СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(29.04–26.05)

2013 № 10

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(29.04–26.05)
№ 10

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

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

Редакційна колегія:
В. Касаткін, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2013

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Социальная сеть М. Цукерберга теряет миллионы пользователей из-за появления альтернативных площадок для общения, выяснили американские социологи. Только за последние полгода Facebook потеряла почти 9 млн аккаунтов в США и 2 млн в Великобритании, сообщает newsoboz.org. со ссылкой на russian.rt.com.

Гораздо реже на свою страницу в Facebook стали заходить пользователи из Канады, Испании, Франции, Германии и Японии. Сегодня к Facebook активно присоединяются лишь жители Южной Америки и Индии.

Представители Facebook объясняют отсутствие роста на наиболее важных рынках тем, что в США и Великобритании все желающие завести свою страницу уже сделали это.

Вместе с тем, стремительно набирают популярность новые соцсети, появившиеся в Интернете. Самые лучшие показатели у сервиса Instagram, созданного для обмена фотографиями. Теперь Facebook может повторить судьбу MySpace – некогда самой популярной социальной сети в мире.

Также известно, что американцы стали не только реже заходить на свои страницы в Facebook, но и проводить там меньше времени, отдавая предпочтение новым приложениям для смартфонов.

Именно на смартфоны сделал ставку основатель Facebook М. Цукерберг, пытаясь противостоять новоявленным конкурентам. В начале апреля Facebook представил публике социальную оболочку Facebook Home для смартфонов на базе Android. Facebook Home позволяет обмениваться сообщениями, даже когда на экране открыто другое приложение. Вместо стандартных виджетов на рабочем столе отображаются сообщения из ленты новостей соцсети, а также фотографии, опубликованные друзьями пользователя ***(Facebook теряет пользователей // NewsOboz (http://newsoboz.org/obshchestvo/facebook-teryaet-polzovateley-29042013124500). – 2013. – 29.04).***

***

Популярный фотосервис Instagram запустил новый раздел в профиле «Фотографии со мной». Теперь на снимках можно отмечать других пользователей и даже бренды, сообщают «РИА Новости» ссылаясь на пресс-службу Instagram.

До сих пор отмечать на фотографиях в Instagram других людей можно было лишь одним способом – упомянув нужного пользователя в комментариях добавив символ @.

С сегодняшнего дня пользователи мобильных приложений Instagram для платформ iOS и Android могут отмечать друзей, знаменитостей, бренды или посещенные ими места на своих снимках, сообщили в российской пресс-службе соцсети Facebook, которой принадлежит Instagram. Все фотографии, на которых

отмечен пользователь, можно посмотреть в разделе «Фотографии со мной» его профиля.

Тот пользователь, которого хотят отметить на фотографии, получит уведомление об этом, однако лишь в том случае, если снимок не скрыт настройками приватности. В противном случае уведомления он не получит, а снимок не будет отображаться в его профиле. При необходимости пользователь может настроить функцию таким образом, чтобы для каждой отметки было необходимо его одобрение. Пользователи смогут удалять отметки себя одним нажатием на имя либо удалив снимок из раздела «Фотографии со мной» ***(Пользователи Instagram смогут отмечать друзей, знаменитостей и бренды на фото // InternetUA (http://internetua.com/polzovateli-Instagram-smogut-otmecsat-druzei--znamenitostei-i-brendi-na-foto). – 2013. – 03.05).***

***

Новое веб-приложение – смерть Twitter?

Программисты разработали новое веб-приложение Efemr, особенность которого состоит в том, что при его помощи в Twitter можно будет публиковать самоудаляющиеся сообщения. Они исчезают с вашей страницы через заданный промежуток времени с момента публикации.

Данный эффект сервиса заключается в использовании принципа фотосообщений SnapChat, которые существуют не более десяти секунд. Интегрировав подобный механизм в приложение, синхронизированное с Twitter, его использование довольно просто. Для этого необходимо просто зайти на сайт и залогиниться при помощи своей учётной записи в социальной сети, разрешив при этом доступ приложения к своей учётной записи.

Для того, чтобы функция самоудаления сработала, необходимо поставить специальный хэштег. Так, например, тег #5 соответствует сообщению, которое будет удалено через пяти секунд после публикации, а при использовании тега #2h сообщение будет удалено через два часа.

Основная цель разработки подобного приложения состоит в том, чтобы защитить интернет-репутацию своих пользователей, но проблема в том, что сервис не может защитить от ретвитов, так как просто не в состоянии их удалить. Эффективным он будет только тогда, когда аккаунт в соцсети полностью «закрыт» ***(Новое веб-приложение – смерть Twitter? // NovostiUA (http://novostiua.net/techniks/36847-novoe-veb-prilozhenie-smert-twitter.html). – 2013. – 06.05).***

***

Теперь страницу в сосцетях можно вести...и после смерти!

Агентство Irony Production запускает услугу по ведению страниц умерших пользователей в социальных сетях

По замыслу авторов услуги, после заключения договора о передаче прав на посмертную модерацию страницы, клиент сможет определить будущее оформление и наполнение своего аккаунта.

Помимо традиционной услуги по удалению всего контента, предусмотрено несколько вариантов ведения страниц. Клиент может заранее приготовить текст для посмертных публикаций, или же просто утвердить общее направление ведения страницы. Так же агентство собирается предоставлять услугу свободного ведения страницы силами собственных копирайтеров.

Примечательно, что в планах Irony Production предоставлять данную услугу в «ВКонтакте», Facebook, Twitter, «Одноклассниках», Instagram, Vine, а также в пародийной социальной сети «Втлену», в которой отсутствует возможность любых публикаций и обновлений ***(Теперь страницу в сосцетях можно вести...и после смерти! // UAInfo (http://uainfo.org/heading/public/138896-teper-stranicu-v-soscetyah-mozhno-vestii-posle-smerti.html). – 2013. – 13.05).***

***

Facebook Home: всего миллион загрузок за месяц

Дебют Facebook Home пока сложно назвать успешным. Социальная сеть на днях сообщила, что за месяц надстройку для Android скачали всего миллион раз. Учитывая, что число мобильных пользователей Facebook недавно перевалило за 750 млн, результаты явно не поражают воображение. Но самая плохая новость в том, что адаптация Facebook Home заметно замедлилась.

Рубеж 500 тыс. юзеров Facebook Home удалось преодолеть относительно быстро – примерно за неделю. Но после того как ажиотаж в прессе спал, оболочка мало кому оказалась нужна: не помогла даже реклама с участием М. Цукерберга.

По данным аналитической компании Distimo, единственной страной, где к началу мая Facebook Home оставался в 150 самых популярных эппов Google Play, оказался крошечный Люксембург. На самых же крупных рынках – в США, Великобритании, Канаде – Home в данный момент не входит даже в топ-500. И позиции приложения стремительно ухудшаются.

Безусловно, частично это связано с тем, что Home доступен лишь для некоторых смартфонов вроде Galaxy S III, Galaxy S4 и HTC One. С другой стороны, все это – одни из самых популярных моделей в мире. Не стоит также забывать, что оценка Home в Google Play до сих пор колеблется в районе двух звездочек. Как много скачавших приложение людей по-прежнему им пользуются? ***(Facebook Home: всего миллион загрузок за месяц // InternetUA (http://internetua.com/Facebook-Home--vsego-million-zagruzok-za-mesyac). – 2013. – 14.05).***

***

Facebook закрив доступ до додатка Social Roulette, який видаляв дані користувача з ймовірністю один до шести, пише Корреспондент.net (http://ua.korrespondent.net/business/web/1558609-facebook-zaboroniv-rosijsku-ruletku-z-akauntami-jogo-koristuvachiv).

У компанії вирішили, що додаток негативно впливав на імідж соцмережі. Зауваження викликав і логотип програми, із зображенням барабана пістолета із позначкою Facebook як кулі.

Цензори, проте, не послалися на підкріплені своїми висновками витяги з угод із розробниками. Останні пообіцяли, що будуть домагатися скасування заборони.

Додаток Social Roulette розпочав роботу 11 травня 2013 р. З його допомогою користувач Facebook міг зіграти в «російську рулетку»: у випадку «програшу» додаток виділяв його акаунт разом з усіма записами. Сам акаунт можна було відновити, проте записи зникали назавжди. Творці проекту розповіли, що додаток призначався користувачам, які хотіли позбутися залежності від Facebook, але не могли зважитися на цей крок ***(Facebook заборонив російську рулетку з акаунтами його користувачів // Корреспондент.net (http://ua.korrespondent.net/business/web/1558609-facebook-zaboroniv-rosijsku-ruletku-z-akauntami-jogo-koristuvachiv). – 2013. – 14.05).***

***

23 статистических факта о пользователях социальных сообществ и медиа.

1. 76 % пользователей Twitter постят твиты. (в 2010 г. лишь 47 % посылали твиты, в то время как остальные молча наблюдали).
2. Суммарная продолжительность звонков Skype составляет порядка 10 млн мин. в день (Brandwatch).
3. Кнопка +1 от Google используется около 5 млн раз в день (Huffington Post).
4. 23 % пользователей Facebook проверяют свой аккаунт пять или более раз в день.
5. В день раздается порядка 2,7 млрд «лайков» (Digital Trends).
6. 80 % пользователей Pinterest – женщины (Huffington Post).
7. Люди в возврасте 18–29 лет, как правило, используют Facebook, Twitter, Instagram и Tumblr (Pew Internet).
8. 42 % пользователей LinkedIn регулярно обновляют информацию о себе (Social Times).
9. 80 % пользователей предпочитают следить за брендами в Facebook (Huffington Post).
10. Люди с высшим образованием менее склонны к использованию социальных медиа (Pew Internet).
11. Ежедневно постится более 2 млн записей и статей в блогах (Brandwatch).
12. Леди Гага и Джастин Бибер наиболее популярны в Twitter (по масштабу подписчиков) с общим количеством 71,9 млн фоловеров (Twitter Counter).
13. В среднем каждую секунду еще один пользователь создает аккаунт в Instagram (Digital Buzz).

14. 12 % пользователей искали и воспользовались предложениями и скидками в социальных сетях (Mediabistro).

15. Более чем 20 млн пользователей в США указали свои дату и год рождения в профиле Facebook (Mediabistro).

16. Каждую минуту в Instagram загружается порядка 3,480 фотографий (Digital Buzz).

17. 58 % «социальных» геймеров (игры в социальных сетях с каким-то взаимодействием внутри сети) старше сорока и при этом большинство из них – женщины (Digital Buzz).

18. 1,3 млрд мобильных приложений было скачано пользователями устройств Apple и Android (Digital Trends).

19. Около трети блоггеров – матери (Hubspot).

20. 40 % людей проводят больше времени общаясь online, чем вживую (Mediabistro).

21. Facebook зарегистрировал 67 %-ый рост годовой мобильной аудитории (AllFacebook).

22. 60 % пользователей LinkedIn кликали на рекламные баннеры (Social Times).

23. Более 10 % пользователей Wiebo – не из Китая (Mediabistro) ***(23 статистических факта о пользователях социальных сообществ и медиа // InternetUA (http://internetua.com/23-statisticseskih-fakta-o-polzovatelyah-socialnih-soobsxestv-i-media). – 2013. – 16.05).***

***

Музыкальный YouTube: SoundCloud – уникальный проект или очередной пузырь?

Проект, начавшийся с небольшой программы по обмену звуковыми файлами между друзьями, приобретает черты социальной сети

А. Льюнг выглядит слегка растерянным, переходя б-р Уилшир. Черная олимпийка и кроссовки Nike Free – стандартный набор одежды для Лос-Анджелеса, но сигарета и хмурый вид выдают европейское происхождение 31-летнего генерального директора компании SoundCloud. Сейчас проходит церемония Грэмми, но А. Льюнг преодолел 6000 миль, приехав из Берлина, не для того, чтобы получить награду, а ради продвижения платформы SoundCloud среди руководителей звукозаписывающих лейблов, музыкантов и фанатов. Он считает, что SoundCloud – это будущий YouTube звукового контента.

Если вы недавно слушали звуковые файлы в социальных сетях вроде Facebook или Tumblr, то, вероятно, вам встречались вездесущие оранжевые медиаплееры, – это и есть SoundCloud. В отличие от Spotify и Pandora – контент-провайдеров для пассивного прослушивания – SoundCloud позволяет любому человеку поделиться аудиозаписью, которую он создал, будь то музыка, запись детского голоса по телефону или речь Б. Обамы.

Как и другие проекты, SoundCloud испытывал трудности в начале пути. Легче создать социальные платформы для визуального контента, чем для звука. Например, MySpace изначально планировался как средство связи слушателей с музыкантами, а в действительности стал популярен как обычная социальная сеть. Odeo, невезучий сервис подкастов, так и не нашел своей аудитории, пока не переориентировался на короткие текстовые сообщения и не превратился в Twitter.

«Суть в том, – рассказывают А. Льюнг и его партнер 33-летний Э. Вальфорс, – чтобы превратить звук в то, с чем люди смогут взаимодействовать, отсюда и появление функции комментирования и визуализация звуковых волн, позволяющая пользователям “видеть” свои записи». На руку SoundCloud сыграло и распространение смартфонов и мобильного Интернета – теперь любой человек может записывать, пересылать или напрямую заливать контент, который раньше нужно было записывать на CD или скачивать на свой iPod.

Учась в Стокгольме в Королевском технологическом институте, А. Льюнг, работавший до этого звукооператором, и Э. Вальфорс, музыкант-любитель, загорелись идеей создания программы с одной простой функцией, позволяющей перебрасывать звуковые файлы между их Макбуками. Приятели купили домен soundcloud.com за 400 дол. «В то время сервисы хранения файлов и MySpace были просто ужасны, – рассказывает Э. Вальфорс. – С помощью SoundCloud мы в первую очередь решали свои собственные проблемы».

В 2007 г. приятели переехали в Берлин, сняв квартиру в районе Пренцлауэр-Берг. У них было мало денег – А. Льюнг вспоминает, как они мастерили себе рабочие столы из досок, найденных на улице, – но вскоре проект получил поддержку андеграундных электронных музыкантов Берлина, которые решили выкладывать свои треки на SoundCloud.

