о покупке Waze участвует Google ***(Facebook отказалась от покупки Waze // InternetUA (http://internetua.com/Facebook-otkazalas-ot-pokupki-Waze). – 2013. – 31.05).***

***

Разработчик и поставщик игр для соцсети Facebook объявил об увольнении 18 % сотрудников, сообщает Обозреватель со ссылкой на официальный блог компании (http://tech.obozrevatel.com/news/36180-razrabotchik-igr-dlya-facebook-uvolnyaet-poltyisyachi-sotrudnikov.htm).

Без работы останутся 520 человек. Увольнения произойдут во всех подразделениях компании. По словам гендиректора Zynga М. Пинкуса, они необходимы для дальнейшего развития компании.

Директор поблагодарил всех уволенных сотрудников за хорошую работу и пообещал щедрое выходное пособие ***(Разработчик игр для Facebook увольняет полтысячи сотрудников // Обозреватель (http://tech.obozrevatel.com/news/36180-razrabotchik-igr-dlya-facebook-uvolnyaet-poltyisyachi-sotrudnikov.htm). – 2013. – 4.06).***

***

В Google говорят, что мобильные продажи рекламы на YouTube за последние полгода утроились и достигли уровня в 350 млн дол. В компании говорят, что для YouTube этот показатель является рекордным и примерно четверть из того 1 млрд человек аудитории, что пользуются YouTube, заходят на сайт с мобильных устройств. Об этом сообщает CyberSecurity.ru.

Л. Уотсон, вице-президент по продажам YouTube, говорит, что объемы мобильного рекламного продвижения растут одновременно с объемами мобильного трафика и аудитории. Независимые аналитики говорят, что Google практически никогда не раскрывает данные по финансам, касающимся YouTube, однако предоставленные сейчас цифры говорят, что YouTube не только по трафику обходит платных конкурентов, таких как Hulu, но и отнимает у них заметный кусок рекламных бюджетов.

В компании EMarketer говорят, что в США к 2017 г. мобильные продажи видеорекламы достигнут 2,69 млрд дол., что почти в 10 раз больше, чем в 2012 г. «Коммерческая мобильная реклама входит в стадию активного мобильного роста. Это большая часть нашего бизнеса», – говорит Л. Уотсон.

По оценкам Wedge Partners, на сегодняшний день портал YouTube генерирует около 10 % общей выручки компании. С учетом, что в прошлом квартале выручка компании составила 14 млрд дол., можно говорить о том, что квартальная рекламная выручка YouTube составляет 1,1–1,4 млрд дол., из которых 350 млн дол. приходятся на мобильные показы рекламы.

Согласно данным Nielsen Holdings, в марте этого года примерно половина американской аудитории YouTube или примерно 70 млн человек работали с YouTube через мобильные устройства – это на 42 % больше, чем годом ранее ***(YouTube неожиданно утроила продажи мобильной рекламы за полгода // IT Expert (http://itexpert.in.ua/rubrikator/item/26780-youtube-neozhidanno-utroila-prodazhi-mobilnoj-reklamy-za-polgoda.html). – 2013. – 6.06).***

***

Создатель Microsoft Б. Гейтс вложил 35 млн дол. в стартап ResearchGate – социальную платформу для общей работы над научными исследованиями. Проект представляет собой определенный хаб для ученых, позволяя исследователям презентовать свои работы широкой общественности и формировать вокруг них группы для дальнейших исследований в сфере.

Отметим, что социальная платформа ResearchGate была запущена в 2008 г. по инициативе бывшего ученого-медика, а ныне бизнесмена И. Мадиша. Доктор медицины, который разочаровался в привычных формах общения между учеными в ходе подготовки диссертаций, запустил в Интернете социальный ресурс, позволяющий ученым трудиться над своими темами подобно тому, как программисты работают над открытым ПО.

Веб-платформа, организованная И. Мадишем, дает исследователям возможность публиковать в открытом доступе как готовые публикации, так и «сырые» данные тестов, которые нуждаются в анализе и обработке. Социальные функции ResearchGate дают исследователям возможность вести

научные дебаты, а также находить коллег, занятых в той же сфере, и объединяться в группы для общей работы. Подход ResearchGate, таким образом, почти полностью аналогичен модели разработки софтверных проектов.

«Мы хотим быть лидерами в открытой науке по аналогии с открытым программным обеспечением», – хвалит И. Мадиш свой стартап. По мнению И. Мадиша, целью проекта является как минимум стремление «изменить само представление ученых о процессе исследования».

По мнению бизнесмена, консервативный подход старшего поколения ученых поменять достаточно непросто, тем не менее, проект находит все больше и больше признания у молодых исследователей, которые зарабатывают авторитет в своих областях и интересуются инновационными подходами, заверяет создатель проекта. Сейчас на сайте уже более 2,9 млн пользователей, среди которых больше всего ученых в области биологии, медицины, IT, физики и истории.

Сообщается, что идеалистический фокус проекта понравился многим инвесторам – среди которых, в частности, основатель Microsoft Б. Гейтс, который знаменит своим интересом к благотворительности, связался с организатором ResearchGate, после чего лично прибыл во Францию для переговоров об инвестициях. В результате проекту досталось 35 млн дол. из персонального капитала создателя IT-гиганта ***(Билл Гейтс вложит миллионы долларов в соцсеть для ученых // Минфин (http://minfin.com.ua/2013/06/06/768028/). – 2013. – 6.06).***

***

Маркетологи, планирующие продвигать проекты в социальных сетях, сталкиваются с необходимостью выбора площадки, аудиторию которой они будут покорять. Практически все популярные сети, включая Facebook, Twitter, LinkedIn, Google+ и YouTube, предоставляют специалистам уникальные возможности для раскрутки бизнеса. Однако большинство B2B-маркетологов работает в условиях ограниченного бюджета. Это заставляет их фокусироваться на одной-двух площадках, реализуя маркетинговые кампании.

В этой статье вы найдете сравнение наиболее популярных социальных сетей в контексте возможности их использования для маркетинга проектов в сегменте «бизнес для бизнеса».

Ключи к победе в социальном B2B-маркетинге

Организации, работающие в сегменте B2B, используют социальные сети для повышения узнаваемости бренда, привлечения аудитории и генерации лидов. Они должны превратить свои страницы, паблики и группы в источник авторитетной и релевантной информации, чтобы обеспечить успех маркетинговой кампании. Чтобы сделать это, бизнес должен разработать качественный медиаплан.

Выбор конкретного информационного канала – первый шаг медиапланирования. Выбирая социальную сеть для проведения маркетинговых кампаний, ориентируйтесь на следующие критерии:

1. Разбивка аудитории площадки по демографическим, социальным и другим признакам.

2. Популярность социальной сети среди представителей целевой аудитории вашего проекта.

3. Типы контента, предпочитаемые аудиторией площадки и вашего бизнеса.

4. Цели социальной сети (например, цель LinkedIn – развитие профессиональных контактов, а сеть «ВКонтакте» изначально задумывалась в качестве площадки для общения выпускников вузов).

5. Тон общения в социальной сети.

6. Уровень вовлеченности аудитории.

7. Наличие инструментов, которые можно использовать для реализации B2B-маркетинга.

Кроме этого, учитывайте региональные особенности, выбирая социальную площадку для проведения маркетинговой кампании. Например, популярный на Западе LinkedIn только завоевывает свою аудиторию в Рунете, что нельзя игнорировать при планировании бюджета на раскрутку.

Google+ – новые перспективы SMM в сегменте B2B

Google+ на наших глазах превращается в новую большую социальную сеть для бизнеса. Активная аудитория площадки составляла 350 млн пользователей в марте 2013 г. По этому показателю Google+ опережает LinkedIn, Twitter, Pinterest и YouTube.

Публикуя контент или ссылки в Google+, вы прямо влияете на его позиции в поисковой выдаче. В первую очередь, это возможно благодаря отображению публикуемых материалов на странице персональной выдачи пользователей поисковой системы Google, находящихся в ваших кругах Google+. Кроме этого, Google+ поддерживает публикацию разных типов контента, включая онлайн-видео (помните, YouTube принадлежит Google).

Публикация анонсов контента вашего канала YouTube в Google+ – хорошая идея. Ссылки с Google+ влияют на поисковую выдачу, поэтому вы увеличиваете эффективность контент-маркетинга, анонсируя видео в социальной сети, принадлежащей крупнейшему «поисковику» в мире.

Социальные сигналы, включая ссылки, лайки, репосты, комментарии и т. п., являются золотыми самородками для контент-маркетологов. Это связано со стремлением поисковых систем достоверно определять популярность и ценность контента.

Google+ позволяет создавать бизнес-страницы брендов. Пользователи могут подписываться на них и взаимодействовать с проектами на персональном уровне. В свою очередь, бренды получают возможность использовать это взаимодействие для выстраивания отношений с аудиторией. А B2B-продажи – это ни что иное, как выстраивание отношений.

Сервис «ВидеоВстречи» – еще один подарок Google+ B2B-маркетологам. Этот инструмент позволяет моментально организовать видеоконференцию. Боле того, вы можете опубликовать запись конференции в Google+ после ее завершения.

Массовое использование Google+ для тиражирования развлекательного контента является негативной стороной использования этой площадки для реализации B2B-маркетинговых кампаний. Многие пользователи этой сети игнорируют деловые сообщения, что уменьшает ее ценность с точки зрения маркетинга.

Кроме этого, бизнесмены все еще не воспринимают Google+ в качестве серьезного маркетингового инструмента. Создателям сети придется инвестировать дополнительные ресурсы в ее развитие и позиционирование в качестве бизнес-ресурса.

LinkedIn – возможности для профессионалов

Социальная сеть для профессионалов LinkedIn относится к наиболее удобным площадкам для реализации маркетинговых кампаний. Здесь вы можете быстро найти потенциальных клиентов в сегменте B2B, так как данный ресурс разрабатывался для делового общения. Аудитория LinkedIn составляет 225 млн пользователей по состоянию на март 2013 г.

Главными возможностями использования данной сети в качестве маркетингового инструмента являются персональный брендинг топ-менеджеров, привлечение новых потребителей в ходе личного общения и таргетированная реклама. Ежедневное взаимодействие с коллегами и партнерами и коммуникация в тематических группах относятся к ключевым факторам успеха маркетинга в LinkedIn.

Точное таргетирование является одним из основных преимуществ рекламы в социальной сети для профессионалов. Публикуя объявления, вы можете определять целевую аудиторию по географическому признаку, принадлежности к конкретной отрасли, демографическим и профессиональным критериям. А инструмент Lead Collection, представляющий собой расширение для сайта, позволяет реагировать на генерированные лиды в режиме реального времени.

Используя LinkedIn, компания может развивать персональные отношения с потребителями и партнерами. Для этого бизнес-проект должен публиковать интересный и полезный контент, стимулирующий аудиторию подписываться на обновления страницы. Общение в тематических группах также относится к мощному инструменту маркетинга в LinkedIn.

Социальная сеть предоставляет бизнесу платные инструменты стимулирования продаж. Lead Builder является одним из них. Он дает возможность специалистам по продажам выполнять следующие действия:

1. Создавать и сохранять списки потенциальных клиентов.
2. Находить пользователей LinkedIn, соответствующих заданным критериям.

3. Объединять потенциальных клиентов в группы по выбранным признакам, используя инструмент Profile Organizer.

Сеть LinkedIn позволяет B2B-маркетологу получить важную информацию о потенциальном клиенте. Кроме этого, ресурс дает возможность легко устанавливать контакт с выбранным пользователем, избегая неэффективных «холодных» продаж.

Наличие множества бесполезных и отвлекающих функций относится к негативным характеристикам LinkedIn в качестве маркетингового инструмента. Также данная сеть не входит в число наиболее популярных в Рунете площадок. Численность русскоязычной аудитории LinkedIn составила 752 тыс. человек в апреле 2013 г.

Twitter – общение для занятых бизнесменов

Сервис микроблогинга Twitter – самый простой способ быстро сообщить миру важную новость для всегда спешащих бизнесменов. Эта сеть позволяет пользователям общаться с помощью коротких сообщений и ссылаться на важные веб-страницы.

Twitter – удобный инструмент для B2B-маркетологов. В частности, вы можете находить здесь потенциальных потребителей и группировать их в приватные списки. Отслеживая сообщения пользователей, вы узнаете об их интересах и предпочтениях. Это первый шаг к эффективному взаимодействию с будущим партнером.

Успех B2B-маркетинга в Интернете зависит от трех ключевых факторов – онлайн-репутации, способности влиять на аудиторию с помощью идей и узнаваемости бренда. Twitter можно использовать для развития каждого из компонентов успеха.

Следующие характеристики сервиса микроблоггинга позволяют рассматривать его в качестве эффективного инструмента маркетинга:

Горячие новости часто появляются именно в Twitter.

Пользователи Twitter часто общаются друг с другом в режиме реального времени, что превращает этот сервис в онлайн-чат с расширенной функциональностью.

Используя приложение Twitter для смартфона, вы можете вести прямой репортаж с места любых событий.

Событийный маркетинг относится к наиболее эффективным инструментам продаж в сегменте «бизнес для бизнеса». Поисковый алгоритм Twitter и использование хэштегов позволяет организаторам мероприятий быстро распространять информацию о конференциях, воркшопах, семинарах и других событиях.

Twitter не принадлежит Google, что относится к его негативным характеристикам. Это значит, что ссылка на контент, опубликованная в Twitter, в большинстве случаев будет ранжироваться ниже аналогичной публикации в Google+. Кроме этого, пользователи Twitter чаще игнорируют сообщения по сравнению с аудиторией других сетей. Вы можете легко найти здесь потенциальных клиентов, но это не значит, что они будут взаимодействовать с

вами. Наконец, многие пользователи считают сервис микроблоггинга заспамленным бесполезными ссылками, поэтому не воспринимают его всерьез.

YouTube – важнейший инструмент B2B-маркетинга

Онлайн-видео является одним из наиболее эффективных инструментов контент-маркетинга. В свою очередь, YouTube, принадлежащий Google, – лучшая площадка для публикации видеоконтента в рамках B2B-маркетинговых кампаний. Описание одного из успешных примеров использования видео для привлечения клиентов в сегменте «бизнес для бизнеса» вы найдете здесь. Качественные ролики, публикуемые на данном ресурсе, привлекают аудиторию и генерируют лиды.

Обратите внимание, под качественным видео в данном контексте следует понимать интересные, запоминающиеся, полезные для аудитории материалы. Мы писали, что создателям маркетингового видео не следует состязаться с Голливудом в масштабности спецэффектов.

Основное полезное качество YouTube в качестве маркетингового инструмента – возможность встраивать видео с этого сервиса на любые сайты и блоги. Данную социальную сеть не стоит рассматривать в качестве полноценной самостоятельной площадки для реализации маркетинговых кампаний. Сложно представить, как можно устанавливать отношения с целевой аудиторией, используя ее. Гораздо эффективнее транслировать свой канал на корпоративном ресурсе, повышая узнаваемость бренда и привлекая аудиторию полезными материалами.

Facebook – тяжеловес B2B-маркетинга

Самая крупная социальная сеть в мире бесспорно является лучшей площадкой для маркетинга в сегменте «бизнес для клиента». Однако ее можно использовать и в качестве площадки для B2B-кампаний.

Бизнес-страницы и тематический группы – главный инструмент B2B-маркетинга на Facebook. Кроме этого, владельцы бизнес-страниц имеют доступ к удобным инструментам Email-маркетинга, позволяющим осуществлять рассылку подписчикам или членам групп.

Развитие отношений с бизнес-партнерами и прямые B2B-продажи можно осуществлять с помощью Facebook. Однако это является трудновыполнимой задачей.

Итак, лучшей социальной сетью для B2B-маркетинга признается...

…LinkedIn. Эта сеть является единственной, позволяющей эффективно и целенаправленно развивать отношения между организациями и осуществлять B2B-продажи. Смело считайте LinkedIn главной маркетинговой площадкой, если ваш рынок не ограничивается постсоветским пространством.

Главная профессиональная социальная сеть мира пока только борется за русскоязычного пользователя. Поэтому обратите внимание на площадку для B2B-маркетинга № 2, если ваши потребители преимущественно разговаривают на русском языке. А второе место в нашем обзоре поделили между собой Google+, Facebook, Twitter и YouTube.

Продвинутые B2B-маркетологи должны работать с каждой из этих площадок, продвигая проекты. Но если вы постоянно работаете в условиях нехватки времени, сфокусируйтесь на общении в одной-двух сетях ***(Какая социальная сеть лучше подходит для B2B-маркетинга // Sostav.ua (http://sostav.ua/publication/kakaya-sotsialnaya-set-luchshe-podkhodit-dlya-b2b-marketinga-54823.html). – 2013. – 28.05).***

***

Руководство крупнейшей в мире социальной сети Facebook приняло решение сократить количество рекламных инструментов с 27 до 6. Об этом стало известно на специальном мероприятии для рекламодателей, которое состоялось накануне, сообщает пресс-служба Facebook.

Компания осознала сложность собственных рекламных инструментов и решила значительно упростить их. Новые инструменты будут внедрятся постепенно на протяжении шести последующих месяцев.

Согласно сообщению, Facebook предложит рекламодателям комплексные решения, которые будут решать определенные задачи: увеличивать аудиторию реальных покупателей, увеличивать количество загрузок приложения или повышать онлайн-конверсию.

В частности, соцсеть приняла решение удалить формат «Вопрос», ведь маркетологи могут задать вопрос в посте и получить ответ на него в комментариях.

Кроме того, удалены будут онлайн-предложения, поскольку опыт рекламодателей показал, что гиперссылка в посте работает намного лучше. Также будет изменен сам формат рекламного сообщения ***(Facebook запускает новую рекламную стратегию // Минфин (http://minfin.com.ua/2013/06/07/768527/). – 2013. – 7.06).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Подростки устали от Facebook, они не могут расслабиться в нем

Казалось бы, социальная сеть Facebook должна импонировать молодому поколению. Однако недавнее исследование свидетельствует о том, что подростки не могут расслабиться в ней и рассматривают её как продолжение школы и дома.

