СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(10–24.06)

2013 № 12

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(10–24.06)
№ 12

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

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

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2013

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ 4

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 10

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 19

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 28

Інформаційно-психологічний вплив мережевого спілкування на особистість 28

Маніпулятивні технології 36

Зарубіжні спецслужби і технології «соціального контролю» 42

Проблема захисту даних. DOS та вірусні атаки 49

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Поиск по хештегам теперь доступен и в социальной сети Facebook, сообщают информагентства.

Социальная сеть Facebook ввела функцию поиска по хештегам, теперь пользователи могут снабжать поисковые забросы соответствующим словом со знаком «#», также как в Instagram, Twitter, Tumblr, Pinterest.

Facebook начала разрабатывать хештеги из-за растущей конкуренции со стороны Twitter. По мнению экспертов, с внедрением хештегов, крупнейшая социальная сеть получит возможность индексировать беседы по темам и тем самым упростит процесс поиска, что привлечет больше пользователей.

Хештег – слово или фраза со знаком без пробела «#» в начале. При поиске по хештегу можно увидеть сообщения и страницы других пользователей по запрашиваемой вами теме ***(Facebook ввели поиск по хештегам // Час Пик (http://vchaspik.ua/zhizn/160849facebook-vveli-poisk-po-heshtegam). – 2013. – 13.06).***

***

Компанія Facebook оголосила про запуск у роботу нового дата-центру, який став першим таким активом компаній, які перебувають за межами США (http://ua.korrespondent.net/business/realestate/1570098-facebook-rozshiryue-gorizonti-kompaniya-vidkrila-pershij-data-centr-za-mezhami-ssha).

Новий дата-центр Facebook розташований за полярним колом на території Швеції у місті Лулеа, і площа його становить 28 тис. кв. м. Операційний директор Facebook Т. Фурлонг заявив, що актив призначений, в основному, для обслуговування європейських користувачів Facebook.

Причому в компанії зазначили, що всі дані зі шведського дата-центру копіюються на інших серверних майданчиках Facebook, що розташовані на території США. Експерти ж вважають, що найближчим часом можна буде очікувати значного зростання кількості дата-центрів у таких країнах, як Ісландія, Фінляндія, Швейцарія і Канада.

Причиною цього є, у тому числі і те, що на місці розташування нового майданчика Facebook, наприклад, необхідність в охолодженні серверів або повністю відпадає, або потрібна в мінімальних масштабах. Середньорічна температура тут становить лише 2 градуси тепла за Цельсієм, а влітку вона рідко піднімається вище 30 градусів.

Завдяки цьому економія на охолодженні робить новий дата-центр одним з найбільш енергоефективних у світі. Фінські та шведські експерти також стверджують, що на території їхніх країн є безліч потужних майданчиків з точки зору енергопостачання, оскільки раніше в цих регіонах і так планувалися різні виробничі активи ***(Facebook розширює горизонти: компанія відкрила перший дата-центр за межами США // Корреспондент.net (http://ua.korrespondent.net/business/realestate/1570098-***

facebook-rozshiryue-gorizonti-kompaniya-vidkrila-pershij-data-centr-za-mezhami-ssha). – 2013. – 13.06).

***

Геолокационный сервис Foursquare запустил функцию Time Machine, которая позволяет визуализировать всю историю чек-инов пользователя в одной инфографике.

Инфографика составляется в автоматическом режиме на основе анализа активности пользователя. Начиная с первого чек-ина, пользователь может отследить свои перемещения по интерактивной карте, а частоту отметок – по временному графику. В отдельных блоках демонстрируются недавние чек-ины и наиболее популярные категории мест, где бывает пользователь.

В инфографике также представлены данные о любимых местах пользователя для чек-инов утром, днем или вечером, а также в выходные. Также Foursquare напомнит пользователю, в скольких местах он побывал, в какую неделю, день и месяц он оставил наибольшее число отметок, по каким городам путешествовал, а также сколько фотографий опубликовал. Инфографикой можно поделиться с друзьями по социальным сетям.

На сервисе Foursquare зарегистрировано более 25 млн пользователей, которые оставили за четыре года около 4 млрд чек-инов. Нынешняя стратегия развития Foursquare в сторону геотаргетированных рекомендаций интересных мест создает широкие возможности для монетизации. Сервис доступен пользователям через приложения для iPhone и Android, а также через веб-интерфейс ***(Foursquare позволил пользователю создать инфографику из своих чек-инов // Marketing Media Review (http://mmr.ua/news/id/foursquare-pozvolil-polzovatelju-sozdat-infografiku-iz-svoih-chek-inov-35055/). – 2013. – 14.06).***

***

Социальная сеть MySpace в ходе редизайна удалила персональные блоги старого формата, что вызвало возмущение со стороны пользователей ресурса, которые не были предупреждены о каких-либо изменениях, а тем более о возможном исчезновении контента. В настоящее время участники сети просят руководство ресурса вернуть содержимое обратно (историю посещений и снимки), но компания пока не дает каких-либо гарантий на возвращение.

Представители MySpace прокомментировали ситуацию, сообщив, что компания старается предоставить пользователям улучшенный опыт обмена музыкой, но вместе с тем жертвами изменений стали блоги, личные сообщения, видеоролики, комментарии и сообщения, персональные фоновые изображения и игры ***(MySpace удалил блоги пользователей // InternetUA (http://internetua.com/MySpace-udalil-blogi-polzovatelei). – 2013. – 16.06).***

***

Соціальна мережа Facebook дозволила прикріплювати фотографії і картинки до коментарів, які користувач залишає до записів своїх друзів і на публічних сторінках на сайті (http://ua.korrespondent.net/business/web/1572585-slidom-za-vkontakte-facebook-dozvolila-vstavlyati-zobrazhennya-u-komentari).

Про це свідчать скріншоти, опубліковані на своїй сторінці одним з розробників Facebook Б. Болдуіном.

Картинки, які прикріплюються, мають бути збережені у форматах JPG або PNG – аналогічний функціонал є в російській соцмережі «ВКонтакте». Однак Facebook, як і раніше, не дозволила додавати до коментарів анімовані GIF-зображення, пише техноблог GigaOM.

Як пише Mashable, публікувати фотографії в коментарях поступово зможуть користувачі по всьому світу як з десктопів, так і з мобільних пристроїв.

Очікується, що нові формати коментарів дадуть змогу Facebook, аудиторія якої перевищує мільярд користувачів, активізувати обговорення публікованих записів і контенту ***(Слідом за «ВКонтакте» Facebook дозволила вставляти зображення у коментарі // Корреспондент.net (http://ua.korrespondent.net/business/web/1572585-slidom-za-vkontakte-facebook-dozvolila-vstavlyati-zobrazhennya-u-komentari). – 2013. – 20.06).***

***

Сервис Instagram предоставил пользователям возможность размещать видеоролики длиной от трех до 15 секунд, сообщил на пресс-конференции глава команды по разработке Instagram К. Систром.

Теперь в Instagram наряду с кнопкой для съемки фотографий появится отдельная кнопка для создания видео, а ролики будут отмечаться в ленте новостей специальной иконкой в правом верхнем углу, передает NewsOboz.org со ссылкой на Корреспондент.net.

Кроме того, пользователь сможет отредактировать ролик, удалив его часть и записав ее заново. Instagram также запускает 13 новых фильтров, разработанных специально для обработки видео.

Сообщается, что новый функционал Instagram станет конкурентом видеосервису Vine, который ранее запустил Twitter. Отметим, с помощью Vine пользователи могут создавать шестисекундные видеоролики с мобильных устройств на iOS и Android.

Пользователи Instagram смогут снимать видеоролики как с iOS, так и с Android-устройств, а просматривать их – в iOS и Android-приложениях и веб-версии.

Пользователь может выбрать превью ролика из нескольких кадров, добавить хэштеги и геолокационную метку.

Аудитория Instagram, по словам К. Систрома, превышает 130 млн человек. Пользователи сервиса разместили на нем более 16 млрд фотографий, к которым каждый день оставляют более 1 млрд отметок Мне нравится ***(Пользователям Instagram теперь доступна функция видеосъемки // NewsOboz (http://newsoboz.org/it_tehnologii/polzovatelyam-instagram-stala-dostupna-funktsiya-videosemki-21062013003800). – 2013. – 21.06).***

***

Страничка статистики в Facebook станет более полной и даст владельцам больше информации о том, как аудитория реагирует на их записи.

Впервые с конца 2011 г. Facebook решила серьезно взяться за статистику страниц и анонсировала в своем блоге изменения в Page Insights. Основная идея перемен – сделать так, чтобы владельцы страниц лучше понимали, что работает, а что нет и как тот или иной подход отражается на активности аудитории. Чтобы достичь этой цели, Facebook некоторые показатели выделяет в отдельные цифры и графики, некоторые – объединяет.

Например, данных в People Talking About This теперь будет существенно больше – можно будет отдельно увидеть «лайки», клики, количество комментариев и тех, кто поделился записью. Virality, в свою очередь, будет переименована в Engagement Rate и в этот показатель теперь включат точное количество кликов на посты.

Facebook также даст возможность увидеть статистику по конкретным записям и покажет как позитивные моменты – «лайки», комментарии, клики, количество поделившихся – так и негативные. К последним относятся, например, количество тех, кому «разонравилась» страница после этого поста, кто отметил ее как спам или просто спрятал. Сегодня, чтобы найти такую информацию, нужно погрузиться в статистику с головой и, возможно, даже использовать сторонние сервисы.

Наконец, Facebook также покажет демографическую и географическую статистику обо всех людях, которые так или иначе взаимодействовали с контентом на странице. Это особенно важно для бизнеса, так как позволяет понять, какую именно аудиторию «окучивает» их страница в Facebook.

На сегодняшний день социальная сеть тестирует новую версию Page Insights «на небольшой группе» страниц, более широкий охват ожидается в ближайшем будущем. Facebook также не собирается на этом останавливаться и намерена теперь чаще добавлять в статистику новые возможности ***(Facebook делает более мощную статистику страниц // Marketing Media Review (http://mmr.ua/news/id/facebook-delaet-bolee-moschnuju-statistiku-stranic-35137/). – 2013. – 20.06).***

***

В Facebook для медиаконтента появились отрицательные оценки. Вместо Like соцсеть ввела комплект из нейтральной, положительной, очень положительной и отрицательных оценок.

Кроме того, iPhone приложение научилось у «ВКонтакте» отображать прослушиваемую сейчас музыку в статусе ***(В Facebook появилась оценка «Очень не нравится» // InternetUA (http://internetua.com/v-Facebook-poyavilas-ocenka--ocsen-ne-nravitsya). – 2013. – 20.06).***

***

Идея предоставлять людям бесплатный WiFi в обмен на информацию об их местоположении родилась в компании Facebook в рамках эксперимента, который реализовали двое разработчиков в мае 2012 г. после однодневного хакатона. Тогда казалось, что это просто забавная идея: залогиниться в брендовые хотспоты Facebook WiFi, используя свой логин и пароль в социальной сети. Но компания Facebook с тех пор планомерно расширяет рамки этого эксперимента, открывая фирменные хотспоты в кафетериях Пало-Альто и Сан-Франциско.

Более того, месяц назад в рамках совместного проекта с Cisco выпущена даже линейка маршрутизаторов Cisco Meraki WiFi со встроенной авторизацией через Facebook-аккаунт.

По мнению аналитиков, планомерное распространение хотспотов Facebook WiFi свидетельствует о том, что социальная сеть стремится собрать все больше и больше информации о своих пользователях, включая информацию об их физических перемещениях. Это важно для более точного рекламного таргетинга и привлечения рекламодателей. Тем более, что у главного конкурента на рынке интернет-рекламы, компании Google, информация о местоположении пользователей уже имеется (благодаря операционной системе Android) ***(Бесплатный WiFi от Facebook в обмен на ваши координаты // InternetUA (http://internetua.com/besplatnii-WiFi-ot-Facebook-v-obmen-na-vashi-koordinati). – 2013. – 21.06).***

***

Блог-сервис LiveJournal анонсировал новый вид главной страницы сайта Livejournal.com, сообщается в пресс-релизе, поступившем в редакцию «Ленты.ру». В рамках реформирования облика главной страницы сервиса было принято решение закрыть дайджест LiveJournal.ru, материалы с которого будут появляться на основной странице ЖЖ.

Новый дизайн главной страницы ЖЖ выполнен по макетам Студии Артемия Лебедева. Одно из ключевых изменений – новый вид и принцип формирования главных записей топа ЖЖ. В частности, появится категоризация рейтинга: помимо общего рейтинга будут доступны еще и категории «Новости», «Позитив», «Полезное», «Общество», «Дискуссии», «Медиа», «Путешествия», «18+» и «Жыр». На обновления топ-15 записей

рейтинга можно будет подписаться в ЖЖ и «ВКонтакте» (последняя функция доступна только для пользователей, подписанных на кириллические сервисы «Живого журнала»).

Рейтинг ЖЖ можно будет настраивать индивидуально, чтобы не видеть записей от нежелательных пользователей. Редакционные дайджесты интересных постов в новой версии главной страницы будут расположены в рубрике «Редакция».

Обновленная главная страница ЖЖ будет представлена публике в ночь с 24 на 25 июня 2013 г.

Сервис Livejournal существует с 1999 г. В настоящее время он входит в состав российского холдинга SUP Media ***(ЖЖ анонсировал новую главную страницу // InternetUA (http://internetua.com/jj-anonsiroval-novuua-glavnuua-stranicu). – 2013. – 24.06).***

***

Социальная сеть «ВКонтакте» добавила в раздел диалогов «важные сообщения», которые можно сохранять отдельно. Для этого необходимо нажать звездочку возле времени отправления. Также доступна групповая работа с сообщениями. Чтобы найти «Важные сообщения», нужно нажать соответствующую кнопку в правом верхнем углу списка диалогов.

Также сообщается о еще одном нововведении – возможности менять заглавные фотографии в групповых беседах. Для этого нужно зайти в «Действия» и выбрать пункт «Обновить фотографию беседы». «После чего ваш уютный чатик обретет уникальное лицо», – уверяет администрация ресурса. Эта же фотография будет находиться рядом с окошком набора текста.

Также коснулись изменения перечня кнопок в «Действиях». Их заменила одна – «Показать материалы беседы». Она объединяет в себе все то, что было раньше: фото, видео, аудио и документы, которые пользователи отправляли друг другу за время общения ***(В соцсети «ВКонтакте» появились важные сообщения // InternetUA (http://internetua.com/v-socseti--vkontakte--poyavilis-vajnie-soobsxeniya). – 2013. – 24.06).***

***

На волне массовых удалений музыки, соцсеть «ВКонтакте» обновила поиск непиратской музыки. В раздел «Популярное» музыкального меню добавили ссылки на группы и страницы исполнителей. Перейдя по ним, пользователь будет попадать к списку композиций, загруженных музыкантами. Об этом сообщается в группе «Команда “ВКонтакте”».

«ВКонтакте существуют сотни сообществ, в которых музыканты выкладывают собственную музыку. Сегодня мы обновили раздел Популярное, чтобы такие сообщества было проще найти», – говорится в сообщении. Отмечается, что добавлять ссылки на свою музыку могут сами исполнители, для этого им следует подать заявку ***(«ВКонтакте» упростила***

поиск легальной музыки // InternetUA (http://internetua.com/vkontakte--uprostila-poisk-legalnoi-muziki). – 2013. – 22.06).

***

Twitter купил «напоминающий» социальный стартап Spindle

Новый продукт поможет пользователям узнать, что происходит неподалёку от них прямо сейчас.

Стало известно, что популярный сервис микроблогов приобрёл социальный стартап для iPhone – Spindle. Это приложение, которое сообщает пользователям о ближайших событиях, определяя их местоположение, пишет The Verge.

«Мы потратили последние два с половиной года на создание продукта, который поможет вам ответить на вопрос – «Что происходит неподалеку прямо сейчас?» – сообщает компания в своем блоге. – Объединившись с Twitter, мы сможем гораздо больше помогать вам находить интересную, своевременную и полезную информацию об окружающих событиях». Приложение интегрировано с такими социальными сервисами, как Twitter, Facebook, Foursquare и Yelp.

На сегодняшний день Spindle удалено из App Store. Работать как самостоятельное приложение сервис перестанет автоматически. А рабочая команда, которая была основана бывшими инженерами Microsoft, переедет из Бостона в Сан-Франциско к команде сервиса Twitter ***Twitter купил «напоминающий» социальный стартап Spindle // InternetUA (http://internetua.com/Twitter-kupil--napominauasxii--socialnii-startap-Spindle). – 2013. – 22.06).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Найпопулярнішими ресурсами в Інтернеті для українців залишаються соціальні мережі – 63 % людей заходять у мережу виключно заради особистого, не пов’язаного з професійним обов’язком спілкування.

Про це свідчать дані регулярного дослідження ринку телекомунікаційних послуг, яке здійснює GfK Ukraine, передає Укрінформ.

«Збільшилася частка інтернет-користувачів, які протягом тижня проводять у мережі до 5 годин для особистих, не пов’язаних з роботою цілей (з 38 % до 43 %). Найпопулярнішими причинами користування Інтернетом серед українців залишаються соціальні мережі. Частка таких користувачів у I кварталі 2013 р. зросла до 63 %, що на 11 п.п. вище за минулорічні показники», – повідомили соціологи.

Серед інших найбільш згадуваних причин використання мережі – електронна пошта, завантаження музики та фільмів, пошук інформації про певні продукти чи послуги. У GfK Ukraine також зазначили, що протягом

року зросла популярність таких послуг як інтернет-телефонія (Skype, тощо) та системи швидких повідомлень.

У соціологічній компанії повідомили, що загальна вибірка щомісячного опитування становить за цей період 1000 респондентів ***(Дві третини українців заходять в Інтернет заради соцмереж // Інформаційне агентство «Регіональні Новини» (http://regionews.ua/node/99297). – 2013. – 7.06).***

***

Хочешь узнать, как изменится Интернет? Спроси у бабушки.

Моей бабушке больше 80 лет. Ей всегда интересно, как дела у детей, внуков, правнука, бывших учеников и старых знакомых, важно знать все новости и быть в курсе событий. Да, раньше все мы часто приходили к ней в гости. Но со временем кто-то переехал, у кого-то много работы, появились семьи, и часто навещать бабушку, чтобы поделиться с ней всеми новостями, стало трудно. Она отказалась мириться с таким положением дел и стала активным пользователем Интернета.

Это нередкая история. Наши пожилые родственники в какой-то момент понимают, что единственный способ оставаться в курсе жизни детей, внуков и правнуков, разъехавшихся по миру или просто очень занятых, – это приобщиться к технологиям. Разумеется, им это дается непросто, ведь с возрастом осваивать новые явления и системы становится сложнее, чему есть и неврологические и психологические причины.

Возможна ли сеть для пожилых?

Конечно, сразу нашлись люди, которые задались целью сделать Интернет проще и доступнее для бабушек и дедушек. Первое, что приходит в голову, – социальная сеть для пожилых. Но эта идея обречена на провал.

Бабушки и дедушки не хотят в цифровой дом престарелых, они хотят быть там же, где их дети и внуки, а значит, им приходится осваивать «Одноклассники», «ВКонтакте», Facebook и Twitter.

Скоро должен запуститься проект под кодовым названием «17 Million Grandmas On Facebook», который обещает создать простой и понятный интерфейс для пользования Facebook. Пока его нет, наблюдение за тем, как пожилой, не имеющий компьютерного опыта человек пытается освоить базовые и интуитивно понятные для нас, «опытных пользователей», электронные сервисы, – бесценный кладезь информации об истинном устройстве привычных нам интерфейсов и систем.