Официально SoundCloud стартовал в октябре 2008 г., уже имея 20 тыс. пользователей и получив небольшие средства от посевных инвесторов, которых Э. Вальфорс знал по своей прошлой работе. Но у компании так и не было предложений от венчурных фондов. Даже при маленьком штате – менее десяти работников – А. Льюнг не был уверен, выживет ли его компания. В итоге инвестор нашелся – SoundCloud получила 3 млн дол. от лондонского фонда Doughty Hanson Technology Ventures в апреле 2009 г.

Деньги и сарафанное радио среди пользователей привели к росту проекта. Сервис достиг отметки в 1 млн пользователей в мае 2010 г., уже привлекая таких известных исполнителей, как Foo Fighters, которые использовали сайт как площадку для продвижения их альбома. Через год количество пользователей увеличилось в пять раз и после этого SoundCloud получила 10 млн дол. от венчурных фондов Union Square Ventures и Index Ventures.

Сегодня у SoundCloud 38 млн зарегистрированных пользователей (к концу года ожидается 55 млн), около 5 % из них – платные. Модель freemium дает вам доступ к каталогу песен, звуковых фрагментов и подкастов. Нет никаких лицензионных ограничений – все пользователи могут загружать свой

уникальный контент. Хотите иметь больше места для своих загрузки файлов? За 4 дол. в месяц вы получаете объем, достаточный для четырех часов музыки, а за 12 дол. – безлимитный доступ к сервису.

Несмотря на значительное количество платных пользователей, SoundCloud пока убыточен. 2011 г. компания закончила с 10 млн пользователей, выручкой в 6 млн дол. и убытком в 5 млн дол. В 2012 г. SoundCloud, по оценке Forbes, выручила около 20 млн дол.

Следующий шаг – большее вовлечение пользователей и увеличение прибыли. Для этой цели сервис недавно полностью изменил дизайн. Вместе с визуальными улучшениями – более качественными картинками и изящными медиаплеерами – новая версия сайта позволяет поделиться музыкой (что-то вроде ретвита), использовать эмоциональные пометки – «лайки» и предоставляет возможность поиска связанных треков.

В январе 2012 г. компания привлекла около 45 млн дол. от инвесторов, возглавляемых венчурным фондом Kleiner Perkins. Во сколько же оценили SoundCloud? Обычно разговорчивые А. Льюнг и Э. Вальфорс предпочитают не распространяться на эту тему. Но, основываясь на планируемом доходе и сравнении с такими компаниями, как Pandora и Spotify, Forbes оценивает стоимость SoundCloud в 350–400 млн дол.: эту оценку подтверждают источники, близкие компании.

Но один из инвесторов SoundCloud еще более оптимистичен. «Мы думаем, что эта компания будет стоить столько же, если даже не больше, чем Pandora и Spotify, – уверен Х. Нада из GGV Capital, который также является инвестором в Pandora, чью стоимость недавно оценили в 2,2 млрд дол. – Такого контента, как на SoundCloud, больше нигде нет» ***(Музыкальный YouTube: SoundCloud – уникальный проект или очередной пузырь? // InternetUA (http://internetua.com/muzikalnii-Youtube--SoundCloud---unikalnii-proekt-ili-ocserednoi-puzir). – 2013. – 17.05).***

***

В Армении начала функционировать социальная сеть для водителей и автовладельцев www.4car.am, сообщает «Обозреватель» (http://tech.obozrevatel.com/news/58290-sotsset-dlya-voditelej-poyavilas-v-armenii.htm).

Сеть помогает получать данные о нарушениях и штрафах, в том числе фиксируемых дорожными видеокамерами. Пользователь может своевременно посмотреть видео или фото нарушения, ознакомиться с характером и размером штрафа.

На сайте уже зарегистрировалось более 2 тыс. автомобилистов. Вскоре должна заработать и мобильная версия сайта.

Проект реализует компания «Никита Мобайл Армения» совместно с Инновационным центром Microsoft Armenia, в сотрудничестве с полицией Армении.

Напомним, в 2011 г. в Интернете появилась социальная сеть для покойников. На сайте «Помни про» пользователи могут заводить страницы, посвященные скончавшимся людям ***(Соцсеть для водителей появилась в Армении // Обозреватель (http://tech.obozrevatel.com/news/58290-sotsset-dlya-voditelej-poyavilas-v-armenii.htm). – 2013. – 19.05).***

***

В YouTube ежеминутно пользователи загружают около 100 ч. видео, что эквивалентно четырем дням просмотра. Об это говорится в сообщении в блоге YouTube, который посвящен восьмилетию сервиса.

Спрос на такой объем контента тоже соответствующий: каждый месяц на портал заходит более миллиарда человек. Это значит, что каждый седьмой житель планеты Земля хотя бы раз в месяц заходит на Youtube. Интересно, что до 800 млн посетителей портал добрался еще в октябре 2011 г.

«Итак, в наш восьмой день рождения мы хотели поблагодарить всех пользователей за то, что они сделали сервис таким, каким он есть сейчас. За то, что помогли показать всему миру, что видео способно создавать связи между людьми, расширять границы. За то, что кликали на ссылки на наш сайт, даже когда не знали, что увидите, но просто доверяли нам. Короче, спасибо за то, что ежедневно делаете нас лучше – в общем и в частности», – говорится в сообщении.

Руководство Google отмечает, что глубина просмотра сайта растет еще быстрее, чем число уникальных посещений. За месяц сервис транслирует 4 млрд ч. видео, что на 50 % превышает показатель годовой давности.

Также отметим, что на просмотры со смартфонов и планшетов приходится 25 % всех просмотров видео. Google инвестировала существенные средства, чтобы обеспечить совместимость своих видео с Android и iOS, отмечают эксперты. Мобильные устройства уже называют одним из главных движителей популярности Youtube. На просмотры со смартфонов и планшетов приходится 25 % всех просмотров видео.

Два года назад YouTube сообщал, что пользователи загружают порядка 48 ч. видео каждую минуту, а в прошлом году эта цифра равнялась 72 ч.

Компания была основана в феврале 2005 г. тремя бывшими работниками PayPal в Сан-Бруно, Калифорния. Они использовали технологию Flash Video (flv), позволяющую получить относительно хорошее качество записи при небольшом объеме передаваемых данных. Проект стал хорошим средством развлечения и, сформировав свое сообщество, по данным статистики аналитической компании Alexa, опередил по популярности социальную сеть MySpace.

В ноябре 2006 г. была завершена покупка YouTube компанией Google за 1,65 млрд дол. До покупки YouTube у Google был сервис схожей направленности – «Google Видео». Представители Google не намеревались закрывать его, а стали использовать его как место поиска видео по всем

видеохостинговым сайтам. В настоящее время поиск Google Video включает и YouTube.

Недавно YouTube принял решение о предоставлении пользователям платной подписки примерно на 50 своих каналов стоимостью 1,99 дол. в месяц. Платная контент-платформа позволит самой Google и поставщикам видео разделять доход от видеовещания. Кроме того, YouTube таким образом получит новый источник дохода, который не будет зависеть от показов рекламы. Ранее сообщалось, что около 45 % выручки YouTube будет забирать себе, остальная часть средств будет распределяться между производителями контента.

Монетизация контента, задуманная корпорацией Google, которой принадлежит YouTube, – это попытка отыскать источники дохода, отличные от основного бизнеса интернет-гиганта, завязанного на поисковой рекламе, которая, например, в IV квартале прошлого года принесла ему 96 % дохода ***(В YouTube пользователи ежеминутно загружают около 100 часов видео // Минфин (http://minfin.com.ua/2013/05/20/759450/). – 2013. – 20.05).***

***

Twitter запатентовал функцию «Потяните для обновления»

Сервис микроблогов Twitter 21 мая 2013 г. получил патент на функцию «Потяните для обновления» (Pull To Refresh), сообщает Obozrevatel.com (http://tech.obozrevatel.com/news/59234-twitter-zapatentoval-funktsiyu-potyanite-dlya-obnovleniya.htm).

Функция «Потяните для обновления» позволяет пользователю обновлять списки, проведя пальцем по сенсорному экрану линию вниз от верхней границы списка. Она используется во многих мобильных приложениях, включая Facebook.

«Потяните для обновления» изобрел сотрудник компании Atebits Л. Брихтер. Данная компания разработала Twitter-клиент Tweetie. Когда Twitter купил Atebits, Л. Брихтер перешел на работу в сервис микроблогов.

Ранее Twitter пообещал не судиться с другими компаниями, которые применяют функцию «Потяните для обновления» в своих программах ***(Twitter запатентовал функцию «Потяните для обновления» // Обозреватель (http://tech.obozrevatel.com/news/59234-twitter-zapatentoval-funktsiyu-potyanite-dlya-obnovleniya.htm). – 2013. – 22.05).***

***

Facebook, Google+ и Twitter возглавили ТОП самых популярных социальных сетей мира.

Агентство eMarketer опубликовало рейтинг популярности крупнейших социальных сетей, составленный на базе исследования компании GlobalWebIndex. Исследование «Stream Social: Quarterly Social Platforms Update» было посвящено социальной активности пользователей Интернета

Так, Facebook, согласно результатам аналитических изысканий, по-прежнему остаётся социальной сетью № 1. При этом более половины

пользователей Facebook'а заходят на сайт соцсети хотя бы раз в месяц. По оценкам eMarketer, к концу текущего года численность пользователей этой социальной сети может приблизиться к 60 % от общего числа интернет-пользователей.

Следующей по популярности среди пользователей является Google+, численность ее аудитории приближается к 26 % от всей интернет-аудитории. Весьма любопытно, что Google+ не получила особой популярности среди пользователей США. В то же время во всех остальных странах мира соцсеть получила значительную популярность, обогнав даже видеохостинг YouTube, которому отдали предпочтение 25 % интернет-пользователей.

Сервис микроблогов Twitter занимает четвёртую строчку в рейтинге популярности социальных сервисов среди пользователей.

Говоря о популярности функционала социальных сетей среди пользователей, важно отметить, что активное использование мобильных устройств напрямую повлияло на рост популярности отдельных возможностей сервисов. Сегодня всё чаще пользователи предпочитают осуществлять общение на социальных площадках при помощи планшета. Так, 93 % пользователей предпочитают просматривать видео, загруженное их друзьями в соцсети, с планшетных компьютеров, 47 % – со смартфонов, еще 47 % с этой целью используют ПК.

Не менее часто люди используют планшет для того, чтобы поделиться интересной ссылкой с друзьями – так поступают 72 % пользователей, 47 % отправляют ссылки со смартфонов и лишь 44 % пользователей используют с этой целью стационарные компьютеры.

Однако чаще всего – в 91 % случаев – владельцы смартфонов становятся активными фолловерами страниц брендов в соцмедиа. 53 % пользователей подписываются на корпоративные страницы, используя смартфоны, и только 40 % используют для этого действия ПК.

Что касается сервиса микроблогов Twitter, то сегодня Россия занимает пятое место по интенсивности роста числа пользователей этого сервиса.

Наибольший рост числа пользователей в первом квартале 2013 г. показали страны Азии. Так, первое место занимает Индонезия – рост численности аудитории Twitter для этой страны составил 44,2 %, на втором месте – Саудовская Аравия (41,66 %), на тертьем – Сингапур (34,7 %), на четвёртом – США (34,48 %) ***(Facebook, Google+ и Twitter возглавили ТОП самых популярных социальных сетей мира // Marketing Media Review (http://mmr.ua/news/id/facebook-google-i-twitter-vozglavili-top-samyh-populjarnyh-socialnyh-setej-mira-34738/). – 2013. – 22.05).***

***

Yahoo выпустила новую версию фотохостинга Flickr.

В компании говорят, что новый Flickr – это решение, соответствующее XXI в., с новым дизайном, новыми расценками на коммерческое использование и новым Android-приложением для работы через смартфоны и планшеты.

Как было рассказано на презентации в Нью-Йорке, Flickr полностью обновил внешний вид, сменив небольшие иконки с большим количеством метаданных на полноразмерные картинки по умолчанию, а также возможностью получения дополнительных сведений о фотографиях. Впрочем, режим Flickr Lightbox, когда вокруг фото убирается рамка и снимок показывается в увеличенном масштабе, остался.

На заглавной странице обновленного сервиса, как и раньше, выводятся наиболее красивые (по мнению модераторов) снимки, а на странице персонального раздела выводятся фотоленты друзей. Кроме всего прочего, в обновленном Flickr появился режим Explore, который предназначен для обзора каталогов фото. В компании говорят, что в первую очередь Flickr – это сайт для фотообмена, поэтому здесь все должно быть подчинено этой идее. В новой версии Yahoo добавила обновленные возможности для обзора коллекций и их сортировки.

Одновременно с этим, компания представила и новую ценовую модель работы проекта, которая практически несопоставима с прежней. У старой модели были два направления: бесплатное и Pro. Первое было ограничено ничтожными 300 мБт и двумя видео в месяц. За 25 дол. в год можно было получить неограниченное количеств фото и видео в месяц, а также работу без рекламы.

В новой версии бесплатные аккаунты значительно либеральнее: здесь пользователи получают 1 тБт пространства и могут загружать неограниченное количество фото и видео (видео ограничены тремя минутами и качеством 1080p). Платных аккаунтов два типа – за 50 дол. в год, компания ничего не меняет, но убирает рекламу, а за 500 дол. – в год увеличивает пространство до 2 тБт.

Отметим, что на первый взгляд отметка в 500 дол. может показаться большой, но он в реальности она дешевле, чем те же 2 тБт на Picasa, которые стоят 99 дол. в месяц или 1200 дол. в год.

Новые аккаунты Pro больше недоступны, хотя нынешние пользователи их могут продлевать. В компании не сообщили, как долго этот вариант будет работать.

Одновременно с этим, Yahoo выпустила и новую версию Android-приложения для Flickr, которая черпает новый внешний вид от основного сайта, предназначена практически полностью для работы с фото, а также для работы с каталогами и контактами пользователя, позволяя просматривать фотоленты друзей.