Подростки не могут быть собой в Facebook. И причина вовсе не в том, что родители могут увидеть их фотографии, которые они предпочли бы скрыть, а от «необходимости» лайкать посты друзей, обсуждать картинки в профиле и т. п.

Согласно опросу, хотя 77 % из всех подростков в онлайне имеют свой аккаунт в Facebook, они не спешат делиться со всеми своими печалями и радостями. Почти половина респондентов стирали свои посты или чужие комментарии и удаляли отметки себя с фото. Три четверти удаляли людей из друзей и 58 % блокировали какого-либо пользователя. Как пишут в исследовании, «хотя некоторым респондентам из фокусной группы нравится использовать Facebook, намного большее число подростков ассоциировало соцсеть с присутствием взрослых, давлением со стороны других, негативными социальными взаимодействия, или им мешает то, что другие делятся слишком большим объёмом информации».

Впрочем, тинейджеры вовсе не против, что их информацию получают сторонние компании. Только 9 % опрошенных были «очень обеспокоены» этим фактом. С другой стороны, среди их родителей этот показатель составляет 81 %. Это означает только одно: подростки не понимают, что происходит с их данными.

В этой ситуации, когда Facebook воспринимается подростками как продолжение школы и дома, всё больше молодых людей стараются завести аккаунты на других сервисах. Например, уже 24 % тинейджеров имеют свой аккаунт на Twitter (год назад было 16 %) ***(Подростки устали от Facebook, они не могут расслабиться в нем // UAInfo (http://uainfo.org/heading/public/144223-podrostki-ustali-ot-feysbuka-oni-ne-mogut-rasslabitsya-v-nem.html). – 2013. – 25.05).***

***

Новое исследование, результаты которого должны быть опубликованы в июньском выпуске Journal of Media Psychology, показывает, что пользователи Facebook могут значительно повысить чувство собственного достоинства, проведя пять минут на своей страничке в соцсети.

«У большинства пользователей широкая аудитория друзей и они могут выборочно демонстрировать “лучшую версию себя”, но делать это старательно», – рассказала ABC News доцент К. Тома, которая возглавляла данное исследование Университета Висконсин-Мадисон.

«Facebook дает вам очень хороший образ самого себя и после этого вам не нужно искать его в другом месте», – добавляет она. Таким образом мотивация человека преподнести себя хорошо уже в какой-то мере удовлетворена, и он чувствует себя лучше, снизив эту потребность, говорится в статье, которая называется «Самоутверждение лежит в основе использования Facebook».

Как уточняется, испытуемых исследовали с помощью теста неявных ассоциаций (Implicit Association Test), позволяющего узнать скрытые мотивы, которые могут быть недоступны на сознательном уровне. После того как пользователи побывали всего в течение пяти минут на своей странице в Facebook, их самоописания в тесте становились более положительными, по

сравнению с теми, кто на Facebook не заходил. Правда, как долго держится такой эффект – неясно.

Также в ходе исследования было зафиксировано, что пользователи соцсети заходят в свои аккаунты для восстановления самооценки, когда их эго был нанесен какой-то урон.

В Корнелльском университете был проведен еще один эксперимент. Там испытуемых студентов попросили произнести речи. Затем части из них разрешили бегло зайти к себе в профиль на Facebook. Когда после этого им дали негативные отклики на их выступления, те студенты, которые заглянули в соцсеть, восприняли критику проще.

В то же время, в 2012 г. исследование Университета Западного Иллинойса показало, что эксгибиционизм в Facebook может наоборот негативно сказаться на самооценке. К похожим выводам пришли швейцарские исследователи, обнаружившие, что у людей, подолгу пребывающих в соцсети, самооценка не на высоте ***(Ученые предложили лечить низкую самооценку пребыванием в Facebook // Версии.com (http://www.versii.com.ua/news/280120/). – 2013. – 4.06).***

***

Ученые из Вашингтонского университета выяснили, что залогом победы в споре являются громкий крик и излучение уверенности в своей правоте и себе. Это действует даже в том случае, когда человек не прав.

Исследователи сделали такой вывод, проанализировав активность пользователей сети Twitter. Чем больше человек самоуверен, тем более надежным и влиятельным он выглядит.

Специалисты изучили более миллиарда твиттов, которые были опубликованы во время проведения различных спортивных мероприятий, например, чемпионата Америки по футболу – Суперкубка–2013.

Выяснилось, что те люди, которые громче остальных заявляют о себе в Интернете, считаются более влиятельными и надежными. У них больше последователей. Чтобы доказать эту теорию, два студента экономического университета изучили язык, на котором говорят спортивные эксперты, часто кричащие для привлечения внимания.

Они сравнили сообщения профессионалов и твитты простых любителей спорта. Позже студенты создали программу, чтобы проанализировать более миллиарда сообщения. Во внимание принимались слова «победа» и созвучные с ним.

В 47 % случаях эксперты были правы в своих предсказания. Причем, у любителей этот показатель составляет 45 %. Но тем менее, рейтинг доверия у профессионалов равнялся 0,480, в то время как у любителей он был равен 0,313 ***(Излучение уверенности в себе и громкий крик – залог успеха в споре // NovostiUA (http://novostiua.net/obschestvo/38383-izluchenie-uverennosti-v-sebe-i-gromkiy-krik-zalog-uspeha-v-spore.html). – 2013. – 3.06).***

***

Коммуникационная группа уверена, что пора вернуться от цифры к человеческому общению

«Эра диджитал окончена. Люди мечтают избавиться от цифровой зависимости и вернуться к живому общению», – такое сенсационное заявление сделал М. МакКейб, директор по стратегии компании Leo Burnett North America. Выступление состоялось в ходе ежегодного мероприятия Investors Day, организованного Publicis Groupe и посвященного самым последним трендам на рынке коммуникаций.

В своем выступлении М. МакКейб рассказал о том, что уклон на диджитал – кампании и кампании в соцсетях исчерпал себя. Люди все чаще признаются, что страдают симптомами цифровой зависимости и это мешает спокойно жить, вызывает раздражение и проблемы в реальной жизни.

Основанием для такого утверждения стали результаты глобального исследования аудитории в возрасте 16–50 лет, проведенного Leo Burnett Worldwide в нескольких странах и нацеленного на изучение влияния Интернета, социальных сетей и всевозможных гаджетов на жизнь людей.

В целом результаты говорят о том, что во всех странах растет количество «отказников» Интернета, снижается время, проводимое в социальных сетях.

Почти 20 % опрошенных заявили, что все чаще и чаще задумываются закрыть свой аккаунт в социальных сетях. 35 % отметили, что стараются раз в месяц устраивать для себя день без Facebook и Twitter.

Во время отпуска стали реже использовать Интернет почти 40 % респондентов, а 22,8 % сказали, что порой им кажется, что писать смс и комменты в соцсетях для них стало проще, чем говорить с человеком вживую.

Помимо собственного исследования, в своем выступлении М. МакКейб сослался на статью «Иметь аккаунт в Facebook уже не круто: компания теряет тинейджеров», опубликованную в популярном техноблоге The Verge. В ней приводятся данные о том, что Facebook стремительно теряет популярность среди молодежи.

Также он ссылался на данные годового отчета Facebook, в котором потеря интереса молодежной аудитории названа риском номер один: «Возможно наши усилия по увеличению количества пользователей платформы Facebook и взаимодействию с ними не столь успешны».

«Все это говорит о том, что повальный тренд на создание диджитал кампаний и продвижение в социальных сетях исчерпал себя. Бренды, которые действительно хотят быть HumanKind брендами, должны поддерживать желание людей общаться вживую, должны радовать их новым опытом, знаниями в реальной жизни, а не через экран монитора или смартфона. Количество людей, которые хотят пойти в ванную или в туалет без смартфона растет. Разве это не повод задуматься?», – заявил М. МакКейб.

В качестве подтверждения инсайта о том, что не все в жизни можно обеспечить с помощью диджитал, эксперт привел уже хорошо известную кампанию Emma! Leo Burnett Paris. Также М. МакКейб рассказал об

уникальном эксперименте, в котором поучаствовали главы стратегических департаментов Leo Burnett со всего мира.

«Мы испробовали это сами на себе. Мы отправились на Бали на пять месяцев без айфонов, айпадов и всего прочего. Честно скажу, не все дошли до финала. Я был одним из тех, кто провел в полной изоляции пять месяцев, в стране, где некоторые люди даже не знают, что такое QR-code, так что я знаю, о чем говорю».

Председатель совета директоров Leo Burnett Worldwide Т. Бернардин также заявил, что в связи с этими данными и общей политикой HumanKind Leo Burnett по всему миру переориентируется на создание более живых и аналоговых рекламных подходов и сократит количество диджитал департаментов по всему миру.

«Уже каждый пятый стремится не включать компьютер как можно дольше, приходя на работу. И растет количество тех, кто вообще не берет смартфон с работы домой. Думаете, это случайность? Это знак! Символ Leo Burnett – карандаш, а не мышь!», – подчеркнул Т. Бернардин ***(Leo Burnett объявил о закате диджитал эры // InternetUA (http://internetua.com/Leo-Burnett-ob-yavil-o-zakate-digital-eri). – 2013. – 3.06).***

***

Всем известно, что опрометчивый публичный пост в Facebook или «ВКонтакте» может аукнуться отказом при попытке устроиться на работу в серьезную компанию. Исследование, проведенное недавно компанией Device Research, выявило, что работодатели действительно очень часто проверяют аккаунты в социальных сетях своих потенциальных работников. Отказать в приеме на службу могут и из-за одного-единственного не понравившегося поста. И, пожалуй, главная цифра – каждый десятый человек в возрасте от 16 до 34 лет хоть раз сталкивался с тем, что его не принимали на работу из-за неудачной записи или комментария в Facebook, Twitter или другой соцсети.

Несмотря на столь удручающую статистику, 66 % молодых людей не заботятся о том, что их профайлы в соцсетях могут помешать карьере. Большинство людей воспринимают свои аккаунты как нечто для друзей, а не для работодателей. Отметим, что в США некоторые штаты начали бороться с увольнениями из-за постов на соцмедиа. Введены законы, по которым работодатель не имеет права требовать от сотрудников предоставлять пароли от своих профайлов в соцсетях ***(Социальные сети опасны для карьеры // InternetUA (http://internetua.com/socialnie-seti-opasni-dlya-kareri). – 2013. – 4.06).***

Маніпулятивні технології

На Волині процвітає торгівля людьми: як себе убезпечити

У кожному районі Волинської обл. трапляються випадки торгівлі людьми. Жертвами стають як чоловіки (переважно трудове рабство), так і

жінки (сексуальне та трудове рабство). Лише в 2013 р. працівниками УМВС України у Волинській обл. зафіксувано 14 кримінальних правопорушень у сфері суспільної моралі, з яких п'ять справ перебувають у суді. Ці дані були озвучені у Волинському прес-клубі на прес-конференції з питань протидії торгівлі людьми.

Найбільш поширеними схемами є: вербування молоді через Інтернет (зокрема через соціальні мережі «ВКонтакте» та «Одноклассники»), через друзів і знайомих, модельні та туристичні агенції агенції з працевлаштування. І не обов'язково, аби в людини забирали документи на місці працевлаштування. Дуже поширеним методом є психологічний тиск. «Можна зґвалтувати, записати на відео і шантажувати, аби людина і далі працювала, можна шантажувати сім'єю, підробити міграційну карту і не виплатити заробітну плату. Методів є багато», – зазначив оперуповноважений в особливо важливих справах УМВС України у Волинській обл. В. Кравчук.

Основною причиною існування проблеми торгівлі людьми є необізнаність громадян з правами людини і повна переконаність в тому, що «конкретно мене це ніяк не стосується».

Аби змінити ситуацію, в Україні (й на Волині зокрема) громадські організації, правоохоронні органи та відповідні управління державних органів проводять превентивну роботу.

«Попередити злочин і є нашим основним завданням», – наголосила асистент з превентивної роботи Кампанії «А21» А. Зоренко. Днями вона зі своїми колегами провела дискусійні зустрічі з молоддю в 10 освітніх закладах Волині. «У молоді існує ряд міфів. Основний із них – "мене це не торкнеться". Однак, як свідчать статистичні дані, будь-яка людина, навіть із трьома вищими освітами, може потрапити в рабство. Треба, щоб молодь зрозуміла: сучасне рабство стосується кожного з нас і воно є не десь далеко, а тут, у Волинській обл. Не достатньо простого розуміння проблематики, має бути сформоване усвідомлення», – резюмувала А. Зоренко.

Цьогоріч на волинян чекає широка інформаційна кампанія, спрямована на протидію торгівлі людьми. Аби достукатися до людини, котра прагне потрапити за кордон, громадські діячі з ВОГО «Волинські перспективи» запланували фотовиставку (автор ідеї – волонтерка та журналістка Т. Зубрик), спектакль «Сім історій» за участю жертв торгівлі, а також навчання 400 сільських голів і працівників центрів зайнятості, які не обізнані з цією проблемою і не знають, як реагувати та спілкуватися з жертвами рабства.

Фахівці з питань протидії торгівлі людьми зауважують: якщо ви все ж вирішили їхати за кордон, поцікавтеся в правоохоронних органах, чи має посередник ліцензію на діяльність, зробіть ксерокопії своїх паспортів і договору, повідомте всім родичам і близьким, куди їдете, і обов'язково запасіться контактами тих структур, куди ви можете звернутися за допомогою (телефони й адреси посольств, представництв міжнародних організацій тощо)

(На Волині процвітає торгівля людьми: як себе убезпечити // Четверта влада (http://4vlada.com/volin/25703). – 2013. – 27.05).

***

Полиция успешно завершила операцию по спасению 13-летнего мальчика из города Карачи (Пакистан), которого злоумышленники выманили через социальную сеть Facebook, а затем похитили. Они притворились другом парня и какое-то время вместе играли в онлайн-игры.

В Пакистане похищения, в основном, являются делом рук боевиков, которые склонны требовать выкуп. За мальчика, о котором идет речь в этой статье, просили 500 тыс. дол. Да, это не просто парень с улицы, а сын высокопоставленного таможенного инспектора.

К сожалению, похищения людей в стране случаются часто, однако злоумышленники до недавних пор редко призывали на помощь в организации преступления социальные сети.

Полиции удалось выйти на преступников по распечаткам телефонных звонков. Пятеро похитителей были убиты во время спасательной операции.

Власти страны просят родителей тщательно следить за тем, с кем их ребенок общается в Интернете ***(Подростка похитил «друг» из соцсети // InternetUA (http://internetua.com/podrostka-pohitil--drug--iz-socseti). – 2013. – 29.05).***

***

«ВКонтакте» назвали самой опасной для детей соцсетью

Дети в социальной сети «ВКонтакте» могут без особых проблем получить доступ к группам, содержащим порнографические картинки, видео и другой нежелательный контент, сообщил ведущий антивирусный эксперт «Лаборатории Касперского» С. Голованов.

Эксперты провели исследование трех российских социальных сетей: «ВКонтакте», «Одноклассники» и «Мой Мир». В ходе недельного исследования эксперты выяснили, что ребенку в возрасте 13 лет в соцсети «ВКонтакте» по запросу «порно» выдается список из закрытых групп, но при введении в поисковый запрос синонимов этого слова ребенок получает перечень открытых групп, содержащих информацию по запрашиваемой тематике, и может без проблем ее просмотреть. Кроме того, ребенок не застрахован от общения с педофилами в соцсети, может подвергаться моральному насилию и запугиванию, а также столкнуться с мошенниками.

В социальной сети «Одноклассники» по запросу «порно» и его синонимов ребенку становится доступен список закрытых групп, в которые нельзя получить доступ. В этой социальной сети подросток может рассчитывать только на «легкую эротику». Общение с педофилами в «Одноклассниках» сведено к минимуму, а каких-либо видов мошенничества эксперты в сети не обнаружили.

Анализ третьей соцсети – «Мой Мир» – показал, что порнографический контент в ней либо отсутствует, либо труднодоступен. За неделю исследования эксперты выяснили, что педофилы – не частые гости в данной социальной сети, а фишинга и мошенничества обнаружено не было.

«Коварство социальных сетей заключается в том, что они содержат в себе весь опасный контент, который есть в Интернете, а кроме того, представляют для ребенка дополнительную опасность в виде мошенничества от лица “друзей”, общения с незнакомцами и потенциальных пересечений с преступниками», – отметил С. Голованов ***(«ВКонтакте» назвали самой опасной для детей соцсетью // InternetUA (http://internetua.com/vkontakte--nazvali-samoi-opasnoi-dlya-detei-socsetua). – 2013. – 31.05).***

***

За дев’ять днів протестних виступів у Туреччині були госпіталізовані 915 цивільних осіб. Про це повідомив глава МВС М. Гюлер.

…М. Гюлер особливо відзначив, що кожен громадянин країни повинен захищати закон і не використовувати соціальні мережі в провокаційних цілях. Турецька влада вважає головним знаряддям пропаганди провокаторів мережу мікроблогів Twitter. За кілька днів протестів кількість повідомлень на тему турецьких протестів у ній перевищила один мільйон, а це більше, ніж за весь час нестабільності в Єгипті. Кілька десятків людей було затримано за заклики до заворушень, розміщені у Twitter ***(Протести в Туреччині: майже тисячу осіб госпіталізовано // Західна інформаційна корпорація (http://zik.ua/ua/news/2013/06/07/412919). – 2013. – 6.06).***

***

Как дурят пользователей социальных сетей

С появлением Интернета в соцсетях очень просто стало творить добро. Нажал кнопку Like («Класс», «Нравится» или им подобную) – и сделал доброе дело, например, поддержал пострадавшую от землетрясения Японию. Сделал «перепост» просьбы о помощи к себе на страницу – помог больному человеку найти донора крови. Казалось бы, все хорошо, если бы не одно небольшое «но».