Сам факт интуитивности того или иного интерфейса субъективен. Для молодых людей, «родившихся с компьютером», или для опытных пользователей, прошедших с индустрией весь путь от первых GUI-систем до Mountain Lion, на освоение новых программ и сайтов уходит очень мало времени, ведь новые решения логично следуют общей парадигме устройства программ и онлайн-сервисов. У пожилых людей этой парадигмы нет.

Простой пример: мы привыкли к тому, что электронные сервисы используют метафоры. «Рабочий стол», «папки», «окна» – когда-то они были действительно похожи на свои прообразы из реального мира, но сейчас работают абсолютно не так, как можно ожидать, если смотреть только на название.

Один пожилой человек, например, буквально воспринимает понятие «электронная почта», считая ее полным аналогом обычной, но только в Интернете. Поэтому дома он использует один адрес, но в гостях у сына пользуется другим, так как почтовый адрес должен соответствовать месту нахождения. Логично, правда?

Мы по-прежнему пытаемся уподобить новые сервисы объектам из «старого», реального мира: YouTube – это как бы новый телевизор, Instagram – как бы новый «полароид», Yelp – вроде «желтых страниц», Twitter, Foursquare, Path... всё, аналогии кончились.

И чем дальше, тем сложнее их будет придумывать. Пока основная аудитория – люди, жившие до «эпохи Интернета», для продвижения новых сервисов мы будем проводить аналогии. Иначе как объяснить, о чем вообще речь? Но следующему поколению это не потребуется. Их эппы не будут нуждаться в реальном аналоге, их будут рекламировать в лучшем случае как «YouTube для Twitter» (это Vine, да).

Помимо этого, нам очевидна, например, вложенность компьютерных систем – мы можем не разбираться в деталях, но понимаем, что запускаем операционную систему на компьютере, программу-браузер в операционной системе, открываем сайт-поисковик в этом браузере с помощью адресной строки и в соответствующее поле на странице поисковика вводим некий запрос.

Пожилой человек вводит запрос «в компьютер». Он может верно ответить на вопрос, чем он ищет, – «Яндексом», но, по сути, не видит разницы между всеми уровнями этой системы, так же как абзацем выше я проигнорировал кучу уровней между «железом» и операционной системой, понятных любому компьютерщику.

Но чем дальше, тем реальная сложность систем будет выше, и тем сложнее будет ее понимание обычному юзеру. То есть нынешние непродвинутые пользователи из старшего поколения показывают нам, как мы сами будем воспринимать технологии по мере их развития. Грань между разными слоями уже стирается: возьмите компьютеры на ChromeOS или телефоны с Facebook Home. Где там что, уже совсем неясно. Ясно главное – этот компьютер или телефон может решить вашу задачу, то есть, например, найти нужную информацию.

Закрытость надежней открытости

Из этого можно сделать и более конкретный вывод: о проигрыше более «открытых» систем более «закрытым». То есть с «Андроидом», конечно, ничего плохого не случится. Но, исходя из этой теории, можно ожидать, что голая, прозрачная версия, которая дает доступ к файлам, ручным настройкам

и т. п., останется только для программистов, а обычные пользователи будут работать либо с проприетарными системами типа iOS, либо со сборками «Андроида» или надстройками на нем (как, например, в Kindle). У пользователя отберут лишние возможности, которые его могут отвлечь и запутать.

Здесь уместно задуматься о том, не окажется ли через 15–20 лет каждый, кто не может сам программировать или хотя бы не умеет работать с консольными командами, в том же положении, в котором сегодня находятся пенсионеры.

Это будет положение пользователя, ограниченного стандартными сценариями и способного решать новые задачи только покупкой программных решений от производителя своего устройства (но это тема для отдельной статьи, которую, в общем, уже написал на Colta М. Куртов).

Вот другой пример модели поведения неопытных взрослых пользователей, которая постепенно распространяется на большинство вообще: почти все пожилые люди пользуются навигационными запросами в поисковиках. Это когда вы вбиваете в Google не «сайт, где можно найти друзей», а «ввв вконтакте ру», то есть не ищете информацию, а просто пытаетесь попасть на какую-то конкретную страницу.

Пожилой пользователь не может так легко разобраться в хитросплетениях транскрипции: нужно ли писать www, где ставить точки, что такое доменная зона и так далее. Он хочет попасть на нужный сайт. Даже когда он ищет ответ на какой-то вопрос, он не пользуется языком запросов, не отличает органическую выдачу от рекламной и в итоге будет попадать туда, куда его направит умелая рука поисковых оптимизаторов и маркетинговой службы самого поисковика. Не зря Google давно уже объединил адресную строку Chrome с поисковой строкой своей системы: это отвечает реальному поведению пользователей, но и дает гораздо больше контроля над тем, как и куда он попадает.

Больше доверия

Наблюдая, как пожилые люди пользуются сетью, я обратил внимание еще на ряд особенностей, которые можно объединить под названием «некритическое отношение к информации». В широком смысле это вера любому электронно-печатному слову, при том что надежность его, как известно, невысока.

Пожилые люди ужасаются броским заголовкам трафикообменных систем типа «Галкин убил Пугачеву!» (своей новой прической, конечно, что же вы за сердце схватились?), верят баннеру «Вы наш миллионный посетитель и выиграли приз» и не кликают на него только потому, что боятся, что не смогут правильно оформить заявку на его получение. Это происходит не от глупости, разумеется, а от того, что человек не способен критически оценивать информацию, если она идет из того же источника, которому он в принципе доверяет, если она выглядит правдоподобно и ее очень, очень много.

И этот тренд тоже можно видеть спускающимся к широкой, молодой аудитории: привычка доверять соцсетям, невнимательность к тому, опубликован ли цитируемый текст на Lenta.ru или на сайте «Экспресс-газеты». Огромный поток постов приводит к тому, что люди, в разумности которых вы уверены, публикуют перепост новости о том, что Онищенко запретил котов в России, не задумываясь ни на секунду.

«Свой» Интернет

Последнее наблюдение, о котором хочется сказать, оказалось несколько парадоксальным: как раз сейчас в западной прессе идет активная дискуссия по поводу «me me me generation» – нового поколения юных нарциссов, которое наблюдают западные социологи.

Лично я никогда не наблюдал более эгоцентричного пользователя сети, чем бабушка: она подсознательно уверена, что вся информация, попадающая на экран ее собственного компьютера, адресована лично ей.

Случайно увидев в Twitter неизвестного ей пользователя что-то против Навального, она очень возмутилась: «Как они могут мне такое писать?! Как им не стыдно!?»

И дело не в том, что бабушка не совсем понимает, как устроен Twitter. Она привыкла, что все сервисы для нее персонализированы – лента новостей «ВКонтакте», «Одноклассников» и Facebook, главная страница «Яндекса», стартовая страница браузера с ее любимыми сайтами, сайт «Эха Москвы» (он не персонализирован технически, просто бабушка – его 100 %-ная ЦА, и ей интересно все, что там пишут). Для нее наличие «чужого» Интернета с неправильными мнениями – большой удар.

Предположу, что это тоже тенденция, которая будет распространяться на все большее число пользователей: алгоритмы персонализации улучшаются, читать и смотреть только то, что подходит тебе, гораздо быстрее и удобнее, чем фильтровать тонны контента в поисках интересного. Но вместе с этим пользователь теряет возможность найти нечто принципиально новое, познакомиться с людьми не из своего круга, узнать мнение, не разделяемое его друзьями, окунуться в область, к которой он никогда не имел отношения.

Описанные характеристики поведения пожилых людей, которые уже скоро станут, возможно, не маргинальными, а, наоборот, типичными для среднего пользователя сети, могут напугать. Да, большинство всегда и во все времена готово променять свободу исследования на удобство. Те ограничения, которые на себя накладывают пенсионеры в Интернете просто потому, что не умеют пользоваться сетью иначе, младшие поколения могут выбрать сознательно, чтобы облегчить свой быт. И то, что сейчас создается как «безопасный браузер» для пожилых (или для детей), может в итоге просто заменить для большинства небезопасный и сложный браузер без ограничений ***(Хочешь узнать, как изменится Интернет? Спроси у бабушки // InternetUA (http://internetua.com/hocsesh-uznat--kak-izmenitsya-internet--sprosi-u-babushki). – 2013. – 10.06).***

***

В Администрации Президента уже более двух месяцев разрабатывают проект представительства Президента В. Януковича в социальных сетях.

Об этом говорится в ответе Администрации Президента на информационный запрос «Украинской правды».

«Проект Официального представительства Президента в социальных сетях находится в стадии разработки Главным управлением пресс-службы и коммуникаций Администрации Президента», – говорится в ответе.

Однако в АП отказались ответить на вопрос о конкретной дате появления В. Януковича в социальных сетях.

Как известно, еще 20 марта в АП «Украинской правде» сообщили, что проект представительства В. Януковича в соцсетях находится в стадии разработки ***(Януковича никак не могут «запустить» в соцсети // InternetUA (http://internetua.com/yanukovicsa-nikak-ne-mogut--zapustit--v-socseti). – 2013. – 13.06).***

***

После опубликованных в Facebook фотографий туалета поезда Севастополь – Киев пользователи социальной сети начали распространять петицию, обращенную к Президенту и Премьер-министру. Высших должностных лиц государства просят срочно обновить парк пассажирских поездов «Укрзалізниці».

«Не у всех граждан вашей страны есть возможность поехать на море новыми скоростными экспрессами. А при всей дешевизне билета в обычные поезда путешествие в них часто становится мукой. После посещения такого поезда задаешься вопросом – вошла ли на самом деле Украина в XXI век? Как можно представить себе подобные условия передвижения в государственном, народном транспорте современной европейской страны?» – говорится в тексте петиции.

По словам авторов петиции, из-за уменьшающегося количества составов, которые списываются ввиду изношенности, пассажиры вынуждены обращаться к спекулянтам за билетами на фирменные поезда – с более новыми вагонами, кондиционерами и хотя бы приемлемым уровнем комфорта.

«Мы знаем, что средства на покупку нового пассажирского состава должны выделяться из государственного бюджета. В этом году впервые Президент дал задание осуществить покупку за счет госбюджета. Сделайте это! Ведь раньше новые поезда (и скоростные в том числе) приобретались лишь за счет “Укрзалізниці”», – говорится в петиции.

Напомним, 12 июня Премьер-министр Н. Азаров на заседании правительства сообщил, что «если нужно будет вводить дополнительные поезда – они будут введены». «Но такие дополнительные поезда, как упомянутый выше состав по маршруту Севастополь – Киев, нам не нужны!

Мы не хотим пугать своих детей видами туалетов и купе, напоминающих тюремные камеры военного времени», – сказано в петиции.

Сообщение с петицией уже опубликовано пользователями Facebook на личной странице Н. Азарова, однако Премьер пока на него не отреагировал ***(После фотографий кошмарного поезда Севастополь – Киев в соцсетях написали петицию Януковичу // Левый берег (http://lb.ua/news/2013/06/14/206579_posle_fotografiy_koshmarnogo_poezda.html). – 2013. – 14.06).***

***

Социальная сеть Facebook разрешила публиковать фотографии людей, перенесших мастэктомию. Такое решение было принято после петиции, подписанной 21 тыс. человек, пишет «Обозреватель» со ссылкой на MedPortal (http://tech.obozrevatel.com/news/71924-polzovatelyam-facebook-razreshili-publikovat-foto-s-udalennoj-grudyu.htm).

В компании признали, что мастэктомия меняет жизнь пациентов, а фотографии людей, перенесших операцию, могут помочь повысить осведомленность о раке молочной железы.

«Такие снимки – поддержка для женщин и мужчин, столкнувшихся с диагнозом “рак груди”, а также для тех, на чьем теле остались шрамы после операции», – отметили в Facebook.

Все началось с блокировки в социальной сети Facebook страницы американского фотографа Д. Джея, автора проекта SCAR, в рамках которого он публиковал снимки людей после мастэктомии. Страница фотографа была заблокирована на месяц.

Такая политика соцсети возмутила пользователей. В защиту работ Д. Джея выступила С. Баррингтон, страдающая раком груди четвертой стадии. Вскоре ее петиция собрала 21 тыс. подписей ***(Пользователям Facebook разрешили публиковать фото с удаленной грудью // Обозреватель (http://tech.obozrevatel.com/news/71924-polzovatelyam-facebook-razreshili-publikovat-foto-s-udalennoj-grudyu.htm). – 2013. – 17.06).***

***

Общественники находят извращенцев в соцсети и заманивают на встречу.

В Днепропетровске отлавливают по три педофила в день. Такой информацией с «Сегодня» поделился член общественного движения «Сопротивление Днепропетровск» Е. Смородин. По его словам, отловом педофилов в городе занимаются люди из их команды совместно с правоохранителями. Находят извращенцев в соцсети, заманивают на встречу, но там их ждут не невинные создания, а люди в форме (http://www.segodnya.ua/regions/dnepr/V-Dnepropetrovske-otlavlivayut-po-tri-pedofila-v-den-443118.html).

«Работа по поиску и переписка ведется каждый день, а вот задерживаем, бывает, по три человека в один день. Поверьте, педофилы есть в у нас в городе, и родителям несовершеннолетних детей следует быть очень внимательными», – говорит Е. Смородин.

Механизм отлова извращенцев следующий: заводится страничка в соцсети от имен реально существующего ребенка, от его имени ведется переписка. Родители несовершеннолетнего находятся в курсе происходящего и по итогам задержания пишут заявление на педофила. Самого ребенка к отлову извращенцев не привлекают вообще.

«Если человек нормальный, то он не станет связывается с малолетним, а тем более слать ему порнографические ролики или приглашать на встречу. Наша цель при переписке раскрутить подозреваемого на то, чтобы он не только пригласил ребенка на встречу, но и прислал ему порнографический ролик – это уже считается развратными действиями по отношению к несовершеннолетнему и грозит лишением свободы сроком на пять лет», – говорит Е. Смородин.

По словам активиста, одним из последних задержанных оказался офицер-контрактник средних лет, по виду которого и не определишь такие ужасные наклонности ***(Яковлева В. В Днепропетровске отлавливают по три педофила в день // Сегодня (http://www.segodnya.ua/regions/dnepr/V-Dnepropetrovske-otlavlivayut-po-tri-pedofila-v-den-443118.html). – 2013. – 19.06).***

***

Страницы феминистского движения FEMEN в соцсети Facebook были заблокированы администрацией ресурса. Об этом сообщается 24 июня 2013 г. на сайте движения.

Facebook заблокировал 23 июня основную страницу FEMEN, а днем ранее – страницу французского представительства движения. В качестве причины блокировки администрация соцсети указала «наличие материалов, содержащих изображения обнаженного тела, материалов порнографического содержания или материалов с предложением сексуальных услуг».

В FEMEN заявили, что обжаловали удаление своих страниц. Как видно из скриншота панели администратора Facebook, опубликованного на сайте движения, в случае, если обжалование будет отклонено, страницы удалят окончательно. На момент написания заметки они оставались недоступны.

Представители движения посчитали, что блокировка их аккаунтов в Facebook «является логическим продолжением интернет-войны, развязанной против FEMEN различными реакционными группами». Всего на удаленные страницы было подписано около 170 тыс. пользователей.

В марте 2013 г. хакеры взломали страницы тунисского представительства FEMEN в Facebook и Twitter. Злоумышленники опубликовали на них цитаты из Корана, а также удалили фотографии местных девушек, снятых с голой грудью.

Движение FEMEN известно своими политическими топлесс-акциями. Обычно полуобнаженные активистки наносят на грудь и спину лозунги или изображения, соответствующие содержанию акции. Участницы FEMEN выступали против президента Беларуси А. Лукашенко, президента России В. Путина, бывшего премьер-министра Италии С. Берлускони и других политиков ***(Facebook заблокировал страницу FEMEN за порнографию // InternetUA (http://internetua.com/Facebook-zablokiroval-stranicu-FEMEN-za-pornografiua). – 2013. – 24.06).***

***

Министр РФ по делам открытого правительства М. Абызов считает, что госслужащие должны использовать социальные сети в определенных границах.

В июне газета Washington Post сообщила, что Агентство национальной безопасности и Федеральное бюро расследований США имеют прямой доступ к центральным серверам ведущих интернет-компаний – Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple – в рамках особо секретной программы PRISM. Директор национальной разведки США подтвердил, что американские спецслужбы собирают персональные данные только тех сетевых пользователей, которые не являются гражданами страны и проживают за рубежом. МИД РФ заявил, что при борьбе с терроризмом необходимо соблюдать нормы международного права.

«Я убежден, что во всем хороша мера. И в использовании социальных сетей, Интернета государственные служащие должны иметь определенные границы. Если это политики федерального уровня, международного уровня, руководители министерств и ведомств, то распространение частной информации, наверное, должно быть в рамках», – сказал М. Абызов журналистам в кулуарах Петербургского международного экономического форума, отвечая на вопрос о том, не откажутся ли чиновники от ведения аккаунтов в соцсетях после скандала в США. Он также отметил, что вопрос киберпреступности актуален и для России, и для зарубежных стран.

«При всем нашем желании по безграничному раскрытию информации, по предоставлению абсолютно свободного доступа к ней, нам необходимо учитывать такие критерии, как национальная безопасность, учитывать требования по сохранению личных данных гражданина. В противном случае использование информации может привести к негативным последствиям, которые нам не нужны», – сказал министр.

М. Абызов подчеркнул, что киберпреступность не знает границ. «В этом смысле разрабатывается российское законодательство о противодействии ей. Важно учитывать международный опыт и кооперацию в таких проектах», – отметил он ***(Госслужащим стоит использовать соцсети в меру // InternetUA (http://internetua.com/gosslujasxim-stoit-ispolzovat-socseti-v-meru). – 2013. – 24.06).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Діловій соцмережі LinkedIn дістався перший рядок у рейтингу найбільш швидкозростаючих технологічних компаній США, складеному Forbes (http://ua.korrespondent.net/business/web/1568665-facebook-postupivsya-zvannyam-najbilsh-dinamichnogo-tehnogiganta-inshij-socmerezhi).

Для підготовки рейтингу Forbes взяв 2,1 тис. прибуткових hi-tech-компаній з мінімальною виручкою в 150 млн дол. і капіталізацією на ринку від півмільярда доларів.

У перелік увійшли ті компанії, прибуток яких зріс як мінімум на 10 % на рік протягом трьох минулих років і на 10 % на місяць протягом 12 минулих місяців.

Більше того, однією з вимог для оцінки став сталий розвиток, який дає можливість прогнозувати зростання доходів на 10 % мінімум у наступні три-п'ять років. Після цього компанії увійшли до рейтингу щодо річних темпів збільшення виручки за минулі три роки.

LinkedIn опинилася на першому місці із середнім зростанням виручки за три роки у 102 %. На друге місце потрапила Facebook (87 %), на третє – Apple (55 %). Ще одна потужна технокорпорація, Google, розмістилася лише на 17-му рядку з зростанням продажів у 29 %.

Зазначимо, що LinkedIn – соцмережа для професіоналів, яка була запущена у 2003 р. У січні цього року аудиторія мережі перетнула позначку у 200 млн користувачів. LinkedIn використовують жителі 200 країн, які говорять 19 мовами. Велика частина «підписників» мережі – американці.

Раніше повідомлялося, що ділова соціальна мережа LinkedIn заборонила повіям пропонувати сервіс у своїх профілях ***(Facebook поступився званням найбільш динамічного техногіганта іншій соцмережі // Корреспондент.net (http://ua.korrespondent.net/business/web/1568665-facebook-postupivsya-zvannyam-najbilsh-dinamichnogo-tehnogiganta-inshij-socmerezhi). – 2013. – 10.06).***

***

Акции крупнейшей в мире соцсети Facebook потеряли почти пятую часть стоимости на Nasdaq за месяц на фоне прогнозов аналитиков о замедлении темпов роста выручки компании и негативной реакции пользователей на запуск программной оболочки Facebook Home, свидетельствуют данные биржи.