Комментируя нововведения, в Yahoo заявили, что до сих пор они не слишком часто реализовывали обновления на Flickr, но новая версия обновила все основные аспекты и в будущем интернет-компания будет реализовывать обновления чаще. Кроме того, в компании признали, что за последнее время довольно сильную конкуренцию начали оказывать социальные сети, также позволяющие размещать фото, однако в отличие от них, специализированные фотохостинги, такие как Flickr, позволяют размещать фото без уменьшения

размеров или ухудшения в качестве, а кроме того, обладают возможностью каталогизации и работы с метаданными ***(Yahoo выпустила новую версию фотохостинга Flickr // InternetUA (http://internetua.com/Yahoo-vipustila-novuua-versiua-fotohostinga-Flickr). – 2013. – 21.05).***

***

Школьники заполонили Facebook и перебираются в Twitter

По данным компании Pew Research, в 2012 г. доля пользователей в возрасте 12–17 лет, имеющих учетные записи в Facebook, составила 94 %. Это на 1 % больше, чем годом ранее. Однако, отмечают исследователи, популярность социальной сети снижается, так как на нее расходуется слишком много времени и здесь часто обсуждаются маловажные вещи.

Twitter, напротив, привлек за прошедшее время новых участников. Если в 2011 г. в нем были зарегистрированы 12 % школьников, то в 2012-м – уже 26 %. Растет популярность и сервиса Instagram. «Если зарегистрироваться в Twitter и Instagram, о Facebook можно забыть», – делится мнением 14-летняя девочка.

Также отмечается, что юные пользователи стали обращать больше внимания на сохранность личных данных и не открывают полный доступ всем желающим к своим профилям в социальных сетях. В то же время подростки стали выкладывать в сеть больше фотографий, чаще предоставлять информацию о месте проживания, номера телефонов и адреса электронной почты ***(Школьники заполонили Facebook и перебираются в Twitter // InternetUA (http://internetua.com/shkolniki-zapolonili-Facebook-i-perebirauatsya-v-Twitter). – 2013. – 22.05).***

***

Независимые исследователи из компании eMarketer пришли к выводу, что примерно 100 млн. учётных записей в Facebook принадлежит не людям…

Впрочем, говорить о нашествии марсиан в социальные сети пока что рано 10 % всех пользователей популярнейшей социальной сети в мире Facebook принадлежит компаниям и животным.

В качестве примера исследователи приводят страницу любимой собаки основателя сети М. Цукерберга – пули по кличке Зверь. На его страницу подписаны более полутора миллионов человек.

Таким образом, специалисты подсчитали, что людям в Facebook принадлежат чуть более 889 млн страниц. И этот показатель перевалит за миллиард только в 2014 г.

По данным аналитиков eMarketer к 2017 г. 54,7 % всех пользователей глобальной сети станут активными пользователями Facebook. Для сравнения, сейчас эта цифра составляет 42,6 %. Наиболее быстрый рост популярности социальной сети наблюдается в Индии, Бразилии, России, Африке и на Среднем Востоке. Предполагается, что в 2013 г. в каждом из этих регионов рост числа пользователей составит около 30 %.

Кроме того, по прогнозам eMarketer в текущем году 63 % пользователей социальной сети по всему миру как минимум раз в месяц зайдут на Facebook. А уже через четыре года этот показатель вырастет на 6,5 % ***(10 % всех пользователей Facebook – не люди // InternetUA (http://internetua.com/10--vseh-polzovatelei-Facebook---ne-luadi). – 2013. – 23.05).***

***

Google+ научили находить на фото еду и цветы

Компания Google доработала сервис поиска фотографий в своей социальной сети Google+. О нововведениях в поиске рассказывается в блоге компании.

Во-первых, пользователь теперь может находить среди своих снимков фотографии, на которых изображены определенные объекты. Например, введя в поисковую строку запрос [my photos of flowers] («мои фотографии цветов»), он увидит все загруженные им снимки цветов.

Уточняющее слово может быть любым. В блоге Google в качестве примеров, кроме цветов, приводятся слова «еда» и «закаты».

Во-вторых, при поиске можно уточнять место и время. Так, по запросу [my photos from New York last year] («мои фото из Нью-Йорка прошлого года») будут показаны все фото, сделанные пользователем в Нью-Йорке в прошлом году. Можно искать не только свои фото, но и фото друзей (в это случае надо указать имя друга).

Запросы, связанные с фотографиями, можно вводить как в поисковую строку в Google+, так и в основной поисковик Google. Поиск работает только в том случае, если пользователь авторизован в Google+. Запросы на русском языке сервис поиска пока не понимает.

Google сообщает, что в основе функции поиска объектов на фотографии лежат технологии компьютерного зрения и машинного обучения.

Соцсеть Google+ была запущена в 2011 г. По состоянию на май 2013 г. ее активная месячная аудитория составляет 190 млн пользователей (для сравнения, у крупнейшей в мире соцсети Facebook этот показатель превышает миллиард пользователей) ***(Google+ научили находить на фото еду и цветы // ВЛАСТИ.НЕТ (http://vlasti.net/news/167112). – 2013. – 24.05).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

У мережі Інтернет шириться громадський рух «Матері проти наркотиків». В його рамках задіяно соціальні мережі, де розгорнуто акцію «Жива книга». Яка її мета? Тут підлітки, що побороли залежність, розповідають ровесникам історію своєї біди, особистим прикладом закликаючи не повторювати їх помилок.

Чому для проведення акції обрано Інтернет? Мотивація організаторів така. Сьогодні школярі й студенти дедалі частіше проводять час у Всесвітній павутині. Їх життя і коло спілкування в основному зосереджені в соціальних мережах і так званих блогосферах. Отже, підлітків, які розповідають там свої історії, швидше почують ***(Вернигора Г. Матері проти наркотиків // Сільські вісті (http://www.silskivisti.kiev.ua/18943/index.php?n=17514). – 2013. – 30.04).***

***

З Головним управлінням Міндоходів у Кіровоградській обл. можна «подружитись» у соцмережах.

Відтепер Головне управління Міндоходів у Кіровоградській обл. представлене у таких популярних соціальних інтернет-мережах, як Facebook, «ВКонтакте» та Twitter, а також має свою сторінку у Livejournal, повідомляє Інформаційно-комунікаційний відділ ГУ Міндоходів у Кіровоградській обл.

Платники податків та клієнти митниці можуть оперативно дізнаватися останні новини та коментувати їх. А що найголовніше – отримати онлайн консультацію, звернувшись безпосередньо до спеціалістів управління.

Сторінка у Facebook: www.facebook.com/MINRDkr, у «ВКонтакте»: www.vk.com/ MINRDkr, у Twitter: www.twitter.com/MINRDkr, у Livejournal: www.kr-rd-ua.livejournal.com ***(З Головним управлінням Міндоходів у Кіровоградській обл. можна «подружитись» у соцмережах // Весь Кіровоград (http://www.kirovograd.net/shortly/2013/5/14/z_golovnim_upravlinnjam_mindohodiv_.htm). – 2013. – 14.05).***

***

Посольство США фінансуватиме українських блогерів та тренерів з роботи у соцмережах

Українські блогери мають шанс отримати фінансову підтримку від Держдепартамету США. Про це вчора, під час відкриття конференції з питань застосування новітніх цифрових технологій «ТехКемп Іван-Франківськ 2.0», розповів прес-аташе посольства США в Україні Д. Вульф.

З його слів, вже незабаром на сайті посольства з'явиться оголошення про відкриття двох нових програм мікрогрантів, спрямованих на розвиток громадянського суспільства в Україні. Обидві програми, як і «ТехКемп», є частинкою широкої програми Держдепартаменту США з розвитку громадянського суспільства в усьому світі – «2.0». Одна з них передбачатиме надання на конкурсній основі мікрогрантів для розвитку мережі блогерів. В рамках другої планується здійснювати мікрогрантову підтримку проведення тренінгів із застосування інструменту соціальних мереж в інтересах громадянського суспільства.

«Інсвестуючи у громадянське суспільство, – прокоментував з даного приводу посол США в Україні Д. Тефft, – ми розраховуємо отримати дуже вигідні дивіденди: якщо ми це робимо в Україні, це сприятиме її процвітанню.

В результаті розвитку громадянського суспільства уряди будуть відповідальнішими перед своїми суспільствами. Жодна демократія в світі не буде успішною без живого громадянського суспільства».

Зі слів Д. Вульфа, адмініструватимуть програми мікрогрантів його помічники – Л. Штеллє та С. Кравченко. Вони ж, між іншим, ведуть сторінки посольства США у соціальних мережах ***(Посольство США фінансуватиме українських блогерів та тренерів з роботи у соцмережах // БРІЗ (http://briz.if.ua/11135.htm). – 2013. – 17.05).***

***

Личность парня, напавшего на журналистов, идентифицирована: у него есть страница «ВКонтакте».

Журналисты нашли страницу «ВКонтакте» бойца, который сначала охранял митинг Партии регионов «Против фашистов», а потом участвовал в драке со «Свободовцами» и напал на корреспондентов, которые снимали драку.

«ВКонтакте» нападающего зовут Вадик Румын. На фотографиях среди его друзей встречаются и другие участники нападения на журналистов.

Через час после того, как появилась эта новость, В. Румын удалил свою страницу из «ВКонтакте». Но у нас остались скриншоты и имена его друзей ***(Личность парня, напавшего на журналистов, идентифицирована: у него есть страница «ВКонтакте» // Левый берег (http://society.lb.ua/accidents/2013/05/18/200003_lichnost_molodchika_napavshego.html). – 2013. – 18.05).***

***

Соціальні мережі Facebook та Twitter зробили додатки для Google Glass. Як відомо, окуляри Google Glass є гучною новинкою компанії Google. Ці окуляри містять зліва невеликий екран і дозволяють отримати доступ до електронної пошти і повідомлень, записувати відео і отримувати інформацію з Інтернету.

Google почав дистрибуцію своїх окулярів минулого місяця в обмеженій кількості, і наразі невідомо, коли новинка стане доступною широкому загалу і якою буде ціна.

Як відомо, служба безпеки України заборонила використання окулярів марки Google в Україні. Заборона відомства пов’язана з тим, що окуляри відомої марки можна віднести до списку заборонених для купівлі та використання предметів.

До такого списку також відносяться: подовжувач для електроприладів з вбудованим мікрофоном, окуляри з вбудованою в оправу на переніссі відеокамерою (як і окуляри Google), годинник з вбудованими адуіо-й відеореєстраторами з пам’яттю 8 гБ, брелок з вбудованою відеокамерою, замаскований під автосигналізацію і т. д.

Всі ці предмети, на думку відомства, є шпигунським устаткуванням та не повинні знаходитися в руках пересічних громадян ***(Соціальні мережі***

Facebook та Twitter зробили додатки для Google Glass // Українська правда. Життя (http://life.pravda.com.ua/technology/2013/05/17/128790/). – 2013. – 18.05).

***

Івано-Франківська податкова «вийшла» в соціальні мережі

У соціальних мережах Facebook, Twitter та «ВКонтакте» розпочали роботу офіційні сторінки Головного управління Міндоходів в Івано-Франківській обл.

На цих інформаційних ресурсах розміщуватиметься чимало актуальної інформації на податкову та митну тематики.

Додати обласне Міндоходів «в друзі», чи вступити до створеного ним співтовариства – наочне втілення в життя гасел з налагодження партнерських відносин із платниками податків і перетворення служби на сервісну.

На думку працівників відомства, таке нововведення дозволить значно швидше доносити до громадян актуальну інформацію щодо податкового та митного законодавства, а головне – забезпечити повноцінний зворотній зв'язок.

Тож приєднуйтесь до ГУ Міндоходів в області за посиланнями:

– http://www.facebook.com/mindohodiv.if;

– https://twitter.com/mindohodiv_if;

– http://vk.com/mindohodiv_if.

Крім того, відеоматеріали щодо роботи відомства можна переглядати, підписавшись на офіційний канал You Tube за посиланням www.youtube.com/user/odpaif?feature=guide ***(Івано-Франківська податкова «вийшла» в соціальні мережі // БРІЗ (http://briz.if.ua/11253.htm). – 2013. – 22.05).***

***

Французские пользователи Facebook устроили акцию протеста против цензуры наготы в социальной сети, сообщает местная газета Metro.

20 мая участники акции разместили в специально созданной группе «День наготы на Facebook» (La Journйe du nu sur Facebook) изображения с обнаженными людьми. Часть пользователей выложили свои собственные фотографии, при этом большинство запостили репродукции знаменитых произведений искусства. Через несколько часов модераторы Facebook удалили страницу группы.

О желании участвовать в акции заявляли восемь тысяч французов, которые подписались на Facebook-событие «День наготы». Автором идеи и создателем группы был парижский фотограф А. Башелье.

По его словам, акция направлена против «нелепой цензуры, которая нарушает основы прав во имя пуританства и моральных норм из другого века». Дата протеста была назначена на день закрытия Европейского фестиваля фотографии «ню» в Арле.

Facebook строго запрещает публикацию обнаженных фото в соцсети. Под запрет попадают даже известные произведения искусства и фотографии с частичным обнажением. Так, в марте соцсеть заблокировала страницу парижского музея современного искусства Же-де-Пом за публикацию одного из экспонатов. При этом администраторы сети пригрозили удалить аккаунт музея, если инцидент повторится.

В 2011 г. Facebook запретил обложку альбома Nirvana Nevermind, на которой изображен голый ребенок в бассейне. Также широкую известность получил случай, когда модераторы соцсети удалили фотографию женщины, приняв ее локти за голую грудь ***(Французы протестуют против цензуры наготы в Facebook // Подробности.UA (http://podrobnosti.ua/internet/2013/05/22/906123.html). – 2013. – 22.05).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Российская социальная сеть «ВКонтакте» сменила владельцев. Теперь на ее развитие будет оказывать влияние энергетический магнат И. Щербович

Фонд United Capital Partners (UCP) выкупил 48 % акций социальной сети у двух собственников-сооснователей В. Мирилашвили (40 %) и Л. Левиева (8 %). Цена сделки не оглашается, однако, по мнению аналитиков, речь может идти о 1,4 млрд дол., поскольку оценочная стоимость «ВКонтакте» превышает 2,8 млрд дол.