Дело в том, что за просьбами сдать кровь очень часто прячутся мошенники. Возникает вопрос – как можно организовать мошенническую схему, основой которой станут призывы сдать кровь? Увы, сетевые проходимцы – персонажи достаточно изобретательные.

...Всякий активный пользователь «ВКонтакте», «Одноклассников» или Facebook наверняка множество раз видел в ленте друзей объявление, начинавшееся со слов: «Нужна помощь!», «Максимальный перепост!», «Ребенку требуется кровь!», «Закрывается собачий приют, животных усыпляют!» и т. д. Далее в тексте обычно следует рассказ, в котором подробно описывается ситуация. В конце указывается телефон «для справок», по которому можно якобы уточнить все детали. При этом никаких денег авторы объявлений не

просят, что, конечно же, подкупает. Однако это просто двухходовка, и она, несмотря на достаточно длительное время жизни в сети, все еще достаточно популярна.

Подавляющее большинство номеров телефонов, указанных после слезных просьб позвонить и, допустим, забрать щенка, принадлежат мошенникам, а за звонок на такой номер с мобильного счета списывается несколько сотен рублей.

Как выделить мошеннические объявления среди остальных? Во-первых, в тексте чаще всего не указывается никакая информация, кроме собственно номера телефона, по которому предлагается позвонить, чтобы узнать все подробности. Настоящие объявления по сбору донорской крови всегда содержат данные о том, кровь какой группы требуется, в каком медучреждении находится больной, сообщаются имена и фамилии людей, которые отвечают за сбор. То же касается и остальных объявлений – мошенники стараются не указывать никакой информации, кроме номера телефона.

Поэтому, прежде чем нажать на кнопку «опубликовать на моей странице» или набрать номер, проверьте, указан ли город, адрес и другие контактные данные. Кроме того, не поленитесь «забить» номер телефона в «Яндекс» или Google: не исключено, что этот телефон уже занесен в «черную» базу данных, где хранятся все мошеннические номера. А в случае со сдачей крови стоит помнить, что человеку, который решил пожертвовать свою кровь, вообще нет необходимости с кем-то созваниваться – достаточно знать адрес станции переливания крови и фамилию того, кому она предназначается.

Так что каждый раз перед тем, как сделать «доброе дело», не поленитесь узнать – действительно ли оно доброе и не помогаете ли вы мошенникам.

Есть и другие способы «отъема денежных средств» у жертв в социальных сетях. Это может быть, например, письмо с извещением о блокировке аккаунта, в котором сообщается о необходимости отправить SMS и получить код разблокировки. Другой вариант – электронное сообщение с предложением перейти по ссылке для активации страницы. Ссылка ведет на мошеннический сайт, дизайн которого в точности повторяет «ВКонтакте» или «Одноклассники». Стоит вам ввести там логин и пароль, как эти данные попадут к преступникам, и ваша страница будет взломана.

В сети «ВКонтакте» процветает еще один вид мошенничества – злоумышленники предлагают своим жертвам узнавать, кто посещал их страницы. В «Одноклассниках» такая возможность предусмотрена по умолчанию, а пользователям «ВКонтакте» она не предоставляется, поэтому не следует вестись ни на какие «сканеры друзей», которые требуют ввести пароль или отправить SMS. Это же касается и различных предложений вроде «отправь сообщение – получи деньги». Бесплатного сыра не существует, и любое сверхвыгодное или очень интересное предложение чаще всего является ловушкой мошенников ***(Как дурят пользователей социальных сетей // InternetUA (http://internetua.com/kak-duryat-polzovatelei-socialnih-setei). – 2013. – 7.06).***

***

В России считают, что США объявили мировую кибервойну

Признание США в том, что они через интернет-компании собирают данные о не являющихся американцами пользователях, представляет собой объявление мировой кибервойны. Так считают в «Интернет Партии РФ», которая написала открытое письмо президенту В. Путину с призывом создать Министерство информационной обороны.

Партия хочет, чтобы Россия в кратчайшие сроки приступила к созданию киберармии и кибероружия, пишет CNews. По словам руководителей организации, с каждым годом потребность в военной технике и оружии снижается, а меры по укреплению информационной безопасности не дают необходимого эффекта.

Ранее под давлением СМИ американские власти признали, что Агентство национальной безопасности и ФБР имеют прямой доступ к центральным серверам Apple, Google, Facebook и Microsoft ***(В России считают, что США объявили мировую кибервойну // InternetUA (http://internetua.com/v-rossii-scsitauat--csto-ssha-ob-yavili-mirovuua-kibervoinu). – 2013. – 7.06).***

Зарубіжні спецслужби і технології «соціального контролю»

DW: Блокування соцмережі «ВКонтакте»: помилка чи попередження?

Популярна соціальна мережа «ВКонтакте» 24 травня деякий час була недоступною у низці регіонів Росії. Виявилося, що домен vk.com опинився у «чорному списку». Чиновники заявляють про помилку. Але є й інші версії, повідомляє Корреспондент.net (http://ua.korrespondent.net/dw/1563067-dw-blokuvannya-socmerezhi-vkontakti-pomilka-chi-poperedzhennya).

Місцеві провайдери на виконання вимог Роскомнагляду 24 травня почали блокувати доступ до сайту vk.com. Коли здійнявся скандал, контролююче відомство заявило про помилку і негайно прибрало популярну соцмережу з «чорного списку». Згідно із законом, який набрав чинності торік, за наказом контролюючих органів провайдери блокують сторінки, що містять, приміром, дитячу порнографію або інструкції з виробництва наркотиків.

Черговий скандал, пов’язаний з «чорним списком» Інтернету, головною дійовою особою якого стала соцмережа «ВКонтакте», знову порушив питання про теперішню систему безпеки в мережі. Навіть якщо занесення популярного в Росії ресурсу до реєстру заборонених сайтів сталося, як стверджують у Роскомнагляді, внаслідок помилки, експерти, опитані DW, вважають, що систему боротьби за чистоту інтернет-контенту потрібно вдосконалювати.

Помилково чи навмисно?

Як зазначив в інтерв’ю DW координатор Центру безпечного Інтернету У. Парфентьєв, наразі можна розглядати дві ймовірні версії того, що сталося. «По-перше, це дійсно міг бути звичайний технічний збій, хоча ми навряд чи дізнаємося, хто конкретно припустився помилки – Роскомнагляд або

провайдер, – розмірковує У. Парфентьєв. – По-друге, можна розглядати і версію про те, що це був “пробний м’яч”, кинутий для того, щоб перевірити реакцію суспільства, або для демонстрації того, що у влади є важелі впливу на Інтернет».

Привертає до себе увагу те, що у випадку з «ВКонтакте» провайдери діяли рішучіше, ніж у ситуації з «Вікіпедією». Тоді провайдери нічого не зробили, незважаючи на присутність у «чорному списку» кількох сторінок вільної енциклопедії, а нині відреагували негайно і жорстко, щойно одна зі сторінок соцмережі потрапила до реєстру заборонених ресурсів. У. Парфентьєв припускає, що блокування «ВКонтакте» могло статися через надмірне завзяття провайдерів, які захотіли «вислужитися і перестрахуватися».

Утім, усе це лише версії, уточнює експерт, оскільки фактів, які підтверджують навмисність у діях тих, хто блокував доступ до популярної соцмережі, немає. Більше того, марно сподіватися, що хтось із безпосередніх виконавців колись зізнається, що ухвалював рішення або отримав вказівку блокувати контент «ВКонтакте». Однак, за словами У. Парфентьєва, подібні методи, спрямовані на «виховання» інтернет-контенту, цілком вписуються в контекст діяльності деяких державних органів.

Не шукати причини, а змінювати систему

Керівник інтернет-проектів лабораторії Касперського А. Ярних вважає, що будувати конспірологічні припущення не має сенсу. За словами експерта, у Росії сьогодні створена така система, що вже немає значення, який саме сайт потрапив в поле зору Роскомнагляду, він все одно може бути заблокований. «У випадку з соцмережею “ВКонтакте” спрацювали ті механізми, які були від початку закладені в процедурі блокування сайтів, прописаній в 139-му Федеральному законі», – сказав А. Ярних в інтерв’ю DW.

Експерти пропонують скористатися нагодою, щоб удосконалювати створену в Росії систему боротьби за чистоту Інтернету. «Повинен з’явитися більш точний і більш точковий алгоритм припинення обігу того чи іншого протиправного контенту, – переконаний У. Парфентьєв. – Тільки в такому разі, звісно, за умови достатньої компетенції співробітників, які реалізовують ці рішення, ефективність закону, спрямованого на боротьбу зі шкідливим контентом, підвищиться, а скандальність зменшиться».

Крім того, за словами У. Парфентьєва, потрібно забезпечити технічну можливість для блокування за url-адресою сторінки, щоб не виникало колізій, схожих на теперішню, коли до реєстру було внесено IP-адресу, – і це призвело до блокування всього ресурсу. А. Ярних додав, що необхідно створити також системи оперативного зворотного зв’язку. «Трапляється, що в адресі міститься помилка і блокується інший сайт, схожий за назвою, – зазначає експерт. – Якщо буде така ситуація, то повинна бути можливість швидко виправити помилки, яких, на жаль, не уникнути» ***(DW: Блокування соцмережі «ВКонтакте»: помилка чи попередження? // Корреспондент.net (http://ua.korrespondent.net/dw/1563067-dw-blokuvannya-socmerezhi-vkontakti-pomilka-chi-poperedzhennya). – 2013. – 25.05).***

***

Роскомнадзор начнет дважды проверять претендентов на добавление в реестр запрещенных сайтов. Процедура блокировки может быть изменена после того, как в черный список по ошибке попал домен социальной сети «ВКонтакте».

«Думаю, что мы введем двойной контроль за принятием решений. Каждый день нашим специалистам приходится обрабатывать довольно большой объем заявок с жалобами на те или иные сайты. К слову, непосредственно на “ВКонтакте” жалуются по несколько раз в день. Уделять должное внимание каждой ссылке становиться невозможно», – заявил представитель Роскомнадзора В. Пиков. Он не исключил, что скоро регулятору придется расширить штат сотрудников ***(Из-за «запрета» соцсети «ВКонтакте» Роскомнадзор изменит правила // Подробности.UA (http://podrobnosti.ua/internet/2013/05/27/907082.html). – 2013. – 27.05).***

***

Популярная социальная сеть «ВКонтакте» удалила со своего сайта скандальные группы о «детской моде» по просьбе Роскомнадзора.

«В своем письме мы просили руководство “ВКонтакте” в связи с обращениями граждан ограничить доступ к противоправному контенту и указали ссылки на более двух десятков групп с детской модой», – сообщил пресс-секретарь Роскомнадзора В. Пиков.

Представители «ВКонтакте» подтвердили, что удалили все подобные группы и впредь будут бороться с таким контентом ***(Из соцсети «ВКонтакте» удалили провокационные детские фото // InternetUA (http://internetua.com/iz-socseti--vkontakte--udalili-provokacionnie-detskie-foto). – 2013. – 28.05).***

***

ФБР успешно провело операцию по поимке педофилов: сотрудники бюро создали порносайт для их приманки. Таким образом были выявлены более 5,6 тыс. человек, пишет Seattle Post Intelligencer.

Операцию по выявлению педофилов ФБР начало в ноябре 2012 г. Тогда агенты ведомства захватили сайт, на котором размещался закрытый форум педофилов (имя сайта не разглашается, в материалах дела он проходит как «Сайт А») и на протяжении двух недель поддерживали его работу.

В результате последовавшего расследования 10 апреля был арестован житель Сиэттла. На его компьютере оперативники нашли изображения группового изнасилования ребенка. Обвинение арестованному пока не предъявлено. Подробности спецоперации пока не раскрываются, так как расследование по делу продолжается.

В России контроль и блокировка детской порнографии в сети осуществляется Роскомнадзором. Существует реестр запрещенных сайтов zapret-info.gov.ru, куда помимо детской порнографии попадают ресурсы с пропагандой

самоубийств и наркотиков. «Чёрный список» сайтов заработал в России с 1 ноября 2012 г. ***(ФБР поймала педофилов «на живца» с помощью фиктивного сайта // Західна інформаційна корпорація (http://reklamaster.com/news/id/41655/index.html). – 2013. – 31.05).***

***

Крупнейшие интернет-компании Google, Facebook, Microsoft, Yahoo, а также Twitter выразили протест против слежки за пользователями Великобритании. Об этом они написали в письме министру внутренних дел Т. Мей, сообщает Обозреватель (http://tech.obozrevatel.com/news/69437-google-facebook-i-twitter-otkazalis-sledit-za-polzovatelyami.htm).

Компании отказались сотрудничать в слежке за пользователями в рамках так называемой «Шпионской хартии». Согласно этому законопроекту, для полиции должны быть доступны личные данные и вся активность британских пользователей в электронной почте, в мессенджерах, в социальных сетях и VOIP-сервисах, а также храниться в течение 12 месяцев.

Американские компании назвали попытку отследить данные всех пользователей на территории Великобритании «потенциально крайне вредной». По мнению компаний, реализация этого плана угрожает положению Великобритании в роли одной из ведущих «цифровых держав», а также страны, пропагандирующей по всему миру свободу слова в сети.

Великобритания стала уже третьей страной в этом месяце, которая пытается усилить контроль за своими гражданами в Интернете. Ранее в России и США были предложены меры, призванные наказать пользователей нелегального контента ***(Google, Facebook и Twitter отказались следить за пользователями // Обозреватель (http://tech.obozrevatel.com/news/69437-google-facebook-i-twitter-otkazalis-sledit-za-polzovatelyami.htm). – 2013. – 1.06).***

***

Девять преступников, пойманных через социальные сети

Многие называют Интернет всемирной помойкой – в сети действительно каждый может оставить свой след и далеко не всегда он сверкает белизной и искрится солнечными зайчиками.

Как бы ни хотелось обратного, но ежедневно негативной информации на различных ресурсах оседает гораздо больше чем позитивной. Иногда откровения в Интернете не просто раздражают читателей, они могут привести автора за решетку.

Истории о «глупых воришках» уже давно стали одной из главных тем местных сплетен, ночных ток-шоу, комедийных и новостных программ на телевидении. Сегодня к услугам непутевых Плохишей вся мощь социальных сетей, которая дает возможность заявить о себе перед громадной аудиторией. Назовем это «Казаки – разбойники 2.0», сказал представитель департамента полиции У. Росс в интервью журналу The Daily Beast. Движимый «саморазрушительным сочетанием невежества, нарциссизма, комплекса

собственной неполноценности и абсолютным игнорированием норм общественной морали», мошенник при помощи социальных медиа значительно облегчает работу полиции. Вот девять преступников, которых удалось обнаружить благодаря таким сервисам как Instagram, YouTube и Facebook.

1. Кража тысяч аккаунтов и дружеский ужин

Правоохранительные органы уже располагали информацией о парочке, которая промышляла совместно, подобно киношным Бонни и Клайду, но специализировалась на краже личных данных, когда в январе 2013 г. налоговая полиция наконец-то, смогла выйти на их след. Осведомитель сообщил налоговикам, что какой-то человек по имени Трой хвастался на одном из интернет-сайтов успешной кражей 700 тыс. пользовательских аккаунтов и личных данных. Информатор, сам в прошлом уголовник, сменивший род занятий с криминала на помощь полиции, смог выследить Троя и его подругу, Т. Томасон, в штате Флорида. Он убедил парочку, что сам крутится в том же бизнесе, и пригласил их на ужин, чтобы обсудить схемы совместной деятельности. На встрече Трой передал ему флэшку, на которой содержались личные данные 46 человек. На этом накопителе полицейские смогли найти и личную информацию Троя, но пока не могли связать его с конкретными преступлениями и кражами личных данных. Но вскоре они наткнулись на фотографию, запечатлевшую порцию макарон с сыром и аппетитный стейк, которая была загружена на Instagram акаунт @troymaye 7 января. Под фото также была сделана подпись «Мортонс» – название ресторана. Дата и место полностью совпадали с заведением, где подозреваемый 44-летний Н. Трой Майе и его подруга встречались с информатором. Н. Трой Майе и Т. Томасон были арестованы в январе и в качестве основного доказательства против подозреваемых в краже личных данных выступало фото Instagram.

2. «Чика грабительница банка» признается во всем на YouTube

Речь пойдет не о клёвых московских «чиках», а об американских. Название семиминутного видео «Чика грабительница банка» говорит само за себя. На экране появляется молодая девушка, блондинка с татуировкой, она сидит на полу в своей спальне, камера фиксирует беспорядок в комнате. Сначала героиня демонстрирует лист бумаги с рукописной надписью: «Я украла из машины», а затем достает пакет марихуаны и трубку. Следующий плакатик говорит: «Потом я украла машину!» Она с гордостью показывает как рада собственным криминальным подвигам. Следующее признание гласит: «Затем я ограбила банк!» Она широко улыбается, а субтитры поясняют «с пистолетом, подушкой и запиской». Она показывает объемную пачку наличных, и сумма «6256 дол.» появляется в титрах нижней части экрана. Девушка, 19-летняя Х. Сабата была арестована 28 ноября, всего через несколько часов после того, как видео было загружено на YouTube. В полицию также позвонил ее бывший друг, предупредивший, что она и ему похвасталась кучей денег после ограбления банка. «Я работаю шерифом 19 лет, 42 года в правоохранительных органах, но ничего подобного не видал», рассказал шериф округа Й. Дейл Рэдклифф газете New York Times.

3. Смертельные ловушки на пешеходных тропах

Двое мужчин были арестованы 21 апреля 2012 г. в штате Юта за установку опасной, потенциально смертельной ловушки, выполненной в средневековом стиле, на популярном туристическом маршруте вблизи городка Прово. Лесные рейнджеры (имевшие опыт военных действий) своевременно заметили и обезвредили подвесное самодельное устройство, которое состояло из камня размером с футбольный мяч, усеянного острыми деревянными шипами, установленного для того, чтобы однажды обрушиться на голову случайного прохожего. Полиция получила информацию, что именно 19-летний Б. Рутковский и 21-летний К. Кристенсен причастны к этой опасной затее, так как парочка открыто обсуждала устройство ловушек на Facebook. Когда их задержали, они утверждали, что ставили ловушки на животных. Вранье, сказал шериф С. Кэннон. «Нет сомнений, что ловушки были установлены для людей, и что подозреваемые знали о смертельной угрозе».