Цена акций Facebook на закрытии Nasdaq в четверг, 6 июня составляла 22,97 дол. – на 18,9 % меньше, чем на закрытии торгов месяц назад, 6 мая. Ценные бумаги Facebook потеряли почти 40 % стоимости по сравнению с ценой, которые они получили в ходе первичного публичного размещения в мае прошлого года.

На снижение могли повлиять как показатели продуктов Facebook, так и прогнозы экспертов. Аналитик Д. Манстер из Piper Jaffray написал клиентам, что популярность Facebook среди молодежи снижается. «Мы также считаем, что есть естественный лимит времени, которое пользователь в среднем может провести на социальных платформах за день. Однако важным остается выбор платформы», – пишет он. Однако операционный директор Facebook Ш. Сандберг на конференции D11 опровергла это опасение, отметив, что подростки по-прежнему активны на Facebook.

По словам Д. Манстера, начиная с июня, может замедлиться рост рекламной выручки Facebook. Однако аналитики из Goldman Sachs подтвердили рекомендацию «покупать» по акциям Facebook, отмечая, что соцсети удается монетизировать мобильное направление. Напомним, что в I квартале на долю мобильной рекламы пришлось порядка 30 % всех рекламных доходов Facebook или 375 млн дол.

На снижение акций Facebook могла повлиять и негативная реакция пользователей на запуск программной оболочки Facebook Home (приложение имеет рейтинг лишь 2,3 балла из 5 в магазине Google Play), а также недавний отказ крупных рекламодателей от продвижения на Facebook из-за системы модерации контента. Так, их реклама появлялась на Facebook рядом с записями, которые пропагандируют насилие над женщинами. Администрация соцсети уже пообещала обновить правила, по которым идентифицируется дискриминирующий контент, и провести тренинг для сотрудников ***(Акции Facebook потеряли почти пятую часть стоимости за месяц // InternetUA (http://internetua.com/akcii-Facebook-poteryali-pocsti-pyatuua-csast-stoimosti-za-mesyac). – 2013. – 10.06).***

***

Сервіс мікроблогів Twitter відкрив своїм користувачам доступ до інструмента, який дає змогу вивчати реакцію читачів на їхні твіти (http://ua.korrespondent.net/business/web/1570578-twitter-dozvoliv-koristuvacham-divitisya-statistiku-i-stvoryuvati-promo-roliki).

Зокрема, Twitter показує, скільки користувачів підписалося і відписалося від акаунту в той чи інший день, а також кількість ретвітів, додавань у вибране і відповідей на кожен твіт.

Крім того, якщо користувач публікував посилання, на сторінці статистики можна подивитися, скільки осіб перейшло за ними (у цьому випадку враховується загальна кількість переходів за посиланням в усьому Twitter).

Сама статистика доступна на сторінці, яка використовується для керування рекламними кампаніями. Після введення своїх даних користувачеві потрібно перейти у вкладку Timeline activity, приховану в меню Analytics в шапці сторінки.

Російськомовні користувачі під час заходу на сторінку зі статистикою бачать попередження, у якому говориться, що рекламу можуть розміщувати

тільки власники англомовних акаунтів, які живуть у США. Самі дані при цьому залишаються доступними. На момент написання замітки частина статистики відображалася некоректно.

Зазначимо, що раніше статистику бачили тільки рекламодавці, що проводили кампанії в Twitter. Для решти користувачів сервіс став доступний без офіційного оголошення.

Промо-відеоролики про акаунт користувача.

Крім того, Twitter спільно з американським стартапом Vizify запустив функцію створення промо-відеороликів, які допоможуть створити у потенційних передплатників перше враження про акаунт користувача.

Як ідеться в повідомленні Twitter, функція під назвою # FollowMe дає змогу зібрати з твітів користувача, списку його постійних читачів, опублікованих ним фотографій і відеороликів коротку відеопрезентацію його акаунту, яка супроводжуватиметься музикою.

Приклади роликів від відомого баскетболіста К. Брайана (за першоджерелом) та актриси Е. Райлі тривають близько 40 секунд кожен.

Для створення відеоролика необхідно дозволити доступ Vizify до свого Twitter-акаунту. Ролик буде створено в автоматичному режимі, однак до його публікації користувач зможе змінити його елементи. У результаті вийде промо-ролик, який візуально продемонструє найбільш яскравий зміст акаунту користувача потенційним передплатникам.

Раніше повідомлялося, що Twitter має намір інвестувати в телекомпанії ***(Twitter дозволив користувачам дивитися статистику і створювати промо-ролики // Корреспондент.net (http://ua.korrespondent.net/business/web/1570578-twitter-dozvoliv-koristuvacham-divitisya-statistiku-i-stvoryuvati-promo-roliki). – 2013. – 14.06).***

***

45 % людей, ищущих отзывы о компании, находят в глобальной сети информацию, изменяющую их мнение, сообщает oborot.ru. При этом мнению родных и знакомых доверяют только 70 % респондентов, в то время как отзывам из Интернета склонны верить 92 % опрошенных.

Отсюда вывод: если не заниматься проблемой репутации собственной компании в сети, недолго остаться без клиентов. В особенности это касается работы с социальными медиа. Как подсчитали аналитики mdgadvertising.com, в соцсетях 70 % пользователей ищут мнения других клиентов той компании, куда они собираются обратиться. А совсем показательно то, что даже в США лишь 40 % специалистов по работе с репутацией готовы к ситуации, когда общественное мнение будет направлено против компании в кризисной ситуации ***(Отзывам в Интернете клиенты доверяют больше, чем родным и близким // InternetUA (http://internetua.com/otzivam-v-internete-klienti-doveryauat-bolshe--csem-rodnim-i-blizkim). – 2013. – 13.06).***

***

Исследование стартапа в сфере рекламы и аналитики – Optimal – показало: сообщества больших брендов быстрее растут в Twitter, чем в Facebook.

Анализ включил 4330 страниц брендов в обеих соцсетях или 3,49 млрд друзей брендов в Facebook и 595 млн «фолловеров» в Twitter. В течение недели (судя по всему, имеется в виду 10–16 июня 2013 г. – Ред.) корпоративные страницы в Facebook подросли на 18,5 млн новых последователей, а аккаунты в Twitter набрали 4,5 млн.

Таким образом, Optimal делает вывод о том, что в процентном соотношении бренды в Twitter растут на 55 % быстрее, чем в Facebook. Однако в абсолютных числах сообщества в Facebook по-прежнему существенно обгоняют Twitter. И хотя аналитики стартапа полагают, что сравнивать две столь непохожие социальные сети – это все равно что сравнивать яблоки с апельсинами, подсчет «фолловеров» пока остается единственным способом оценки продвижения в соцсетях.

Например, Twitter-аккаунт фотосервиса Instagram растет быстрее, чем его аккаунт в Facebook: 279 500 новых подписчиков против 214 300. При этом общее число «фолловеров» Instagram в Twitter значительно превышает аналогичный показатель в Facebook: 21,3 млн и всего 4,6 млн.

По мнению генерального директора Optimal Р. Литерна, исследование доказывает, что микроблоги – более подходящая площадка для маркетинга брендов, поскольку их аудитория, хоть и меньше по размеру, но более активная.

Впрочем, ситуация далеко не однозначна. Известно, что в Twitter широко распространена деятельность посредников, с помощью которых можно купить благосклонность «фолловеров». Купить лайки в Facebook, в общем, тоже можно, но это дороже и сложнее ***(Бренды в Twitter растут быстрее, чем в Facebook // Marketing Media Review (http://mmr.ua/news/id/brendy-v-twitter-rastut-bystree-chem-v-facebook-35102/). – 2013. – 18.06).***

***

Глава компании Facebook М. Цукерберг побывал с кратким визитом в Южной Корее. После встречи с президентом страны П. К. Хе основатель крупнейшей в мире соцсети провел переговоры с вице-председателем Samsung Л. Джей-Йонгом и главой мобильного подразделения Дж. К. Шином.

Как утверждают отраслевые наблюдатели, М. Цукерберг пытался уговорить руководителей Samsung выпустить Facebook-смартфон.

«Facebook всеми силами стремится стать второй Google. Именно с этой целью М. Цукерберг и обратился к Samsung с просьбой об активизации сотрудничества и выпуске смартфона с пользовательским интерфейсом Facebook», – сообщил специалист, имя которого не раскрывается.

По его мнению, ответ Samsung вряд ли будет позитивным, так как сотрудничество с Facebook не принесет корейскому гиганту ни реальной, ни символичной выгоды. Скорее наоборот – Samsung не захочет помогать Facebook и «выращивать» вторую Google, поскольку последняя уже стала для Samsung серьезным соперником на рынке мобильных телефонов, отметил эксперт. Как известно, в 2012 г. Google приобрела Motorola Mobility, и в настоящее время компании готовят к выходу смартфон MotoX, который может стать основным конкурентом iPhone.

Кроме того, выпуск Facebook-смартфона не сможет укрепить имидж торговой марки Samsung. В общем, такой альянс не принесет компании никакой пользы, констатирует наблюдатель ***(Цукерберг просит Samsung выпустить «Facebook-смартфон» // InternetUA (http://internetua.com/cukerberg-prosit-Samsung-vipustit--Facebook-smartfon). – 2013. – 19.06).***

***

Украинские работодатели терпимо относятся к пользованию соцсетями и мессенджерами на работе, а работники обычно не злоупотребляют таким доверием. Больше чем в половине офисов открыт доступ к таким ресурсам, и всего 15 % из тех, кто имеют возможность онлайн-общения, сочли, что делают это чаще, чем стоит, выяснили аналитики кадрового портала hh.ua.

Как сообщили в компании, не все работодатели доверяют своим сотрудникам и открывают для них доступ, к примеру, в Facebook или Twitter. Половина респондентов (53 %) отмечают, что доступ к любым соцсетям у них на работе полный и открытый. Еще 10 % работодателей хоть и позволяют сидеть в соцсетях, но следят за злоупотреблениями. 8 % фирм пускают на такие ресурсы лишь тех, кто непосредственно с ними работает. Не все работодатели доверяют своим сотрудникам и открывают для них доступ, к примеру, в Facebook или Twitter.

Негласно оспаривать политику руководства решаются лишь 12 % опрошенных. Они умеют получать доступ к запретным сайтам и регулярно этим пользуются. Еще треть респондентов не нарушает запрет вопреки знанию схемы. Кроме того, почти половина опрошенных сотрудников (45 %) уважают решение работодателя, полагая, что социальные сети на работе им не нужны.

Опрос выявил, что даже те, кто может общаться в соцсетях, пытаются не злоупотреблять такой возможностью. Чаще всего, делают это изредка, чтобы передохнуть (45 %). Кроме того, для 10 % социальные ресурсы – это часть работы. Лишь 15 % сознались, что «висят» в соцсетях постоянно.

Вопреки тому, что Интернет используется почти во всех офисах страны, а соцсети и мессенджеры – более чем в каждом втором, около трети компаний работает без каких-либо норм и лимитов в этой сфере. В 28 % компаний соцсети и мессенджеры полностью зависят от доброй воли администрации, а еще почти в пятой части (17 %) – от политики IT-отдела.

Отметим, что только 20 % работодателей создали четкую и понятную корпоративную политику относительно этого ***(Опрос выявил отношение украинских работодателей к соцсетям // Минфин (http://minfin.com.ua/2013/06/19/773722/). – 2013. – 19.06).***

***

Facebook сообщила, что количество активных рекламодателей, использующих соцсеть хотя бы раз в 28 дней, по всему миру составило 1 млн. В компании отмечают, что на сегодняшний день подавляющее большинство рекламодателей в Facebook – это представители западного малого бизнеса, пишет «Вести Экономика».

Компания планирует расширять сеть рекламодателей и за счет совсем небольших локальных компаний, занимающихся продажами разных товаров, от ювелирных украшений до одежды.

Неизвестно, какую именно сумму каждый рекламодатель тратит на продвижение в Facebook, но, по оценкам eMarketer, в 2012 г. в США общие затраты на онлайн-рекламу составили около 32 млрд дол.

«Большая часть рекламодателей на Facebook – начинали как простые пользователи социальной сети, затем создавали страницы своих компаний, а потом – становились рекламодателями», – говорит Д. Леви, директор по работе с малым бизнесом Facebook.

По его словам, на сегодняшний день так называемые рекламные аккаунты – это 85 % выручки Facebook. Однако в эту же сумму входят доли от кампаний крупнейших мировых брендов, которые также рекламируются на Facebook.

В прошлом квартале Facebook сообщила о выручке в размере 1,46 млрд дол. Доходы от рекламы возросли на 43 %, показав самый быстрый темп роста с конца 2011 г. Facebook, впрочем, не сообщает, сколько времени потребовалось, чтобы преодолеть порог в 1 млн рекламодателей.

В качестве практического кейса можно привести пример К. Колфилд, которая владеет предприятием малого бизнеса в Калифорнии. Фирма занимается изготовлением ювелирных украшений ручной работы из конского волоса. По словам К. Кимберли, реклама на Facebook помогает ей привлечь новых клиентов. Рекламная кампания обходится ей приблизительно в 25 дол. в день. За эту сумму, она получает аудиторию в 5 млн человек потенциальных клиентов.

Примечательно, что более 50 % владельцев предприятий малого бизнеса используют для рекламы своих товаров и услуг функционал «Страницы» и только 16 % используют обычные рекламные объявления в соцсети ***(Количество рекламодателей Facebook достигло 1 млн // Utro.ua (http://www.utro.ua/ru/zhizn/kolichestvo_reklamodateley_facebook_dostiglo_1_mln1371648446). – 2013. – 20.06).***

***

Компания Facebook объявила о выходе трех обновлений, касающихся брендовых постов со ссылками. Благодаря изменениям рекламодатели получили возможность оптимизировать изображения, создавать неопубликованные посты со ссылками, не уходя со страницы создания объявления. Также владельцы страниц открыли для себя больше опций в настройках и создании объявлений со ссылками на внешний сайт.

Рекламодатели теперь самостоятельно смогут контролировать работу с изображениями: Facebook больше не вытягивает миниатюру с сервера сайта, ссылка которого располагается внутри поста. Для размещения и оптимизации нужного вам изображения можно использовать Page composer, страницу создания объявления, Power Editor или API.

Facebook позволяет создавать новый неопубликованный пост с ссылкой прямо на странице создания объявления. До сих пор рекламодателям приходилось выбирать и продвигать уже существующий пост. Цель этого нововведения – упростить функционал, чтобы рекламодатели могли таргетировать объявления по категориям.

Согласно данным Facebook, рекламные объявления со ссылками по многим показателям обгоняют рекламные блоки, находящиеся с правой стороны страницы. Для того чтобы увеличить число рекламодателей, которые будут публиковать свои объявления в новостной ленте, им предоставили право выбора: размещать рекламный блок с правой стороны страницы или неопубликованный пост с ссылкой в новостной ленте, хотя раньше подобные объявления по умолчанию появлялись в правой колонке.

По заявлению Facebook, эти обновления были реализованы для того, чтобы увеличить внешнюю конверсию и поднять уровень продаж брендов ***(Обновления Facebook: оптимизация рекламных постов со ссылками // Marketing Media Review (http://mmr.ua/news/id/obnovlenija-facebook-optimizacija-reklamnyh-postov-so-ssylkami-35114/). – 2013. – 20.06).***

***

YouTube предлагает сотне ведущих рекламодателей новые возможности по созданию контента для их видеоплатформ. Это самый серьезный, на сегодняшний день, шаг компании, направленный на то, чтобы убедить маркетологов немного отойти от традиционной телевизионной рекламы.

Принадлежащий Google видеогигант для начала заключил договоры с American Express, General Electric, Johnson & Johnson и PepsiCo. Планируется, что в новой программе в целом примут участие сто рекламодателей со всего мира.

«Определенный креативный подход, который принят на YouTube, просто невозможен на телевидении, – сказал на фестивале “Каннские львы” Р. Кинкл из YouTube. – Мы можем выйти за пределы 30-секундного ролика, мы можем снять хоть полноценное шоу. В телевизионной же рекламе очень

мало творческой свободы, в ней невозможно двустороннее общение, ею нельзя поделиться с друзьями и нет того эффекта, который ваш контент получает на YouTube».

Эта инициатива является расширением технической и стратегической поддержки, которую YouTube оказывает ведущим создателям контента. Еще в 2007 г. сайт запустил партнерскую программу, способную помочь в увеличении популярности ведущим пользователям YouTube. Таким, есть Маркес «Нонстоп» Скотт – уличный танцор с рекордным числом подписчиков, снимавшийся в том числе и врекламе разнообразных брендов (к примеру, в ролике Peugeot 208).

В программе в настоящее время участвует больше миллиона ведущих креативщиков, которыми руководят сотни «ютьюбовских» боссов.

«Рекламодатели получат такой же высококлассный сервис, как и креативщики, – сказал Р. Кинкл. – К каждому рекламодателю будет приставлен свой контент-менеджер, который поможет в работе с каналами, в разработке стратегий и проконсультирует по сотрудничеству с аудиторией».

Р. Кинкл, с помощью презентаций кампаний для таких брендов, как Dove и TopShop, рассказал о стратегиях, в рамках которых YouTube становился основным рекламным каналом. Однако в разговоре с Guardian Р. Кинкл отрицал, что его цель – заставить рекламодателей вывести свои рекламные средства с телевидения и перенаправить их на YouTube.

«Рекламодатели, работающие с креативными агентствами, привыкли к тому, что получают меньшее (телерекламу) за большие деньги. Мы же думаем о создании диалога с аудиторией. А это далеко не только телевизионная реклама четыре раза в год. Рекламодателям надо пересмотреть свои бюджеты и понять, что работа с YouTube гораздо более практична. Я говорю о том, что они смогут работать как создатели интересного контента, а не только как рекламодатели».

Четыре рекламодателя-первопроходца начнут свою работу с YouTube в сентябре, когда в их лос-анджелесских офисах пройдут недельные мастер-классы по созданию контента. Планируется, что к концу года в программе примут участие сто рекламодателей ***(YouTube открывает программу для рекламодателей // Marketing Media Review (http://mmr.ua/news/id/youtube-otkryvaet-programmu-dlja-reklamodatelej-35153/). – 2013. – 21.06).***

***

Соцсети лишают экономику РФ 10 млрд дол. В рублях ущерб составляет от 281,7 до 311,5 млрд в год, подсчитали в Институте стратегического анализа ФБК.

Аналитики поставили цель оценить потери от нецелевого использования рабочего времени. Подсчеты строились следующим образом: к концу 2012 г. число россиян – пользователей социальных сетей – достигло 51,8 млн человек. По данным исследования ComScore, в 2012 г.

россияне проводили в социальных сетях в среднем 25,6 мин. в день (или 12,8 ч. в месяц), в том числе и на работе.

«Такое нецелевое использование рабочего времени имеет вполне определенные экономические потери (работодатель, фактически, оплачивает “сидение” работника в соцсети). Я уже не говорю о том, что согласно некоторым (небесспорным) исследованиям, это ведет к существенному снижению производительности труда – чтобы восстановить производительность труда после перерыва, необходимо более 20 мин.», – отметил директор Института стратегического анализа ФБК И. Николаев.

Согласно расчетам, в 2012 г. каждым активным в соцсетях работником было потеряно 3187,2 мин., или 53,1 ч. рабочего времени. Аналитики установили нижнюю и верхнюю границы возможных потерь – исходя из структуры пользования соцсетями работниками разных отраслей и по средним значениям для экономики в целом. В нижней границе размер экономического ущерба составил 281,7 млрд руб., в верхней – 311,5 млрд руб.