Главная интрига в том, что продавцы не поставили в известность двух других совладельцев – представителей Mail.ru Group (39,99 %) и генерального директора сети П. Дурова (12 %). Эксперты по корпоративному праву утверждают, что продать доли покупателям извне можно только после письменного отказа других сособственников. Тем более что А. Усманов (один из совладельцев Mail.ru) в декабре 2012 г. заявлял о своем намерении увеличить долю в социальной сети, а П. Дурову сейчас принадлежит вся полнота власти в ней: весной 2012-го А. Усманов передал ему в управление 39,99 %, принадлежащих Mail.ru.

Впрочем, сделка была проведена юридически грамотно – куплены не сами акции сети, а компании, владеющие бумагами.

В. Мирилашвили и Л. Левиев пытались продать свои доли еще в 2011 г. и тогда оценивали «ВКонтакте» более чем в три миллиарда долларов Покупателей не нашлось. Летом прошлого года выкупить доли В. Мирилашвили и Л. Левиева хотел владелец Marshall Group К. Малофеев, он оценивал компанию в 2,6 млрд дол. Не договорились. Переговоры с UCP начались в январе этого года, а договор купли-продажи был подписан в начале апреля.

«ВКонтакте» с 42 миллионами активных пользователей – самая популярная сеть и второй по посещаемости сайт в России. По данным исследовательской компании TNS, его ежедневная аудитория составляет

27,3 млн человек, больше только у «Яндекса» (29 млн), на третьем месте проекты Mail.Ru Group с 26,6 млн посещений. Компания не разглашает свои финансовые показатели. Российские эксперты оценивают ее выручку в 2010 г. в размере 93,8 млн дол., в 2011 г. – 119,3 млн дол., а в 2012 г. – 172 млн дол.

Надо признать, что «ВКонтакте» слабо зарабатывает на трафике. А политика свободно распространяемого музыкального и видеоконтента принесла ей на Западе недобрую славу хранилища пиратской продукции. Этот факт вполне мог стать серьезной проблемой при выходе на IPO. Впрочем, в мае 2012 г. компания отказалась от этой идеи после не вполне удачного размещения Facebook. С другой стороны, пример американской социальной сети LinkedIn, которая на следующий день после размещения в мае 2011 г. подорожала более чем вдвое, доказывает, что рост возможен – всё зависит от перспектив монетизации соцсетей.

Кто же является новым инвестором «ВКонтакте»? Инвестиционная группа UCP основана в 2006 г., зарегистрирована на офшорных Каймановых островах и управляет средствами трех десятков клиентов, ее активы составляют 3,5 млрд дол. Право принятия основных решений и 67 % акций в инвестиционном консорциуме принадлежат И. Щербовичу, который также входит в состав советов директоров таких компаний, как «Роснефть», «АК Транснефть» и ФСК ЕЭС.

Новоиспеченные совладельцы считают, что интернет-ресурс отстает от мировых лидеров по росту финансовых показателей. В то же время намерений менять руководство или вмешиваться в «творческую и техническую часть» управления UCP не собирается. «П. Дуров руководит профессиональной командой, которая добилась впечатляющих результатов», – отметил И. Щербович. И добавил, что UCP – прежде всего финансовый инвестор, который надеется на конструктивное сотрудничество с другими акционерами.

П. Дуров, один из самых молодых рублевых миллиардеров России, снискал славу жесткого и талантливого предпринимателя. В 2011–2012 г. отношения А. Усманова и П. Дурова были сложными. А. Усманов делал всё для поглощения «ВКонтакте». П. Дуров, известный своими эксцентричными выходками, в открытую назвал Mail.ru Group «трэш-холдингом». Это не помешало бизнесменам мирно договориться, и в прошлом году А. Усманов заявил, что П. Дуров – главная ценность сети «ВКонтакте».

Есть еще один важный момент. В период заключения сделки П. Дурову было предъявлено обвинение по ст. 318 ч. 1 Уголовного кодекса РФ (применение насилия в отношении представителя власти), согласно которому он, будучи за рулем авто, сбил полицейского, когда тот находился при исполнении. За обвинениями последовали обыски в офисе и доме П. Дурова. Российские СМИ активно подхватили тему травли молодого миллиардера и не перестают выдвигать всё новые версии происходящего.

Что значит эта сделка? Одна из наиболее вероятных версий – желание государства контролировать финансы социальной сети и интернет-пространство вообще посредством лояльных олигархов.

Другим реалистичным сценарием может стать дальнейшая продажа 48 % акций кому-то, кто потом таки продаст их А. Усманову. Тогда самый богатый человек России, владеющий также издательским домом «Коммерсант», получит пакет акций около 88 %.

К слову, когда А. Усманов получал контроль над Mail.ru в 2010 г., также не обошлось без череды громких разборок ***(Государская И. Жесткий Контакт // Эксперт Украина (http://www.expert.ua/articles/23/0/11361/). – 2013. – 29.04).***

***

Крупнейшая мировая социальная сеть Facebook сегодня сообщила о получении компанией квартальных итогов выше ожиданий рынка на фоне активного продвижения компании в сферу мобильной рекламы и мобильного таргетинга. Согласно данным Facebook, в первом квартале ее продажи возросли на 38 % до 1,46 млрд дол., тогда как аналитики на Уолл Стрит ожидали от компании этот показатель на уровне 1,44 млрд дол. Операционная прибыль компании составила 12 ц. на акцию, в сравнении с ожиданиями в 13 ц.

Напомним, что с начала этого года глава компании М. Цукерберг постоянно говорил о том, что Facebook бросает все свои силы на продвижение в мобильной сфере и ставит работу на смартфонах и планшетах своим основным приоритетом. Впрочем, реальные действенные шаги в мобильной сфере компания начала предпринимать только недавно, выпустив мобильную среду Home, запустив мобильные рекламные инструменты для бизнеса и оптимизировав рекламные показы для мобильных устройств.

В компании Wedbush Securities говорят, что основные мобильные достижения Facebook еще впереди, но с каждым последующим шагом Facebook работает в мобильной сфере все активнее и успешнее.

В течение первого квартала Facebook сгенерировала около 30 % своей рекламной выручки от работы в мобильной сфере, тогда как в четвертом квартале 2012 г. этот показатель составлял 23 %.

Чистая прибыль Facebook в первом квартале составила 217 млн дол., что на 58 % превышает показатель аналогичного периода 2012 г. (137 млн дол.). В то же время, операционные издержки компании выросли на целых 60 % до 1,09 млрд дол., так как Facebook нанимает все больше сотрудников, закупает все больше оборудования и программного обеспечения.

Аналитики говорят, что хотя Facebook уже и начала показывать признаки роста, компания еще не восстановила своей рухнувшей капитализации. В сентябре 2012 г. ее бумаги достигли абсолютного минимума в 17,73 дол., с тех пор цена бумаг выросла на 54 %, но все же не достигла показателя цены IPO в мае 2012 г.

Финдиректор Facebook Д. Эберсман говорит, что сейчас социальная сеть концентрируется на новых продуктах, которые бы поспособствовали увеличению количества времени, проводимого пользователями на ресурсе. Решение Home – это один из таких шагов. В то же время, Эберсман отметил,

что пока Home работает только на Android и он пока не может определенно сказать, когда оно заработает на iOS и Windows Phone.

Также компания сообщила о том, что сейчас количество пользователей в Facebook достигло 1,11 млрд человек, что на 23 % больше, чем за аналогичный период прошлого года. Количество мобильных пользователей увеличилось на 54 % до 751 млн человек, что составляет 68 % от общей базы ***(Facebook отчиталась лучше прогнозов рынка // InternetUA (http://internetua.com/Facebook-otcsitalas-lucsshe-prognozov-rinka). – 2013. – 2.05).***

***

Принадлежащий компании Google видеохостинг YouTube в четверг запустил пилотный проект платных подписок на каналы.

В официальном блоге YouTube сообщается, что пробная программа касается 53 каналов.

Стоимость подписки составит от 99 ц. до восьми долларов в месяц.

По мнению экспертов, пока неясно, сколько будет пользователей, желающих платить за просмотр каналов, даже если цена подписки не будет превышать долларов в месяц.

Первые сообщения о планах YouTube запустить платные подписки появились еще в январе. Тогда информированные источники заявляли, что новый сервис будет представлен в конце апреля на конференции Digital Content New Fronts.

До запуска платных подписок основным источником дохода для создателей видео на YouTube являлась реклама. Кроме того, с 2011 г. на видеохостинге действует кинопрокат, позволяющий пользователям смотреть фильмы за умеренную плату ***(На YouTube появились платные каналы // Интернет-обозрение Главное™ (http://glavnoe.ua/news/n136268). – 2013. – 10.05).***

***

М. Цукерберг теперь может сделать свое резюме еще более внушительным: его детище, социальная сеть Facebook, смогла попасть в список 500 крупнейших компаний, созданный специалистами издания Fortune. На это ей потребовалось около девяти лет с момента основания и меньше года с момента выхода на биржу. По второму параметру она пока мировой лидер.

Если в прошлом году Facebook занимала 598 место, то теперь обосновалась на 482-м. Свои ежегодные списки Fortune составляет на основе данных о годовой выручке компаний за период, завершающийся 31 января. Во время IPO в мае прошлого года соцсеть привлекла 16 млрд дол. Ее выручка неуклонна росла и в 2012 г. достигла 5 млрд.

В топ-500, естественно, попали и другие технокомпании. Apple, к примеру, заняла 6-е место, Hewlett-Packard – 15-е, IBM – 20-е, Microsoft – 35-е. Amazon оказалась на 49-й строчке рейтинга, а Google – на 55-м. Посмотрим, где

все они будут через год ***(Facebook впервые попала в «Топ-500 богатейших компаний» по версии Fortune // InternetUA (http://internetua.com/Facebook-vpervie-popala-v--top-500-bogateishih-kompanii--po-versii-Fortune). – 2013. – 8.05).***

***

Сервис микроблогов Twitter стоит 9,8 млрд дол. Об этом говорится в сообщении миноритарного акционера Twitter, компании GSVC. Еще в начале года Twitter оценивался в 11 млрд дол.

Сервис микроблогов Twitter стоит 9,8 млрд дол. Об этом говорится в сообщении миноритарного акционера Twitter, компании GSVC. Аналитики фирмы определили, что одна акция стоит примерно 18,5 дол. Исходя из этой оценки и общего количества акций Twitter, совокупная стоимость всего сервиса достигла указанной суммы, сообщает TCH.ua.

Еще в начале года Twitter оценивался в 11 млрд дол. Среди факторов, которые повлияли тогда на рост стоимости компании, отмечалось увеличение числа пользователей, а также появление инструментов монетизации. Ожидается, что Twitter может начать приготовления к IPO уже в конце 2013 г., а само размещение акций состоится в 2014 г.

В конце января сообщалось, что инвестиционный фонд BlackRock сделал предложение о покупке пакета акций сервиса микроблогов Twitter на 80 млн дол. Таким образом, капитализация компании была оценена более чем в 9 млрд дол.

Владельцем системы Twitter является компания Twitter Inc, главный офис которой находится в Сан-Франциско, штат Калифорния. Twitter Inc также имеет серверы и офисы в Сан-Антонио (штат Техас) и Бостоне (штат Массачусетс). По состоянию на 2012 г. в компании работало свыше 900 сотрудников ***(Twitter за несколько месяцев потерял в цене более миллиарда долларов // Vlasti.net (http://vlasti.net/news/166246). – 2013. – 13.05).***

***

Реклама на YouTube стала причиною сварки титанів IT-ринку.

У Google і Microsoft виник конфлікт через мобільну версію відеопорталу YouTube. Так, корпорація з Редмонда випустила версію YouTube для девайсів на ОС Windows Phone. Її основною особливістю стала відсутність реклами, яка залишається ключовим джерелом доходів Google від популярного сервісу (http://ua.korrespondent.net/business/mmedia_and_adv/1559246-reklama-na-youtube-stala-prichinoyu-svarki-titaniv-it-rinku).

Так, пошуковик вже через тиждень після запуску програми скерував Microsoft офіційну вимогу не тільки припинити її поширення, а й стерти існуючі копії.

Повідомляється, що програма створювалася без відома Google, і значна частка зусиль була докладена для розробки спеціального захисту, що блокував би рекламу. Корпорація стверджує, що це є грубим порушенням

норм користування та поширення YouTube. Переховування банерів завдає збитку не тільки самому інтернет-гігантові, а й партнерам, які заробляють завдяки системі AdSense.

Зазначимо, що йдеться в першу чергу про звичайних користувачів, які завантажують ролики на YouTube і отримують дохід, коли кількість переглядів і передплатників досягає певної кількості.

Раніше повідомлялося, що Microsoft відроджує рекламну війну проти Google зі звинувачення в шпигунстві ***(Реклама на YouTube стала причиною сварки титанів IT-ринку // Корреспондент.net (http://ua.korrespondent.net/business/mmedia_and_adv/1559246-reklama-na-youtube-stala-prichinoyu-svarki-titaniv-it-rinku). – 2013. – 16.05).***

***

Facebook потратит миллиард долларов на приложение для автомобилистов.

По сведениям издания Calcalist, переговоры о покупке активов длятся уже около полугода, и сейчас компании сумели договориться о принципиальных условиях сделки, пишет NewsOboz.org со ссылкой на Корреспондент.net.

Отмечается, что Facebook и Waze начали сотрудничество в октябре прошлого года, когда пользователи сервиса геолокации получили возможность сообщать о своим передвижениях друзьям в соцсети. На сегодняшний день услугу использует около 47 млн человек. В случае удачного завершения сделки, это усилит позиции Facebook в мобильном сегменте.

Судя по последнему документу социального гиганта, в настоящее время около 751 млн из 1,1 млрд активных пользователей сети посещают ее при помощи смартфонов. Компании пока не комментируют готовящееся соглашения. Следует отметить, что Waze окажется уже не первым приобретением Facebook в Израиле.

В 2011 г. соцсеть купила Snaptu, разрабатывающую программы для старых моделей телефонов, которые поддерживают только Java, а в 2012 г. – Face.com, которая разрабатывает алгоритмы для автоматического определения лиц на фото. Ранее сообщалось, что цена Facebook-смартфона рухнула в 100 раз ***(Facebook потратит миллиард дол. на приложение для автомобилистов // NewsOboz (http://newsoboz.org/it_tehnologii/facebook-nameren-kupit-prilozhenie-dlya-avtomobilistov-za-milliard-10052013124000). – 2013. – 13.05).***

***

Интернет-компания Yahoo! объявила о покупке блогохостинга Tumblr. Сообщение об этом появилось в понедельник, 20 мая 2013 г., на сайте Yahoo!.