4. Воровство горючего из полицейской машины

16 апреля 2012 г. в дверь жилища 20-летнего жителя штата Кентукки, К. Бейкера, постучал офицер полиции Дженкинс. С фототографией, которую К. Бейкер разместил на своей страничке Facebook, очень быстро успели ознакомиться все две тысячи жителей маленького городка. На фото К. Бейкер, гордо улыбаясь, незамысловатым способом сливает бензин из бака машины Дженкинса, а ведь автомобиль принадлежит Департаменту полиции штата. Получив законное наказание за свой проступок, К. Бейкер уже не так широко улыбался, и разослал всем своим 380 друзьям в Facebook сообщение: «Лол, я попал в тюрьму из-за Facebook».

5. Грудь как улика

20 марта 2012 г. агенты ФБР арестовали Х. Очоа, жителя города Галвестон, штат Техас, по обвинению во взломе четырех веб-сайтов правоохранительных органов. А ниточка, которая привела федералов к 30-летнему Х. Очоа, начиналась с колоритной визитной карточки с фотографией подруги Х. Очоа, на которой она наклоняется в сторону камеры в вызывающем купальнике и держит в руках лист бумаги с надписью «w0rmer & CabinCr3w». Эту визитку хакер оставлял на всех взломанных сайтах в качестве личной метки. Детальный анализ изображения показал, что фотография была сделана с iPhone в Мельбурне, Австралия. Попытка связать имя Х. Очоа с надписью «w0rmer», вывела агентов ФБР на страницу Х. Очоа в сети Facebook, с которой они узнали, что у него в Австралии есть знакомая девушка, как раз обладающая соответствующим размером бюста. Нашлись и совместные снимки Х. Очоа с этой женщиной (в более скромных нарядах) на страничке самого хакера.

6. «Посмеялся» над жертвой, используя краденый ноутбук

В январе 2011 г. полиция Вашингтона, округ Колумбия, арестовала 19-летнего Р. Найта, за вторжение в дом журналиста Washington Post М. Фишера и кражу куртки, наличных денег и ноутбука, принадлежавшего сыну М. Фишера. Вернувшись домой с добычей, Р. Найт включил похищенный

компьютер и не придумал ничего лучшего, чем войдя в аккаунт сына жертвы в социальной сети Facebook, выложить свеженькое фото себя любимого, одетого в украденную куртку и с похищенными купюрами в руках. «Фото в полный рост, замечательно», сказал М. Фишеру один из полицейских. Другой офицер, К. Роу, назвал Р. Найта самым глупым преступником из всех, с которыми он когда-либо встречался.

7. Торговля наркотиками и следы в Facebook

М. Грассо исчез из сицилийского курортного городка Таормина в 2008 г., как только полиция решила арестовать его за торговлю наркотиками. Хотя он и был заочно осужден в 2011 г., итальянские власти понятия не имели о его местонахождении... пока он сам не навел их на верный след своей страничкой в Facebook. Сначала на ней появились фотографии снеговика, затем снимки на фоне двухэтажных красных автобусов и, наконец, откровенное признание, что он в Лондоне, с большим количеством фотографических подтверждений, как у любого рядового туриста. В январе он опубликовал фотографии, по которым было видно что он работает в пиццерии, а один из снимков даже запечатлел фасад заведения и его название. 11 февраля 2012 г. 27-летний М. Грассо был арестован по ордеру Интерпола и экстрадирован в Рим.

8. Побег из тюрьмы и искушение судьбы

К. Линч сбежал из тюрьмы графства Саффолк, Англия, в сентябре 2009 г. – совсем немного «недосидев» до окончания своего семилетнего срока за кражу со взломом. А следующие четыре месяца он провел, играя в со Скотланд-Ярдом в странную, но весьма увлекательную игру. Он регулярно размещал ключи и подсказки по поиску своего местонахождения на Facebook со множеством фотографий. Он развлекался тем, что дразнил полицейских, а полиция, в свою очередь, была занята рутинным процессом разработки этих подсказок. К тому времени, когда полицейские его поймали (в январе 2010 г.), у К. Линча на его страничке в Facebook было более 40 тыс. поклонников.

9. Не стоит троллить полицейских

5 января 2012 г. офис шерифа округа Джефферсон, штат Алабама, выдал ордер на арест Д. Маккомбса. Фото обвиняемого в действиях насильственного характера разместили с пометкой «Особо опасен» на страничке в сети Facebook, озаглавленной «беглец недели». Д. Маккомбс сам решил вмешаться в обсуждение этой новости, начав пространный комментарий тирадой: «Как хорошо, что я уехал из штата». Несколько комментариев спустя Д. Маккомбс сказал, что он считает титул «главного беглеца недели» диффамацией. 3 февраля Д. Маккомбс был арестован в штате Огайо, во многом благодаря собственным обильным словоизлияниям на страничке Facebook.

Глупые воришки часто попадают в анекдотические ситуации. Два предприимчивых, но не очень умных друга, жители одного маленького американского городка, решили обогатиться. С этой целью поздно ночью они поехали к местному отделению банка на джипе одного из приятелей. Там, не долго думая, они привязали банкомат, вмурованный в стену банка, прочным тросом к бамперу автомобиля. Увидав, что на улице показались разноцветные

огоньки полицейской машины, сидевший за рулем дал по газам. Бампер не выдержал и оторвался, оставшись вместе с регистрационным номером на месте неудавшегося преступления. Полиция была дома у горе-похитителей раньше их самих. В этом случае, как говорится, обошлось без Интернета, но именно сеть разнесла эту историю по всему миру... ***(Девять преступников, пойманных через социальные сети // InternetUA (http://internetua.com/9-prestupnikov--poimannih-cserez-socialnie-seti--foto). – 2013. – 3.06).***

***

Весьма пикантный скандал разгорелся в израильской армии. Девушки, которые проходят военную службу в армии на юге страны были уличены в том, что выкладывали свои полуобнаженные фото на страничках социальных сетей.

Снимки с девушками в нижнем белье и военном снаряжении появились в Facebook. На одном из скандальных снимков девушки предстали перед общественностью лишь в касках и военном снаряжении, которое едва прикрывало обнаженные тела. На сегодняшний день уже установлены имена и фамилии нарушительниц армейского устава, однако эти данные не разглашаются для широкой общественности.

Израильское новостное агентство Walla сообщило, что за непристойное для израильских военнослужащих поведение все девушки получат дисциплинарное взыскание.

Стоит отметить, что такое поведение для израильских военных не в новинку. Уже ранее в этой стране вспыхивали скандалы, связанные с фотографиями военнослужащих, выложенными в соцсетях.

Ранее были прецеденты, когда в социальных сетях появлялись фотографии израильских военных на фоне связанных палестинцев. Тогда израильское правительство даже выдало запрет на пользование социальными сетями для военнослужащих, однако неизвестно действует ли он до сих пор ***(Израильские женщины-военные оскандалились, выкладывая обнаженку в соцсетях // NovostiUA (http://novostiua.net/obschestvo/38322-izrailskie-zhenschiny-voennye-oskandalilis-vykladyvaya-obnazhenku-v-socsetyah.html). – 2013. – 3.06).***

***

Израильским военным закроют доступ к социальным сетям.

Армия Израиля в ближайшее время пересмотрит свое отношение к социальным сетям и сервисам – доступ военных к ним будет сильно ограничен, и чем выше служащий по званию, тем жестче будет запрет.

Внедрение новых ограничений напрямую связано с опасениями Израиля относительно ведения разведывательных операций со стороны других стран с использованием социальных сетей. Ограничение доступа к ним коснется всех солдат израильской армии, вне зависимости от ранга и положения.

Запрет коснется всех наиболее популярных сервисов для общения и обмена информацией, таких как Facebook, Twitter, Instagram и другие.

Некоторым военным будет запрещено иметь аккаунты в этих проектах, а некоторым, например, пилотам и офицерам разведки, будут сделаны некоторые послабления. В частности, как пишет CNET.com, они смогут создавать профили, но им строго-настрого запрещено сообщать о своей причастности к рядам вооруженных сил Израиля и тем более выкладывать свои фотографии в военной форме.

Один из старших офицеров армии Израиля сообщил, что социальные сети в настоящее время имеют сильное влияние на все слои населения, в том числе и на солдат. По его словам, армия не хочет оставаться в тени, но и лишнюю информацию о себе раскрывать не желает, поскольку социальные сети могут нести не только пользу, но и вред. Офицер уверен, что разведка других стран все чаще использует социальные сервисы для сбора информации.

Израиль – не первая страна, в которой армия с недоверием и даже с некой враждебностью относится к социальным проектам. Относительно недавно власти Канады предупредили солдат своей армии об опасности, которую может нести в себе простое размещение фотографий в Интернете. Это влечет за собой прямую угрозу не только всей армии в общем, но и каждому конкретному солдату в частности, так как их страницы могут быть просмотрены членами террористических организаций. Командование армии Австралии, кстати, полностью разделяет мнение канадцев.

Как сообщается, намерение Израиля ограничить своим военным доступ к Facebook, Twitter – это уже не просто слова: к концу текущего месяца армия Израиля выпустит специальный «Кодекс этики в социальных сетях» для своих солдат, в котором и будут описаны все правила использования ресурсов в соответствии со званиями ***(Израильским военным закроют доступ к социальным сетям // Бизнес и Политика (http://www.business-politika.net/world_news.php?id_news=209460). – 2013. – 7.06).***

***

Власти Турции заблокировали в стране доступ к социальным сетям, пишет Обозреватель (http://tech.obozrevatel.com/news/96580-v-turtsii-perekryili-dostup-k-sotssetyam-smi.htm).

По информации СМИ, доступ к Facebook и Twitter был сильно затруднен. Также поступали сообщения о глушении сигнала со стороны властей на площади Таксим во время проведения демонстраций.

Источники, пожелавшие остаться неизвестными, сообщили, что скорость доступа намеренно снижена до минимальной. Таким образом, доступ к ресурсам официально не заблокирован, однако ни одна из крупнейших мировых социальных сетей не доступна. По сообщениям других источников, доступ через 3G также заблокирован.

Отмечается, что доступ был затруднен именно в часы максимального пика, когда протестующие пытались пробраться в парк Гези. Примерно через полчаса, после того, как полиция покинула территорию парка, доступ к Twitter и Facebook был восстановлен.

Представители Facebook комментировать ситуацию отказались, заявив лишь, что «Интернет дает людям во всем мире возможность коммуницировать. Поэтому очень важным вопросом является возможность беспрепятственно общаться и делиться информацией и ограничение доступа в Интернет может стать серьезной темой для обсуждения в мировом сообществе».

Напомним, акции протестов идут в Стамбуле уже несколько дней. Демонстранты протестуют против планов властей построить на месте парка Гези в Стамбуле торгово-развлекательный комплекс. Выступления сопровождались беспорядками и быстро распространились по всей территории страны ***(В Турции перекрыли доступ к соцсетям – СМИ // Обозреватель (http://tech.obozrevatel.com/news/96580-v-turtsii-perekryili-dostup-k-sotssetyam-smi.htm). – 2013. – 3.06).***

***

В турецком городе Измир полиция арестовала 25 человек за то, что они на своих страницах в сети микроблогов Twitter «призывали людей протестовать». Об этом сообщает «Би-би-си» со ссылкой на местные СМИ.

Местные власти, в свою очередь, назвали данные заявления в Интернете, сделанные активистами, «дезинформацией» ***(Турецкая полиция арестовала 25 человек за призывы к протесту в Twitter // Версии.com (http://www.versii.com.ua/news/280271/). – 2013. – 5.06).***

***

Арбитражный суд Московской обл. привлек к административной ответственности подмосковного интернет-провайдера «Тефо» за то, что тот не блокировал доступ к сайтам с запрещенной в России информацией. Размер штрафа составит 30 тыс. руб., передает Обозреватель (http://tech.obozrevatel.com/news/31682-v-rossii-vpervyie-oshtrafovali-provajdera-za-otkaz-blokirovat-sajtyi.htm).

«Это первый случай вынесения административного наказания в отношении оператора связи за подобный вид правонарушений», – отметили в Роскомнадзоре.

В декабре 2012 г. управление Роскомнадзора по Москве и Московской обл. установило, что провайдер «Тефо» не авторизован на веб-сервисе zapret-info.gov.ru, а значит, не принимает сведения из Единого реестра интернет-ресурсов, содержащих противозаконную информацию, и не ограничивает к ней доступ. В бездействии провайдера чиновники усмотрели нарушение при предоставлении телематических услуг связи.

Компания обжаловала это решение в Десятом Арбитражном апелляционном суде, однако апелляционная жалоба не была удовлетворена ***(В России впервые оштрафовали провайдера за отказ блокировать сайты // Обозреватель (http://tech.obozrevatel.com/news/31682-v-rossii-vpervyie-oshtrafovali-provajdera-za-otkaz-blokirovat-sajtyi.htm). – 2013. – 4.06).***

***

Міліціонери шукають порнографію на профілях тернополян в соцмережах.

В редакцію інтернет-газети «ДОБА» звернувся житель обласного центру з повідомленням про те, що правоохоронці звинувачують його у розповсюдженні відео порнографічного характеру в мережі Інтернет. Приводом до цього став жартівливий рекламний ролик еротичного змісту, який тернополянин розмістив у себе на сторінці на сайті «ВКонтакте». «Мене обурило те, що міліціонери мені претензії почали висовувати, адже кругом злочинність і беззаконня, а вони "збоченців" шукають там, де їх нема, – каже "ДОБІ" пан Олександр. – Мені повідомили, що відео, яке є у мене на сторінці – сумнівного характеру. Знаєте, це вже занадто, адже від таких звинувачень моя репутація, виходить, також сумнівною стає?! Я трохи "покопав глибше" і, як виявляється, схожі випадки свавілля міліції стають вже звичною справою».

«За словами молодого чоловіка, нещодавно в Бережанах з такими ж претензіями правоохоронці завітали «в гості» до одного з місцевих мешканців. Прийшли вони з ордером на обшук, а комп'ютер забрали «на експертизу» до Тернополя. Справа в тому, що в міліції не так давно з'явився цілий новий відділ по боротьбі з кіберзлочинністю. Отож, тепер будь-хто може не лише осоромитися перед знайомими через проблеми з міліцією, але й заробити неприємностей на навчанні чи на роботі, адже правоохоронці про такі «незаконні дії» громадян доводитимуть до відома відповідні установи та організації. Єдине, що можу порекомендувати тим, хто має еротичне відео в себе на профілі в Інтернеті – видаліть його! – переконує пан Олександр. – Здається, що наша міліція вже знайшла всіх злочинців, залишилось лише це. Будьте уважними, адже те, що може вам видатися безневинним жартом, для наших захисників закону і порядку може стати "червоною тряпкою", за якою послідує ряд проблем» ***(Міліціонери шукають порнографію на профілях тернополян в соцмережах // Газета «ДОБА» – інтернет-видання Тернопільщини (http://doba.te.ua/novyny/militsionery-shukayutna-pornohrafiyu-na-profilyah-ternopolyan-v-sotsmerezhah.html). – 2013. – 4.06).***

***

«Регионалы» пытаются законодательно закрепить возможность удаления из сети Интернет «недоброкачественной» информации.

Народный депутат от Партии регионов В. Олийник зарегистрировал в Верховной Раде проект закона «О внесении изменений в закон Украины "О защите общественной морали" (относительно защиты информационного пространства)».

Политик считает необходимым регламентировать на законодательном уровне механизмы государственного регулирования информации, которая содержится в Интернете. По его мнению, некоторая информация «адресного пространства украинского сегмента» глобальной сети может представлять

угрозу физическому, интеллектуальному, моральному и психологическому состоянию населения.

На сегодняшний день украинское законодательство запрещает распространение информации, которая содержит в себе пропаганду войны, национальной и религиозной вражды, смены путем насилия конституционного строя или территориальной целостности страны. В. Олийник же дополнил этот список запретом на распространение информации, которая посягает на права и свободы человека, содержит призывы к совершению террористических актов и других уголовных преступлений.

Провайдеры же по решению суда будут обязаны удалять ресурсы, на которых размещена недоброкачественная информация ***(Партия регионов подготовила закон о «зачистке» интернет-сайтов // Новый Регион (http://www.nr2.ru/kiev/442415.html). – 2013. – 5.06).***

***

СМИ: ФБР имеет доступ к серверам Facebook и Skype

Агентство национальной безопасности (АНБ) и Федеральное бюро расследований (ФБР) США имеют прямой доступ к центральным серверам девяти ведущих интернет-компаний, сообщает газета The Washington Post, пишет Обозреватель (http://tech.obozrevatel.com/news/58402-smi-fbr-imeet-dostup-k-serveram-facebook-google-i-skype.htm).

По данным издания, которые цитирует РИА Новости, спецслужбы извлекают с серверов необходимую информацию: аудио, видео, фотографии, сообщения электронной почты, которые позволяют отслеживать передвижения людей и их контакты.

Особо секретная программа с кодовым названием PRISM никогда не называлась публично, хотя и была утверждена в 2007 г., пишет газета. Конгрессмены, которые знают о ней, дали обязательство о неразглашении информации.

Издание утверждает, что в программе участвуют всемирно известные компании Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.

Расследование The Washington Post опубликовано на фоне другого скандала с утечкой персональных данных – газета Guardian сообщила, что АНБ добилось более месяца назад разрешения суда на получение данных о звонках абонентов крупнейшей американской сотовой компании Verizon вплоть до 19 июля текущего года.