«Конечно, это примерная оценка, – добавил И. Николаев. – Для того чтобы назвать точные цифры, необходимо детализированное исследование аудитории соцсетей, данные о времени, проводимом в соцсетях представителями каждого сегмента аудитории, данные о размере заработных плат таких работников и т. д». Тем не менее, по словам эксперта, полученная оценка позволяет судить о масштабе потерь.

«Оценки, безусловно, весьма приблизительные, – согласилась аналитик Инвесткафе Д. Пичугина. – Думаю, что корректно оценить ущерб невозможно, так как для этого необходимо провести более масштабное исследование, говорить с пользователями соцсетей напрямую, а не усреднять данные. Сотрудники могут общаться по работе, могут делать это без ущерба, например, в обеденный перерыв. Кроме того, можно находиться онлайн, но при этом не быть вовлеченным в общение. Здесь очень много деталей, которые учесть за счет усреднения и экстраполяции невозможно. Гораздо большие потери, по идее, должны приносить перекуры, так как курят больше людей, чем сидят в соцсетях. Также нет точных исследований о том, что соцсети снижают работоспособность. Зато известно, что работник должен делать перерывы в работе каждый час на некоторое время для повышения эффективности труда».

Если исходить из структуры использования соцсетей работниками разных отраслей (тут большое значение имеет уровень зарплаты по тому или иному виду экономической деятельности), то наибольший экономический ущерб причинили те, кто трудится в сфере финансов и операций с недвижимым имуществом, аренды и предоставления услуг (67,9 млрд руб.), на втором месте – работники образования (39,8 млрд руб.), на третьем – государственного управления и обеспечения военной безопасности и социального страхования (36,6 млрд руб.). Самые

незначительные экономические потери от активных в соцсетях россиян, занятых сельским и лесным хозяйством (0,9 млрд руб.).

Впрочем, есть и оптимистичный вывод: по сравнению с аналогичными оценками по США и Великобритании в России экономические потери от соцсетей выглядят не такими уж большими.

Так, ежегодные потери экономики США от социальных сетей оцениваются в 650 млрд дол. По мнению экспертов ФБК, пока проблема использования соотечественниками соцсетей не является острой, но в будущем ситуация может измениться.

«Работодатели уже осознают серьезность проблемы и даже предпринимают определенные меры. Можно прогнозировать, что они будут вынуждены активизировать усилия по противостоянию “сидению” работников в соцсетях, особенно с учетом того, что проблема повышения производительности труда в российской экономике остается по-прежнему актуальной», – резюмировал И. Николаев ***(Соцсети лишают экономику РФ 10 млрд долларов // InternetUA (http://internetua.com/socseti-lishauat-ekonomiku-rf-10-mlrd-dollarov). – 2013. – 24.06).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Facebook может стать причиной разлада семейных отношений. Об этом заявили специалисты по психологии из университетов Миссури и Гавайев. Эксперты обнаружили, что час в день, потраченный на эту социальную сеть, повышает риск ссор между мужем и женой, а следовательно и последующего развода.

Так, 80 % участников проведенного эксперимента отметили, что действительно стали ругаться с близкими именно из-за Facebook и времени пребывания в сети. Причем, если партнер начинает интересоваться аккаунтом своего спутника или спутницы, это приводит к ревности, скандалам и конфликтам.

Пользователи соцсети частенько любят посетить страничку своих бывших возлюбленных, что тоже плохо влияет на отношения. Психологи рекомендуют пореже заходить в Facebook, а чаще общаться со своей второй половинкой в реальности. Как отмечают эксперты, в прошлом году в Великобритании одна треть разводов произошла именно из-за чрезмерного увлечения социальными сетями ***(Facebook может привести к разводу // NovostiUA (http://novostiua.net/obschestvo/38656-facebook-mozhet-privesti-k-razvodu.html). – 2013. – 8.06).***

***

Зачем визуализировать свою жизнь в соцсетях.

О множестве явлений (природных и общественных) многие из нас узнают из социальных сетей, не включая телевизор и не выглядывая в окно. Специалисты говорят о стремительном распространении феномена фотовизуализации своей жизни и всего того, что человеку приходится видеть и слышать. С чем это связано и в чем кроется опасность?

Что думают специалисты

Часто движущей силой для человека становится сопричастность и выражение признательности. Для многих людей такого рода общение повышает степень собственной значимости. Человек – создание социальное, обретение одобрения зачастую становится смыслом жизни.

Можно сделать вывод: в ситуации, когда собственное внутреннее чувство удовлетворения не является предопределяющим, необходимо постоянное его подкрепление из внешней среды. Тогда, благодаря чужой оценке вашей жизни, самому удается убедиться в том, что у вас все хорошо. Есть еще дин важный момент: ощущение себя сопричастным к большому числу людей помогает одолеть нервозность, тревогу, а иногда и стыд. Но очень важно не увлечься, не путать внешнюю составляющую жизни – некий фантик, с внутренней – подлинными чувствами, которые стоят за этой внешней деятельностью.

Если человек фотографирует каждый свой шаг

Вне сомнения такому человеку не достаточно внимания. Причем это может в равной степени относиться и к тем, кто стремится к пиару будто бы по работе. Сколько бы внимания человеку не отпускалось в реальной жизни, если он проявляет показательное усердие в выкладывании себя любимого, это означает, что по какой-то причине внимания ему необходимо больше. При этом число лайков в этом случае для него будет отражением степени его признания и популярности, что обеспечит ощущение собственной востребованности ***(Зачем визуализировать свою жизнь в соцсетях // InternetUA (http://internetua.com/zacsem-vizualizirovat-svoua-jizn-v-socsetyah). – 2013. – 11.06).***

***

Подписи под фотографиями в социальных сетях имеют для пользователей куда меньшее значение, чем сами снимки.

К такому выводу пришли исследователи Университета Огайо (The Ohio State University), США в результате проведенных экспериментов.

В ходе исследований 195 студентам было предложено посмотреть учётные записи нескольких людей, в которых присутствовала фотография и небольшой рассказ человека о себе.

Первая учётная запись содержала изображение человека в кругу друзей, подписанную: «Я обожаю веселиться с друзьями». Во второй

учётной записи была фотографию человека, в одиночестве сидящего на скамейке и подпись: «Я люблю проводить время в одиночестве».

Подписи под третьей и четвёртой фотографиями не соответствовали снимкам. Человек, изображённый в кругу друзей, был подписан: «Я не очень люблю встречи с друзьями и вечеринки». А под фотографией, где человек был заснят в одиночестве, говорилось, что он любит веселиться.

Людей, принимающих участие в исследовании, просили оценить степень экстравертности каждого из этих людей.

Как выяснилось, подопытные безоговорочно поверили фотографиям, несущим положительные эмоции. Подавляющее большинство студентов оценили людей, изображенных в кругу друзей, как экстравертов, вне зависимости от текста.

Изучая фотографию человека-одиночки, они же обращали внимание на текст. У человека, который был изображён в одиночестве, и подпись которого гласила о том, что он любит общаться с друзьями, баллы были выше.

Таким образом, исследователи сделали вывод, что фотографии являются решающим фактором при оценке человека ***(При оценке человека в соцсетях фотографии важнее, чем подписи к ним // InternetUA (http://internetua.com/pri-ocenke-cseloveka-v-socsetyah-fotografii-vajnee--csem-podpisi-k-nim). – 2013. – 13.06).***

***

Публикация совместных фото в социальных сетях укрепляет семейные отношения. К такому выводу пришли учёные университета Калифорнии в рамках исследования данных супружеских пар, которые присутствуют в популярных социальных сетях. Учёные исследовали настроение людей, их отношение друг к другу и как зависит публикуемый контент от того, насколько партнёры счастливы в браке.

В результате были представлены весьма интересные выводы. Так, те супруги, которые выкладывают в социальные сети информацию о свои отношениях, будь то фотографии, видео или текстовые сообщения, намного больше довольны своими отношениями, чувствую себя защищёнными и счастливыми.

Также было доказано, что люди, которые часто публикую в социальной сети общие фотографии с супругом, чаще говорят о том, что счастливы в браке, а их семья – крепкая. Ещё одной интересной закономерностью стало то, что информацию о своих отношениях с супругом, пользователи чаще публикуют именно в те моменты, когда они особенно довольно браком.

Напомним, что это не первое исследование такого рода. Так, недавно, были опубликованы данные о том, что люди, познакомившиеся в сети Интернет, практически в два раза менее подвержены риску развода ***(Публикация совместных фото в социальных сетях укрепляет семейные***

отношения // InternetUA (http://internetua.com/publikaciya-sovmestnih-foto-v-socialnih-setyah-ukreplyaet-semeinie-otnosheniya). – 2013. – 13.06).

***

Зачем пользователи соцсетей фотографируют себя.

В социальных сетях наблюдается настоящая мания обмена «самострелами» – автопортретами, сделанными самостоятельно с помощью фронтальной камеры смартфона.

В приложении обмена фотографиями Instagram к этому моменту загружено более 23 млн фотографий с хэштегом #selfie («самострел») и еще 51 млн снимков с хэштегом #me («я»).

Знаменитости – Рианна, Джастин Бибер, Леди Гага и Мадонна – регулярно публикуют «самострелы» на своих страницах в социальных сетях. Британская модель К. Брук настолько увлеклась публикацией автопортретов, что ей пришлось самой для себя заблокировать эту возможность.

Фоторепортеры запечатлели, как дети Б. Обамы фотографировались на камеру смартфона во время инаугурации своего отца. Даже астронавт С. Робинсон сфотографировал себя во время ремонта космического челнока «Дискавери».

Когда же всех захватила эта мания?

Переломным моментом стало появление смартфонов с фронтальной камерой. Теперь все, что вам нужно, чтобы сфотографировать себя – свободная секунда и наличие у вашего смартфона фронтальной камеры. Камеры, которые могут автоматически фокусироваться на расстоянии вытянутой руки, позволяют делать автопортреты-«самострелы» в любой обстановке. Потом этим снимком сразу же можно поделиться с тысячами пользователей социальных сетей: «Посмотрите, где я! Смотрите, что я делаю! Посмотрите, как я выгляжу!» Некоторым это кажется захватывающим занятием.

19 век: первый «самострел»

Первый фотографический автопортрет, как считается, был сделан Р. Корнелиусом в 1839 г., однако неясно, можно ли приравнять такой автопортрет к нынешним «самострелам». «Похоже, что с ним был друг или ассистент, который помог ему выставить нужную выдержку», – говорит историк и генеральный директор Королевского фотографического общества М. Притчард. По его словам, вероятнее всего, первый самостоятельный автопортрет все-таки был сделан позже. Первые фотоаппараты с таймерами появились в конце 1880-х годов, они давали фотографу 5–10 сек., для того чтобы принять соответствующее положение перед съемкой. «У некоторых камер был длинный кабель, который позволял нажимать кнопку спуска затвора на расстоянии», – говорит М. Притчард. Обмен автопортретами существовал задолго до появления Интернета. В 1860-х гг. был очень популярен обмен визитками – маленькими фотокарточками.

В 1948 г. появился Polaroid, однако по-настоящему мгновенные снимки с помощью этой камеры можно было сделать только, начиная с 1970-х годов. Polaroid позволял фотографировать себя с расстояния вытянутой руки. «Большое преимущество камеры Polaroid в том, что вам не нужно проявлять пленку», – поясняет М. Притчард. Это освободило тех фотолюбителей, у которых не было специальной темной комнаты для проявления пленки, от необходимости передавать пленку в чужие руки, когда кто-то другой первым увидит сделанный вами снимок.

Некоторые люди предпочитают фотографии, которые они сделали сами. «Зеркальное отражение – это что-то очень личное и мимолетное», – говорит директор научно-исследовательского Центра медиа и психологии в Бостоне П. Рутледж. «В зеркале мы видим себя живыми и динамичными, в движении», – поясняет П. Рутледж.

Момент тщеславия

22-летняя Э. Кук из Линкольна считает, что такие «автопортреты» создают чувство уюта. «Всегда приятно запечатлеть, что у тебя в такой-то день была хорошая прическа, или ты был хорошо одет», – говорит Э. Кук. По словам девушки, в Instagram лояльное, и в основном хорошее, отношение к «самострелам». Э. Кук признается, что в публикации «самострелов» есть и момент тщеславия: если кто-то похвалит фотографию, то это может поднять настроение, когда тебе взгрустнулось. Она также считает, что публикация фотографий иногда заменяет слова. «Вместо того чтобы писать, что вы идете на работу, можно опубликовать свою фотографию в форме», – говорит Э. Кук.

По словам П. Рутледж, нам нравится экспериментировать с разными образами, и автопортреты, сделанные с помощью камеры смартфона, позволяют играть с образами. «Мы все хотим попробовать примерить новый образ и представить, как бы мы чувствовали себя в нем», – говорит П. Рутледж.

Согласно одной из теорий, автопортреты дают представление о том, как мы бы хотели, чтобы нас воспринимали. По словам психотерапевта А. Балика, автора книги о мотивации действий пользователей социальных сетей, у нас у всех есть активная и пассивная индивидуальность в соцсетях.

«Пассивная индивидуальность – эта та, над которой у вас нет контроля. Например, это та информация о себе, которую вы можете найти в сети. Или когда кто-то из ваших друзей публикует информацию о вас», – поясняет психотерапевт.

«Активная индивидуальность – та, которую вы можете контролировать, например ваш профайл в Facebook», – говорит А. Балик.

Критика и риски

«Автопортреты – это способ формирования активной индивидуальности, над чем у вас есть контроль. Вы можете делать множество снимков, но поделитесь с друзьями только тем, который вам самим нравится – даже если он простой и неприглядный», – уверен психотерапевт.

Публикации «самострелов», несмотря на свою популярность, вызывают массу критики. У многих публикация подобных портретов ассоциируется с фотографиями сексуального характера. Конечно, большинство героев «автопортретов» одеты и выглядят безобидно, однако это не избавляет авторов от возможных проблем. «Как и в случаях других действий, разрушающих социальные рамки, те, кто публикует провокационные фотографии, чтобы обратить на себя внимание, получат в ответ не только то внимание, на которое они рассчитывают, но и риск спровоцировать другую реакцию, от которой они рады были бы избавиться», – говорит П. Рутледж.

По словам Э. Кук, она не публикует ничего такого, что она постыдилась бы отправить своей маме. «Самострелы» вызывают также критику из-за того, что считаются проявлением нарциссизма и тщеславия. «С точки зрения современной культуры, люди не должны выставлять себя напоказ – особенно женщины. Но вопрос в том, как мы относимся к совместному использованию личной информации в Интернете. Увеличение уровня доступа к личной информации и изображениям, возможно, в скором времени изменит наши представления о норме», – предполагает П. Рутледж ***(Зачем пользователи соцсетей фотографируют себя // InternetUA (http://internetua.com/zacsem-polzovateli-socsetei-fotografiruuat-sebya). – 2013. – 17.06).***

***

Каждый третий украинец общается через социальные сети с друзьями чаще, чем вживую. А 18 % наших соотечественников общаются ежедневно онлайн с людьми, которых они не знают лично в жизни. Таковы результаты исследования трендов коммуникации, проведенного в Украине компанией GFK, передает «Сегодня».

Телефонные разговоры, Skype, смс и переписка в социальных сетях в большинстве случаев заменяют общение вживую в будни для 64 % наших сограждан, опрошенных в ходе исследования.

Украинцы в большинстве случаев вживую общаются в кругу семьи, или с коллегами по работе. А вот с друзьями при личной встрече мы общаемся в настоящее время в среднем на один час в день меньше, чем еще пять лет назад. И только 36 % наших граждан больше общаются вживую, чем по телефону или онлайн.

Наиболее активно (каждый или почти каждый день) украинцы общаются с мужем или женой и коллегами по работе – 78 и 75 % респондентов соответственно. Почти столько же (17 %) опрошенных каждый день общаются с родственниками, живущими отдельно (кроме родителей и детей).

При этом больше половины опрошенных (61 %) негативно относится к сокращению времени, проводимого лично с друзьями и близкими. Еще большее количество украинцев (91 %) считает общение без помощи

современных средств коммуникации более душевным и наполненным, а 85 % опрошенных отдают предпочтение общению при личной встрече. Ведь при коммуникации онлайн человеку кажется, что он постоянно контактирует с людьми, хотя на самом деле он все больше скрывает свои истинные эмоции за чередой смайликов.

55 % опрошенных считает, что при общении через Интернет легко обманывать и преувеличивать. 61 % подтверждают, что сами говорили неправду, общаясь по Интернету.

Нехватка живого общения – это не только украинские реалии. По данным компаний Badoo и Performics, 39 % американцам, 36 % англичанам и 35 % немцам комфортней общаться онлайн, нежели при личной встрече. «Поколение одиноких» – такой термин начинают использовать в своей работе психологи за рубежом.

Специалисты объясняют такое явление следующим образом: электронная почта и текстовые сообщения вызвали так называемую эпидемию застенчивости. Заочно гораздо легче создать и поддерживать определенный образ, умолчать об отрицательных чертах и сделать акцент на положительных качествах. В подтверждение этому 61 % наших соотечественников признаются, что как минимум однажды говорили неправду, общаясь по Интернету ***(Каждый третий украинец общается в соцсетях больше, чем вживую // InternetUA (http://internetua.com/kajdii-tretii-ukrainec-obsxaetsya-v-socsetyah-bolshe--csem-vjivuua). – 2013. – 19.06).***

***

Студенты, склонные к нарциссизму показывали более высокую активность публикаций в Twitter.

Постоянные «обновления статуса» и «записи на стене» в социальных сетях, которые делают люди, стремясь стать частью интернет-сообщества, могут свидетельствовать о тревожной склонности к эгоцентричному поведению. Такие выводы сделали американские ученые, опираясь на результаты сразу нескольких исследований.

Они изучали, насколько нарциссизм влияет на ежедневное количество публикаций в социальных сетях и частоту их посещения. В исследовании принимали участие 486 студентов и 93 взрослых. Средний возраст студентов составил 19 лет, 75 % из них – девушки. Средний возраст взрослых – 35 лет, большинство – белые женщины.

Оказалось, что студенты, имевшие один или несколько видов нарциссизма, показывали более высокую активность публикаций в Twitter, в то время как взрослые эгоцентрики предпочитали многократно обновлять статусы в Facebook. Именно эта социальная сеть зеркально отображает самовлюбленные склонности взрослых людей. Все дело в создании собственного желаемого имиджа и проверке общественной реакции на него. Обычно взрослые люди среднего возраста уже сформировали свое

социальное «Я». Социальные сети нужны им для получения одобрения от тех, кто уже находится в их окружении (проще говоря «в друзьях»).

Twitter наиболее популярен среди молодых людей, склонных к нарциссизму. Они часто переоценивают важность своего мнения. С помощью Twitter они стараются расширить свой круг общения и продемонстрировать свои взгляды на различные темы и проблемы.

Результаты исследования свидетельствуют о том, что студенты и взрослые используют социальные сети по-разному, но с одинаковой целью – удовлетворить свое эго и контролировать восприятие себя окружающими. Однако ученые не получили достоверной информации, подтверждающей теорию о повышенном использовании социальных сетей эгоцентричными людьми, а также о том, что социальные сети вызывают развитие нарциссизма ***(Как влияют на людей социальные сети? // Luganews – фабрика луганских новостей (http://www.luganews.com/obshhestvo/kak-vliyayut-na-lyudej-socialnye-seti.html). – 2013. – 19.06).***

***

Психологи советуют не запрещать на работе игры онлайн и социальные сети.

Есть немало людей, которые стараются использовать рабочий компьютер не только по прямому рабочему назначению, но и для того, чтобы скрасить свое рабочее время. Не секрет, что иногда работать не хочется категорически, поэтому в ход идут все средства, от поиска новых кулинарных рецептов до онлайн игрушек.