Блогохостинг обойдется Yahoo! в 1,1 млрд дол., а закрытие сделки запланировано на вторую половину 2013 г. Tumblr, подчеркивают в Yahoo!, продолжит существовать как отдельный продукт.

Благодаря сделке месячная аудитория Yahoo! возрастет на 50 % и превысит миллиард пользователей, отмечается в заявлении компании. Кроме

того, Tumblr сможет использовать технологии персонализации и поиска, разработанные Yahoo!, в своих сервисах. Также компании намерены объединить рекламные площадки.

Слухи о возможной покупке Tumblr интернет-компанией Yahoo! появились в СМИ еще 17 мая. Источники изданий подчеркивали, что сделка направлена на «омоложение» аудитории Yahoo!.

В заявлении Yahoo! Tumblr назван самой быстрорастущей соцсетью в мире. Каждый день, говорится в нем, в блогохостинге регистрируется по 120 тыс. пользователей, а в месяц на него заходит 300 млн уникальных пользователей.

Tumblr позволяет загружать фотографии, видео и музыку, а также публиковать текстовые статусы. Каждую секунду пользователи публикуют в блогохостинге по 900 постов, а в месяц суммарно проводят на сайте по 24 млрд минут (в среднем по 80 минут на пользователя) ***(Yahoo! подтвердил покупку блогохостинга Tumblr // Mmr.Ua (http://mmr.ua/news/id/yahoo-podtverdil-pokupku-blogohostinga-tumblr-34715/). – 2013. – 21.05).***

***

CEO интернет-гиганта Yahoo! М. Майер после недавнего приобретения блог-платформы Tumblr за 1,1 млрд дол. рассказала о грядущих изменениях ресурса.

Как сообщается, первые изменения будут касаться в основном рекламной политики. Так, в следующем году на блогах Tumblr ожидается большее количество рекламных объявлений. Контент из избранных блогов будет транслироваться на сайты Yahoo!, передает NewsOboz.org со ссылкой на Вести.ру.

М. Мейер добавила, что собирается использовать приобретение так, чтобы «не напортачить».

Отметим, что еще до появления сообщений о развитии рекламной модели сайта начался массовый отток пользователей. Аудитория Tumblr опасается, что нынешний владелец «придушит» свободу ресурса и наводнит его непривлекательным для нынешних пользователей контентом.

Исполнительный директор Yahoo! М. Майер пообещала главе и основателю Tumblr Д. Карпу, что оставит его в должности руководителя блог-платформы, которая продолжит работу под своим брендом, и что в социальную интернет-площадку не будут агрессивно встраиваться сервисы Yahoo!, но внешний вид Tumblr будет адаптирован к более эффективной монетизации – через рекламу и дистрибуцию.

«Мы полагаем, что Tumblr мы можем монетизировать способами, которые являются значимым вкладом в пользовательский опыт. Сегодня Tumblr уже работает с подобной рекламной моделью. Мы хотели бы изучить это глубже, чтобы понять, как ввести большее количество объявлений, которые соответствуют ожиданиям пользователей и могут быть им реально полезны». М. Майер также отметила, что Yahoo!, возможно, будет работать с топовыми

блоггерами: спрашивать разрешения на показ рекламы оговоренного формата с возможными отчислениями с дохода.

Tumblr был запущен в 2007 г. Крупнейшим акционером компании является Д. Карп, в числе ранних инвесторов – фонды Union Square Ventures, Spark Capital и Sequoia Capital. В конце 2011 г. Tumblr привлекла 85 млн дол. венчурных инвестиций – тогда компанию оценили в 800 млн дол.

На первых порах монетизацией ресурса Карп не занимался: важно было сначала обрасти аудиторией. Поэтому реклама на Tumblr появилась лишь в середине прошлого года. В 2012 г. выручка сервиса составила лишь 13 млн дол., а в этом году компания рассчитывает увеличить показатель до 100 млн дол ***(Yahoo! будет развивать рекламу в Tumblr // NewsOboz (http://newsoboz.org/it_tehnologii/lish-by-ne-naportachit-novye-vladeltsy-tumblr-rasskazali-21052013153000). – 2013. – 22.05).***

***

Податкові ігри: одна з популярних російських соцмереж двічі за місяць змінила власника.

ТОВ «Одноклассники», власник однойменної соціальної мережі, до 27 березня 2013 р. належало британській Odnoklassniki Ltd. Від 27 березня її власником стала кіпрська Nessly Holdings Limited. А вже 17 квітня власник знову змінився – тепер це кіпрська Odnoklassniki Holdings Limited, передає Корреспондент (http://ua.korrespondent.net/business/web/1561253-podatkovi-igri-odna-z-populyarnih-rosijskih-socmerezh-dvichi-za-misyac-zminila-vlasnika).

Видання зазначає, що водночас кінцевий власник колишній – Mail.Ru Group.

У Mail.Ru Group заявили: «Передача цієї юрособи (ТОВ Одноклассники) здійснена в рамках юридичної реорганізації, метою якої є створення єдиної холдингової структури для російських операційних компаній, які входять до Mail.Ru Group. Це планова реорганізація, яка має технічний характер».

«Зміна британської юрисдикції на кіпрську з величезною імовірністю пов'язана з питаннями податків, – припускає заступник генерального директора однієї з інвестиційних компаній Д. Панченко. – Можливо, Mail.Ru Group планує вивести прибуток «Одноклассників» у вигляді дивідендів – робити це через Кіпр, де дивіденди не обкладаються податком, вигідніше».

Переведення з однієї кіпрської компанії на іншу, на думку Д. Панченка, також могло бути пов'язане з податками. Щоб перевести актив з Лондона на Кіпр, треба оформити угоду купівлі-продажу і заплатити в Лондоні податки з відповідної суми. Щоб багато не платити, можна перший раз продати за невеликою ціною, а другий раз – за більш великою, припустив Д. Панченко.

Аналітики «ІК Церіх Кепітал Менеджмент» вважають, що все виглядає логічно.

Можливо, мова йде про підготовку «Одноклассников» до продажу, зазначає Д. Панченко. Дохід від подібної угоди також вигідніше концентрувати в кіпрській юрисдикції, нагадує він.

Раніше повідомлялося, що фонд United Capital Partners, очолюваний І. Щербовичем, став власником 48 % найбільшої російської соціальної мережі «ВКонтакте», купивши частки співзасновників В. Мірілашвілі та Л. Левієва ***(Податкові ігри: одна з популярних російських соцмереж двічі за місяць змінила власника // Корреспондент.net (http://ua.korrespondent.net/business/web/1561253-podatkovi-igri-odna-z-populyarnih-rosijskih-socmerezh-dvichi-za-misyac-zminila-vlasnika). – 2013. – 21.05).***

***

Участники системы WebMoney Transfer получили новые инструменты для сбора средств на развитие своих проектов. Собирать средства можно с помощью виджетов WebMoney на сайтах или через бизнес-группы Деловой сети Events.WebMoney.

Получить поддержку бизнес-проекта в Интернете стало проще, чем когда-либо. С помощью быстрого конструктора можно создать виджет для сбора средств и добавить его на любой сайт. При этом проект автоматически получает собственную бизнес-группу в Деловой сети Events.WebMoney – посетители группы тоже смогут поддержать проект.

Для существующих бизнес-групп можно включить сбор средств в настройках. Полученные средства накапливаются на балансе группы проекта. Создатель группы всегда может вывести средства на свой WebMoney-кошелек.

Events.WebMoney (http://events.webmoney.ru) – Деловая сеть системы WebMoney Transfer. Сервис предоставляет эффективные инструменты обмена информацией в рамках бизнес-взаимодействий пользователей.

WebMoney Transfer – международная система расчетов и среда для ведения бизнеса в сети, основанная в 1998 г. В системе зарегистрировано более 20 млн аккаунтов.

В WebMoney Transfer предусмотрены сервисы, позволяющие автоматизировать прием средств и расчеты, вести учет, обменивать расчетные средства, оперативно находить партнеров, решать споры и заключать безопасные сделки.

Особое внимание в системе уделено интеграции с ресурсами, принимающими платежи. Благодаря программным интерфейсам, любой ресурс получает возможность принимать оплату в автоматическом режиме. В WebMoney появились новые инструменты для сбора средств ***(WebMoney представила новые инструменты для бизнес-проектов // www.mirineta.com (http://mirineta.com/1572-webmoney-predstavila-novye-instrumenty-dlya-biznes-proektov.html). – 2013. – 21.05).***

***

Аналітики пророкують експансію реклами в соцмережі, які володіють колосальним обсягом даних про користувачів

Соціальні мережі, у першу чергу Facebook та Twitter, щодня залучають мільйони користувачів, а розміщена на їхніх сайтах реклама дедалі більше орієнтується на цільову аудиторію з урахуванням демографії, соціальних зв'язків, інтересів та звичок клієнтів, пише Кореспондент (http://ua.korrespondent.net/business/mmedia_and_adv/1562264-analitiki-prorokuyut-ekspansiyu-reklami-v-socmerezhi-yaki-volodiyut-kolosalnim-obsyagom-danih-pro-kori).

Про це свідчать дані, отримані внаслідок дослідження, проведеного Business Insider.

Треба зазначити, що в дослідженні аналізується поточний стан рекламного ринку соціальних мереж та його перспективи розвитку. Крім основних гравців (Facebook і Twitter) експерти розглядають Tumblr (як нову рекламну платформу), а також зростаючу роль мобільних засобів.

Як стало відомо, на тлі фрагментації медіа-середовища соціальні мережі стають дедалі більш привабливими для рекламодавців. Соцмережі мають колосальну базу даних про своїх користувачів. Згідно з даними на липень 2012 р. американці в середньому проводять у соціальних мережах 12 год. на місяць, а у віковій шкалі від 18 до 24 років – близько 20 год.

Ця величезна аудиторія дає рекламодавцям унікальні можливості для просування своїх брендів.

Дослідники також зазначають, що компанії витрачають величезні кошти за можливість розповісти про свій продукт одночасно великій аудиторії, що не так просто в роздробленому медіа-середовищі.

Соцмережі роблять ставку на «гарантовану увагу» і відмовляються від традиційних рекламних банерів (подібних до тих, які були на Facebook у правому боці екрану). У моду увійшов термін так званої «рідної реклами» (native advertising), коли увага користувача привертається за допомогою контенту, який цікавить особисто його.

Аналітики дійшли висновку, що обсяг реклами в соціальних медіа різко збільшиться. Рекламний ринок у соціальних медіа з'явився зовсім недавно, і поки що на нього припадає від 1 % до 10 % рекламного бюджету компаній. Але є всі підстави вважати, що ця частка різко збільшиться. Згідно з прогнозом BIA/Kelsey у 2017 р. рекламний ринок у соціальних мережах досягне 11 млрд дол. (минулого року він становив 4,7 млрд дол.).

Експерти також наголосили, що широке використання мобільних засобів є потужним двигуном зростання рекламного ринку. За оцінками частка реклами, призначеної для мобільних засобів, у 2017 р. становитиме 2,2 млрд дол., або 20 %. Скоріше за все, частка буде набагато вищою.

Уже сьогодні більше 50 % користувачів Facebook і Twitter відкривають свої сторінки за допомогою мобільних пристроїв. Реклама на мобільних пристроях у першій половині 2012 р. становила 11 % від усіх доходів Facebook.

У IV кварталі минулого року ця частка досягла вже 23 %. Причому у Twitter прибуток від реклами на мобільних пристроях перевищив отриманий рекламний прибуток на настільних комп'ютерах ***(Податкові ігри: одна з популярних російських соцмереж двічі за місяць змінила власника // Корреспондент.net (http://ua.korrespondent.net/business/mmedia_and_adv/1562264-analitiki-prorokuyut-ekspansiyu-reklami-v-socmerezhi-yaki-volodiyut-kolosalnim-obsyagom-danih-pro-kori). – 2013. – 23.05).***

***

Авторы вирусного видео зарабатывают на юзерах от сотни до миллионов долларов.

За миллион просмотров на YouTube можно заработать более 5 тыс. дол.

Южнокорейскому исполнителю PSY удалось удивить и заразить своим Gangnam Style едва ли не всю планету.

Кореец в очках заставил мир повторять его неприхотливые движения, а сенсационный клип на Gangnam Style посмотрел едва ли не каждый 7-й житель планеты.

Такая интернет-истерия и называется вирусным видео. Включается сарафанное радио: от одного пользователя к другому видео гуляет по всемирной сети, говорится в сюжете программы «Гроші».

«Если ты потратил немного денег и создал качественный продукт, то у тебя есть большие шансы, что о нем и дальше безвозмездно расскажет очень много людей», – комментирует интернет-маркетолог.

По его словам, за миллион просмотров видео можно заработать около 5–6 тыс. дол.

Проведя собственный эксперимент, журналистам «Грошей» удалось заработать 5 тыс. дол. за одно только видео, выложенное на YouTube.

В рамках эксперимента было создано очередной кавер на Gangnam Style. В ролике авторы соединили собственно рекордный клип и трек Gangnam Style с песней украинской группы ТиК «Сірожене Пірожене».

На раскрутку видео было потрачено всего лишь 400 грн. За них было приобретено 10 тыс. просмотров. Дальше дело стало только за рекламодателем. Именно он и предложил 5 тыс. дол. за размещение рекламы на видео журналистов.

Как известно, крупнейшие видеопорталы, такие как YouTube, стали платить пользователям и владельцам видеоблогов за количество просмотров ***(Авторы вирусного видео зарабатывают на юзерах от сотни до миллионов долларов // ru.tsn.ua (http://internetua.com/avtori-virusnogo-video-zarabativauat-na-uazerah-ot-sotni-do-millionov-dollarov). – 2013. – 22.05).***

***

Сайт Twitter представил в четверг 23 мая новый рекламный сервис, позволяющий показывать в твитах телезрителям ту же рекламу, которую они только что видели в эфире. Об этом сообщает The Wall Street Journal.