Общественные организации заявили о беспрецедентном вторжении в частную жизнь граждан. Ранее считалось, что власти отслеживают звонки только подозреваемых в совершении преступлений ***(СМИ: ФБР имеет доступ к серверам Facebook и Skype // Обозреватель (http://tech.obozrevatel.com/news/58402-smi-fbr-imeet-dostup-k-serveram-facebook-google-i-skype.htm). – 2013. – 7.06).***

***

У національній розвідці США заявили, що стежать за громадянами інших країн через Інтернет.

Директор національної розвідки США Д. Клеппер заявив 6 червня 2013 р., що американські спецслужби збирають через інтернет-компанії інформацію тільки про користувачів, які не є громадянами США і знаходяться за межами цієї країни.

Як передає Reuters, це, за словами Д. Клеппера, дозволяють американські закони.

Таким чином директор розвідки прокоментував статті у виданнях The Washington Post і Guardian, в яких стверджувалося, що спецслужби США стежать за громадянами країни через Інтернет і телефон. За словами Д. Клеппера, матеріали газет містять «численні неточності».

…Після появи цього матеріалу ряд згаданих в ньому компаній – Facebook, Yahoo, Google, Apple і Microsoft – спростували, що надають спецслужбам доступ до своїх серверів ***(У США зізналися, що стежать за іноземцями через Інтернет // Західна інформаційна корпорація (http://zik.ua/ua/news/2013/06/07/412916). – 2013. – 7.06).***

***

Anonymous отомстили США за слежку в Интернете.

Члены хакерского движения Anonymous выложили документ, в котором, по их мнению, подтверждаются планы спецслужб США по слежке за интернет-пользователями. Заявление группировки доступно на сайте Pastebin, а сам документ хакеры выложили на специально созданный сайт.

Опубликованный документ датирован 2008 г. и подписан советником министерства обороны США. В тексте документа описываются планы по созданию Глобальной информационной сети (GIG), призванной объединить единой закрытой сетью войска, высшие должностные лица и обслуживающий их персонал. В этой сети они смогут обмениваться секретными файлами. GIG будет полностью закрыта от внешнего доступа и никак не связана с Интернетом и корпоративными сетями. Выложенный хакерами документ описывает устройство NetOps – системы, которая занимается управлением и мониторингом сети.

Стоит отметить, что о планах по развертыванию GIG Агентство национальной безопасности США (NSA) официально объявило еще в 2008 г. Большая часть описанной в опубликованном Anonymous документе находится в свободном доступе. Проект GIG все еще находится в разработке, хотя транспортная инфраструктура для него уже создана. NSA ранее также заявляла о планах доработать проект и адаптировать его согласно современным угрозам. Также в планах агентства переименовать сеть ***(Anonymous отомстили США за слежку в Интернете // InternetUA (http://internetua.com/Anonymous-otomstili-ssha-za-slejku-v-internete). – 2013. – 8.06).***

Проблема захисту даних. DOS та вірусні атаки

Сайты государственных ведомств Саудовской Аравии, в том числе ресурс министерства информации королевства, подверглись скоординированной атаке хакеров, передает Обозреватель (http://tech.obozrevatel.com/news/26914-hakeryi-vzlomali-gosudarstvennyie-sajtyi-saudovskoj-aravii.htm).

Некоторое время на взломанных интернет-страницах был размещен флаг Алжира, однако никаких заявлений от алжирских или иных хакерских групп пока не последовало.

Помимо правительственных интернет-ресурсов, злоумышленники смогли получить доступ и к серверам информационного агентства Al-Ekhbariya, телеканалов Al-Riyadiyah и Channel One, а также радиостанции Quran Radio. Также пострадала сетевая инфраструктура Центра культуры имени короля Фахда.

Ранее в мае этого года от действий хакеров пострадал сайт министерства внутренних дел королевства ***(Хакеры взломали государственные сайты Саудовской Аравии // Обозреватель (http://tech.obozrevatel.com/news/26914-hakeryi-vzlomali-gosudarstvennyie-sajtyi-saudovskoj-aravii.htm). – 2013. – 25.05).***

***

На днях огромное количество интернет-пользователей сообщило о том, что злоумышленникам удалось заполучить доступ к учетным записям в iTunes Store. Как утверждают пострадавшие, они получили письмо, якобы отправленное сотрудниками Apple, с подарочным сертификатом, после чего ввели свои данные на инфицированном подставном сайте. Это, в свою очередь, привело к потери доступа к учетной записи, а затем – и денег.

Примечательно, что ссылка, которая содержится в письме, ведет на страницу маскирующуюся под раздел iTunes Store. На текущий момент практически любой веб-браузер идентифицирует страницу как фишинговую и ограничивает к ней доступ.

Для активации подарочного сертификата на 100 дол. пользователей просят ввести свой логин и пароль от Apple ID. После инфицирования компьютера мошенники получают доступ к данным о банковских картах пользователей ***(Злоумышленники похищают Apple ID при помощи инфицированных подарочных сертификатов // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2013/05/27/fake-certs.html). – 2013. – 27.05).***

***

Комиссия по воровству американской интеллектуальной собственности (Commission on the Theft of American Intellectual Property) представила доклад, в котором на 84 страницах предлагается отслеживать нелицензионный контент в сети при помощи шпионского ПО.

В последнее время кражи интеллектуальной собственности путем нелегального скачивания контента приобрели массовый характер, поэтому Голливуд намерен распространять шпионские программы вместе с кинофильмами через популярные торрент-трекеры. Подобную практику применяют правоохранительные органы многих стран, устанавливая шпионские программы на компьютеры и мобильные устройства подозреваемых.

В докладе Комиссия рекомендует устанавливать шпионское ПО, которое при открытии нелицензионного файла сможет блокировать компьютер пользователя как улику до прибытия полиции. По такому примеру работает ПО, используемое вымогателями (ransomware), которое блокирует систему пользователя и требует перечислить деньги для разблокировки.

Чтобы ПО не блокировалось антивирусными решениями, разработчикам придется договориться с производителями не включать его в свои антивирусные базы.

Кроме того, авторы доклада предлагают предоставить владельцам интеллектуальной собственности право уничтожать пиратские файлы на компьютерах пользователей, фотографировать людей за компьютером с помощью веб-камеры и даже физически выводить из строя их системы ***(Голливуд намерен распространять шпионское ПО вместе с фильмами через торрент-трекеры // InternetUA (http://internetua.com/gollivud-nameren-rasprostranyat-shpionskoe-po-vmeste-s-filmami-cserez-torrent-trekeri). – 2013. – 28.05).***

***

Китайские хакеры в ходе нескольких кибератак похитили у США проекты ряда оборонных систем, составляющих основу американской противоракетной обороны. Об этом, как пишет газета The Washington Post, говорится в докладе научного совета министерства обороны США (DSB), который будет представлен руководству Пентагона, правительству и главам американских оборонных компаний. Все похищенные данные могут быть использованы Китаем при разработке собственных систем военного назначения.

Согласно подготовленному для Пентагона докладу, в руках хакеров оказались сведения о зенитных ракетных комплексах Patriot PAC-3, противоракетных комплексах THAAD и корабельной многофункциональной боевой информационно-управляющей системе Aegis. Кроме того, были украдены и данные о проектах палубных истребителей F/A-18 Super Hornet, конвертопланах V-22 Osprey, многоцелевых вертолетах UH-60 Black Hawk, новых боевых кораблях прибрежной зоны проекта LCS и перспективных истребителях F-35.

В докладе содержатся данные о похищенных проектах (не уточняется, были ли украдены проекты целиком или только некоторые их части) за последние несколько лет. В частности, впервые об утечке информации об F-35

стало известно еще в январе 2007 г. Любопытно, что DSB не возложил вину за кражу информации непосредственно на китайских хакеров, однако руководители американских оборонных компаний и представители министерства обороны США заявили, что речь идет именно о кампании Китая, направленной на похищение американских военных секретов.

В начале мая 2013 г. сообщалось, что хакеры из Китая в ходе нескольких кибератак украли у ряда американских компаний ценную информацию, связанную с перспективными разработками. Атаки продолжались в течение 2007–2010 гг. Под удар попала, в частности, компания Qinetiq North America, разработчик роботов и спутниковых разведывательных систем. По данным аналитиков, за этими атаками может стоять хакерская группа Comment Crew, базирующаяся в Шанхае.

В январе текущего года министерство обороны США одобрило план пятикратного увеличения численности подразделений кибербезопасности. В настоящее время они насчитывают 900 человек, однако штат планируется увеличить до 4,9 тыс. сотрудников. Благодаря увеличению штата Кибернетическое командование в составе Стратегического командования вооруженных сил США сможет эффективнее отражать атаки на американские компьютерные сети, включая информационные сети Пентагона ***(Китайские хакеры украли секреты американской ПРО // InternetUA (http://internetua.com/kitaiskie-hakeri-ukrali-sekreti-amerikanskoi-pro). – 2013. – 28.05).***

***

Специалисты по информационной безопасности из компании F-Secure говорят, что недавно введенная сетью Twitter система двухфакторной аутентификации содержит изъян, который может привести к тому, что доступ к пользовательскому блогу получат злоумышленники.

Напомним, что Twitter запустила систему двухфакторной аутентификации на прошлой неделе как ответ на участившиеся случаи взлома аккаунтов резонансных пользователей. Хакеры воруют или угадывают логины и пароли пользователей Twitter, поэтому соцсеть реализовала систему одноразовых паролей, которые получаются с SMS-сообщением на мобильный телефон владельца блога. Пользователи могут включить систему двухфакторной аутентификации или же не пользоваться ею, если нет такого желания или местные сотовые операторы ее не поддерживают.

Как говорит Ш. Салливан, советник по ИТ-безопасности F-Secure, атакующие могут злоупотребить данным функционалом, чтобы получить несанкционированный доступ к тем аккаунтам пользователей, которые еще не включили поддержку двухфакторной аутентификации. Если атаку удастся совершить, то реальный владелец блога уже не сможет восстановить контроль над блогом простым сбросом пароля. Это становится возможным, ввиду того, что Twitter не использует дополнительных методов верификации для тех, кто

неавторизованно завладел пользовательским блогом и включил на нем двухфакторную аутентификацию.

Когда возможность двухфакторной аутентификации включена (Account Security) в разделе управления аккаунтом, сайт отправляет тестовое сообщение на телефон. Пользователи просто нажимают «Да» (даже если они и не получили сообщения). Ш. Салливан говорит, что Twitter вместо этого нужно было бы отправлять ссылку с подтверждением по электронной почте, которая была указана в аккаунте и работает даже при подключении двухфакторной аутентификации.

В F-Secure полагают, что выявленный ими метод могут использовать такие организаторы атак, как Сирийская электронная армия и другие, для угона пользовательских Twitter-аккаунтов. Кроме того, в компании говорят, что система двухфакторной аутентификации Twitter в ее нынешнем виде непригодна для некоторых групп пользователей, например для поставщиков новостей и компаний с распределенной географической организацией, где многие сотрудники имеют доступ к аккаунтам.

В Twitter пока никак не прокомментировали сообщение F-Secure ***(Система двухфакторной аутентификации Twitter может стать инструментом хакеров // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2013/05/28/2-step-auth.html). – 2013. – 28.05).***

***

Исследователи из компании Eset обнаружили вредоносную шпионскую программу, применяющую необычные методы маскировки. Вредонос, получивший название Win32/Syndicasec.A, исполняет в Windows 7 привилегированные команды в обход механизма UAC.

Вирус пользуется дефектом белого списка UAC, задокументированным еще в 2009 г. Л. Дэвидсоном, причем практически без изменений применяется код, предложенный самим исследователем в качестве образца. С его помощью запускается другой компонент, регистрирующий посторонний код JavaScript в сервисе Windows Management Instrumentation. Этот код, в свою очередь, загружает RSS-поток блога, созданного на бесплатном сервисе. Теги «постов» в зашифрованном виде содержат ссылки на реальные управляющие серверы вируса. Как выяснили исследователи, атакующие просматривают файловую систему зараженных хостов, а также собирают информацию о сетевых настройках, накопителях и работающих программах.

Судя по датам файлов, шпион действует как минимум с лета 2010 г. Как сообщают в Eset, масштаб заражения невелик и охватывает только Непал и Китай. Точную цель операции выяснить не удалось, но ряд признаков указывает на то, что она направлена против тибетских сепаратистов ***(Обнаружен кибершпион, использующий концептуальный код от исследователя // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2013/05/28/new-cyberspy.html). – 2013. – 28.05).***

***

Сирийские хакеры взломали все приложения британского канала Sky для платформы Android, заменив программы в цифровом магазине Google Play. Об этом сообщается 26 мая в микроблоге техподдержки Sky.

Пользователей попросили удалить программы со своих устройств до последующих заявлений. По состоянию на 14:00 по московскому времени 27 мая новых записей в микроблоге техподдержки не появилось. При этом взломанные приложения Sky+ и Sky News, ссылки на которые канал дал ранее, оказались удалены из магазина приложений Google Play.

Как уточняет The Drum, за взломом стоит хакерская группировка «Сирийская электронная армия». Хакеры изменили описание приложений в Google Play на фразу Syrian Electronic Army Was Here («Здесь была Сирийская электронная армия») и заменили логотип приложения на собственную эмблему.

Вместе с тем поиск по Google Play выдает несколько программ Sky, в описании которых нет следов взлома. В частности, доступны погодное и посвященное скачкам приложения.

Взлом приложений Sky произошел менее чем через две недели после того, как в одном из официальных микроблогов канала появился твит Colin was here («Здесь был Колин»). Позже запись удалили. Представители канала заявили, что аккаунт был взломан, но доступ к нему восстановлен.

«Сирийская электронная армия», выступающая на стороне президента Сирии Б. Асада, отметилась взломом ряда популярных СМИ. Жертвами хакеров становились микроблоги Associated Press, Agence France-Presse, Би-би-си, «Аль-Джазиры» и других мировых изданий. Кроме того, в мае злоумышленникам удалось опубликовать несколько однотипных записей на сайте Financial Times.

Британская сеть Sky была образована в 1990 г. Ее клиентами по состоянию на лето 2012 г. являлись более 10 млн человек. Рыночная капитализация корпорации составляет около 12 млрд фунтов стерлингов (более 18 млрд дол.) ***(«Сирийская электронная армия» взломала приложения канала Sky для Android // InternetUA (http://internetua.com/siriiskaya-elektronnaya-armiya--vzlomala-prilojeniya-kanala-Sky-dlya-Android). – 2013. – 28.05).***

***

В понедельник, 27 мая, крупная телекоммуникационная компания XCom Global Inc. сообщила о том, что данные более 100 тыс. кредитных карт клиентов были похищены неизвестными злоумышленниками.

Представители компании сообщили, что хакерам удалось получить доступ к таким конфиденциальным данным, как имена владельцев кредитных карт, их номера, а также с информации о сроке их действия. Несмотря на то, что от клиентов XCom Global Inc. пока не поступало никаких жалоб, связанных с действиями преступников, компания настоятельно рекомендует им подать в банки запросы о блокировке карт ***(Хакеры похитили данные более ста тысяч***

кредитных карт клиентов компании XCom Global Inc. // InternetUA (http://internetua.com/hakeri-pohitili-dannie-bolee-sta-tisyacs-kreditnih-kart-klientov-kompanii-XCom-Global-Inc). – 2013. – 28.05).

***

Как взломать систему управления железной дорогой через Интернет и зачем охотникам за банкоматами тепловизоры? Почему уязвимы все мировые системы управления технологическими процессами и могут ли хакеры устроить настоящую техногенную катастрофу? В Москве прошла Международная хакерская конференция Positive Hack Days III.

Атаки на банкоматы

На PHD проходили конкурсы, доклады и мастер-классы по самому широкому кругу тем: скрытые возможности iOS и Andorid, атаки на систему SAP, взлом и вывод денег через интернет-банкинг, вскрытие реальных замков и многое другое.

Например, как устроен банкомат и как воруют данные чужих карт – подробную демонстрацию провела эксперт Positive Technologies О. Кочетова. Оказывается, помимо скиммеров (накладки на карто-приемники, которые незаметно считывают данные карт), существуют трэппинги – специальные ленты, которые задерживают карту внутри и позволяют ее вытащить, когда владелец отошел в сторону. То есть если карту клиента банкомат зажевал – это не обязательно означает, что аппарат неисправен.

Есть также кэш-трэппинги – это замаскированные ловушки, которые забирают деньги из отсека выдачи. Купюры, которые выдает банкомат, заворачиваются в маленький «карман», соответственно владелец карты, не знающий правил безопасности, денег не получает и уходит. Далее приходят мошенники, снимают свой кэш-трэппинг и забирают чужие средства. Скорее всего, такая схема может быть рассчитана только на невнимательных людей и едва ли может использоваться часто, но всегда нужно проявлять внимательность – читать информационные сообщения на экране банкомата и использовать смс-информирование обо всех операциях по карте.

Также наряду со скиммерами могут применяться шиммеры – это тончайшее электронные устройства (0,1–0,2 мм), которые преступник засовывает в картоприемник. Шиммер подключается к электронике банкомата и записывает данные вводимых карт. Определить шиммер в банкомате для рядового пользователя вообще невозможно, хоть он и не перехватывает пин-код.

Зато пин-код записывает накладная клавиатура или, например, тепловизор в руках мошенника, который подойдет к банкомату следом за жертвой и проверит, на каких кнопках осталось тепло пальцев. Чтобы сбить с толку возможных мошенников и их аппаратуру, эксперты советуют выбирать сумму, которую вы хотите получить, не на восьми кнопках вокруг экрана, а на клавиатуре вручную.

Тепловизор считывает пин-код

Советы: всегда нужно осматривать банкомат на предмет наличия нештатной аппаратуры, проверять нет ли на нем маленьких видео-камер и зеркал. Разумеется нельзя допускать, чтобы кто-то подсматривал пин-код. Ну, а если вы обнаружили скиммер или поддельную клавиатуру на банкомате, не пытайтесь их отломать – за банкоматом могут следить сами преступники, которые установили скиммеры, или спецслужбы, которые этих преступников ждут, – это может закончиться очень печально.