Игрушки, по мнению некоторых специалистов психологии, для гиперактивных людей являются настоящей панацеей для того, чтобы не сгореть на работе. Это совсем не говорит, что они плохие работники, просто для многих постоянное сидение на месте является тяжелым испытанием из-за собственной активности. И им просто необходимо отвлекаться на что-то, что потребует переключения внимания и спровоцирует выброс адреналина.

Многие работодатели запрещают на работе устанавливать собственные программы, общаться в социальных сетях, полагая, что все эти компьютерные развлечения просто крадут рабочее время работодателя, которое он все равно оплачивает. Однако квалифицированный труд, особенно если работа творческая, требует со стороны работодателя определенных жертв. Тем более фактор наличия-присутствия все чаще становится малоактуальным из-за того же развития высоких технологий. Ведь по большому счету важно, чтобы работа была сделана качественно и в срок.

Поэтому психологи советуют работодателям не запрещать сотрудникам маленькие радости. Работа от этого не пострадает, потому что если человек хочет отлынивать от работы, он найдет как это сделать. А переключение в процессе совершения работы иногда просто необходимо, чтобы не закипели мозги ***(Психологи советуют не запрещать на работе***

игры онлайн и социальные сети // InternetUA (http://internetua.com/psihologi-sovetuuat-ne-zapresxat-na-rabote-igri-onlain-i-socialnie-seti). – 2013. – 24.06).

Маніпулятивні технології

Віце-прем'єр РФ Д. Рогозін назвав соціальні мережі одним з видів зброї в кібервійні, у тому числі проти Росії. За його словами, з їхньою допомогою інші держави впливають на громадську думку росіян (http://ua.korrespondent.net/world/russia/1568126-prava-ruka-medvedeva-nazvav-socmerezhi-znaryaddyam-u-kibervijni-proti-rosiyi).

«Через них іде найпотужніша маніпуляція громадською думкою, адже різні лайки та інші кнопки, які ви там натискаєте, моментально вводять вас у певні групи, які потім аналізуються, систематизуються», – заявив Д. Рогозін.

На його думку, соціальні мережі дають можливість маніпулювати людьми, які, наприклад, дотримуються опозиційних поглядів, заманюючи їх в окремі спільноти.

«Тим самим збільшується кількість тих людей, які починають отримувати спеціальну контентну інформацію, яка підриває авторитет влади та цінності держави. Ми знаємо, що це активно застосовується», – розповів заступник голови російського кабміну.

За словами чиновника, в США навіть є спеціальний департамент, який займається подібними речами, і що він зустрічався з головою цього відділу. За інформацією Д. Рогозіна, завданням такого відомства є «застосування соціальних мереж для досягнення США своїх військових цілей невійськовим шляхом».

Крім того, у квітні 2013 р. на засіданні ради при військово-промисловій комісії Д. Рогозін повідомив про важливість забезпечення країни кібербезпекою, сказавши, що «кошти для кіберборотьби виходять на перший план» ***(Права рука Медведєва назвав соцмережі знаряддям у кібервійни проти Росії // Корреспондент.net (http://ua.korrespondent.net/world/russia/1568126-prava-ruka-medvedeva-nazvav-socmerezhi-znaryaddyam-u-kibervijni-proti-rosiyi). – 2013. – 7.06).***

***

Экстремисты через соцсети занимаются обработкой потенциальных сторонников, а некоторые части «всемирной паутины» стали инкубатором их идей, заявил глава ФСБ России А. Бортников на заседании Национального антитеррористического комитета (НАК).

«В социальных сетях создаются закрытые группы, активизируется деятельность сайтов, на которых ведется целенаправленная идеологическая обработка пользователей, развернута широкомасштабная работа по привлечению новых сторонников. Часть Интернета, по существу, становится

своеобразным инкубатором и источником идей экстремизма», – приводит слова А. Бортникова НАК.

В связи со всем этим, как заявлял в начале июня А. Бортников, спецслужбы мира должны занять в Интернете не оборонительную, а наступательную тактику против экстремистских сайтов ***(Глава ФСБ: социальные сети – инкубатор экстремизма // Главком: Новости политики и экономики (http://glavcom.ua/news/133673.html). – 2013. – 11.06).***

***

Группа родителей из США обратилась в компанию Facebook с призывом отменить установку по умолчанию опции определения местоположения пользователя (геолокацию) для сервиса публикации фото в Интернете Instagram. Обращение размещено на интернет-ресурсе change.org.

Родители указывают на то, что при регистрации несовершеннолетними пользователями аккаунта в Instagram они зачастую не обращают внимания на то, что в сервисе по умолчанию установлена функция определения местоположения пользователя в момент выкладки фото в Интернет, хотя возможность ее отключения есть. При этом также по умолчанию в Instagram включена функция публичности сети, то есть открытого доступа ко всем размещенным фото и данным их авторов, включая сведения о местоположении.

В результате, как указывают родители, несовершеннолетние дети подвергаются опасности, так как данные об адресах их школы, дома, наиболее часто посещаемых мест оказываются доступны практически любому пользователю Интернета.

Поэтому родители обратились к руководству компании Facebook, которой принадлежит сервис Instagram, с призывом установить в нем по умолчанию для несовершеннолетних пользователей выключенными функции определения местоположения и публичности сети. Они также призвали всех заинтересованных присоединиться к обращению. На сегодня, судя по данным ресурса change.org, обращение поддержали 20 тыс. пользователей ***(Родители требуют отменить геолокацию в Instagram // InternetUA (http://internetua.com/roditeli-trebuuat-otmenit-geolokaciua-v-Instagram). – 2013. – 10.06).***

***

Экс-министр финансов Крыма А. Гресс, вот уже три года находящийся за решеткой в ожидании приговора, с помощью одного из крымских журналистов завел страницу в Facebook – рукописи представителю СМИ передает адвокат. В соцсети А. Гресс критикует судебную систему, обвиняя правоохранителей в фабрикации уголовного дела против него, передает сайт «Крым.Комментарии».

А. Гресс сообщил, что, будучи на свободе, он не вел блогов и не заводил страниц в соцсетях, но сейчас ощутил в этом потребность.

«Сегодня, находясь в тюрьме, пожалуй, это один из действенных способов не только справиться с мукой – мукой не высказанного слова, но и высказываться минуя систему – напрямую, без корректур. И ценность этой возможности несоизмеримо больше, чем для тех, кто находится по другую от меня сторону решетки. Своего рода эта возможность позволяет пройти сквозь эту решетку, в т. ч. и назло всем этим рабам системы – прокурорам, судьям, тюремщикам – людям без собственного мнения. Их почему-то очень бесит эта возможность иметь собственное мнение и открыто высказываться», – пишет А. Гресс.

Он также выразил возмущение, что приговор в отношение него до сих пор не вынесен. «Когда он будет, я не могу и предположить. Уголовное дело заказное, контролируется из Киева. Фабрикация дела выполнена топорно: отсутствует не просто состав преступления, а и вообще – событие преступления. Что писать в приговоре? – самому интересно. В правосудие разумеется не верю. Нельзя верить в то, чего, точно знаешь, не существует», – написал экс-министр.

При этом он предположил, что в ответ на его заявления с помощью правоохранителей в СМИ могут появиться порочащие его публикации.

«Сразу прошу всех “законников” в погонах, в т. ч. и Службу опасности (которая фабриковала по мне дело), в общем всех, кого в тюрьме называют одним емким словом – мусора, не срываться с одного места как угорелые, чтобы пресечь это безобразие. Не надо заставлять зависимых от вас хозяев некоторых СМИ, размещать в ответ пасквили – какой я негодяй. Рейтинги меня давно не интересуют, а доверия правоохранительной системе это и так не добавит – вам же никто не доверяет. Не заблуждайтесь – век ваш не вечен. А насчет мусоров, то это верно. Вы ненужный мусор для страны, который даже для переработки не годится», – написал он.

Напомним, 12 июня 2010 г. правоохранители арестовали председателя наблюдательного совета института «КрымНИИпроект», экс-министра финансов Крыма А. Гресса, которого подозревают в незаконном присвоении 60 млн грн и крупных земельных махинациях ***(Крымский экс-министр из-за решетки драконит в соцсетях силовиков // Территория Крым (http://t-crimea.com/novosti-kryma/2040-krymskiy-eks-ministr-iz-za-reshetki-drakonit-v-socsetyah-silovikov.html). – 2013. – 13.06).***

***

Зачем за вами следят американцы?

С 2001 г. в Соединенных Штатах работает система слежки за гражданами. Ее инициировал тогдашний президент США – Д. Буш. А на прошлой неделе газеты The Washington Post и Guardian сообщили: американское правительство следит за иностранцами в онлайне. Зачем и что в этом удивительного?

В мае 2013 г. 22-летнего американца Д. Д. Симса приговорили к шести месяцам тюрьмы. В своем Twitter он написал: «Секретная служба будет бессильна, когда я направлю винтовку в лоб Бараку». Федеральный суд Северной Каролины посчитал это сообщение угрозой президенту США.

В решении суда есть простая логика. Б. Обама – главный человек в США, принимающий финальное решение: куда направить войска, и в какую сторону «смотрят» ракеты с ядерными боеголовками. А Д. Д. Симс – исламист, возможно, террористического толка. Тюремный срок для него – это назидание всем прочим острословам, кто угрожает смертью президенту в публичном месте.

Важно понимать, что социальная сеть – это именно публичное место. Не важно, где человек делает свои громкие заявления – на многолюдной улице, или в Twitter. В двух местах его могут услышать тысячи людей. Разница незначительная. В Интернете можно скрыть себя под выдуманным именем, или фотографией другого человека. На улице это сделать сложнее. Но смысл слов в обеих случаях идентичен. Философ М. Маклюэн утверждал, что «медиа – это дополнительная нервная система человека». То есть, любая форма медиа – это эмуляция реальной жизни.

PRISM – это вынужденное решение. США – страна завоевателей, ведущая активную, и часто, агрессивную политику. У нее много недоброжелателей, особенно в числе исламских фундаменталистов. В реальной жизни против них применяют армию и полицию. Чтобы не распоясались. У армии есть разведка, которая сообщает о передвижениях противников, их числе и составе. У полиции тоже есть осведомители. Аналогичный инструмент нужен в Интернете.

Арабские революции и конфликты арабской молодежи с европейскими политиками начинались в электронных коммуникациях – через Twitter, мессенджеры в Blackberry, смс-ки. Для коммуникаций друг с другом нужно использовать максимально эффективные средства. Если таковыми сейчас являются социальные сети, то почему нет?

Для предупреждения массовых волнений любые средства хороши. Для этого и был придуман PRISM – в сущности обычная, пускай и с флёром загадочности, система отслеживания реакций людей на что-то. Это называется – «система отслеживания репутации».

Точно таким же образом американский PRISM отслеживает репутацию США у своих граждан. И когда наступает момент «вмешательства полиции, суда или армии», система сыграет свою ключевую роль. Если бы Великобритания могла парализовать систему обмена сообщениями Blackberry, то задушила бы арабский бунт в первый же день. А если бы использовали PRISM, то никакого бунта, сожженных домов и разграбленных магазинов не было бы.

Самое забавное, что ключевая суть PRISM в сборе публичных данных, а ее вмешательство в частную жизнь американцев или иностранцев не

доказано. Например, Facebook и Apple опровергли информацию о том, что они предоставляют свои серверы для изучения сотрудниками ФБР или ЦРУ.

А если и вмешиваются, то обычному человеку скрывать нечего. Американскому правительству нет дела до его любимых игрушек из секс-шопа, если он не собрался убивать президента. Американцы следят за вами, чтобы сохранить целостность своей страны и не допустить повторение 11 сентября 2001 г. Как бы высокопарно это не звучало, но лучшего способа ловить террористов до совершения ими преступления не существует.

В дополнение ко всему, директор национальной разведки США Д. Клеппер заявил: «Информация, собранная в рамках этой программы, является наиболее важной и ценной и используется исключительно для защиты нашей нации от множества угроз. Несанкционированное раскрытие информации об этой важной и полностью узаконенной программе является предосудительным и подвергает риску безопасность американцев» ***(Дидковский С. Зачем за вами следят американцы? // Левый берег (http://world.lb.ua/news/2013/06/13/206217_zachem_sledyat_amerikantsi.html). – 2013. – 13.06).***

***

Феномен вітчизняної пенітенціарної системи: сидячи в камері під найсуворішою, здавалося б, охороною, українські арештанти примудряються вільно виходити в Інтернет та невимушено спілкуватися з друзями в соціальних мережах. Звучить, як анекдот, але це на жарти, а чистісінька правда, до якої нещодавно дошукалася прокуратура Херсонщини. Під час моніторингу всіляких Facebook та Живих Журналів правоохоронці виявили там персональні сторінки громадян, чиї обличчя здалися їм до болю знайомими. Дводенна перевірка дозволила переконатися, що сторінки належать дев'ятьом громадянам, котрі у даний час арештовані за підозрою у скоєнні тяжких і особливо тяжких злочинів, та знаходяться у слідчому ізоляторі Херсона. Звісно, вони могли створити сторінки у мережах до арешту, однак на них хтось регулярно розміщував свіжі фотографії арештантів та їхніх співкамерників, ще й із гордовитими коментарями – ось, мовляв, ми які, для нас і решітки не перепона!

«Найпершим для нас питанням було – яким чином арештовані примудрялися виходити в Інтернет? Для відповіді на нього організували обшуки у камерах, де знаходилися власники сторінок, і відшукали в них заборонені предмети – три мобільні телефони з тими ж фотографіями, що викладалися у соціальних мережах. Це здалося дуже дивним – адже лише за два дні до того у камерах уже був обшук, і ніяких телефонів тут чомусь не знайшли, – спантеличений начальник відділу нагляду за дотриманням законів при виконанні судових рішень по кримінальних справах прокуратури Херсонщини С. Донєв. – За наслідками перевірки до обласного управління Державної пенітенціарної служби внесли подання про притягнення до

дисциплінарної відповідальності посадовців із числа співробітників слідчого ізолятору».

«Подання разом із знімками вже отримали, але з фотографій не видно, де вони зроблені – у камері слідчого ізолятору, на “пересилці”, чи може, у міліцейському ізоляторі внутрішнього тримання. Призначили службове розслідування, будемо розбиратися. Поки висновки робити зарано», – продовжив начальник обласного управління Державної пенітенціарної служби України, генерал-майор В. Піньокас.

За технічним прогресом закон не встигає

Словом, загадкові арештантські сторінки у соціальних мережах уже наробили чимало галасу та можуть «поховати» кілька кар’єр у пенітенціарному відомстві. Та як не парадоксально, власникам цих сторінок особливо нічого не загрожує – максимум відсидять кілька днів у карцері. Адже українське законодавство за технічним прогресом не встигає – воно взагалі не регламентує, кому з в’язнів можна користуватися Інтернетом, а кому ні, і як будуть карати порушників цього «табу».

А дарма: спілкування у віртуальному світі може бути безневинним базіканням задля «вбивання часу», а може бути засобом для передачі зашифрованих повідомлень та надання конкретних доручень спільникам. Натякнув, скажімо, слідчий на допиті про існування небезпечного свідка – зробіть так, аби він замовк навіки!

Занадто багато спілкування

Співробітники пенітенціарного відомства кажуть: у Верховній Раді начебто обговорюють можливість відкоригувати законодавство, внісши пряму заборону на користування Інтернетом для арештованих та в’язнів, котрі відбувають основну частину терміну, і дозволивши мобільні телефони з комп’ютерами для засуджених, котрі готуються до умовно-дострокового звільнення, працюють на волі, а живуть на так званих дільницях соціальної реабілітації поза межами «зони». Хоча можна не сумніватися, що охочі порушувати писані закони в нас все одно були й будуть – охочі тихцем пронести до камери мобільний термінал чи якийсь інший заборонений «прибамбас» серед корумпованих охоронців тих же слідчих ізоляторів не переводяться.

Факт. Лише 2012 р. під час загальних обшуків у камерах СІЗО Херсона вилучено 138 мобільних телефонів, 12,5 л спиртних напоїв, 1280 грн і 50 дол. США готівкою. Дані прес-служби обласного управління Державної пенітенціарної служби.

Тому українським пенітенціаріям (якщо, природно, вони не бажають бути посміховиськом на всю Європу з приводу «якісної ізоляції» небезпечних злочинців), уже варто від «протоколів про наміри» переходити для конкретних дій, придбавши апаратуру для глушення без провідного зв’язку, та встановивши її у колоніях і слідчих ізоляторах. Це й душевного спокою потерпілим від злочинів також додасть. Навряд чи батькам дівчини, зґвалтованої та убитої якимось маніяком, буде корисно для здоров’я і

сподобається, що цей маніяк після арешту доправлятиме їм електронні листи з насмішками просто зі своєї камери ***(Небезпечні злочинці виходили до соціальних мереж зі слідчого ізолятору Херсона // Голос України: Інформаційний портал (http://golosukraine.com/publication/prigodi/za-i-poza-zakonom/12642-nebezpechni-zlochinci-vihodili-do-socialnih-merezh/). – 2013. – 11.06).***

***

Некоторые правообладатели, активно защищающие авторское право в сети, сами выкладывают свою музыку в свободном доступе. Так произошло со «Студией СОЮЗ», утверждает пресс-секретарь «ВКонтакте» Г. Лобушкин. По его словам, студия, предъявившая судебный иск к соцсети, сама выкладывает треки на своей страничке.

«Нехитрое дело – загрузить свои же композиции в "ВКонтакте", чтобы потом сразу же бежать в суд», – написал представитель ресурса. Г. Лобушкин уточнил, что речь идет о песнях групп «Ария», «Король и Шут», «Дискотека Авария» и певицы Елки, передает «РИА Новости».

Ранее «Студия СОЮЗ» подала в суд на «ВКонтакте» за нарушение авторских прав. Правообладатели хотят получить от соцсети компенсацию в размере 4,5 млн р. (около 140 тыс. дол.) ***(«ВКонтакте»: правообладатели сами загружают музыку, а потом подают в суд // InternetUA (http://internetua.com/vkontakte---pravoobladateli-sami-zagrujauat-muziku--a-potom-podauat-v-sud). – 2013. – 19.06).***

Зарубіжні спецслужби і технології «соціального контролю»

Российские спецслужбы могут получить доступ к серверам интернет-компаний, работающих на российском рынке, только по решению суда или на иных основаниях, предусмотренных действующим законодательством РФ, рассказали Digit.ru представители крупнейших игроков интернет-рынка.

Так, в пресс-службе «Яндекса» говорят, что спецслужбы РФ не имеют прямого доступа к серверам компании, а также что в истории «Яндекса» не было случаев изъятия серверов из российских или зарубежных дата-центров.

«Вместе с тем „Яндекс“ обязан отвечать на законные запросы уполномоченных органов. Информация может быть получена только в порядке и в соответствии с процедурами, установленными законодательством (например, УПК, законом об оперативно-розыскной деятельности и т. д.)», – отмечают в компании. Доступ к отдельным данным – например, к содержимому электронной почты, которое охраняется конституционным правом на тайну переписки, – «Яндекс» предоставляет только по решению суда.

Представитель Google С. Анурова заявила, что компания действует в рамках действующего законодательства во всех странах присутствия, в том

числе, и в России «Черного хода», с помощью которого спецслужбы могут получить прямой доступ к пользовательским данным, у Google нет. Сохранность личных данных пользователей является главным приоритетом Google», – говорит С. Анурова.

По словам руководителя юридической службы Mail.Ru Group А. Мальгинова, компания может гарантировать пользователям конфиденциальность данных в рамках существующего законодательства России. «Исключение составляют предусмотренные законом случаи, когда информация о конкретном пользователе может быть предоставлена правоохранительным учреждениям. Это указано в пользовательском соглашении, условия которого пользователь принимает при регистрации аккаунтов», – отмечает он.