Новый сервис работает по следующему принципу: Twitter в режиме реального времени отслеживает по записям пользователей, какие телепрограммы они смотрят, и соотносит это с данными о рекламе, которая в этот момент идет в эфире телеканалов. После этого пользователям, которые твитят о программе, покажут ту же рекламу, которую они только что видели в эфире. Сервис разработан совместно с компанией Bluefin Labs, которая занимается анализом влияния телевидения на социальные сети.

Проект рассчитан в первую очередь на сотрудничество с рекламодателями, однако телекомпании также могут получить свою часть прибыли, если они присоединятся к другой рекламной программе соцсети – Twitter Amplify. Этот сервис был также официально представлен 23 мая, однако в качестве проекта он анонсировался и ранее. Twitter Amplify предполагает сотрудничество с телеканалами: телекомпании зарабатывают на видеорекламе, которая включается перед показом роликов, публикуемых в их Twitter-аккаунте; Twitter зарабатывает, когда рекламодатели платят за продвижение этих твитов с видео. Совместно с официальной презентацией проекта Twitter также представил новых партнеров: помимо телекомпаний ESPN, BBC America и Fox к Twitter Amplify присоединились Bloomberg TV, Discovery, а также издательские дома Conde Nast и Time Inc.

Сервис микроблогов Twitter был запущен в 2006 г. В настоящее время в социальной сети зарегистрировано более 500 млн пользователей. В последнее время компания проявляла активный интерес к сотрудничеству в телевизионной сфере. В феврале 2013 г. Twitter купил компанию Bluefin Labs, чтобы анализировать какие телешоу и какую телерекламу обсуждают пользователи социальных сетей. Еще ранее сервис микроблогов объявил о сотрудничестве с компанией Nielsen, подсчитывающей телевизионные рейтинги ***(Телевизионная реклама догонит зрителей в Twitter // InternetUA (http://internetua.com/televizionnaya-reklama-dogonit-zritelei-v-Twitter). – 2013. – 26.05).***

***

Европейские операторы откладывают запуск HTC First – первого смартфона со встроенной программной оболочкой Facebook Home – по просьбе самой соцсети, которая хочет доработать приложение в соответствии с откликами пользователей, пишет The Wall Street Journal.

Смартфон HTC First с предустановленным ПО Facebook Home вышел на рынок США 12 апреля. Его стоимость без контракта оператора составляет около 450 дол. Изначально стоимость устройства двухгодичным контрактом AT&T составляла 100 дол., однако недавно оператор снизил цену до 0,99 дол.

Как сообщили изданию представители Facebook, руководство соцсети обращалось к операторам связи Orange и EE в Великобритании и Франции с просьбой «придержать» запуск смартфона HTC First для доработки программной оболочки. Кроме того, Facebook намерена временно ограничить поддержку Home на новых устройствах. По словам представителей EE и Orange, они прислушались к рекомендации Facebook и изменили планы по выпуску устройства на рынок. Представители HTC от комментариев отказались.

«Мы выслушали отклики наших пользователей о Home. Хотя многим программа нравится, мы получили отличные рекомендации, как сделать Home существенно лучше. В результате в ближайшие несколько месяцев мы сфокусируемся на том, чтобы добавить функции кастомизации», – говорится в заявлении Facebook. Сроки выхода HTC First на европейский рынок не уточняются.

Приложением Facebook Home могут воспользоваться владельцы и других Android-смартфонов – HTC One, One X и One X+, Samsung Galaxy S III, Galaxy Note II и Galaxy S4, в том числе, в России. По данным магазина Google Play, число загрузок Facebook Home превысило 1 млн за первый месяц. В то же время пользователи выставили приложению среднюю оценку лишь 2,3 из 5 баллов ***(Европейские операторы откладывают запуск смартфона HTC с Facebook Home // InternetUA (http://internetua.com/evropeiskie-operatori-otkladivauat-zapusk-smartfona-HTC-s-Facebook-Home). – 2013. – 25.05).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Лидером по пропаганде суицида в Интернете является социальная сеть «ВКонтакте». Об этом свидетельствуют результаты исследования компании «Интегрум», которая занимается мониторингом социальных медиа, передает Обозреватель (http://obozrevatel.com/technology/84702-vkontakte-obyavlen-liderom-po-propagande-suitsida.htm).

«По количеству сообщений (публикации пользователей в открытом доступе) о самоубийстве лидирует социальная сеть «ВКонтакте», на втором месте Twitter, на третьем месте YouTube. Меньше всего данная тема освещается в блогосфере: Livejournal, BlogSpot, Mail.ru и др.», – отмечено в пресс-релизе компании.

Так, по ее данным, на долю этой соцсети приходится 66 % сообщений о самоубийствах, в то время как доли Twitter и YouTube составляют 18 % и 7 % соответственно.

Также компания насчитала во «ВКонтакте» 1340 посвященных суициду сообществ ***(«ВКонтакте» объявлен лидером по пропаганде суицида //***

Обозреватель (http://obozrevatel.com/technology/84702-vkontakte-obyavlen-liderom-po-propagande-suitsida.htm). – 2013. – 7.05).

***

Социальные сети названы главной причиной транзиторного психоза и галлюцинаций.

Исследователи из Тель-Авивского университета связали психотические эпизоды (транзиторный психоз) и галлюцинации с зависимостью от Интернета, в частности от виртуальных отношений, которые культивируются на сайтах социальных сетей. Об этом сообщает raut.ru.

Транзиторный психоз представляет собой скоротечный психоз, представляющий собой приступ психической болезни. Все участники исследования испытывали проблемы одиночества, решение которых они искали в социальных сетях, находя утешение в интенсивных виртуальных отношениях.

И хотя на первый взгляд эти отношения казались положительными, они в конечном счете привели к чувству обиды, ощущению предательства и вторжению в частную жизнь. В каждом случае была обнаружена связь между постепенным развитием и обострением психотических симптомов, в которые включены бред, беспокойство, спутанность сознания и интенсивное использование компьютерных коммуникаций.

Хорошей новостью является тот факт, что все пациенты при правильном лечении и уходе восстанавливались и выходили из этого опасного состояния. К некоторым проблемным особенностям Интернета относятся вопросы географических и пространственных искажений, отсутствие невербальных сигналов, а также тенденция идеализировать своего визави, не встречаясь с ним при этом в реальной жизни ***(Социальные сети названы главной причиной транзиторного психоза и галлюцинаций // IT Expert (http://itexpert.in.ua/rubrikator/item/25976-sotsialnye-seti-nazvany-glavnoj-prichinoj-tranzitornogo-psikhoza-i-gallyutsinatsij.html). – 2013. – 7.05).***

***

Американские учёные опросили более 2 тыс. работников о их текущей работе и привычке заходить на свой аккаунт в социальной сети. Как выяснилось, те из опрошенных, у кого было много друзей в Facebook, намного хуже относятся к своей работе, чем люди с небольшим количеством друзей.

К тому же работники, которые часто обновляют свой «статус», чаще задумывались об увольнении. Учёные объясняют это тем, что из-за частого посещения страничек друзей в Facebook, человек начинает думать, что другие живут лучше и чувствуют себя счастливее.

Так как большинство пользователей социальных сетей хотят выкладывать о себе только такую информацию, которая показывает их в лучшем свете. «Но, мы не можем исключить, что людям просто становится скушно время от времени, и они отдыхают от работы, заходя в Facebook», – комментирует автор

исследования Р. Хаммонд ***(Как Facebook вредит Вашей работе // InternetUA (http://internetua.com/kak-Facebook-vredit-vashei-rabote). – 2013. – 2.05).***

Маніпулятивні технології

Twitter-аккаунты знаменитостей заполонили «мертвые души»

Итальянские исследователи А. Стропа и К. де Мишели работают над изучением различных махинаций с Twitter уже довольно долго. Они провели кропотливую работу, подсчитав примерное количество фальшивых фолловеров на рынке, их стоимость, а также совокупный объем рынка. Как оказалось, в мире существует около 20 млн поддельных «твиттерян», которые приносят своим создателям, по разным оценкам, от 30 до 360 млн дол. в год, пишет The New York Times.

В новом исследовании пристальное внимание было уделено аккаунтам, которые внезапно получили или потеряли сразу большое количество фолловеров в один день. Оказалось, что столь резкие колебания в количестве читателей происходили с аккаунтами таких крупных брендов, как Pepsi, Mercedes Benz и Louis Vuitton.

Более того, подозрительные колебания в количестве подписчиков, указывающие на приобретение фальшивых фолловеров, было замечено в аккаунтах некоторых политиков и звезд шоу-бизнеса. По утверждению А. Стропа и К. де Мишели, поддельных читателей привлекали в Twitter-аккаунты американского политика Н. Гингрича, конгрессмена Д. Полиса и реперов 50 Cent и P Diddy.

Эксперты по соцсетям отмечают, что фальшивые читатели неплохо помогают брендам продвигать себя в Интернете. Чем больше у бренда или персоны «фолловеров», тем привлекательнее они выглядят для других потенциальных читателей – мол, другие читают, и вам будет интересно. Кроме того, фальшивые фолловеры помогают получить живых читателей, которые будут переходить по ссылкам. Таким образом, можно получить много дополнительного траффика на сайт и поднять его в выдаче посиковиков на более заметные позиции.

С. Этлингер, аналитик в Altimer Group, постаралась объяснить, зачем бренды и медиа-персоны докупают себе читателей-ботов. «Многие бренды пытаются любой ценой увеличивать количество читателей в социальных медиа. Компании пытаются показать импульс своего развития, чтобы каждый следующий день аудитория была больше, чем вчера», – отметила она в интервью New York Times.

Несмотря на всеобщее стремление накрутить количество читающих официальные аккаунты людей, эффективность продвижения в соцсетях до сих пор под вопросом. К примеру, недавно Coca-Cola – бренд, имеющий 700 тыс. читателей в Twitter и 60 млн на Facebook – опубликовал исследование, в котором утверждается, что онлайн-продвижение не влияет на продажи, по крайней мере в краткосрочной перспективе.

Исследователи особо отметили, что ни один аккаунт в Twitter не может получить за день более 70 тыс. читателей честными способами. «Пики активности читателей, которые мы наблюдаем в отмеченных нами аккаунтах, недостижимы методами рекламных кампаний, вот почему все уверения в неверности наших выводов не убеждают нас», – отметил К. де Мишели.

В настоящее время существует около двух десятков онлайн-сервисов, продающих фальшивых фолловеров. Их популярность продолжает стремительно расти. «Всегда будут люди, которые пытаются обойти систему, однако следует учитывать, что Twitter и Facebook в последнее время очень хорошо борются с поддельными читателям. Вот почему любая накрутка читателей будет временной», – отметила С. Этлингер ***(Twitter-аккаунты знаменитостей заполонили «мертвые души» // InternetUA (http://internetua.com/Twitter-akkaunti-znamenitostei-zapolonili--mertvie-dushi). – 2013. – 2.05).***

***

Группа «Детская мода» появилась в социальных сетях несколько месяцев назад. За относительно небольшой период на это сообщество «ВКонтакте» успели подписаться почти 2,5 тыс. человек. Большинство из посетителей – жители стран СНГ. Приглашение вступить в ряды любителей «Детской моды» пришло и киевлянке М. Колпак. У девушки подрастает пятилетняя дочь, и она решила принять предложение.

«Подтвердила свое участие в группе, а потом зашла на их страничку. Ожидала увидеть новинки детской одежды на теплый сезон, а вместо этого обнаружила откровенные фотографии девочек. На них практически не было одежды, некоторые стояли в извращенных позах. В общем, ничего, что могло бы касаться детей и моды», – рассказала М. Колпак.

М. Колпак утверждает, что сразу же написала администрации сообщества – попросила немедленно убрать порно-изображения несовершеннолетних и вернуть группе статус развлекательной.

«Мне ответили, что я больная на голову, что группа не пропагандирует извращения, а все комментарии, оставленные под фото с полуголыми школьницами, – это проделки недоброжелателей активного сообщества», – сообщила Колпак.

«Обозреватель» также зашел на страницу «Детской моды» в соцсети «ВКонтакте». В сообществе выложены несколько сотен фотографий полуобнаженных девочек. По словам администрации, школьницы всего лишь рекламируют одежду. Но никакой информации о ценах, размерах или моделях нижнего белья в группе указано не было.

Автором одного из последних «фотосетов» является москвич А. Новиков. Парню 24 года, и он считает нормальным фотографировать полуобнаженных детей. Особенно – у себя дома, да еще и на кровати. Вот изображение, которое, по мнению Новикова, не является извращением:

«Девочка меряет папину рубашку, пока он на работе. Я заметил, что дети часто так делают, когда скучают по родителям», – объяснил идею снимка А. Новиков.

Под серией интимных детских фотографий из группы «Детская мода» вспыхнула дискуссия. Одни, как и киевлянка М. Колпак, просят немедленно закрыть сообщество и пишут жалобы администрации социальной сети.

Другие, как, например, 25-летний житель Бердянска Р. Комейко, считают, что грань морали в группе никто не переступает. Одежду здесь, по мнению Р. Комейко, пусть и не продают, зато от увиденного можно получить эстетическое удовольствие.

«Подобные фотографии – это всего лишь фотографии. Они несут эротический характер для тех, кто хочет видеть в них эротику», – прокомментировал изображения полуголых девочек Р. Комейко.

«Удочерю девочку, со мной ей будет лучше», – дядя-педофил

Обсуждения в стиле «морально-аморально» в группе встречаются под каждой из выложенных фотографий. Но открыто обсуждать свои наклонности внутри сообщества рискуют далеко не все. Мужчины разного возраста приглашают перейти из группы на их личные странички «ВКонтакте» и там уже делятся опытом секса с детьми.

Одним из самых активных участников группы является Б. Блумберг. Житель Кракова активно призывает к общению единомышленников, а на своей открытой странице «ВКонтакте» выкладывает фото понравившихся ему девочек.

Некоторых из детей Б. Блумберг называет «своими». Девочка на изображении сверху, исходя из информации со страницы Блумберга, любит его, но… уже надоела. Теперь Б. Блумберга не интересуют кратковременные связи – мужчина опубликовал пост, где речь идет о его неистовом желании удочерить сироту.