Угон поезда Choo Choo Pwn

Один из самых интересных конкурсов – захват системы управления железной дорогой. Системы, которые используются в ЖД-транспорте, по сути, такие же, как те, которые управляют технологическими процессами на предприятиях и любых критически-важных объектах (АСУ ТП). К интерфейсам таких систем можно зачастую подключиться в Интернете или через подключенные к ним внутренние сети, которые также могут иметь подключение через Интернет.

На форуме был представлен игрушечный макет железной дороги, но система управления реальная. Она позволяет управлять как поездом, так и элементами железной дороги – стрелки, шлагбаумы, грузовой кран для погрузки контейнеров. Задача хакеров – подключиться к системе, используя уязвимости промышленных протоколов, и обойти аутентификацию SCADA-систем и веб-интерфейсов промышленного оборудования. Далее – работу системы управления можно нарушить разными способами.

Эксперты Positive Technologies рассказали, что в реальной жизни нередко можно встретить компьютерные системы для контроля железнодорожного транспорта, напрямую подключенные к Интернету. То есть веб-интерфейс такой системы можно найти через Google, далее можно пройти различные уровни защиты (в первую очередь подобрать логин и пароль с помощью специальных программ) и перейти непосредственно к управлению железной дорогой. Более того, таким способом можно отправить управляющим компьютерам и диспетчеру ложные данные. Это может вызвать масштабный сбой оборудования или настоящую катастрофу. Такого рода атаки особенно опасны для подвижных составов, которые путешествуют полностью на автопилоте – без машинистов. Причем веб-интерфейсы российских железно-дорожных систем в России тоже можно найти в сети, говорят специалисты.

«Инженеры в первую очередь делают так, чтобы все работало, а вопросы безопасности – вторичны», – пояснил специальному корреспонденту «Вестей.Хайтек» эксперт Positive Technologies И. Карпов.

Техногенные кошмары SCADA

Подобные системы управляют не только движением поездов – от них зависит вся критически-важная инфраструктура, которая обеспечивает привычную жизнедеятельность современных стран. Это атомные и гидроэлектростанции, нефтяные и металлургические заводы, газопроводы, системы водопровода и канализации, метрополитены, системы распределения электроэнергии и многое другое.

О критических уязвимостях АСУ ТП в целом и в частности на форуме говорили много. «То, что системы SCADA не подключены к Интернету, это миф», – отметил замгендиректора Positive Technologies С. Гордейчик. Доступ в сеть они имеют главным образом для удобства обслуживания. В США, например, за работу разных критически-важных объектов отвечают сторонние сервисные компании. Промышленных компьютерных сетей с подключением к Интернету там очень много, но от нападения они защищены лучше, тогда как в России таких систем гораздо меньше, но и защищены они хуже.

Таким образом, если эти системы подключены к Интернету (напрямую или через офисные компьютерные сети), есть возможность их атаковать, внедрить вредоносный код и в конце концов перехватить управление или задать неверную обработку событий.

Статистика Positive Technologies об уязвимостях систем АСУ ТП такова:

• с 2010 г. в 20 раз возросло число обнаруженных уязвимостей;

• 50 % уязвимостей позволяют хакеру запустить выполнение кода;

• более 40 % интернет-доступных систем могут взломать хакеры-любители;

• треть доступных в Интернете систем находятся в США;

• уязвимы 54 % интернет-доступных систем в Европе, 39 % в США;

• уязвима каждая вторая система в России, имеющая выход в Интернет.

Дело не только в том, что эти системы подключены к Интернету, но и в том, что программное обеспечение, используемое сегодня в SCADA, разрабатывалось еще в 90-е годы, когда о вопросах безопасности мало кто задумывался. «В АСУ ТП нет ни одного компонента, которому можно доверять», – уверен главный архитектор ПО «Лаборатории Касперского» А. Духвалов.

О том, что атаки на SCADA вовсе не миф, можно судить по истории с червем Stuxnet, который в 2010 г. сбил управление урановыми центрифугами на ядерных объектах в Иране.

Другой интересный пример – в 2011 г. весь мир облетела новость о том, что русские хакеры сломали канализацию в Иллинойсе. Со ссылкой на Антитеррористический разведывательный центр штата Иллинойс газеты сообщили, что некие злоумышленники из России вошли в компьютерную SCADA-систему, управлявшую водонасосной станцией, и вывели ее из строя. Как доказательство – российский IP-адрес, отобразившийся в логах системы управления.

Вскоре выяснилось, что инженер компании, обслуживающей компьютерную систему водонасосной станции, находился в отпуске в России и со своего смартфона зашел в систему через веб-интерфейс, чтобы произвести какие-то настройки. Соответственно, станция сломалась по другим причинам, но русский IP-адрес остался, и это многое объясняет.

Разумеется, проблема актуальна не только для Ирана и США, но и для всего мира. И заключается она не только в том, что отсутствует нормальная защита. Важную роль играет и человеческий фактор – компьютеры для

управления техническими процессами работники повсеместно используют для интернет-серфинга, а также вставляют в них флэшки. Это уже создает большую угрозу.

Уязвимости в системах SCADA открывают возможности не только для атак, но и для мошенничества штатного персонала. Например, сотрудники АЗС могут в свою пользу менять данные и логику подсчетов в кассовых и топливораздаточных аппаратах, обсчитывая клиента или свою компанию, рассказал С. Гордейчик.

На форуме приводилась также статистика о том, что на первом месте по количество компьютерных инцидентов объекты ТЭК, на втором – объекты водоснабжения, на третьем – пищевая промышленность, а на четвертом – металлургия.

Все эксперты сходятся во мнении, что для безопасности жизнедеятельности общества нужна иная операционная система, которая будет работать только по заранее заданным сценариям ***(«Пальчики и цифры» – поезд под откос. Что могут хакеры // InternetUA (http://internetua.com/palcsiki-i-cifri----poezd-pod-otkos--cto-mogut-hakeri). – 2013. – 28.05).***

***

Во «ВКонтакте» обнаружены случаи, когда из-за неправильного использования одной из функций пользователи открывают всем желающим доступ к своим аккаунтам в соцсети и на сторонних ресурсах. Об этом сообщило 28 мая издание «Цукерберг позвонит».

Речь идет об использовании адресов электронной почты вида ***@post.vk.com, выданных пользователям соцсетью «ВКонтакте». Такие адреса используются для публикации новостей: любое электронное письмо, отправленное на эту почту, появляется на странице пользователя. По всей видимости, несанкционированный доступ к аккаунтам открывается в случае, когда сам пользователь использует полученный от «ВКонтакте» адрес для регистрации на сторонних ресурсах.

Рассылки от сторонних сайтов зачастую содержат уникальные ссылки, перейдя по которым, можно получить прямой доступ к соответствующему аккаунту или определенным настройкам. Отправленные на почту @post.vk.com, такие письма появляются на странице пользователя во «ВКонтакте» и оказываются доступны как во внутреннем поиске соцсети, так и в поиске «Яндекса» по блогам (в последнем случае сохраняется текст даже удаленных записей).

Под угрозу, отмечает издание, попали рассылки соцсети Facebook, игры World Of Tanks, купонных сайтов Biglion и Kupikupon.ru и других ресурсов. В компании KupiVIP, указавшей на уязвимость, решили приостановить рассылку и уничтожить старые адреса, пишет «Цукерберг позвонит».

Письма от сторонних ресурсов, автоматически появляющиеся во «ВКонтакте», также содержат адреса электронной почты самих пользователей. Благодаря этому злоумышленники могут несанкционированно публиковать

записи и на «стенах» пользователей во «ВКонтакте», отправляя электронные письма на такие адреса. При этом сам аккаунт остается в руках владельца.

Электронная почта является одним из официальных способов публикации новостей и фотографий во «ВКонтакте». В настройках пользователь может запросить уникальный адрес, который придет ему по SMS. В случае утечки он может запросить там же новый адрес. При этом остается неясным, по какой причине пользователи оставляли эти адреса на сторонних ресурсах ***(Электронная почта поставила под угрозу безопасность пользователей «ВКонтакте» // InternetUA (http://internetua.com/elektronnaya-pocsta-postavila-pod-ugrozu-bezopasnost-polzovatelei--vkontakte). – 2013. – 28.05).***

***

Министерство культуры России представило обновленную версию антипиратских поправок к законодательству 28 мая на заседании специальной рабочей группы в Госдуме России, пишет издание «Обозреватель» (http://tech.obozrevatel.com/news/23048-v-rossii-hotyat-shtrafovat-torrent-polzovatelej.htm).

Так, Минкультуры предложило ввести в Закон «Об информации, информационных технологиях и защите информации» определение «пользователя файлообменной сети». Они должны будут вместе с владельцами сайтов и хостинг-провайдерами нести ответственность за распространение пиратского контента.

Происходить это будет так: правообладатель направляет оператору связи заявление с указанием IP-адреса пользователя файлообменной сети, нарушающего авторские или смежные права. Оператор в свою очередь обязан в течение суток перенаправить его самому пользователю и уведомить того о необходимости удалить информацию либо блокировать доступ к ней (речь идет о контенте, размещенном именно на торренте).

В противном случае ему грозит административная ответственность наравне с владельцами сайтов и провайдерами, проигнорировавшими обращения правообладателей: 5 тыс. руб. (1 тыс. 250 грн) – для граждан, 50 тыс. руб. (12 тыс. 500 грн) – для должностных лиц и предпринимателей и 1 млн руб. (250 тыс. грн) – для юридических лиц. Если пользователь не принимает мер в течение суток, у оператора связи есть 12 часов, чтобы самостоятельно удалить информацию или блокировать доступ к ней.

Владельцев сайтов в свою очередь предлагается обязать самостоятельно отслеживать легальность размещенного контента. Для этого им придется сверяться с государственной информационной системой в области интеллектуальной собственности, на создание которой Минкультуры предлагает уполномочить один из федеральных органов власти.

При этом специалисты Российской ассоциации электронных коммуникаций считают, что проект выдвигает к операторам связи и владельцам сайтов невыполнимые требования, являясь лишь попыткой одного бизнеса решить свои проблемы за счет другого ***(В России хотят штрафовать***

торрент-пользователей // Обозреватель (http://tech.obozrevatel.com/news/23048-v-rossii-hotyat-shtrafovat-torrent-polzovatelej.htm). – 2013. – 29.05).

***

Атаки хакеров на социальные сети и СМИ – главные события в сфере IT-безопасности в I квартале 2013 г., свидетельствуют данные отчета антивирусной лаборатории PandaLabs компании Panda Security, производителя «облачных» решений безопасности.

По данным отчета, в феврале сервис микроблогов Twitter стал жертвой атаки, в результате которой хакеры получили доступ к данным более 250 тыс. пользователей. Спустя пару недель стало известно, что система социальной сети Facebook была подвержена сложной атаке, в результате которой данные пользователей не пострадали.

Газета The New York Times в конце января поместила на первой полосе статью о том, как они стали жертвами атаки, в результате которой китайские хакеры получили доступ к их компьютерам. Спустя один день The Wall Street Journal заявила, что она также стала жертвой подобной атаки со стороны китайских хакеров. В обоих случаях хакеры сумели получить доступ ко всем типам данных, но при этом сфокусировались только на получении информации о журналистах и сотрудниках, отмечается в исследовании.

Через некоторое время другой американский медиа-гигант The Washington Post заявил, что они сталкивались с подобной атакой в 2011 г., которая была проведена, предположительно, также из Китая.

По словам Л. Корронса, технического директора PandaLabs, многие страны подозрительно смотрят на Китай, подозревая его в организации атак на крупные организации и общественные институты во всем мире. «Доказать, кто реально стоит за каждой атакой, представляется крайне сложным, даже в случаях с простыми кибер-преступлениями. В течение последних нескольких лет люди обращают свое внимание на Китай в тех случаях, когда происходят подобного рода инциденты, но при этом нет каких-либо реальных доказательств того, что правительство Китая стоит за этими атаками», – отметил Л. Корронс ***(Главные цели хакеров в I квартале 2013 года – социальные сети и СМИ // InternetUA (http://internetua.com/glavnie-celi-hakerov-v-I-kvartale-2013-goda---socialnie-seti-i-smi). – 2013. – 30.05).***

***

Адміністратори Facebook-сторінок, будьте уважні: повідомлення нібито від служби безпеки соціальної мережі з інструкціями як підтвердити свої права на сторінку є фішингом.

Фішингове повідомлення від Facebook Security запевняє, що соціальна мережа запустила нову опцію безпеки Fan Page Verification Program. Мовляв, багато сторінок крадуть і нам доводиться їх видаляти, а ваша сторінка має багато лайків ы якісний контент і «підходить» для цієї програми. Щоб

завершити процес, адміністраторам пропонують обрати 10-значне число – «код безпеки». Цей код безпеки нібито має стати паролем при зміні важливих налаштувань сторінки – ролей адміністраторів або «інших важливих налаштувань».

І якщо не завершити цей процес до 30 травня, обіцяють зловмисники, сторінку заблокують назавжди. І нижче – лінк, за яким потрібно пройти всі фішингові процедури. Тобто ввести в тому числі свій логін (електронну пошту) і пароль.

Коли адміністратор сторінки відправляє ці дані, зловмисники йому дякують і запевняють, що все пройшло успішно – треба лише зачекати на підтвердження протягом 24 годин:

Таким чином, зловмисники мають 24 години для того, щоб неквапляючись заволодіти акаунтом такого адміністратора – й отримати доступ до всіх його сторінок. Нагадаємо, у Facebook немає Fan Page Verification Program – якщо ви отримали таке повідомлення, не клікайте на посилання і, тим більше, не вказуйте жодних своїх даних ***(Увага, у Facebook немає «Fan Page Verification Program», це фішинг // UkrainianWatcher (http://watcher.com.ua/2013/05/30/uvaha-u-facebook-nemaye-fan-page-verification-program-tse-fishynh/). – 2013. – 30.05).***

***

Подростки доверяют соцсетям все больше личных данных

Несмотря на то, что тема защищенности личных данных в социальных сетях по-прежнему обсуждается очень широко, последние статистические исследования показывают, что молодежь в последнее время довольно легкомысленно подходит к этому вопросу.

На протяжении последних нескольких лет социальные сети (особенно Facebook в мире в целом и «ВКонтакте» на территории России и стран ближнего зарубежья) прочно вошли в повседневную жизнь практически всех обладателей настольных компьютеров и мобильных устройств. Недавнее исследование американской аналитической компании Pew Research Center показало, что молодежь 12–17 лет все больше доверяет социальным сетям личную информацию.

Так, большинство респондентов не считает нужным выставлять настройки приватности, не видя ничего зазорного в том, чтобы транслировать свой поток мыслей всему миру. Лишь 24 % пользователей Twitter ставят замок на свои записи. В целом всего 9 % опрошенных пользователей серьезно озабочены безопасностью своих данных в сети. Более трети респондентов не задумывается об этом, а еще 22 % не имеют какого-либо определенного мнения на этот счет. 92 % пользователей зарегистрированы в соцсетях под своим настоящим именем, 84 % указывают свои истинные интересы, 82 % – свою настоящую дату рождения, 62 % – свой актуальный статус в отношениях.

Все эти данные, собранные вместе, помогают создать практически полный портрет человека. Исходя из результатов проведенного исследования становится ясно, что юные пользователи не сильно заботятся о собственной

приватности в социальных сетях. Подростков скорее волнует образ, который их сверстники могут создать, исходя из вводных данных предоставленных самими пользователями, нежели надежное сохранение личной информации ***(Подростки доверяют соцсетям все больше личных данных // InternetUA (http://internetua.com/podrostki-doveryauat-socsetyam-vse-bolshe-licsnih-dannih). – 2013. – 1.06).***

***

Атаки вредоносов могут распространяться через датчики мобильных устройств.

Группа ученых университета Алабамы в Бирмингеме (США) описала новое поколение вредоносных атак, поражающих мобильные устройства: образцы вредоносов могут распространяться через датчики аппаратов, причем быстро. Это не первое исследование такого рода. В 2012 г. Ч. Миллер показал, что заражение может происходить через чипы NFC. Но, как выяснилось, NFC – не единственные ворота для инфекций.

В теории атака нового типа может использовать разные датчики (оптические, магнитные и даже микрофон), т. е. каналы, которые позволяют охватить сразу множество устройств. И, в отличие от обычных вредоносов, новые не удастся отловить во время мониторинга систем коммуникаций, т. е. обычными инструментами безопасности.

На практике вредоносное ПО, распространяемое через сенсоры, можно использовать для создания локальных ботнетов и проводить с их помощью DDoS-атаки. Кроме того, инфицированные устройства особенно уязвимы для целевых атак и постоянных сложных угроз (advanced persistent threat, APT) ***(Атаки вредоносов могут распространяться через датчики мобильных устройств // Firefoxsoft (http://firefoxsoft.ru/stati/bezopasnost-os/ataki-vredonosov-mogut-rasprostranjatsja-cherez-datchiki-mobilnyh-ustroistv.html). – 2013. – 31.05).***

***

Украина – заповедник кибер-преступников.

Отсутствие профильного законодательства и пассивность органов власти превратили Украину в рай для кибер-преступников. Такое мнение выразили представители бизнес-структур и ИКТ-общественности во время проведения круглого стола на тему «Кибер-угрозы для Украины в глобализированном мире». Мероприятие было организовано Ассоциацией «IT-Украины».

Власть и ИКТ

Несмотря на стремительные темпы развития высоких технологий в мире и не менее активное их внедрение на территории Украины, в сознании представителей власти слово «кибер-преступность» звучит как выдумка из футуристического кинофильма. Чиновникам не совсем понятно, как эту выдумку необходимо интерпретировать в реальном мире и для чего искать ей место в украинском законодательстве.

В последнее время урегулирование проблемы роста кибер-преступлений на территории Украины стало одним из главных требований не только мирового политикума, но и отечественных бизнес-структур. Ведь в реальном мире кибер-атаки парализуют деятельность серьезных фирм, электронных СМИ, а украинцы теряют деньги, благодаря различным мошенническим схемам.