Российское представительство компании Microsoft и социальная сеть «ВКонтакте» не смогли оперативно предоставить комментарии. Как заявил ранее агентству Рейтер представитель Apple С. Доулинг, компания не обеспечивает правительственные агентства прямым доступом к своим серверам, и любое агентство, которое требует пользовательские данные, обязано сначала получить судебный ордер ***(Российские силовики получают данные интернет-сервисов только по закону // InternetUA (http://internetua.com/rossiiskie-siloviki-polucsauat-dannie-internet-servisov-tolko-po-zakonu). – 2013. – 10.06).***

***

Председатель совета компании Google Э. Шмидт ответил на вопросы журналистов в штаб-квартире Google, которые собрались на годовом собрании акционеров интернет-гиганта. Среди вопросов были и связанные с деятельностью Google в Китае, которая, как известно, заморожена с 2010 г., когда интернет-компания со скандалом ушла с китайского рынка. Судя по всему, в обозримом будущем Google не собирается возвращаться в КНР, сообщает CyberSecurity.ru.

«Приходится констатировать, что по-прежнему поступают отчеты о цензуре и гонении на граждан», – заявил он. По словам Э. Шмидта, именно из-за тотальной цензуры компания решила приостановить свою деятельность в Китае в 2010 г.

Между тем Э. Шмидт признал, что Китай сейчас с его 560 млн интернет-пользователей является интересным для развития рынком.

Очевидно, что были и вопросы, связанные с программой PRISM, по которой интернет-компании, якобы, передавали данные в АНБ США. Отвечая на этот вопрос, Э. Шмидт заявил, что ему о данной программе неизвестно, а если Google и передавала данные в правительство, то сведения об этом постоянно публикуются, а вся передача ведется только по постановлениям суда ***(Google не собирается возвращаться в Китай // IT Expert (http://itexpert.in.ua/rubrikator/item/26855-google-ne-sobiraetsya-vozvrashchatsya-v-kitaj.html). – 2013. – 7.06).***

***

Французский суд на этой неделе обязал Twitter раскрыть имена авторов расистских и антисемитских «твитов». Популярный сервис микроблогов будет обязан предоставить эти данные Союзу еврейских студентов Франции (UEJF) и другим четырём организациям по правам человека, пишет The Verge.

В ноябре 2012 г. UEJF обратило своё внимание на Twitter после хэштегов #unbonjuif («хороший еврей») и др. #unjuifmort («мертвый еврей»). Некоторые спорные «твиты» были удалены, однако предоставить имена авторов меток администрация сервиса отказалась. 12 июня суд постановил, что компания обязана выполнить данное требование.

«Нашей целью является положить конец чувству безнаказанности, которое ощущают авторы расистских и антисемитских сообщений в Интернете, – отметил представитель UEJF. – И Twitter обязан сотрудничать с нами в этих моментах».

Похожий случай произошёл в Германии, где Twitter пришлось заблокировать неонацистские аккаунты по просьбе немецких властей. В январе прошлого года компания объявила, что она начнет цензуру контента в отдельных странах в случае запросов от местных властей ***(Суд Франции приказал раскрыть имена авторов антисемитских «твитов» // InternetUA (http://internetua.com/sud-francii-prikazal-raskrit-imena-avtorov-antisemitskih--tvitov). – 2013. – 13.06).***

***

Останнім часом українська міліція починає притягувати до кримінальної відповідальності за порнографію. Такі випадки рідкість, але все таки трапляються. Як приклад – чотири процеси в Кіровоградській обл., передає «Утренний город».

Молодий хлопець з обласного центру вирішив поділитися з друзями своєю колекцією порно через сторінку «ВКонтакте». На цей «подарунок» натрапили співробітники МВС, швидко встановили особу та віддали під суд. Новоспечений порно-магнат відбувся двома роками умовно.

Житель с. Павлиш знайшов на смітнику гральні карти, виконані в стилі «Hardcore porno». Дав подивитися іншому та отримав штраф у розмірі 850 грн.

У Кіровограді судили експедитора однієї з приватних фірм, який створив «ВКонтакте» співтовариства «Секс Кіровоград + 18» і пару років розміщував там фотографії та відеоролики відповідного змісту. Чоловік активно розсилав користувачам мережі запрошення вступити до клубу, поки його не накрили правоохоронці. Як наслідок, сластолюбець покараний штрафом у розмірі 1700 грн.

Кіровоградський інвалід 3-ї групи організував у будинку ДВД-студію. Він скачував з Інтернету, а потім записував на диски порно-відео. Готовий продукт чоловік рекламував на сайті служби знайомств і продавав по 30–

35 грн за диск. Суд призначив покарання у вигляді трьох років позбавлення волі з випробувальним терміном два роки. Також суд стягнув із засудженого на користь держави судові витрати за проведення експертизи у розмірі 3761 грн 66 коп. Речові докази – диски із записами порнофільмів – суд постановив знищити, а комп'ютер повернути власнику.

У Кримінальному кодексі України для боротьби з порнографією існує ст. 301, яка передбачає покарання від штрафу у 850–1700 грн до трьох років позбавлення волі за створення, ввезення та розповсюдження порнографії ***(В Кіровограді згадали про порно // Кіровоград.comments.ua (http://kirovograd.comments.ua/news/2013/06/17/121232.html). – 2013. – 17.06).***

***

Социальная сеть Facebook заявила, что получила 18 000–19 000 запросов со стороны Агентства национальной безопасности во второй половине 2012 г., которые были связаны с местной преступностью. Microsoft тем временем утверждает, что получила 6 000 и 7 000 подобных запросов.

Разглашение секретной информации о проведении тайного мониторинга и прослушивания со стороны спецслужб США позволяет предположить, что электронная программа наблюдения, используемая США, является гораздо более обширно, чем считалось раньше.

Стало известно, что интернет-компании, в том числе Facebook, Google, Yahoo, Apple и Microsoft, на прошлой неделе предоставили Агентству национальной безопасности США «прямой доступ» к их серверам в рамках программы сбора данных, которая называется призмой. Фирмы отрицают эти обвинения, говоря, что они не предоставляли такой доступ, но выполняли все законные запросы.

В попытке успокоить своих пользователей, Facebook написал в своем блоге, что после обсуждений с соответствующими органами было впервые дано разрешение на раскрытие информации, связанной с запросами со стороны Агентства национальной безопасности США.

По словам соцсети, все полученные запросы охватывают широкий диапазон от поиска пропавшего ребенка местным шерифом до отслеживания сбежавшего из тюрьмы преступника федеральным маршалом ***(Facebook раскрыл подробную информацию о количестве запросов // NovostiUA (http://novostiua.net/techniks/39040-facebook-raskryl-podrobnuyu-informaciyu-o-kolichestve-zaprosov.html). – 2013. – 15.06).***

***

Госслужба интеллектуальной собственности разработала законопроект «О внесении изменений к некоторым законодательным актам относительно защиты авторского права и смежных прав в сети Интернет» во избежание финансовых санкций со стороны США, а также с целью исполнения международных обязательств по защите авторских прав. Впрочем, этот документ является «клоном» российского аналога, а именно: законопроекта

«О внесении изменений в отдельные законодательные акты Российской Федерации в целях прекращения нарушений авторских и смежных прав в информационно-телекоммуникационных сетях, в том числе в сети Интернет». Об этом в комментарии IT Expert рассказала юрист юридической фирмы «Гвоздий и Оберкович» Н. Мисник.

Напомним, что украинские чиновники хотят создать «чёрный список» сайтов. Государственная служба интеллектуальной собственности Украины придумала решение, призванное, по её мнению, нанести интернет-пиратству в уанете мощный удар.

Эксперт напоминает, что согласно заключению Международного альянса интеллектуальной собственности 2012 г., более известному как «Список 301», Украина была удостоена первого места среди наиболее злостных нарушителей авторского права. Одной из причин, послуживших для принятия такого решения, аналитики назвали отсутствие в законодательстве Украины эффективных мер по защите авторских прав и неудовлетворительная работа правоохранительных органов в этой сфере.

Во избежание финансовых санкций со стороны США, а также с целью исполнения международных обязательств по защите авторских прав Госслужбой интеллектуальной собственности (ГСИС) был разработан законопроект «О внесении изменений к некоторым законодательным актам относительно защиты авторского права и смежных прав в сети Интернет».

Как отмечает Н. Мисник, к наиболее существенным нововведениям законопроекта можно отнести то, что документ предлагает правообладателям обращаться с жалобой на пиратские сайты в ГСИС. При обращении заявителю необходимо будет предоставить копии регистрационных документов, нотариально заверенные копии договоров, подтверждающих его авторские или смежные права, перечень пиратских файлов, размещенных в Интернете, а также заверенные переводы документов, если они выпущены на иностранных языках. Одновременно правообладатель должен будет обратиться к хостинг-провайдеру, на мощностях которого размещен пиратский контент. Последний, в свою очередь, будет обязан в двухдневный срок уведомить администрацию ресурса о жалобе.

«ГСИС предоставляется 10 дней на рассмотрение обращения правообладателя – за этот период она обязана определить, законно ли размещен контент, а также опубликовать на своем сайте перечень адресов, по которым находится пиратская продукция. После публикации у администрации ресурса-нарушителя есть две недели, чтобы предоставить ведомству документы, подтверждающие законность размещения. После получения этих документов Госслужба в течение 10 дней будет обязана принять окончательное решение о том, имеет ли место нарушение авторских или смежных прав, а затем направить решение заявителю, администрации ресурса и хостинг-провайдеру», – рассказывает Н. Мисник.

Как подчеркивает юрист, признание контента пиратским является основанием для блокирования доступа к соответствующим объектам авторского права.

По мнению специалистов, законопроект ГСИС о защите авторских прав в сети Интернет очень напоминает российский аналог, а именно: законопроект «О внесении изменений в отдельные законодательные акты Российской Федерации в целях прекращения нарушений авторских и смежных прав в информационно-телекоммуникационных сетях, в том числе в сети Интернет», который не так давно был передан на рассмотрение Государственной думы Российской Федерации.

Однако при детальном анализе, рассказывает Н. Мисник, приходится констатировать, что российский законопроект предусматривает гораздо более жесткие методы борьбы с интернет-пиратством. Например, в отличие от украинского законопроекта, русский аналог предусматривает не только механизм блокировки контента, запрещенного авторским правом, но и досудебный порядок его удаления.

При этом достаточным фактом нарушения авторского права в России считается не только копирование контента, но даже размещение ссылки на ресурс, на котором собственно размещена информация, изображение или видео, охраняемое законом об авторском праве (в том числе в соцсетях).

А пожаловаться на «пирата» в России можно еще проще и быстрее, чем у нас. Законопроект предусматривает возможность отправки жалобы электронной почтой.

После получения жалобы у провайдера есть всего одни сутки на блокировку доступа к указанной информации, а владелец сайта, на котором она размещена, должен в течение суток уточнить в реестре объектов авторского права, нарушает ли контент закон, после чего в течение этих же суток его удалить. После блокировки доступа к контенту, нарушающему, по мнению заявителя, его авторское право, у владельца сайта есть 10 дней, чтобы опротестовать это решение.

«Отсюда вывод, что в российском варианте борьба с пиратством предусматривает более радикальные меры. Однако, судить об их эффективности можно будет только в процессе исполнения принятых нововведений», – отмечает Н. Мисник ***(Н. Мисник: Законопроект про «чёрный список» сайтов создан во избежание финансовых санкций со стороны США // IT Expert (http://itexpert.in.ua/rubrikator/item/27177-zakonoproekt-pro-chjornyj-spisok-sajtov-sozdan-vo-izbezhanie-finansovykh-sanktsij-so-storony-ssha-n-misnik.html). – 2013. – 18.06).***

***

Google отказалась исполнять требования Роскомнадзора.

По мнению представителей американского поисковика, они не обязаны соблюдать российское законодательство и уведомлять власти об обработке персональных данных россиян.

Регистрация пользователя в онлайновых сервисах Google означает его согласие на условия пользования и политику конфиденциальности, соответствующие законодательству США. Поэтому Google не обязана уведомлять Роскомнадзор об обработке персональных данных россиян. Такой ответ компания прислала на запрос российского ведомства о конфиденциальности данных пользователей. Об этом «Известиям» сообщил начальник управления по защите прав субъектов персональных данных Роскомнадзора Ю. Контемиров.

Роскомнадзор направил в компанию Google запрос о соблюдении конфиденциальности персональных данных россиян в почтовом сервисе Gmail. Как уже сообщали «Известия», вопросы об использовании персональных данных в этой веб-почте компании Google ранее возникали и у Федеральной антимонопольной службы РФ.

Gmail анализирует содержание писем пользователей, чтобы определить, на какую тему лучше показывать рекламу конкретному человеку. Если он недавно обсуждал какую-то тему с партнерами по переписке, реклама по этой теме может его активно заинтересовать. Содержание писем анализируют не люди, а компьютер, рассказывали изданию представители Google. Поэтому, по их мнению, о нарушении тайны переписки речь не идет.

Как известно, в России Роскомнадзор является уполномоченным органом по защите прав субъектов персональных данных. По закону компании, которые собираются обрабатывать персональные данные, должны об этом уведомить Роскомнадзор. У этого требования есть исключения, одно из них – когда данные обрабатываются по договору с соответствующим человеком и при этом не предоставляются на сторону без его согласия.

В компании уверены, что прохождение пользователем регистрации – это заключение договора, поэтому Google может обрабатывать персональные данные россиян без уведомления Роскомнадзора. При этом корпорация считает возможным предоставлять персональную информацию о пользователе без его согласия третьим лицам. Например, в случае обязательного к исполнению запроса госучреждения.

В ответ на запрос Роскомнадзора представители Google сообщили, что их компания зарегистрирована на территории США в округе Санта-Клара штата Калифорния. Регистрация пользователя в системе Google выражает его волеизъявление к присоединению к условиям пользования и политике конфиденциальности, которые составлены в соответствии с американским законодательством. Все иски, связанные с условиями пользования, находятся в компетенции калифорнийских судов.

По словам депутата Госдумы И. Костунова, пользовательские соглашения не всегда способны понять даже юристы, не то что обычные пользователи. Поэтому с ними обычно соглашаются, не читая.

«Пользовательское соглашение изначально составлено так, чтобы компания могла избежать любой ответственности перед пользователем,

безнаказанно собирать информацию о нем, чтобы выполнить обязательства перед АНБ и ЦРУ, наживаться на продаже рекламы, – поясняет депутат. – Как я и ожидал, Google будет прикрываться американской юрисдикцией и пользовательским соглашением. Фактически компания всех российских пользователей “послала на Санта-Клару”».

По мнению главы юридического департамента Координационного центра национального домена сети Интернет С. Копылова, если у Google нет в России серверов с персональными данными пользователей, то компания не должна регистрироваться в Роскомнадзоре как оператор персональных данных. В Google «Известиям» заявили, что серверов в России у них нет.

По мнению депутата Госдумы Р. Шлегеля, логично, чтобы компании, работающие с данными россиян, регистрировались в России и соблюдали наше законодательство. «Необходимо добиться, чтобы даже иностранная компания соблюдала российское законодательство, – уверен Р. Шлегель. – Возможно, надо заключить какой-то международный договор или выработать конвенцию, которая бы описывала эту процедуру. Вопрос надо тщательно проработать».

В Роскомнадзоре предлагают изменить ситуацию с помощью поправок в законодательство о персональных данных. Эти вопросы планируется обсудить на заседании консультативного совета при уполномоченном органе по защите прав субъектов персональных данных в сентябре этого года.

В запросе Роскомнадзора, отправленном в Google, содержался еще один вопрос относительно проекта Street View. Он был вызван информацией о том, что при съемках уличных панорам компания Google собирала данные о местонахождении точек беспроводного доступа Wi-Fi и сведения с роутеров, раздающих Wi-Fi, включая пароли, сведения о посещаемых сайтах пользователями. В своем запросе Роскомандзор поинтересовался, собирает ли подобные данные американская компания в России при реализации проекта Street View. В Google ответили, что в России оборудование, собирающее такую информацию, не использовалось.

«Сейчас это можно поставить под сомнение, – говорит Р. Гаттаров. – Американское правительство признало, что они имеют доступ к серверам Google, но сама компания до сих пор утверждает, что это не так» ***(Google отказалась исполнять требования Роскомнадзора // InternetUA (http://internetua.com/Google-otkazalas-ispolnyat-trebovaniya-roskomnadzora). – 2013. – 24.06).***

Проблема захисту даних. DOS та вірусні атаки

Б. Обама призвал Китай соблюдать «правила дорожного движения» в области кибербезопасности

Заявление было сделано американским лидером в ходе двухдневных неформальных переговоров с председателем КНР С. Цзиньпином в Калифорнии. Оно касалось многочисленных атак китайских хакеров на

сервера американских финансовых организаций и государственных ведомств, в том числе Пентагона. Б. Обама подчеркнул, что международная киберпреступность тормозит прогресс в двусторонних отношениях США и Китая, который наблюдается по многим другим направлениям, сообщает lenta.ru.

По итогам встречи в Калифорнии стороны договорились провести специальные переговоры по теме кибербезопасности в июле 2013 г. На них к обсуждению должны подключиться рабочие группы американских и китайских специалистов в этой области.

Советник президента США по безопасности Т. Донильон рассказал, что в целом саммит в Калифорнии прошел в конструктивном ключе и «беспрецедентно неформальной» обстановке. В частности, стороны пришли к согласию относительно ситуации на Корейском полуострове, договорившись совместными усилиями способствовать стабилизации обстановки в регионе.

Неформальная встреча Б. Обамы и С. Цзиньпина проходила в Калифорнии на вилле «Саннилэндс», которая принадлежит семейному фонду Анненбергов, оказывающему поддержку некоммерческим организациям в США и по всему миру. Предполагалось, что формат переговоров позволит политикам пообщаться не только на рабочие темы, но и обсудить общие увлечения, например баскетбол. Традиционно лидеры США и КНР проводили переговоры только в Белом доме – саммит в Калифорнии стал первой встречей на высшем уровне, проведенной двумя странами в подобном формате.

С. Цзиньпин пригласил Б. Обаму нанести ответный неформальный визит в Китай. Американская сторона дала предварительное согласие, однако дата поездки пока не уточняется ***(Обама призвал Китай соблюдать «правила дорожного движения» в области кибербезопасности // IT Expert (http://itexpert.in.ua/rubrikator/item/26883-obama-prizval-kitaj-soblyudat-pravila-dorozhnogo-dvizheniya-v-oblasti-kiberbezopasnosti.html). – 2013. – 9.06).***

***

Троян заразил не менее 50 тыс. пользователей соцсети «ВКонтакте». Компания Cezurity, российский разработчик средств защиты от вредоносных программ и хакерских атак, сообщила о том, что в текущий момент характер заражения пользователей социальных сетей троянской программой Trojan.RpcTonzil принимает характер эпидемии.

Так, по оценке вирусной лаборатории Cezurity, сегодня этой вредоносной программой заражено не менее 50 тыс. участников «ВКонтакте». К такому выводу привел анализ данных, получаемых с помощью Cezurity Cloud – облачной технологии антивирусной защиты, которая способна обнаруживать подобные угрозы с помощью выявления аномалий в файлах. Заражению могут быть подвержены компьютеры под

управлением операционных систем Microsoft Windows, причем как 32-битных, так и 64-битных, считают в Cezurity.

Как рассказали CNews представители компании, в результате заражения злоумышленники получают целый ряд возможностей – от получения доступа к аккаунтам в социальной сети и последующей рассылки спама с взломанных страниц до похищения персональных данных пользователей и SMS-мошенничества.