По словам Б. Блумберга, в его доме несовершеннолетней девочке «будет в любом случае лучше, чем в детдоме».

Преступление и наказание

В соседних для Украины России и Молдове борются с доказанными педофилами так, как это принято делать во многих цивилизованных странах мира (США, Канада, Польша, Швеция, Дания) – методом принудительной химической кастрации.

В Молдове такой закон вступил в силу 1 июля 2012 г. Автор проекта, депутат от Либеральной партии Молдовы В. Мунтян заявил, что необходимость создания подобного правила появилась, когда статистическое количество педофилов в их стране возросло почти вдвое.

Освободившись после отбытия наказания, педофилы снова и снова совершают такие преступления. За последние пять лет 15 таких правонарушителей были повторно привлечены к уголовной ответственности за педофилию», – сказал В. Мунтян, выступая в парламенте.

В феврале 2012 г. подобный закон вступил в силу и в России. Документ был подписан тогдашним президентом Д. Медведевым после того, как положение о принудительной химической кастрации педофилов приняла Государственная Дума. В России также решили усилить наказание для педофилов-рецидивистов – вплоть до пожизненного заключения. Химическую кастрацию закон в России позволяет проводить только после тщательной медицинской и психиатрической проверки осужденного за педофилию.

Не отставать от своих «соседок» решила и Украина. Правда, подошла к вопросу несколько иначе. Осенью 2011 г. уже экс-депутат от Партии регионов В. Сивкович выдвигал законопроект о принудительной химической кастрации педофилов, но из положенных 226 голосов за закон проголосовали только 205 народных избранников.

А в феврале 2012 г. в ВР поддержали законопроект по усилению ответственности за преступления против половой свободы и половой неприкосновенности, предложенный народными депутатами от ВО «Батьківщина» Н. Катеринчуком и С. Терехиным. С тех пор, благодаря изменениям, внесенным в Уголовный кодекс Украины, за изнасилование малолетних предусматривается наказание в виде пожизненного лишения свободы.

Психологи, в свою очередь, отмечают, что педофилия занимает первое место по распространенности среди половых отклонений, и в то же время является самым тяжелым из них.

Проблема онлайн педофилии особенно распространена в странах СНГ. По украинскому законодательству доказать, как и просто зафиксировать извращения по отношению к детям, – практически невозможно. А детская психика страдает, как от виртуального, так и от реального сексуального развращения, оставляя жертв педофилов инвалидами на всю жизнь ***(Онлайн педофилия // From-UA.Новости Украины (http://www.from-ua.com/crime/e662e2d324cc7.html). – 2013. – 17.05).***

***

В социальных сетях предлагают поучаствовать в митингах оппозиции 18 мая за 100 грн. Об этом свидетельствуют записи пользователей социальных сетей «ВКонтакте» и Facebook, в которых предлагается 18 мая возможность за 4–5 часов работы в массовке в ходе оппозиционной акции «Вставай, Украина» получить 75–100 грн.

«18.05, 11:30, метро «Университет», оплата 25 грн/час, стоим 4 ч., итого – 100 грн. Дополнительно платим: держать флаг + 25 грн, каждый человек от вас 30 грн. Внимание, много кидал! Стоим за БЮТ! Кидков не будет!», – говориться в записи одного из пользователей сети «ВКонтакте». Кроме метро «Университет», согласно записям, сбор массовки будет производиться возле метро «Золотые ворота», метро «Арсенальная», возле «Европейской площади», а также Арки Дружбы Народов.

Другие пользователи предлагают похожие условия. Кроме того, организаторам, собравшим от 20 участников митинга предлагается бонус – 40 грн за каждого человека… ***(В соцсетях предлагают поучаствовать в митингах оппозиции за 100 грн // Эксперт-центр (http://expert.org.ua/statias/?st=2&id=106742). – 2013. – 17.05).***

***

У соцмережах активно публікуються оголошення з пропозицією на платній основі взяти участь в політичних мітингах, які відбудуться в Києві в суботу, 18 травня.

Так, за адресою http://vk.com/rabota_kievv можна знайти відразу два оголошення з пропозицією «просто стояти та дивитися концерт». Користувач Роман Вікторович пропонує за участь у п'ятигодинній акції (з 10:00 до 15:00) оплату 15 грн за годину + 5 грн за кожну приведену людину. При цьому збір «масовки» призначено на 8:30 на оглядовому майданчику під Маріїнським Палацом.

Кореспондент НБН зателефонував за вказаним в оголошенні номером телефону і з'ясував, що «концерт» організовують від Партії регіонів, яка в суботу, як відомо, має намір провести «антифашистський» мітинг.

Таким чином, за «просто подивитися» можна заробити всього 75 грн (якщо нікого не вдасться залучити до заходу). Крім того, Роман Вікторович запевнив, що жодних заворушень не очікується, «все буде спокійно».

Трохи нижче за тим самим посиланням користувач М. Щербак пропонує вигідніші за іншого користувача умови: 110 грн за п'ять годин. Як з'ясувалося, він також збирає масовку для Партії регіонів: «Мітинг відбудеться на "Арсенальній". Так, проводять антифашисти», – сказав пан М. Щербак.

Збирається цей мітинг на станції метро «Арсенальна» також о 08:30.

Водночас за посиланням http://vk.com/vremennaya_rabota_kiev можна знайти ще кілька оголошень. За одним із вказаних у них номером телефону деякий Олексій розповів, що «треба просто постояти, нікуди ходити не треба, максимум що попросять, помахати реквізитом». Збір на цей захід також призначено на 8:30 на вул. Інститутська біля входу до станції метро «Хрещатик». Однак на всі спроби з'ясувати, хто саме проводить цей мітинг, пан Олексій відповідав стандартно: «Концерт відбудеться завтра в Маріїнському парку з 10 до 15. Усе без обману, гроші протягом півгодини».

Згідно з оголошенням, за концерт в Маріїнському парку можна заробити «100 грн за п'ять годин + 5 грн за кожну приведену людину».

Як повідомляв НБН, в суботу, 18 травня, опозиція проведе фінальний мітинг у рамках всеукраїнської акції «Вставай, Україно!». Захід розпочнеться на Європейській площі о 12:00, потім колона рушить по вул. Михайлівській на Софіївську площу.

Водночас Партія регіонів також має намір в суботу зібрати людей в центрі Києва. У рамках акції «До Європи – без фашизму» провладна партія проведе антифашистський мітинг, який розпочнеться о 13:00 на Європейській площі.

Мітингу передуватиме марш від музею пам'яті ВВВ через Арсенальну площу на Європейську площу ***(Соцмережі рясніють оголошеннями про платні мітинги в Києві у суботу // Незалежне Бюро Новин (http://nbnews.com.ua/ua/news/88296/). – 2013. – 17.05).***

***

Майские праздники традиционно открывают сезон «уличной» политики. Использованием проплаченной массовки на разного рода митингах уже давно никого не удивишь. В свете недавних киевских событий, интересно было бы узнать как происходит рекрутизация «протестующих», и насколько готовы украинцы зарабатывать на проплаченных митингах.

Многим киевлянам (в их числе, и журналисту нашей редакции), начиная с 15 мая, засыпали почту подобными сообщениями.

Как все уже наверное догадались, речь идет о любви к Родине за деньги. Нас заинтересовал способ вербовки «патриотов», а также вопрос – собираются ли наши сограждане участвовать в акциях протеста и согласны ли делать это бесплатно?

Чтобы ответить на эти вопросы, интернет-портал Bigmir и исследовательская компания Opinion провели онлайн-исследование среди интернет-пользователей в возрасте 18–45 лет. Исследование проводилось 26–30 апреля 2013 г. методом онлайн-интервью на репрезентативной access-панели Opinion. Выборка исследования составила 400 респондентов (максимальная теоретическая погрешность выборки составляет 5 %). Данные исследования репрезентируют мнение всех интернет-пользователей Украины на всей территории, включая городское и сельское население. Уровень проникновения Интернета для аудитории 18–45 лет составляет 74 %.

Согласно полученным данным, 45 % пользователей не готовы участвовать в политических акциях протеста, 40 % приняли бы участие в акции, если её цели совпадают с позицией респондента и только 15 % готовы принимать участие в акциях на платной основе.

Любопытно, что когда встал вопрос о сумме вознаграждения, доля респондентов, не собирающихся участвовать в акциях протеста, уменьшилась с 45 % до 27 %. Из них 13 % принципиально не станут участвовать в акциях за деньги, 14 % откажутся от участия в политических акциях при любых условиях.

Таким образом, 65 % респондентов смогли определить сумму, за которую они бы согласились присоединиться к любой акции протеста. Респонденты могли назвать любой размер вознаграждения, вопрос формулировался как открытый. Таким образом, вопрос о сумме вознаграждения смог изменить изначальные установки не участвовать в политических акциях либо же не участвовать в них за деньги.

Среди потенциальных участников протестных акций преобладают мужчины. Так, свою готовность участвовать в акциях в целом подтвердило 65 % мужчин и только 45 % женщин. Статистически значимо больше мужчин

готовы участвовать в акциях как из-за своих убеждений, так и за вознаграждение.

Региональных отличий в намерениях опрошенных выявлено не было, за единым исключением: представители Западного региона значимо меньше готовы участвовать в акциях протеста за деньги и значимо выше в акциях, отражающих их личную позицию.

Существенно влияет на намерения возраст потенциальных участников политических акций. Так, среди молодых людей 18–25 лет ожидания по размеру вознаграждения значительно ниже, а среди аудитории 26–35 лет значительно выше доля тех, кто потребует максимального вознаграждения за свое вовлечение (1000 грн и более).

Как отмечает И. Дубинский, директор компании Opinion, «когда мы говорим о репрезентативных исследованиях интернет-аудитории, важно понимать, что речь идет, как правило, о несколько более мобильной, активной и обеспеченной части населения, в сравнении с непользователями Интернета. Вместе с тем, когда уровень проникновения Интернета достигает 50–60 % и выше (для исследуемой аудитории жителей Украины в возрасте 18–45 лет он составляет сегодня 74 %), результаты исследования могут быть экстраполированы на всю аудиторию жителей страны. Иными словами, исследование отражает позицию украинцев в целом по отношению к участию в политических акциях. С тем лишь предположением, что у неинтернетизированной части населения в этом возрасте намерение участвовать в подобных акциях, возможно, не ниже, а ожидаемый размер вознаграждения за участие предположительно меньший» ***(Как вербуют «демонстрантов» через сеть // InternetUA (http://internetua.com/kak-verbuuat--demonstrantov--cserez-set). – 2013. – 22.05).***

***

Когда нация становится жертвой: Концептуальные основы информационно-сетевых войн.

Начало XXI в. охарактеризовалось появлением нового вида войн, при которых победа достигается не за счет уничтожения вооруженных сил и экономики противника, а посредством воздействия на его морально-психическое состояние.

Если придерживаться классификации войн с точки зрения смены общественных формаций и используемых технологий, в настоящее время мы вступили в эпоху войн седьмого поколения – информационно-сетевых, которые явились следствием следующих факторов: развития средств вычислительной техники и коммуникаций, что привело к возрастанию роли информации в жизни общества, по эффективности своего влияния превзошедшей многие материальные виды ресурсов; успехов психологии в области изучения поведения людей и управления их мотивациями, позволившими оказывать заданное воздействие на большие группы людей; разработки нелетальных средств воздействия, заменивших традиционные виды оружия.

Скрытая, но эффективная угроза

Традиционная война против государства, обладающего ядерным оружием, в наше время чрезвычайно опасна. Современные политтехнологи, обслуживающие интересы правящих верхушек стран Запада, стремятся перевести агрессию из материального пространства в информационное. В первую очередь осуществляется переориентация или уничтожение традиционных ценностей народа, чтобы информационная атака извне воспринималась данным обществом как соответствующая его стремлению к прогрессу. Внешняя агрессия в массовом сознании приобретает вид цивилизационной трансформации отсталого общества другим, стоящим на более высокой ступени развития.

Технологии сетевых войн были хорошо отработаны уже в годы холодной войны как формы тотального разрушения геополитического противника. Информационно-сетевая война заключается в подрыве с последующим разрушением базовых характеристик нации, осуществляемом преимущественно в скрытой форме. В зависимости от конкретных задач воздействия на противника та или иная область его общественной жизни может становиться приоритетным объектом агрессии.

Целью информационно-сетевой войны является закрепление большей части стратегически важных ресурсов страны за геополитическим агрессором. При этом «передача» этих ресурсов агрессору осуществляется элитой страны-жертвы в значительной степени добровольно, поскольку воспринимается ею не как захват, а как путь к развитию. Это порождает сложность в распознавании технологии и методов информационно-сетевой войны по сравнению с традиционной, а также отсутствие своевременной реакции на действия агрессора, так как у жертвы не оказывается никаких мер противодействия им. При этом если результаты «горячих» войн со временем оспариваются и пересматриваются (примерами тому являются Первая и Вторая мировые войны), то результаты информационно-сетевой войны пересмотру не подлежат до тех пор, покуда ее авторы-агрессоры не утратят своих позиций.

Признаки нападения

Каким образом будут утрачены эти позиции, в настоящее время неясно. Сложность вопроса состоит в том, что фронт информационно-сетевой войны располагается в ментальном пространстве человеческого общества, в котором уже произошло замещение базовых ценностей нации-жертвы на психологические установки и мифы агрессора. Массовое сознание неспособно своевременно распознать факт имплантации ментальных вирусов. А политическая и культурная элиты, ставшие объектом информационно-сетевой войны, не имея достаточной квалификации для выявления информационной агрессии и организации адекватного отпора сетевому врагу, обречены на сокрушительное геополитическое поражение.

Фактически к информационно-сетевой войне подключаются практически все общественные институты, в первую очередь СМИ и религиозные организации, учреждения культуры, неправительственные организации,

общественные движения, финансируемые из-за рубежа. Даже деятели науки, работающие по зарубежным грантам, вносят свой вклад в разрушение государства. Все они осуществляют так называемую распределенную атаку, нанося многочисленные точечные разрушающие удары по общественной системе страны под лозунгами развития демократии и соблюдения прав человека. Благодаря современным политтехнологиям и накопленному опыту воздействия на массовое сознание геноцид населения можно осуществлять без применения газовых камер и массовых расстрелов. Достаточно создать условия для сокращения рождаемости и увеличения смертности.