Несмотря на более чем 20-летний законодательный опыт и сверхвысокие темпы развития Интернета, в Украине все еще отсутствует законодательная база, отдельно определяющая понятие «кибер-преступление». Весной 2012 г. Кабинетом Министров Украины принято Распоряжение «Об утверждении плана мероприятий по выполнению в 2012 г. общегосударственной программы адаптации законодательства Украины к законодательству Европейского Союза» № 156-р. В соответствии с п. 10 Распоряжения, до сентября 2012 г. должен быть разработан проект закона Украины «О борьбе с кибер-преступностью». Основой нового закона должна стать Конвенция Совета Европы о кибер-преступности.

12 марта 2012 г. Кабинет Министров Украины одобрил законопроект № 2483, направленный на борьбу с кибер-преступлениями. К списку преступлений, составляющих угрозу национальной безопасности, власть предлагает отнести несанкционированное вмешательство в работу государственных информационных ресурсов, пропаганду в Интернете культа насилия, жестокости, порнографии и сепаратизма. «Обсуждение изменений к Закону длится уже не первый год, и было определенно, что нужно начать с трактовки используемых терминов, таких как “кибер-пространство” и “кибернетическая безопасность”. Законопроект был согласован во многих ведомствах, в том числе,Министерстве юстиции Украины, однако принят не был», – сообщил начальник управления по борьбе с кибер-преступностью МВД Украины М. Литвинов.

На сегодняшний день в Украине кибер-преступлениями считаются преступления против информационной безопасности (предусмотрены разд. 16 Уголовного кодекса Украины), преступления в сфере использования платежных карт, преступления в сфере телекоммуникаций общеуголовного характера (мошенничество, распространение наркотиков, оружия при помощи телекоммуникационных технологий и т. д.), преступления в сфере оборота противоправного контента и преступления в сфере хозяйственной деятельности и электронной коммерции (игровой бизнес, нелегальная деятельность финансовых пирамид, продажа нелицензированной программной продукции и т. д. «Украинское законодательство на сегодняшний день требует модернизации с учетом общих темпов развития современных технологий. В Украине до сих пор не криминализированы некоторые противоправные деяния, которые в цивилизованном мире уже много лет регулируются законодательством о кибер-преступлениях», – отмечает юрист компании Arzinger О. Баранова.

Сами чиновники, ответственные за кибер-безопасность Украины, помнят об отсутствии «концептуальной базы» и несоответствии УПК конвенциям о кибер-безопасности. «Рост количества политически-мотивированных кибер-атак, как и общая уязвимость украинского информационно-коммуникационного пространства, говорят о том, что Украина сегодня нуждается в целостной и комплексной стратегии кибернетической безопасности», – сообщил руководитель отдела по вопросам безопасности в информационной среде СНБО Г. Корниенко.

Кроме этого, чиновники из МВД и СБУ имеют представление и о масштабах проблемы. «Несмотря на значительное отставание в экономическом развитии, Украина стала одним из центров международной кибер-преступности», – проинформировал начальник отдела департамента контрразведывательной защиты интересов государства в сфере информационной безопасности СБУ Е. Зайцев. Вместе с тем представитель СБУ добавил, что благодаря работе его ведомства Украина уже не является «раем для хакеров». «Интернет-СМИ неоднократно обнародовали недостоверную информацию относительного того, кто и как защищает украинское кибер-пространство. За прошлый год мы обезвредили пять больших группировок, действовавших на территории Украины. Большинство из правонарушителей – это граждане Украины, которые могли бы работать легально и получать копейки с аутсорсинговых проектов. Для многих из этих айтишников нарушение закона было едва ли не единственным способом заработать деньги на территории Украины, исходя из своих умений», – добавил Е. Зайцев. Интересно, сколько же зарабатывает чиновник, оценивающий заработок украинских программистов категорией «копейки»?

В это же время СМИ пестрят сообщениями о том, как силовые структуры «воюют» с украинской кибер-преступностью. В большинстве случаев эта «война» заканчивается закрытием таких сайтов, как EX.ua – по обвинению в распространении контрафактной продукции, erio.com.ua – якобы распространение порнографии. Иногда борьба за соблюдение закона в виртуальном пространстве доходит даже до изъятия серверов у местных провайдеров без каких-либо объяснений.

Вместе с тем МВД периодически придумывает законодательные решения тому, как обеспечить себе пожизненную бездеятельность. Совсем недавно чиновники пытались протолкнуть законопроект, предлагающий внести изменения в ст. 39 Закона Украины «О телекоммуникациях», обязующий провайдеров устанавливать у себя системы оперативно-розыскных мероприятий с целью контроля над деятельностью пользователей. Необходимые технические средства силовики предлагают закупать за счет операторов и провайдеров телекоммуникационных услуг.

«В Украине нет общей стратегии защиты кибер-пространства, которой руководствовались бы госорганы. До сих пор не совсем понятно, какими вопросами из сферы кибер-безопасности занимается СБУ, какими МВД, а какими Государственная служба специальной связи и защиты информации.

Последняя, складывается впечатление, существует только формально», – говорит эксперт компании BMS Consulting Д. Петращук. «Вместе с тем высокий интеллектуальный потенциал украинских IT-специалистов и сложности их занятости в законных рамках создают благоприятную почву для процветания кибер-преступности», – добавил эксперт.

Следует отметить, что «сложности с занятостью» айтишников целенаправленно создаются самой властью. Напомним, недавно правительство Украины поддержало предложение Министерства социальной политики изменить законодательство, чтобы урегулировать ситуацию на рынке аутсорсинга. В случае принятия закона Верховной Радой, компании смогут привлекать аутсорсеров только при наличии соответствующего разрешения.

Страна и бизнес под прицелом кибер-преступников

«В сегодняшней ситуации от кибер-атак общенационального масштаба Украину защищает только отставание в темпах информатизации. Сегодня даже мировое кибер-пространство – это Дикий Запад. В будущем это пространство может стать главной ареной для международных войн. Важно, чтобы в этом будущем Украина имела свое кибер-оружие. Для этого нужно стимулировать развитие национального производителя программной продукции», – говорит глава отдела исследований информационного общества и информационных стратегий Национального института стратегических исследований при Президенте Украины Д. Дубов.

Эксперты отмечают, что сегодня не только государство не понимает масштабов кибер-угроз. Представители бизнес-структур также часто остаются пассивными в отношении выявления и предупреждения кибер-атак. «Латентность потерпевших от кибер-преступлений является одной из главных причин процветания кибер-преступности. К примеру, финансовые учреждения часто классифицируют кибер-преступления как сбои в работе программного обеспечения», – сообщила юрист компании Arzinger О. Баранова.

Эксперт компании BMS Consulting А. Лысюк отмечает, что сегодня самыми распространенными типами кибер-атак являются кража конфиденциальной информации, атаки на финансовые учреждения и правительственные организации. «В большинстве случаев от начала атаки до ее выявления проходит семь–восемь месяцев. На протяжении этого времени преступник может безнаказанно пользоваться секретной информацией или переводить средства со счетов клиентов компании», – добавил эксперт.

Ранее мы отмечали, что в этом году следует ожидать роста числа атак, целью которых будут лица или организации, отстаивающие определенные политические, религиозные и т. д. взгляды, определяющие сторону в том или ином социально-политическом конфликте. Охотиться за персональными данными пользователей будет мобильное рекламное программное обеспечение (madware, mobile advertising software). Эта безобидная вещь может не только сильно помешать процессу использования устройства, но и выдать злоумышленникам детали вашего местоположения, контактные данные, а также идентификационные данные устройства. Новые угрозы принесет также и

монетизация социальных сетей. Опасность монетизации соцсетей заключается и в том, что такая тенденция связана с огромным количеством маленьких по объему, но весьма рискованных транзакций. Дополнительный риск возникает и в случае привязки банковских карт или иных платежных данных к учетной записи пользователя. Но главной целью злоумышленников в 2013 г. станут облачные и мобильные платформы. Об этом говорит стремительный рост числа вредоносных программ для ОС Android в 2012 г. Некоторые вредоносные мобильные программы не будут выходить за рамки уже существующих угроз. Например, это может быть все та же кража персональных данных ***(Украина – заповедник киберпреступников // InternetUA (http://internetua.com/ukraina--zapovednik-kiberprestupnikov). – 2013. – 31.05).***

***

Держслужба інтелектуальної власності підготувала законопроект «Про захист авторських і суміжних прав в Інтернеті». 2 червня 2013 р. документ був опублікований для громадського обговорення на сайті Міністерства освіти і науки.

Ініціатива відомства спрямована на боротьбу із зростанням рівня піратства в мережі, ідеться в аналізі його регуляторного впливу. Нинішні норми Закону України «Про авторські та суміжні права» діють ще з 2001 р. і не дозволяють ефективно захищати інтелектуальну власність в Інтернеті, наголошується в документі, пише «Коммерсантъ Украина».

Законопроект пропонує правовласникам звертатися зі скаргою на піратські сайти в Держслужбу інтелектуальної власності. При зверненні заявнику необхідно буде надати копії реєстраційних документів, нотаріально завірені копії договорів, що підтверджують його авторські або суміжні права, перелік піратських файлів, розміщених в Інтернеті, а також завірені переклади документів, якщо вони випущені на іноземних мовах.

Одночасно правовласник повинен буде звернутися до хостинг-провайдера, на потужностях якого розміщений піратський контент. Останній у свою чергу буде зобов’язаний у дводенний термін повідомити адміністрацію ресурсу про скаргу.

Держслужбі інтелектуальної власності надається 10 днів на розгляд звернення правовласника – за цей період вона зобов’язана визначити, чи законно розміщений контент, а також опублікувати на своєму сайті перелік адрес, за якими розміщена піратська продукція. Після публікації у адміністрації ресурсу-порушника є два тижні, щоб надати відомству документи, що підтверджують законність розміщення.

Після отримання цих документів Держслужба протягом 10 днів буде зобов’язана прийняти остаточне рішення про те, чи має місце порушення авторських або суміжних прав, а потім надіслати рішення заявнику, адміністрації ресурсу і хостинг-провайдеру.

Новий законопроект набагато ліберальніший щодо інтернет-ресурсів та хостинг-провайдерів, ніж попередня ініціатива держслужби.

«Новий законопроект почали розробляти в лютому, після того як на адресу України посипалися перші звинувачення від правовласників. Ця ініціатива – наш аргумент на користь того, що прогрес у боротьбі з піратами є», – сказало джерело в Держслужбі інтелектуальної власності.

Утім, правовласники називають ініціативу відомства занадто бюрократизованою. «Запропонований метод роботи ще менш ефективний, ніж звернення до суду, – вважає директор юрфірми «Виндекс» (представляє інтереси розробників ПЗ Adobe Systems, Graphisoft, Nav N Go, медіа груп «1+1», StarLightMedia,» Медіа Група Україна» та НТКУ) П. Миколюк. – Великі мейджори просто не стануть збирати весь пакет документів і переводити договори про авторські права на кожну пісню». Він називає терміни розгляду питання держслужбою надмірно затягнутими, а плату за розгляд заяв – необгрунтованою. «До того ж офіційна процедура на практиці може призвести до того, що ті деякі ресурси, які зараз добровільно видаляють піратський контент за заявою правовласників, перестануть робити це без вказівки держоргану», – говорить юрист.

Хостинг-провайдери вважають, що виконати вимоги законопроекту практично неможливо.

«Для того щоб перекривати доступ до кожного конкретного файлу, потрібні додаткові технічні та людські ресурси, навряд чи хтось піде на це, а значить, доступ перекриватимуть до всього сайту, – пояснює президент компанії «Інтернет Інвест» (володіє найбільшим у країні доменним реєстратором imena.ua і хостингової компанією MiroHost) О. Ольшанський. – Таким чином, несудові скарги на піратський контент можуть стати новим інструментом боротьби з конкурентами в Інтернеті, що викличе масовий відплив клієнтів у зарубіжні дата-центри» ***(Держслужба інтелектуальної власності пропонує новий спосіб боротьби з піратством // Західна інформаційна корпорація (http://zik.ua/ua/news/2013/06/04/412208). – 2013. – 4.06).***

***

Выявлена кибершпионская сеть, атаковавшая за 10 лет 40 стран.

Эксперты антивирусной компании «Лаборатория Касперского» выявили кибершпионскую сеть, получившую название NetTraveler и затронувшую более 350 компьютерных систем в 40 странах мира, сообщает Обозреватель (http://tech.obozrevatel.com/science/97345-vyiyavlena-kibershpionskaya-set-atakovavshaya-za-desyat-let-sorok-stran.htm).

Атаке подверглись государственные и частные структуры, в том числе правительственные учреждения, посольства, научно-исследовательские центры, военные организации, компании нефтегазового сектора, пишет РИА Новости.

В десятку наиболее пострадавших стран в порядке убывания вошли: Монголия, Россия, Индия, Казахстан, Киргизия, Китай, Таджикистан, Южная Корея, Испания и Германия.

Кампания шпионажа стартовала в 2004 г., но пик ее пришелся на период с 2010 по 2013 г. В последнее время в сферу интересов атакующих входили такие отрасли, как освоение космоса, нанотехнологии, энергетика, в том числе ядерная, медицина и телекоммуникации.

Заражение компьютеров жертв происходило при помощи электронных писем с вредоносными вложениями, использующими уязвимости в Microsoft Office. Компания Microsoft уже выпустила обновления для закрытия этих уязвимостей, но они все еще часто используются для таргетированных атак, полагают эксперты.

В процессе расследования эксперты «Лаборатории Касперского» получили журналы доступа с нескольких командно-контрольных серверов NetTraveler, через которые осуществлялась установка дополнительного вредоносного ПО на зараженные машины и загружались украденные данные.

Объем похищенных данных на всех серверах NetTraveler составляет более 22 Гб. Среди них чаще всего встречаются списки системных файлов, записи нажатий клавиш и различные типы документов ***(Выявлена кибершпионская сеть, атаковавшая за десять лет сорок стран // Обозреватель (http://tech.obozrevatel.com/science/97345-vyiyavlena-kibershpionskaya-set-atakovavshaya-za-desyat-let-sorok-stran.htm). – 2013. – 4.06).***

***

Microsoft: хакерская сеть, похитившая в США 500 млн дол., базируется в Украине.

Компания Microsoft и агенты ФБР, а также представители властей 80 стран приступили к совместному расследованию в отношении хакерской сети Citadel Botnets, предположительно, похитившей около 500 млн дол. с банковских счетов по всему миру, пишет «Обозреватель» (http://tech.obozrevatel.com/news/03748-microsoft-hakerskaya-set-pohitivshaya-v-ssha-500-mln-baziruetsya-v-ukraine.htm).

Специальное подразделение Microsoft уже обезвредило свыше тысячи вредоносных бот-сетей, инфицировавших около 5 млн компьютеров. В США атаки совершались на банки, в числе которых Bank of America, Citigroup, JPMorgan Chase и др. По данным корпорации, активными остаются еще 400 вирусных сетей.

В Microsoft полагают, что киберпреступники могут базироваться в России или Украине, так как в этих странах не фиксировалась вирусная активность. Пока специалистам не удалось выяснить имена лидеров группировки, «однако существенный удар по технологиям уже нанесен», сообщили в компании.

Citadel Botnets является своеобразной платной «социальной сетью» для хакеров. На данной площадке анонимные пользователи могут обмениваться сообщениями, голосовать за новые идеи, предлагать свою стоимость определенной разработки или усовершенствования нового хакерского модуля.

Сеть активно действует в США, Европе, Австралии, Индии, Гонконге ***(Microsoft: хакерская сеть, похитившая в США 500 млн дол., базируется в Украине // Обозреватель (http://tech.obozrevatel.com/news/03748-microsoft-hakerskaya-set-pohitivshaya-v-ssha-500-mln-baziruetsya-v-ukraine.htm). – 2013. – 6.06).***

***

Anonymous атаковали сайт премьер-министра Турции.

Глобальное хакерское объединение Anonymous совершила в среду массированную хакерскую атаку на официальный сайт премьер-министра Турции (http://tech.obozrevatel.com/news/86547-anonymous-polozhili-sajt-premer-ministra-turtsii.htm).

Сайт www.basbakanlik.gov.tr в настоящее время не открывается.

Как сообщается ehackingnews, данные, размещенные на сервере правительства, оказались под угрозой.

«Турецкое сопротивление в стамбульском парке Гези является одним из самых благородных общественных восстаний в новейшей истории. Турецкий народ – женщины, дети, молодежь и старики, давно угнетаемые всемогущим режимом, сегодня проснулись. Страх перешел на другую сторону: Турецкий народ больше не боится, а вот его угнетатели наоборот», – говорится в пресс-релизе Anonymous.

Ранее хакеры уже проводили серию атак. 2 июня 2013 г. были заблокированы сайты ряда провластных турецких СМИ в ответ на применение жестких методов против протестующих в стамбульском парке Гези.

В видеообращении, размещённом в YouTube, Anonymous провозгласили войну турецкому правительству ***(Anonymous атаковали сайт премьер-министра Турции // Обозреватель (http://tech.obozrevatel.com/news/86547-anonymous-polozhili-sajt-premer-ministra-turtsii.htm). – 2013. – 5.06).***

***

Хакеры взломали сайт Министерства образования Крыма.

На странице сайта размещены призывы освободить от «тиранов» Сирию, Чечню и Палестину.

Со вчерашнего вечера сайт Министерства образования Крыма не работает. На сегодня на его главной странице размещена англоязычная надпись No God But Allah And Mohammad Peace Be Upon Him He is Messenger of Allah, что в переводе означает «Нет Бога, кроме Аллаха, и Мухаммед, да благословит его Аллах – Пророк Его».

Отметим, что эта фраза – шахада, первый из столпов Ислама. Тот, кто ее произносит, таким образом «заявляет» о своей вере в Аллаха и посланническую миссию пророка Мухаммада.