Троянская программа Trojan.RpcTonzil модифицирует запросы компьютеров к DNS-серверу. В результате при попытке зайти в социальную сеть пользователь оказывается на специально созданной злоумышленниками фишинговой веб-странице, которая имитирует и практически неотличима от страницы «ВКонтакте», где сообщается о том, что аккаунт социальной сети был взломан. Злоумышленники предлагают создать новый пароль и верифицировать привязку своего номера мобильного телефона к аккаунту в социальной сети. Пользователей может обмануть адрес, который отображается в адресной строке браузера – он полностью соответствует правильному и возникает ощущение, что страница действительно принадлежит «ВКонтакте».

Троян также блокирует доступ к сайтам большинства антивирусных компаний и серверам обновления Microsoft. Таким образом, у антивирусных лабораторий зачастую нет достаточного количества данных для того, чтобы заметить распространение заражения.

«Отдельные варианты Trojan.RpcTonzil были обнаружены и детектировались антивирусными компаниями уже с начала марта этого года. Однако на сегодняшний день распространение Trojan.RpcTonzil продолжается, и большинством антивирусов вредоносная программа либо вообще не обнаруживается, либо детектируются лишь некоторые модификации», – отметили в Cezurity.

По словам специалистов компании, трудность обнаружения всех модификаций Trojan.RpcTonzil связана с тем, что в троянской программе используется достаточно сложная техника сокрытия от антивирусов. При этом на компьютеры жертв троянская программа может попадать различными способами. В некоторых случаях заражение может быть предотвращено встроенными в антивирусы поведенческими механизмами защиты.

«После заражения компьютера троянская программа существует только в зашифрованном виде. Ее расшифровка и автозапуск осуществляется с помощью небольшой модификации системной библиотеки rpcss.dll, – рассказал К. Пресняков, ведущий вирусный аналитик Cezurity. – Троян использует технику заражения, похожую на метод EPO (Entry Point Obfuscation, скрытая точка входа). Большинство антивирусов не способно детектировать заражение, произведенное таким образом, то есть не зная вируса “в лицо”, они могут обнаружить этот троян только по поведению.

Осложняет детектирование и тот факт, что внедренный в системную библиотеку фрагмент носит условно-случайный характер».

Другим возможным препятствием для обнаружения и лечения вредоносной программы может быть географическая направленность атаки – троян нацелен на пользователей российских социальных сетей.

Компания Cezurity рекомендует пользователям проверить компьютер бесплатным «Антивирусным сканером», который сегодня обнаруживает все известные модификации Trojan.RpcTonzil ***(Троян заразил не менее 50 тыс. пользователей соцсети «ВКонтакте» // InternetUA (http://internetua.com/troyan-zarazil-ne-menee-50-tis--polzovatelei-socseti--vkontakte). – 2013. – 11.06).***

***

Компания «Доктор Веб» сообщила об обнаружении новой версии троянской программы Linux.Sshdkit, представляющей опасность для работающих под управлением операционной системы Linux серверов. Согласно собранной вирусными аналитиками статистике, на сегодняшний день от действий зловредов данного семейства пострадало уже несколько сотен серверов, среди которых имеются серверы крупных хостинг-провайдеров.

Обнаруженный троян представляет собой динамическую библиотеку, разновидности которой существуют для 32-х и 64-разрядных версий дистрибутивов Linux. После успешной установки в систему зловред встраивается в процесс sshd, перехватывая функции аутентификации данного процесса. После установки сессии и успешного ввода пользователем логина и пароля они отправляются на принадлежащий злоумышленникам удаленный сервер посредством протокола UDP.

Новая версия вредоносного приложения получила название Linux.Sshdkit.6. В ней злоумышленники внесли ряд изменений с целью затруднить перехват вирусными аналитиками украденных паролей. В частности, вирусописатели изменили метод определения адресов серверов, на которые троянец передает краденую информацию. Теперь для вычисления целевого сервера используется специальная текстовая запись, содержащая данные, зашифрованные RSA-ключом размером 128 байт. Кроме того, был модифицирован алгоритм получения троянцем команд: теперь для их успешного выполнения вредоносной программе передается специальная строка, для которой проверяется значение хеш-функции.

Троянцы семейства Linux.Sshdkit представляют высокую опасность для вычислительных машин, работающих под управлением ОС Linux, поскольку позволяют кибер-преступникам получить данные для несанкционированного доступа на сервер. Администраторам серверов специалисты «Доктор Веб» рекомендуют проверить операционную систему на наличие данной угрозы ***(Троянцы семейства Linux.Sshdkit продолжают угрожать Linux-серверам***

// InternetUA (http://internetua.com/troyanci-semeistva-Linux-Sshdkit-prodoljauat-ugrojat-Linux-serveram). – 2013. – 12.06).

***

Компания Eset сообщила об обнаружении массированной спам-атаки в Skype. Злоумышленники использовали методы социальной инженерии, предлагая перейти по ссылкам и увидеть заманчивые фотографии. На самом деле, прилагаемые к сообщениям ссылки вели на вредоносное ПО. За первые 48 часов с начала кампании по вредоносным ссылкам перешло больше полумиллиона пользователей.

Стоит отметить, что подозрительные ссылки были замаскированы с помощью вполне легального сервиса Google URL Shortener, призванного укорачивать длинные ссылки, и ряда аналогичных ресурсов (bit.ly, ow.ly и др.). Только по адресам, начинающимся с http://goo.gl/. перешло более 490 000 пользователей.

Укороченные ссылки в спам-сообщениях перенаправляли пользователей на страницу загрузки вредоносной программы, которая детектируется решениями Eset как Win32/PowerLoader.A. Эта программа, в свою очередь, загружает и запускает дроппер (т. н. «носитель») известного червя Dorkbot.

В функционал червя входит предоставление злоумышленникам полного доступа к зараженному ПК, загрузка и запуск дополнительных вредоносных файлов, а также рассылка спам-сообщений по базе контактов инфицированного устройства. Кроме того, некоторые модификации Dorkbot нацелены на хищение паролей от различных сервисов (аккаунтов социальных сетей, онлайн-банкинга и т. д.). На данный момент жертвами этой спам-кампании стали пользователи всего мира – больше всего пострадали пользователи в Германии, России, Бразилии, Колумбии, Мексике и США. Предположительно, кибер-преступники рассылали сообщения на разных языках, в зависимости от государства, что значительно увеличило эффективность спам-кампании.

По данным Google URL Shortener, 83 % всех переходов выполнялось из систем, работающих под управлением семейства ОС Windows. Остальные 17 % делят между собой iOS, Mac OS X, Linux и BlackBerry.

На сегодняшний день большинство сервисов для укорачивания URL-адресов заблокировали вредоносные ссылки, однако кибер-преступники все еще могут давать инструкции подконтрольным ботам, что позволит им возобновить атаку в будущем. По данным ресурса bit.ly, больше всего переходов по вредоносным ссылкам с использованием этого сервиса – более 8000 – произошло в Германии ***(Обнаружена массированная спам-атака в Skype // InternetUA (http://internetua.com/obnarujena-massirovannaya-spam-ataka-v-Skype). – 2013. – 11.06).***

***

Специалисты по антивирусной безопасности говорят об обнаружении ранее неизвестного троянца, использующего уязвимость в операционной системе Android. Новый вредонос задействует технику, которая используется вредоносами, создаваемыми под Windows для сокрытия собственного присутствия в системе.

В «Лаборатории Касперского» рассказали об обнаружении нового вредоносного кода Backdoor.AndroidOS.Obad.a. По словам антивирусных аналитиков, выявленный код является одним из самых сложных на сегодняшний день. Код создан для отправки SMS на премиум-номера и позволяет атакующим исполнять шпионские команды на зараженных устройствах, открывая фоновую shell-оболочку.

Атакующие могут использовать этот код для кражи широкого диапазона данных, хранящихся на скомпрометированных данных, или для загрузки дополнительных вредоносных программ, причем код может подгружать дополнительные коды в том числе и через порт Bluetooth. В «Лаборатории Касперского» говорят, что вредонос использует стойкий алгоритм шифрования и сокрытия кода для затруднения анализа. «Авторы вредоносных программ, как правило, пытаются максимально усложнить свой код, чтобы антивирусные компании как можно дольше анализировали разработку. Однако у Odad.a код действительно сложный для анализа, он превосходит другие мобильные вредоносы», – говорит Р. Унучек, эксперт «Лаборатории Касперского».

Создатели Backdoor.AndroidOS.Obad.a нашли ошибку в популярной программе dex2jar, которая обычно используется аналитиками для конвертирования APK-файла в более удобный для работы формат JavaArchive (JAR). Обнаруженная злоумышленниками уязвимость нарушает процесс конвертации Dalvik байт-кода в Java байт-код, что в итоге затрудняет статический анализ троянца.

Также злоумышленниками была найдена ошибка в OCAndroid, связанная с обработкой AndroidManifest.xml. Этот файл встречается в каждом Android-приложении и используется для описания структуры приложения, определения параметров его запуска и т. д. Вирусописатели модифицировали AndroidManifest.xml таким образом, что тот не соответствовал заданному Google стандарту, но при этом, благодаря найденной уязвимости, правильно обрабатывался на смартфоне. В результате динамический анализ троянца крайне затруднен.

Создатели Backdoor.AndroidOS.Obad.a использовали еще одну неизвестную ранее ошибку в ОС Android, которая позволяет вредоносному приложению пользоваться расширенными правами DeviceAdministrator, но при этом отсутствовать в списке приложений, обладающих такими правами. В результате удалить со смартфона вредоносную программу, получившую расширенные права, невозможно. Наконец, Backdoor.AndroidOS.Obad.a не имеет интерфейса и работает в фоновом режиме, говорят в компании.

Набор команд для Obad.a позволяет зловреду распространять файлы по Bluetooth. С сервера приходит адрес файла, который должен быть скачан на зараженное устройство. После скачивания файла по очередной команде с сервера вредоносное приложение определяет ближайшие устройства с включенным Bluetooth и пытается передать им загруженный файл.

Несмотря на такие внушительные возможности, Backdoor.AndroidOS.Obad.a не очень распространен. По данным KasperskySecurityNetwork, за три дня наблюдений на его заблокированные установки приходится не более 0,15 % всех попыток заражения мобильных устройств различными вредоносными программами ***(Обнаружен очень сложный Android-троянец // InternetUA (http://internetua.com/obnarujen-ocsen-slojnii-Android-troyanec). – 2013. – 10.06).***

***

Лаборатория McAfee Labs опубликовала отчет McAfee об угрозах за I квартал 2013 г., в котором сообщается о значительном увеличении количества экземпляров червя Koobface, распространяющегося через социальные сети, и о резком увеличении объемов спама. Лаборатория McAfee Labs также стала свидетелем непрерывного увеличения количества и степени сложности целенаправленных угроз: троянских коней для сбора информации, угроз, атакующих основные загрузочные записи (MBR) систем, и т. п., сообщили CNews в компании McAfee.

Так, согласно отчету, специалисты McAfee Labs обнаружили почти в три раза больше образцов Koobface, чем в предыдущем квартале, что является высоким показателем для червя, который атакует пользователей Facebook, Twitter и других соцсетей. После трех лет затишья объемы нежелательной электронной почты резко возросли. В Северной Америке одним из значительных факторов этого роста стало возвращение кампаний «накачка и сброс», заключающихся в рассылке спама потенциальным инвесторам, желающим заработать на рекордно высоких показателях фондового рынка.

Однако самым заметным эволюционным скачком в мире угроз безопасности стал рост количества и степени изощренности постоянных угроз повышенной сложности (advanced persistent threats, сокращенно APT), являющийся отражением того факта, что в киберпреступном мире информация становится такой же ценной, как и деньги, считают в McAfee Labs. В отчете говорится о 30-процентном увеличении количества вредоносных программ, атакующих основную загрузочную запись компьютера, и новых экземпляров троянских коней для кражи паролей, приспособленных для захвата информации о физических и юридических лицах, не связанных со сферой финансовых услуг.

Как пояснили специалисты лаборатории, данный прирост произошел за счет распространения экземпляров вредоносных программ StealthMBR, TDSS, Cidox и Shamoon. «Основные загрузочные записи играют ключевую

роль в загрузке системы и дают злоумышленнику широкий спектр возможностей для управления системой, закрепления в системе и глубокого проникновения в систему. В последние два квартала эта категория демонстрировала рекордно высокие показатели», – отметили в McAfee Labs.

В свою очередь, недавно проведенный в McAfee анализ троянского коня Citadel показал, что эта гроза банковских счетов теперь приспособлена под кражу персональной информации узкого круга лиц, работающих в организациях, не связанных со сферой финансовых услуг. Организации финансовой отрасли должны быть готовы к увеличению количества банковских вредоносных программ, используемых для ведения кибершпионажа внутри нефинансовых и правительственных учреждений.

По словам В. Уифера, старшего вице-президента McAfee Labs, «киберпреступники стали понимать, что конфиденциальная информация о людях и организациях является валютой в их “хакерской экономике”. Возвращение Koobface напоминает нам о том, что социальные сети по-прежнему предоставляют большие возможности для перехвата персональной информации. В корпоративной среде мы наблюдаем превращение троянских коней для кражи паролей в инструменты для сбора информации в целях кибершпионажа. Целенаправленные атаки с целью перехвата учетных данных, интеллектуальной собственности, коммерческих тайн и т. п. достигают новой степени изощренности».

В этом квартале лаборатория McAfee Labs также зафиксировала рост числа подозрительных URL-адресов на 12 %, что, по мнению специалистов, объясняется постепенным отходом киберпреступников от бот-сетей как основного механизма распространения вредоносных программ. Заметное преимущество вредоносных веб-сайтов, запускающих «попутные загрузки», состоит в их большей подвижности и меньшей «чувствительности» к действиям правоохранительных органов, объяснили в компании.

Несмотря на то что темпы роста количества вредоносных программ для мобильных устройств на протяжении квартала слегка снижались, вредоносным программам для Android удалось продемонстрировать прирост на 40 %.

В целом количество новых образцов вредоносных программ для ПК возросло за отчетный период на 28 %, в результате чего «зоопарк» вредоносных программ McAfee, содержащий более 120 млн уникальных вредоносных программ, пополнился 14 млн новых образцов ***(В первом квартале 2013 г. количество экземпляров червя для соцсетей Koobface утроилось // InternetUA (http://internetua.com/v-pervom-kvartale-2013-g--kolicsestvo-ekzemplyarov-cservya-dlya-socsetei-Koobface-utroilos). – 2013. – 14.06).***

***

Похищена скаутская база английского футбольного клуба «Манчестер Сити». Как сообщают местные СМИ, хакеры взломали и украли всю

информацию, которую селекционеры команды собрали за последнее время об интересующих их игроках по всему миру, сообщает ТАСС-Телеком.

Английская полиция уже начала расследование, назвав главной версией преступления промышленный шпионаж ***(Хакеры взломали скаутскую базу «Манчестер Сити», похитив информацию селекционеров команды // IT Expert (http://itexpert.in.ua/rubrikator/item/27109-khakery-vzlomali-skautskuyu-bazu-manchester-siti-pokhitiv-informatsiyu-selektsionerov-komandy.html). – 2013. – 17.06).***

***

В Skype обнаружена уязвимость, которая позволяет блокировать учетные записи пользователей. Брешь касается сервиса, предназначенного для борьбы со спамом. Нажав правой кнопкой мышки на контакте, из контекстного меню можно выбрать пункт «Заблокировать этого пользователя» и поставить галочку в пункте «Сообщить о нарушении правил этим абонентом».

Мошенники решили использовать сервис борьбы со спамом для блокировки «неугодным им» пользователей Skype. Поиск определенных людей осуществляется по логину через skype:insert_username_here?menu, и из поиска можно заблокировать или пожаловаться на пользователя.

Для того, чтобы заблокировать учетную запись, достаточно отправить в ее адрес девять жалоб. В настоящее время хакеры организовывают группы, через социальные сети распространяют информацию об учетной записи, подлежащей блокировке, и в течение короткого периода времени войти в нее становится невозможно.

Самым неприятным моментом является тот факт, что служба поддержки Skype не рассматривает никакие конкретные случаи автоматической блокировки аккаунта. Ответ один – «Вы нарушили пункт 6.3 Условий использования Skype». В результате пользователь теряет все важные контакты, переписку и логин, а также оплаченные подписки и деньги на балансе ***(Очередная дыра в системе безопасности Skype // InternetUA (http://internetua.com/ocserednaya-dira-v-sisteme-bezopasnosti-Skype). – 2013. – 15.06).***

***

Борьба с пиратами: вопреки или благодаря законопроекту?

Представители ««ВКонтакте»» опровергают заявления пользователей о том, что начиная с 14 июня, после принятия Госдумой «антипиратского» законопроекта, руководство социальной сети начало удалять музыку, опубликованную на личных страницах посетителей.

Законопроект был принят в первом чтении 14 июня, и уже в этот день появились сообщения о том, что администрация «ВКонтакте» удаляет из

базы своих аудиозаписей композиции зарубежных исполнителей, передает NewsOboz.org.

На выходных пресс-секретарь соцсети «ВКонтакте» Г. Любушкин в своем блоге заявил, что администрация продолжает удалять музыку в том же порядке, как она делала это до сих пор – после обращения правообладателей.

Между тем законопроект предлагает иной способ решения проблемы нелегального контента – он предусматривает возможность при определенных обстоятельствах блокировать доступ ко всему сайту, на котором размещены записи по решению суда.

Сразу несколько интернет-компаний, отметив, что с помощью этой нормы можно без оснований закрыть вполне законопослушный ресурс – достаточно будет просто пожаловаться в суд на всю площадку, на которой он находится.

Между тем в Госдуме уже заговорили о возможности смягчения законопроекта. В частности, речь может идти об изъятии нормы о блокировке по решению Мосгорсуда доступа к всему ресурсу, где обнаружен нелегальный контент, в новой редакции предлагается говорить о блокировке конкретного URL.

Удаление по требованию

Уже в пятницу пользователи сети «ВКонтакте» стали жаловаться на исчезновение с их страниц музыкальных треков, в основном, зарубежных исполнителей.

Многие сразу стали переименовывать названия песен и имена исполнителей, придумывая им русские кодовые названия. Другие пользователи заявили, что удалят свои страницы, если они лишатся музыки.

Как пояснил представитель пресс-службы сети Г. Любушкин, сеть «ВКонтакте» не стала удалять записи в каком-то особом порядке после рассмотрения Думой законопроекта в первом чтении.

«Мы всегда удаляли аудио- и видеозаписи, когда на них подавались законные жалобы от правообладателей, просто сейчас таких обращений стало больше», – объяснил он на своей странице.

«На этой неделе удалилось не больше, чем на прошлой или позапрошлой, или год назад удалялось», – сказал он в комментарии к одному из своих постов.

Гендиректор Universal Music Russia Д. Коннов в интервью «Ведомостям» признал факт таких обращений. «Мы направили письмо в сеть “ВКонтакте” с просьбой удалить принадлежащий Universal Music контент», – сказал он.

При этом, как пишут «Ведомости», Д. Коннов считает, что ответственность за нелегальный контент несут владельцы сайтов, которые привлекают новых пользователей возможностью его получения.

Эксперты отмечают, что многие правообладатели предпочитают неофициально сотрудничать с торрент-трекерами, и те добровольно блокируют контент на своих сайтах.

URL или IP?

Несовершенство технологий борьбы с размещением информации в Интернете обсуждается уже давно.

Основной способ – блокировка доступа к этой информации. Существует два типа такой блокировки – URL (конкретной страницы) или IP-адреса (всего хостинг-сайта, на котором размещена страница).

Согласно тексту законопроекта, правообладатель, обнаружив на сайте нелицензионный контент, обращается в Мосгорсуд.

Имея на руках решение суда, он пишет в Роскомнадзор и требует ограничить доступ ко всему ресурсу по IP-адресу.

В течение трех дней Роскомнадзор определяет, на чьих серверах находится нелегальный контент, и направляет соответствующему провайдеру уведомление.

После этого провайдер пишет администратору сайта: ему дают 24 часа на удаление спорного контента. Если тот отказывается, провайдер должен ограничить доступ к этому контенту.

Эти предложения были раскритикованы со стороны крупнейших интернет-компаний рунета, включая Яндекс и российское представительство Google, Mail.ru, а также Российской ассоциацией электронных коммуникаций ***(Борьба с пиратами: вопреки или благодаря законопроекту? // NewsOboz (http://newsoboz.org/it_tehnologii/borba-s-piratami-vopreki-ili-blagodarya-zakonoproektu--17062013152800). – 2013. – 18.06).***

***

Федеральная служба безопасности (ФСБ) и Федеральная служба охраны (ФСО) России начали проверку в связи с рассылкой в СМИ сообщений об отставке главы РЖД В. Якунина, которые, как оказалось, не соответствуют действительности.

«Распространенная информация об отставке В. Якунина, оформленная как якобы официальное сообщение пресс-службы правительства, содержала в себе грамматические ошибки и была отправлена с электронного адреса, подделанного под официальную рассылку пресс-службы правительства», – пояснила пресс-секретарь премьер-министра России Д. Медведева Н. Тимакова, передает Лента.ру.

Опровергли отставку своего главы и в пресс-службе РЖД.

Сообщение о замене В. Якунина на первого вице-президента РЖД А. Мишарина было оформлено в стиле правительственного пресс-релиза и содержало традиционные для таких документов элементы, но пришло с IP-адреса, не совпадающего с адресом аппарата правительства.

Пресс-служба президента России призвала СМИ к осторожности при работе с электронными сообщениями. «В связи участившимися проявлениями киберпреступности управление пресс-службы и информации президента Российской Федерации обращается с предложением ко всем СМИ проявлять максимальную осторожность в использовании информации,

поступающей по сети Интернет в виде электронных сообщений пресс-службы президента России», – говорится в сообщении.

Информацию об отставке главы РЖД вечером в среду распространили все российские информагентства и крупнейшие СМИ, включая основные телеканалы. В ИТ-службе агентства отметили, что сервер, с которого рассылались фальшивые пресс-релизы, представился легитимным именем почтового сервера аппарата правительства (aprf.gov.ru), но IP-адрес злоумышленников был отличным от оригинального. «Проведенный анализ показал, что подстановка служебной информации о прохождении данного почтового сообщения через якобы официальные почтовые сервера аппарата правительства исполнена достаточно профессионально, с полной имитацией исходных данных и по всем правилам социального инжиниринга», – объяснил представитель подразделения.

В. Якунин был назначен руководить РЖД в июне 2005 г. по инициативе президента России В. Путина. В июне 2011 г. чиновника переназначили еще на четыре года.

В. Якунин рассказал, что сообщение о мнимой отставке застало его на встрече, которую В. Путин проводил с бизнесменами. «Мы сидели и ели глухаря», – уточнил глава РЖД, отметив, что аппетит новость ему не испортила. В. Путин отнесся к происходящему как к шутке и сказал: «Какое счастье тебе привалило», – рассказал В. Якунин ***(Хакеры «развели» СМИ, уволив главу РЖД // Обозреватель (http://tech.obozrevatel.com/news/19637-hakeryi-uvolili-glavu-rzhd.htm). – 2013. – 20.06).***

***

Секьюрити-компания FireEye сообщила об обнаружении кибер-атаки, использующей систему Google Docs для избежания обнаружения. Цель атаки – похитить пользовательскую информацию, причем FireEye отмечает, что примеры атаки они обнаружили в интернете и организаторы кампании уже, скорее всего, получили данные некоторых пользователей, сообщает CyberSecurity.ru.

Согласно сообщению FireEye, организаторы кампании используют продвинутое вредоносное ПО, а также целевые мошеннические компании для кражи корпоративных и личных данных различных жертв. Сейчас данная атака сосредоточена в основном в азиатских странах. Также компания заявляет, что, скорее всего, реальные жертвы этой атаки уже есть.

«Обнаруженная программа, как обнаружилось, использует ряд продвинутых технологий, которые делают ее интересной с точки зрения исследования», – говорят в компании. «Вредонос использует платформу Google Docs для того, чтобы производить перенаправление пользователей и избежать обнаружения».

Ч. Р. Хва, исследователь из FireEye, говорит, что использование Google Docs на сегодня не является тривиальным ходом, а кроме того, многие

решения для обеспечения безопасности автоматически заносят эту платформу в белый список, что также играет на руку злоумышленникам.

Изюминка атаки заключается в том, что она использует Google Docs как коннектор между пользователем и вредоносным сервером. Традиционно трафик с Google Docs шифруется, что усложняет анализ. В базе FireEye описанный фишинговый инцидент идет за номером CVE-2012-0158 ***(Интернет-мошенники начали использовать Google Docs // IT Expert (http://itexpert.in.ua/rubrikator/item/27276-internet-moshenniki-nachali-ispolzovat-google-docs.html). – 2013. – 21.06).***

***

Вирус, атаковавший «Аэрофлот», пришел из будущего.

В ходе судебных слушаний по делу о Ddos-атаке против «Аэрофлота» выяснилась сенсационная подробность. Файл с вирусом, лежащим в основе обвинения, был создан через два месяца после самой атаки. Причем время создания файла совпадает со временем проведения экспертизы над ним в компании Group-IB.

В ходе слушаний в Тушинском районном суде Москвы по делу о Ddos-атаке против «Аэрофлота» был осуществлен осмотр «цифровых» доказательств по данному делу. Осмотр проводился одновременно двумя экспертами: А. Андриишиным из компании ИВК (был приглашен стороной защиты) и Г. Ануфриевым из «Лаборатории Касперского» (ЛК). Последний сотрудничал по данному делу с ФСБ еще на этапе следствия.

Напомним, 15–24 июля 2010 г. были атакованы сервера платежной системы «Ассист», в результате чего невозможно было купить электронные билеты на сайте ее крупнейшего клиента – «Аэрофлота». Через год ФСБ раскрыла данное преступление, арестовав всех предполагаемых фигурантов: заказчика атаки, владельца системы Chronopay (конкурент «Ассиста») П. Врублевского, исполнителей атаки – братьев Дмитрия и Игоря Артимовичей, а также сотрудника службы безопасности Chronopay М. Пермякова.

Слежку за Артимовичами ФСБ установила еще в августе 2010 г. Благодаря мониторингу используемого ими интернет-канала удалось установить факт захода на размещенную на удаленном сервере панель управления Topol-Mailer. Перехватив пароль от нее, оперативники пришли к выводу, что речь идет о панели управления бот-сетью, использующейся для рассылки спама и Ddos-атак. Там же был найден файл crypted.exe, загружаемый на компьютеры жертв.

Оперативники записали на компакт-диск файл crypted.ex (переименование осуществили во избежание конфликта с антивирусным ПО), а также excel-файл со списком IP-адресов «ботов», атаковавших «Ассист». Этот диск вместе с паролем от Topol-Mailer из ФСБ был передан на экспертизу в Group-IB. Специалисты компании выяснили, что вышеупомянутый файл является вредоносной программой

Rootkit.Win32.Tent.btt (по классификации «Антивируса Касперского»), а треть «ботов», атаковавших «Ассист», совпадает с адресами «ботов» данной сети.

Через год начались аресты подозреваемых, а 9 июня 2011 г. в квартире Артимовичей в Ленинградской обл. был произведен обыск, в ходе которого изъяли два ноутбука Lenovo. Эти ноутбуки запаковали и отправили в Москву, где 27 июня они, в присутствии понятых, были вскрыты в Следственном управлении ФСБ. На ноутбуках, в частности, были найдены исходные коды, из которых, как затем установил Г. Ануфриев из ЛК, и был собран файл crypted.exe.

Несмотря на наличие признательных показаний, в ходе судебного процесса обвиняемые начали активно защищаться. В том числе защита настояла на проведении в суде экспертизы ноутбуков и вышеупомянутого компакт-диска. Анализ же содержимого компакт-диска привел к неожиданным результатам.

Оба эксперта согласились с тем, что файл crypted.ex был скомпилирован из исходных кодов 15 сентября 2010 г., а записан на диск – 22 сентября. Между тем, согласно материалам дела, данный диск из ФСБ в Group-IB был направлен еще 8 сентября, а с 10 по 25 сентября он находился на исследовании в этой компании. Правда, Г. Ануфриев сделал оговорку, что программа PE Tools, с помощью которой был установлен данный факт, сама позволяет изменять время создания файла.

Адвокат И. Артимовича, П. Зайцев, сделал из полученных данных вывод, что файл crypted.ex «был умышленно собран неизвестным лицом в Group-IB с целью фальсификации доказательств по данному уголовному делу». При этом данный вирус никак не мог применяться в атаке на «Ассист», состоявшейся за два месяца до этого, добавил адвокат. Ранее защита уже обращала внимание суда и на другое странное обстоятельство с этим диском.

Оперативно-розыскные мероприятия в отношении братьев Артимовичей, в частности, перехват трафика их интернет-канала, начались после получения 3 августа 2010 г. соответствующей санкции Московского городского суда. Однако санкция этого же суда на получение информации с американских серверов, на которых была расположена панель управления бот-сети Topol-Mailer, была дана только 30 сентября 2010 г.

Между тем в упомянутом ранее запросе ФСБ в Group-IB на исследование панели управления Topol-Mailer от 8 сентября 2010 г. указывается, что санкция суда уже имеется. В документе даже приводится номер соответствующего решения, который совпадает с номером решения от 30 сентября 2010 г. «8 сентября нельзя было знать и иметь на руках решение Мосгорсуда от 30 сентября, и тем более указывать его в документе, – отмечает в своем ходатайстве П. Зайцев. – Таким образом, данный документ сфальсифицирован, а именно подписан задним число с целью придания

видимости законности проводимым сотрудниками ФСБ незаконным мероприятиям».

Проведенный в ходе судебного заседания осмотр ноутбуков Артимовичей также выявил неожиданные результаты. Оказалось, что оба они содержат в совокупности на 3,2 Гб больше данных, чем было зафиксировано в протоколах об их осмотре. Журнал работы компьютеров показал, что они оба включались 10 июня 2011 г. – то есть в период между их изъятием и вскрытием в присутствии понятых. Из этого защита сделала вывод, что на ноутбуки кем-то была записана дополнительная информация и программы.

В связи с этим П. Зайцев подал ходатайство об исключении ноутбуков из числа доказательств обвинением, а компакт-диск переквалифицировать как доказательство со стороны защиты (то есть доказательство того, что обвиняемые не проводили атаку на «Ассист»). Кроме того, адвокат попросил судью направить в Следственный комитет сообщение о преступлении – фальсификации доказательств по уголовному делу – с целью проверки. Судья Н. Лунина ходатайство о переквалификации доказательств отклонила, предложив рассмотреть это на стадии судебных прений. Заявление о преступлении пока осталось без ответа. В Group-IB и «Лаборатории Касперского» от комментариев отказались ***(Вирус, атаковавший «Аэрофлот», пришел из будущего // InternetUA (http://internetua.com/virus--atakovavshii--aeroflot---prishel-iz-budusxego). – 2013. – 24.06).***

***

Facebook обнародовала подробности утечки данных почти 6 млн пользователей.

Одна из крупнейших мировых социальных сетей признала, что допустила утечку личных данных 6 млн пользователей из-за сбоя в программном обеспечении.

«Вследствие неисправности при загрузке архива своего аккаунта в Facebook при помощи инструмента Download Your Information («Загрузить копию вашей информации», DYI) пользователь мог получить адреса электронной почты и телефонные номера других пользователей из своего контакт-листа или тех, с кем он были каким-либо образом связан в социальной сети», – сообщили представители компании на сайте социальной сети.

Для исправления ошибки и устранения ее последствий Facebook отключила инструмент DYI на 24 часа, после чего снова включила этот сервис.

Как сообщается, доступ к данным оставался открытым на протяжении года и обнаружить его помог один из пользователей социальной сети.

Из заявления компании Facebook: «Мы расстроены и находимся в неловком положении, мы удвоим усилия с целью гарантировать, что подобное никогда не повторится».

В соцсети утверждают, что личные данные того или иного пользователя могли получить только несколько человек и нет никаких свидетельств того, что эта информация могла быть использована злоумышленниками ***(Facebook обнародовала подробности утечки данных почти 6 млн пользователей // InternetUA (http://internetua.com/Facebook-obnarodovala-podrobnosti-utecski-dannih-pocsti-6-mln-polzovatelei). – 2013. – 24.06).***

***

23 июня 2013 г., был взломан официальный веб-сайт г. Измаил. При заходе на ресурс посетителей встречает угрожающая картинка с надписью Mafia Security.

Следует отметить, что это уже не первый случай, когда официальный сайт Измаила взламывают. Хочется верить, что взломщики будут наказаны, ведь хакерская атака на любой сайт – уголовно наказуема ***(Хакеры взломали официальный сайт Измаила // InternetUA (http://internetua.com/hakeri-vzlomali-oficialnii-sait-izmaila). – 2013. – 24.06).***

***

Число интернет-пользователей, столкнувшихся с фишинговыми атаками за последние 12 месяцев, увеличилось на 87 % – с 19,9 до 37,3 млн. Чаще всего жертвами этой киберугрозы становятся жители России, США, Индии, Вьетнама и Великобритании. Таковы результаты исследования «Эволюция фишинговых атак в 2011–2013 гг.», проведенного «Лабораторией Касперского» в июне 2013 г. на основе данных облачной системы мониторинга Kaspersky Security Network.

Долгое время фишинг оставался разновидностью угроз, характерных для почтового спама. Однако данные, полученные в ходе исследования, говорят о том, что фишинговые атаки достигли таких масштабов, что правильнее рассматривать их как отдельную опасную угрозу, рассказали CNews в компании. Так, например, на фишинговые атаки, организованные через спам-рассылки, за последний год пришлось чуть более 12 % от всего объема зарегистрированных атак. Во всех остальных 88 % случаев пользователи сталкивались со ссылками на фишинговые страницы отнюдь не в почте, а, например, в процессе веб-серфинга, при общении в интернете (через Skype и т. п.) и использовании соцсетей.

В ходе исследования специалисты «Лаборатории Касперского» проанализировали данные о фишинговых атаках, полученные от более чем 50 млн пользователей Kaspersky SecurityNetwork в период с 1 мая 2012 г. по 30 апреля 2013 г., и сравнили их с данными за аналогичный временной промежуток 2011–2012 гг. По итогам анализа выяснилось, что за период 2012–2013 гг. ежедневно фишинговым атакам подвергалось 102,1 тыс. пользователей по всему миру, а это почти вдвое больше, чем за аналогичный предыдущий период, подчеркнули в компании. При этом лидерами по росту

числа атакованных пользователей оказались четыре страны: Вьетнам, США, Индия и Германия – здесь этот показатель увеличился более чем на 100 %.

Большинство серверов, на которых размещались фишинговые страницы, были зарегистрированы на территориях США, Великобритании, Германии, России и Индии. А более половины (57 %) всех идентифицированных уникальных источников атак располагаются на территории всего 10 стран. При этом количество этих самых источников атак за период с 2012 по 2013 гг. возросло более чем в три раза, сообщили в «Лаборатории Касперского».

Главными целями злоумышленников оказались одни из самых популярных интернет-ресурсов: Yahoo!, Google, Facebook и Amazon. На эти сервисы пришлось свыше 30 % всех фишинговых инцидентов. В то же время более 20 % всех атак были совершены на банки и другие кредитно-финансовые организации. В тридцатку самых подделываемых ресурсов попали также American Express, PayPal, Xbox live и Twitter.

«Объем и разнообразие фишинговых атак, обнаруженных в ходе исследования, указывают на то, что фишинг – не просто один из способов нелегального обогащения злоумышленников, а значимая и заметная угроза. Сравнительная простота организации подобных атак и их эффективность привлекают все большее число киберпреступников к данному виду незаконной деятельности. Объемы фишинговых атак, выросшие почти вдвое всего за год, тому подтверждение», – подчеркнул Н. Швецов, заместитель директора по исследованиям и разработке «Лаборатории Касперского» ***(Число пользователей, атакованных фишерами, за год почти удвоилось // InternetUA (http://internetua.com/cislo-polzovatelei--atakovannih-fisherami--za-god-pocsti-udvoilos). – 2013. – 23.06).***

***

Компания «Доктор Веб» сообщила о росте количества пользователей, пострадавших от действия троянов-шифровальщиков. Наибольшее распространение получила вредоносная программа Trojan.Encoder.94. Также весьма популярен Trojan.Encoder.225: только за последнее время за помощью в восстановлении файлов, пострадавших от действия этого трояна, в антивирусную лабораторию «Доктор Веб» обратилось более 160 пользователей из России и Украины, сообщили CNews в компании.

Трояны семейства Trojan.Encoder представляют собой вредоносные программы, шифрующие файлы на жестком диске компьютера и требующие деньги за их расшифровку. После того как файлы зашифрованы, трояны Trojan.Encoder, в зависимости от модификации, могут помещать на диск текстовые файлы с информацией по восстановлению данных либо менять фон рабочего стола на изображение с указанием дальнейших инструкций. Сумма, требуемая злоумышленниками, может варьироваться от нескольких десятков до нескольких тысяч долларов.

Трояны-шифровальщики чаще всего распространяются с использованием вредоносных спам-рассылок. Например, Trojan.Encoder.225 может попасть в операционную систему с помощью письма, содержащего вложения в виде документа RTF (но с расширением .doc), эксплуатирующего уязвимость Microsoft Office. С использованием этого эксплойта на компьютер жертвы устанавливается троян-загрузчик, который, в свою очередь, скачивает с управляющего сервера Trojan.Encoder. Троян Trojan.Encoder.94 нередко скачивается на компьютер жертвы с использованием бэкдора BackDoor.Poison, который массово рассылается в письмах с вложенными файлами «Порядок работы с просроченной задолженностью.doc» и «Постановление Арбитражного суда.exe».

В июне 2013 г. был отмечен значительный всплеск количества случаев заражения вредоносными программами семейства Trojan.Encoder. Этот троян написан на языке Delphi и имеет три версии. В предыдущей модификации трояна для связи злоумышленники используют адрес электронной почты milenium56m1@yahoo.com, в последней из известных – marikol8965@yahoo.com. Файлы, зашифрованные ранними версиями Trojan.Encoder.225, поддаются расшифровке. Над средством восстановления файлов, пострадавших от более поздней модификации трояна, в настоящее время ведется работа.

Что касается наиболее распространенного трояна-шифровальщика, Trojan.Encoder.94, то он насчитывает рекордное число модификаций – более 350. Файлы, зашифрованные большей частью версий Trojan.Encoder.94, поддаются расшифровке. По данным «Доктор Веб», жертвами Trojan.Encoder.94 за истекший месяц стали более 680 пользователей.

Всего за последние три месяца в антивирусную лабораторию «Доктор Веб» поступило порядка 2,8 тыс. обращений от пользователей, пострадавших в результате заражения трояна-шифровальщиками. Благодаря тому что злоумышленники непрерывно усложняют механизмы шифрования, вирусным аналитикам приходится решать все более сложные математические задачи в условиях возрастающего потока заявок от жертв энкодеров. В связи с большим числом запросов на лечение и заметно возросшей нагрузкой на антивирусную лабораторию с 19 июня 2013 г. помощь в расшифровке файлов оказывается только зарегистрированным пользователям продуктов «Доктор Веб» ***(Число жертв трояновшифровальщиков заметно возросло // InternetUA (http://internetua.com/cislo-jertv-troyanov-shifrovalsxikov-zametno-vozroslo). – 2013. – 23.06).***