Также на взломанной странице сайта размещены призывы освободить от «тиранов» Сирию, Чечню и Палестину. Также на сайте размещены проклятия в адрес христиан Fuck U’Re Cross.

Ответственность за взлом сайта взяла на себя хакерская группировка TeaM omarXarmy ***(Хакеры взломали сайт Министерства образования Крыма // Право на правду (http://www.pravo-kiev.com/events/hakery-vzlomali-sajt-ministerstva-obrazovaniya-kry-ma). – 2013. – 7.06).***

***

Обнаружен троян, который похищает финансовые данные пользователей.

Вредоносная программа устанавливается на устройство, после чего работает в фоновом режиме.

Согласно данным Daily Mail, экспертам по ИБ удалось обнаружить новую вредоносную программу, распространяемую через соцсеть Facebook. Данный троян похищает финансовые данные пользователей.

Как утверждают специалисты, вредоносная программа устанавливается на устройство после того, как пользователь проходит по вредоносной ссылке. Затем троян работает в фоновом режиме. На текущий момент ИБ-эксперты утверждают, что все ссылки были удалены.

После инсталляции вирус начинает отслеживать действия пользователя и перехватывать любые данные, введенные в системах интернет-банкинга, онлайн-магазинах и пр. Собранная информация перенаправляется злоумышленникам, которые получают возможность незаконно снимать денежные средства со счетов своих жертв.

Представитель Facebook заявил, что сайт исследуется на наличие вредоносного ПО и предлагает различные варианты систем безопасности, такие как сканирование и исправление зловредных программ на мобильных устройствах.

Отметим, что это не первый случай обнаружения вредоносного ПО в Facebook. Среди вирусов, атаковавших соцсеть, ИБ-эксперты устраняли троян ZeuS, главной целью которого также была кража данных об учетных записях пользователей ***(Обнаружен троян, который похищает финансовые данные пользователей // InternetUA (http://internetua.com/obnarujen-troyan--kotorii-pohisxaet-finansovie-dannie-polzovatelei). – 2013. – 7.06).***

***

Хакеры рассказали о простом способе «взламывать» самые сложные пароли.

Во время эксперимента, проводимого на известном IT-ресурсе Ars Technica, хакерам удалось взломать 90 % из предложенных 16 449 случайных паролей, при этом каждую минуту взламывалось примерно шесть пассвордов.

Таким образом, команде хакеров удалось взломать 14 800 паролей, большинство из которых оказались простыми и без труда были «отгаданы» вычислительным кластером, однако встречались и так называемые сложные пароли, состоящие из 16 символов, использующих как цифры, так и буквы, такие как qeadzcwrsfxv1331, но и на них взломщикам потребовалось не больше часа.

Хакеры из Ars Technica рассказали, пишет factroom, как им удалось достичь такого результата: они не подбирали никаких комбинаций, а всего лишь скачали в сети список хеш-паролей.

Хеширование – это преобразование информации посредством определённого математического алгоритма в битовую строку. На практике это выглядит так: вы вводите пароль в специальную форму на сайте, система вносит его в хеш, предварительно зашифровав; когда вы вновь пытаетесь авторизоваться на данном ресурсе, система обращается к хеш-коду и, если введённые вами данные совпадают с данными, хранящимися в нём, вы входите на сайт.

Многие эксперты в области компьютерной безопасности полагали, что хеш-коды не представляют опасности, так как информация в них зашифрована, и получить к ней доступ не так-то просто. Однако, как показывает этот эксперимент, нет ничего невозможного ***(Хакеры рассказали о простом способе «взламывать» самые сложные пароли // СумыИнфо (http://sumyinfo.com/society/208-hakery-rasskazali-o-prostom-sposobe-vzlamyvat-samye-slozhnye-paroli.html). – 2013. – 4.06).***

***

Хакеры научили телевизоры добывать BitCoin.

Используя уязвимость в телеприёмниках Hybrid Broadcast Broadband TV, с помощью которой можно получить несанкционированный доступ в удаленном режиме, хакеры смогли превратить их систему по добыче виртуальной валюты BitCoin, сообщает Блог Imena.UA.

Следует отметить, что телеприёмники HbbTV установлены у 20 млн пользователей в Европе. Устройства загружают содержимое по Интернету, так что постоянно находятся в онлайне. В ходе тестирования на целой линейке телевизоров от Samsung стало ясно, что система уязвима сразу для нескольких типов атак – в том числе внедрения управляющих команд и перенаправления запросов с цифровой приставки на сервера, контролируемые злоумышленником.

Принимая во внимание, что хакер может направить запросы к контролируемому источнику, на инфицированном телевизоре становится возможно запустить программу, добывающую виртуальную валюту BitCoin.

С BitCoin не всё так просто...

Реализация программы для добывания виртуальных монет на Java (требует jre и WebStart), предусматривает внедрение кода на любую страницу. Таким образом, каждый посетитель инфицированной страницы будет добывать монеты в фоновом режиме, пока у него открыта соответствующая страница в браузере.

Принимая во внимание количество пользователей телеприёмников Hybrid Broadcast Broadband TV, хакеры могут заработать за чужой счёт кругленькую сумму. К тому же, размещённые таким образом программы чрезвычайно

непросто обнаружить ***(Хакеры научили телевизоры добывать BitCoin // Блог Imena.UA (http://www.imena.ua/blog/bitcoin-tv). – 2013. – 7.06).***

***

«Маки» подверглись атаке первого «настоящего» вируса.

Специалисты по информационной безопасности говорят о выявлении новой концептуальной атаки, направленной на компрометацию операционной системы Mac OS X. Новый вредоносный код под названием Clampzok.A представляет собой кросс-платформенный пакет, который размещает соответствующие операционной системе двоичные файлы. Эти файлы при исполнении в файловой системе поражают расположенные рядом двоичные файлы.

Вредоносное ПО было написано на ассемблере и изначально представлено еще в 2006 г. для операционных систем Windows и Linux, но на сегодня оно было обновлено, чтобы поддерживать 32-разрядные двоичные файлы Mach-O в OS X.

В отличие от троянцев, шпионского софта или рекламных программ, которые прячутся в файловой системе, чтобы пользователь как можно дольше не обнаружил их, данный код наоборот старается растиражировать себя как можно шире, вызывая нарушения в работе операционной системы. Следует отметить, что подобное поведение стало крайне нетипичным для современных вредоносных разработок.

При инфицировании Clampzok модифицирует сегмент _PAGEZERO в нормального бинарного файла и внедряет туда вирусный код. Кроме того, сам вредонос не мешает выполнению зараженного файла в системе, хотя и в структуре файла появляется сноска LC_UNIXTHREAD, отсылающая ОС к куску вредоносного кода. Программа работает таким образом со всеми двоичными файлами в OS X, выполняясь до тех пор, пока не будут поражены все файлы в папке /bin.

Следует отметить, что код работает только с 32-битными файлами, однако таковых файлов в Mac OS X пока остается довольно много. В новых OS X все больше программ переходят на 64-битную адресацию.

Одной из неприятных особенностей работы вредоноса является то, что он «ломает» подписанные в App Store программы и если у тех были модифицированы бинарные файлы, они перестают работать до момента полного удаления ***(«Маки» подверглись атаке первого «настоящего» вируса // InternetUA (http://internetua.com/maki--podverglis-atake-pervogo--nastoyasxego--virusa). – 2013. – 7.06).***

***

Дедалі ширшого поширення набуває ситуація, пов’язана із заволодінням коштами громадян з використанням інтернет-ресурсів або електронного доступу до банківських рахунків.

Причиною скоєння кіберзлочинів є те, що громадяни під час спілкування в Інтернеті чи по телефону з невідомими особами, які представляються співробітниками банків, торгових підприємств, павільйонів, надають повні анкетні дані, номери сім-карток мобільних операторів, банківські та рахункові рахунки. Злочинець отриману інформацію відразу ж використовує в банкоматах, знімаючи з терміналу грошові заощадження.

У подібних випадках громадянам необхідно відразу звертатись у відповідну банківську установу для блокування рахунку, та у правоохоронні органи – з метою запобігання скоєнню злочину.

Поширюється практика заволодіння коштами шляхом обману телефоном, коли зловмисники повідомляють про нещасні випадки, про участь родича в ДТП, затримання родича міліцією, представляються працівником банку які колекторської контори.

Аналіз, як повідомляє ВЗГ ГУ МВС України у Львівській області, показує, що категорія осіб, яка спілкується з майбутніми потерпілими – особи раніше судимі за аналогічні злочини, колишні працівники банківських установ, філій. Під час проведених оперативно-розшукових заходів стало відомо, що більшу частинку злочинів шляхом обману по телефону вчиняються ув'язненими особами в місцях позбавлення волі, які відбувають покарання за різні види злочинів по всій території України (у 2012 р. працівники карного розшуку розкрили три такі злочини).

Причиною даної категорії злочинів є те, що зловмисник, який телефонував потерпілій особі, на час скоєння злочину перебуває у іншому кінці України і після отримання коштів зв'язок відключається повністю. Інформацію про «перспективних» потерпілих злочинці отримують у мережі Інтернет, відслідковуючи щоденно номера телефонів громадян, їхні повідомлення про втрати документів, речей чи місця їх втрати.

Досить поширеною категорією шахрайств є злочини скоєні особами ромської національності. У цьому виді шахрайств предметами найчастіше стають ювелірні та золоті вироби, гроші, валюта, мобільні телефони. Злочинні дії ця категорія осіб вчиняє під приводом зняття порчі, продажу меду, ворожіння, релігійної утворі.

Суб'єктами переважно є неповнолітні особи, учні, студенти та одинокі літні громадяни. Злочинці, які скоюють ці правопорушення, зазвичай з інших областей України, які в місті Львові винаймають квартири на сезон і після скоєння шахрайств переїздять до інших регіонів.

Швидкість реагування міліції на злочин залежить від об'єктивності інформації та своєчасності її отримання. Швидке отримання інформації від громадян про осіб даної категорії, описи їхньої зовнішності, переміщення на автотранспорті, місця реалізації та збуту викраденого тощо – це все стане у пригоді правоохоронцям та сприятиме розкриттю кримінального правопорушення ***(Інтернет-шахрайство й картковий обман все більше ширяться Україною // InternetUA (http://internetua.com/nternet-shahraistvo-i-kartkovii-obman-vse-b-lshe-shiryatsya-ukra-noua). – 2013. – 7.06).***

***

По данным Check Point Software Technologies, в 42 % компаний в мире ущерб от утечки мобильных данных в прошлом году превысил 100 тыс. дол.

Check Point Software Technologies опубликовала свой второй отчет по мобильной безопасности, составленный на основе опроса около 800 ИТ-специалистов. Из него следует, что в большинстве компаний (79 %) за последний год имели место угрозы безопасности доступной с мобильной устройств информации, повлекшие за собой значительные убытки. В опросе компании участвовали IT-специалисты из США, Канады, Великобритании, Германии и Японии.

В отчете отмечается, что в 42 % компаний в мире ущерб от утечки мобильных данных в прошлом году превысил 100 тыс. дол., а 16 % компаний потеряли более 500 тыс. дол.

По данным отчета, в 96 % компаний, в которых сотрудникам разрешено использовать для работы персональные мобильные устройства, число подключений этих устройств к корпоративной сети возрастет, а в 45 % компаний количество персональных мобильных устройств за два последних года увеличилось более чем в пять раз.

Отмечается, что, несмотря на высокий уровень распространения мобильных угроз, 63 % компаний не контролируют использование корпоративной информации на персональных устройствах, а 93 % испытывали трудности при внедрении политики BYOD.

Компании все чаще хранят данные клиентов на мобильных устройствах, по сравнению с прошлым годом количество таким предприятий возросло на 6 % с 47 % до 53 %.

Что касается операционных систем, то около 49 % компаний считают ОС Android платформой с наибольшим потенциальным риском угрозы безопасности по сравнению с Apple, Windows Mobile и Blackberry (в предыдущем году об этом говорили только 30 %) ***(53 % компаний хранят личные данные клиентов на мобильных устройствах // InternetUA (http://internetua.com/53--kompanii-hranyat-licsnie-dannie-klientov-na-mobilnih-ustroistvah). – 2013. – 8.06).***

***

Исследователи научили вирусы получать команды через музыку, свет и магнитное поле.

Эксперты предупреждают, что подобные каналы коммуникации с вредоносным ПО изучать гораздо сложнее.

В рамках конференции по информационной безопасности ASIACCS исследователи из Алабамского университета в Бирмингеме представили доклад о новых революционных методах коммуникации вредоносного ПО.

Согласно заявлению экспертов, вирусные программы нового поколения будут получать команды, эксплуатируя технические возможности инфицированного устройства. Так, с помощью чувствительных камер и

датчиков, постоянного доступа к сети, имеющегося у большинства владельцев смартфонов и т. п., вирусописатели смогут передавать зараженным телефонам команды через музыкальные клипы, свет экрана компьютера или телевизора, магнитное поле или даже с помощью внешних вибраций.

«Идя на концерт или на кофе в Starbucks, вы не ожидаете, что музыка может нести скрытое сообщение. Это является сдвигом парадигмы, так как в обществе сложился стереотип о том, что вирусные атаки связаны только с электронной почтой и Интернетом», – комментирует один из авторов доклада Р. Хасан.

Он также отметил, что в ходе различных экспериментов исследователям удалось активировать вирус на уже инфицированном устройстве с помощью аудиозаписи. При этом зараженный телефон находился в переполненном коридоре на расстоянии 16 м от источника звука.

«В перспективе мы намерены изучить, как различные сенсорные каналы могут быть использованы злоумышленниками, а также разработать эффективный способ блокировки такого типа атак», – пояснил Ш. Завуд. По его словам, на сегодняшний день довольно проблематично изучать подобные способы коммуникации, поскольку в реальности с подобными механизмами никто еще не сталкивался ***(Исследователи научили вирусы получать команды через музыку, свет и магнитное поле // InternetUA (http://internetua.com/issledovateli-naucsili-virusi-polucsat-komandi-cserez-muziku--svet-i-magnitnoe-pole). – 2013. – 9.06).***

***

Пользователям Android угрожает опасный банковский троянец.

Компания «Доктор Веб» предупредила об угрозе со стороны вредоносной программы Android.Tempur.1.origin, направленной на южнокорейских пользователей Android. Этот троянец осуществляет кражу их конфиденциальных сведений, включая банковские реквизиты, а также информацию о входящих СМС-сообщениях и совершаемых телефонных звонках. Кроме того, он способен выполнять отправку коротких сообщений, в том числе и на премиум-номера.

Вредоносная программа Android.Tempur.1.origin, обнаруженная специалистами по информационной безопасности в прошлом месяце, представляет собой троянца, который предназначен, главным образом, для кражи конфиденциальной информации клиентов различных кредитных организаций Южной Кореи. В зависимости от модификации Android.Tempur.1.origin собираемая им информация может включать имя пользователя и его персональный идентификатор, номер социальной страховки, пароль от учетной записи, номер банковского счета, номер сотового телефона и пр.

Одним из известных способов распространения данного троянца до недавнего времени являлось применение злоумышленниками специальной вредоносной программы, содержащей несколько различных вариантов

Android.Tempur.1.origin, каждый из которых имитировал внешний вид официального клиентского приложения того или иного южнокорейского банка. Ссылка на загрузку соответствующего apk-пакета «дроппера» предоставлялась пользователям в мошеннических СМС-сообщениях и вела на домен cect[xxx].com.

Особенность этой вредоносной программы-носителя заключается в том, что перед установкой определенной модификации Android.Tempur.1.origin она выполняет поиск уже имеющихся на мобильном устройстве легитимных версий банковского ПО, и при обнаружении последних пытается выполнить их деинсталляцию. Если мобильное устройство имеет root-доступ, «дроппер» при помощи специальной команды изменяет атрибуты найденных приложений и выполняет их удаление без вмешательства пользователя. В противном случае удаление происходит по стандартной процедуре с демонстрацией соответствующего диалогового окна. После удаления настоящих банковских приложений троянец-носитель пытается установить их поддельные копии.

В случае успешного запуска известные варианты Android.Tempur.1.origin демонстрируют интерфейс, приближенный к внешнему виду официальных банковских приложений, и обманным путем заставляют пользователей ввести свои аутентификационные или персональные сведения. Полученная таким образом информация затем пересылается киберпреступникам. Другой опасной функцией, которой обладает Android.Tempur.1.origin, является возможность перехватывать входящие СМС-сообщения, информация о которых также передается на сервер злоумышленников. Данный функционал может быть использован как для кражи одноразовых mTAN-кодов, применяемых в системах «банк-клиент», так и для перехвата не менее ценных сообщений из личной переписки.

Кроме того, вредоносная программа также способна отслеживать совершаемые телефонные звонки и может выполнить отправку СМС-сообщений на премиум-номера, для чего получает соответствующие параметры с сервера мошенников.

При исследовании данной угрозы специалистам компании «Доктор Веб» удалось обнаружить новую модификацию Android.Tempur.1.origin, которая обладает тем же функционалом, что и остальные версии троянца. Однако в данном случае претерпел изменение способ распространения вредоносной программы: соответствующий троянский apk-файл теперь загружается непосредственно с удаленного сервера злоумышленников, а вспомогательный «дроппер» уже не используется. Отличен и адрес веб-сервера киберпреступников, откуда происходит загрузка Android.Tempur.1.origin: теперь это korea[xxxx].com.

Данный троянец представляет весьма серьезную угрозу, поскольку позволяет злоумышленникам завладеть строго конфиденциальными данными пользователей, в частности их финансовыми реквизитами, что в дальнейшем может быть использовано для шантажа, вымогательства и непосредственной кражи денежных средств. Другие конфиденциальные сведения, такие как

информация о входящих СМС-сообщениях и звонках, также могут быть применены в разного рода мошеннических схемах ***(Пользователям Android угрожает опасный банковский троянец // InternetUA (http://internetua.com/polzovatelyam-Android-ugrojaet-opasnii-bankovskii-troyanec). – 2013. – 9.06).***