Другой особенностью информационно-сетевых войн является отсутствие жесткой иерархии в сетевой структуре агрессора. Это объясняется ее гетерогенностью, выражающейся в значительной автономности государственных и негосударственных элементов данной структуры, где нет ярко выраженных вертикальных связей. Зато имеются многочисленные горизонтальные, действие которых нерегулярно. Отсутствие иерархии и регулярности взаимодействия не позволяет четко выявить существование и деятельность такой сетевой структуры.

Движущие силы

Источником энергии для рассматриваемых сетевых структур, можно сказать «горючим», является информация, которая в них циркулирует, а своеобразными «запалами» – хозяева узловых точек. Примером тому служат серверы социальных сетей Facebook и Twitter, находящиеся под контролем американских спецслужб.

Как сообщила британская The Guardian, в США уже осуществляется пропагандистская работа с использованием Twitter, Facebook и других социальных сетей. Центром управления данной программой является база ВВС США «Макдилл» в штате Флорида, где задействованы 50 операторов, каждый из которых контролирует примерно десять «агентов влияния», зарегистрированных в различных странах мира и ведущих информационную войну по всем правилам политических технологий разрушения государств. Стоимость данной программы, по оценке британской газеты, оценивается в 2,76 млн дол., предусматривая для каждого из таких бойцов информационной войны наличие убедительной легенды и мер защиты от разоблачения. По словам пресс-секретаря Центрального командования вооруженных сил США Б. Спикса, любое воздействие на американскую аудиторию запрещено правилами, для чего исключается использование английского языка. Информация в системе представлена только на арабском, урду, пушту, фарси и некоторых других языках в зависимости от целевых стран.

Выявление и квалификация актов информационной войны являются задачей спецслужб каждого государства, заботящегося о своей безопасности. Это тем более важно, что вследствие непроявленного характера информационной агрессии она не воспринимается обществом в качестве непосредственной угрозы существованию государства. Экспертное сообщество

и спецслужбы должны проявить эти угрозы, объяснив их руководству страны для принятия соответствующих мер.

Сферы и методы

Борьба ведется в следующих пространствах: географическом – за установление контроля над территорией посредством глобальных (в том числе и космических) информационных и разведывательных систем, поощряются сепаратистские движения и террористическая активность в различных формах на территории противника, происходит вовлечение врага в конфликты малой интенсивности, а также организация народных волнений и «цветных революций»; экономическом – посредством навязывания противнику кабальных кредитов, введения эмбарго, организации экономических санкций и провокаций; идеологическом – путем клеветы, искажения информации, подмены понятий, внесения ментальных вирусов и мифологем в сознание населения противника; сетевом – за счет хакерских атак и внедрения компьютерных вирусов в вычислительные и коммуникационные системы и базы данных.

Какова бы ни была конечная цель информационно-сетевой войны, ближайшей задачей всегда является затруднение доступа населения к достоверной информации. Важность этого объясняется тем, что оперативность и качество принимаемых решений на всех уровнях непосредственно зависят от полноты и достоверности представляемой информации.

Основные методы информационного противоборства.

1. Скрывание критически важной информации о положении дел в данной области.

2. Погружение ценной информации в массив так называемого информационного мусора в соответствии с принципом «спрятать лист в лесу».

3. Подмена понятий или искажение их смысла.

4. Отвлечение внимания на малозначимые события.

5. Применение понятий, которые на слуху у публики, но не имеют не только определения, но и значимости.

6. Подача негативной информации, которая лучше воспринимается аудиторией, чем позитивная.

7. Ссылка на факторы, лишенные реального смысла, а также на некорректно проведенные социологические и маркетинговые исследования.

8. Введение табу на определенные виды информации, несмотря на их общеизвестность. Делается это, чтобы избежать широкого обсуждения критичных для определенных структур вопросов и тем.

9. Откровенная ложь с целью недопущения негативной реакции населения и зарубежной общественности.

10. В арсенале информационных войн есть такие средства, как «информационная бомба» и «информационная мина». Первая служит детонатором лавинообразного нарастания процесса в обществе, в то время как вторая закладывается заранее и срабатывает в ходе начавшегося процесса для доведения его до логического завершения. «Информационными минами» стали

утечки из официальных органов государства или из таких сайтов, как «Викиликс».

Типичным примером применения технологии информационно-сетевой войны являются восстания народных масс в странах Ближнего Востока. Если в случае Туниса и Египта эти технологии не были достаточно проявлены, то в Ливии состоялся «генеральный прогон» войн седьмого поколения. Ливийская «революция» предстала на экранах мировых СМИ как некий симулятор, отфотошопленная «копия без оригинала», ход которой был подан глобальными массмедиа без всякого соотнесения с действительностью, зато в точном соответствии со сценарием, написанным западными политтехнологами.

Спровоцированные на «революционные» выступления информационными атаками из социальных сетей Facebook и Twitter, арабские общества вызвали революционную волну на Ближнем Востоке. Взрыв на арабской улице показал, что социальные сети стали «запалом» для неспокойной атмосферы Ближнего Востока. Практически во всех странах, вовлеченных в этот водоворот событий, протестный «флешмоб» был организован посредством рассылки сообщений о намечающихся митингах и протестных акциях через социальные сети, электронную почту и мобильные телефоны. При этом следует помнить, что управляющие серверы глобальных электронных сетей Facebook, Twitter, Hotmail, Yahoo и Gmail находятся в США и контролируются американскими спецслужбами. Это позволяет организовать рассылку сообщений заранее подобранной «клиентуре» – своим агентам влияния в странах Арабского Востока, которые по сигналу извне собирают в нужное время в нужном месте критическую массу людей, используя для этого так называемое сарафанное радио.

Люди арабской улицы, в большинстве своем ничего не знающие об Интернете, социальных сетях, а зачастую и не имеющие компьютеров и мобильных телефонов, готовы бить витрины, жечь автомашины и бросать камни в полицию, потому что почувствовали возможность расквитаться с властью предержащей за бедность, на которую их обрекли правящие режимы. Службы безопасности подвергшихся информационному вторжению государств оказались бессильны противостоять насилию в новой для них форме организации протестного движения, которое сразу же приобрело лавинообразный, неуправляемый характер. Оказалось, что невозможно было предвидеть начало уличных беспорядков, как и источники рассылки подстрекательских сообщений, а отключение доступа в Интернет и мобильной связи после начала беспорядков уже ничего не решало, поскольку процесс приобрел характер лесного пожара.

Социальная опора

Современный мир взрывоопасно насыщен людьми с крайне негармонизированным внутренним миром. «Молодые люмпены», как их называют социологи, деклассированная масса с непроявленными социальными корнями, без четких нравственных понятий и политических ориентиров. Активность таких элементов в повседневной жизни простирается от обычной

коммерческой лихорадки до спекуляций на фондовом и валютном рынках. При нарастании революционной ситуации у них увеличивается антисистемный протестный заряд, развивающийся на фоне нереализованных амбиций.

Так было в случае самосожжения М. Буазизи – тунисского молодого человека с высшим образованием, вынужденного торговать овощами. Такие люди, находясь в постоянном поиске своего места в жизни, по существу становятся марионетками, попадая под влияние социальных сетей, настроений толпы или идеологии радикальных движений. И если у них отсутствует внутренний моральный стержень, то невозможно представить, какие мотивы возобладают в следующий момент.

Освещающие подобные события СМИ и информация в социальных сетях еще более накаляют обстановку массового психоза. Этому способствуют кадры, снятые камерами мобильных телефонов неизвестно кем и неизвестно где, сообщения о многочисленных жертвах, павших от рук правительственных сил, но не показанных «из гуманных соображений», репортажи из якобы захваченных повстанцами городов, беспорядочная стрельба из зенитных пулеметов для демонстрации обстановки боевых действий, обломки якобы сбитых самолетов правительственной авиации, бомбившей повстанцев, «переход» на сторону народа сына М. Каддафи, бегство ливийских дипломатов в США и Францию. Однако если внимательно присмотреться, видно, что в СМИ разыгрывается виртуальная война, смонтированная и отретушированная на компьютерах и вброшенная в виртуальное пространство в качестве информационной жвачки для обоснования санкций Совета Безопасности ООН.

Если Тунис и Египет были первыми пробами заокеанских режиссеров этого псевдореволюционного спектакля, то Ливия – первая реальная боевая операция мировой информационно-сетевой войны Запада против неугодных режимов. Если на Балканах, в Афганистане и Ираке Вашингтон использует все средства и методы глобального передела мира, имеющие целью смену лидеров в странах, которые представляют стратегический интерес для США, то в государствах Ближнего Востока Запад инициирует приведение к власти лидеров нового поколения, идущих на смену тем, кто получил образование в СССР, – технократов западной формации и западного менталитета, которые призваны упрочить позиции США при одновременном вытеснении из региона Большого Ближнего Востока Китая, ЕС и России. Это пример попытки реализации информационно-сетевой стратегии «управляемого хаоса», которая оказалась новым средством сохранения глобального американского лидерства с минимальными финансовыми затратами, если не считать расходы на выдвижение авианосцев к берегам Ливии и издержки мировой экономики от повышения цены на нефть.

В. Золотарев, генерал-майор, действительный государственный советник Российской Федерации 1-го класса, доктор исторических наук, профессор, vpk-news.ru ***(Когда нация становится жертвой: Концептуальные основы информационно-сетевых войн // Флот – 2017***

(http://flot2017.com/posts/new/kogda_nacija_stanovitsja_zhertvoj__konceptualnye_osnovy_informacionnosetevyh_vojn). – 2013. – 23.05).

***

Угроза «Twitter-революций» в России преувеличена

23 мая Фонд развития гражданского общество (ФоРГО) презентовал доклад, который анализирует зарубежный опыт и фильтрацию в Интернете, в том числе введение цензуры, прогнозируя регулирование рунета. Отвергая запретительный подход, авторы доклада тем не менее предлагают государству «мягкие» рычаги влияния на Интернет.

Основываясь на опросах социологических центров, ФоРГО делает вывод о том, что российское население «консервативно настроено по отношению к контенту, который размещается в сети, и считает желательным его регулирование со стороны государства». В основном это касается четырех основных категорий: материалы экстремистского содержания, направленные на разжигание национальной, религиозной и социальной розни; детская порнография; пропаганда употребления наркотиков; пропаганда суицида. Функционирование ограничивающего законодательства, а также действия контролирующих органов граждане считают недостаточным.

Вместе с корректировкой законодательства в докладе предлагается передать «функции ведения реестра запрещенных сайтов от непрофильных государственных ведомств негосударственной организации, обладающей достаточной экспертизой в подобных вопросах и поддержанной всеми значимыми участниками интернет-рынка». Отдельно предлагается доработать закон «О противодействии экстремизму», который «не работает» в Интернете, в частности, «предусмотреть механизмы фильтрации контента, связанного с публичными призывами к насилию в Интернете без нарушения нормального функционирования социальных сервисов». Авторы доклада признают, что столь сложную задачу необходимо решать совместно с представителями интернет-отрасли. Роль социальных сетей и сервисов в событиях, получивших название «Twitter-революций», эксперты считают «во многом переоцененной», поскольку использовались узкой прослойкой протестующих и лишь оперативное выкладывание в сети фото- и видеоконтента, подхваченное традиционными СМИ, имело эффект бумеранга.

При этом наиболее близким к идеалу авторы доклада считают регулирование Интернета в Китае, но признают, что этот опыт в России вводить поздно, поскольку люди привыкли пользоваться иностранными ресурсами и жесткий запрет вызовет недовольство. Действующую модель регулирования Интернета в РФ эксперты ФоРГО называют «континентальной моделью», которая предполагает «четкое законодательное обозначение категорий фильтруемого контента: к ним могут относиться социально опасный контент и сайты, нарушающие авторские права, но не политические или правозащитные ресурсы. В докладе предлагается внедрять “мягкие формы господдержки, включая налоговые льготы”, для развития российских интернет-

компаний», чтобы не допустить доминирования международных неконтролируемых ресурсов. Как разъяснил «Ъ» один из ведущих экспертов доклада С. Апетьян, экстремистским высказывание может признать только суд, но это невозможно в случае, например, с соцсетями. По его мнению, надо закрепить внесудебный порядок, прежде всего, относительно призывов к насилию. Для этого законом надо обязать интернет-сервисы идти на взаимодействие с правоохранительными органами и применять меры реагирования к нарушителям. «Facebook уже сейчас удаляет подобные посты, но не все могут организовать качественную модерацию», – говорит господин С. Апетьян.

«Есть Уголовный кодекс, и если при помощи Интернета готовится или осуществляется преступление, такие люди и владельцы ресурсов должны быть наказаны, как и любые другие преступники. Больше ничего не надо. Другие попытк и отрегулировать Интернет государством – это попытки ввести цензуру, которая служила бы интересами власти, а не общества», – полагает лидер «Яблока» С. Митрохин. «Доклад показывает развилку: с одной стороны, есть желание государства усилить влияние на интернет-сообщество, с другой – интернет-сообщество быстрее, креативнее и обходит многие запреты. Вот, скажем, закрыли подпольные казино, почти что получилось. А в случае с футбольными фанатами, как их ни регулируй, пару-тройку файеров все равно пронесут. С Интернетом, скорее, ситуация пока как с фанатами», – говорит глава фонда «Петербургская политика» М. Виноградов ***(Угроза «Twitter-революций» в России преувеличена // sotovik.ru (http://internetua.com/ugroza--tvitter-revoluacii--v-rossii-preuvelicsena). – 2013. –24.05).***

***

В социальной сети «ВКонтакте» появились сразу несколько групп в поддержку В. Титушко (Румына) , которого подозревают в избиении журналистов во время митинга оппозиции 18 мая 2013 г.

В частности, в группу «Свободу спортсмену ВАДИМУ ТИТУШКО!» присоединилось почти полтысячи человек.

Новостей на тему заключения В. Титушко нет, однако стоит опрос о том, считать ли действия спортсмена преступлением. Интересно, что большинство тех, кто проголосовал, не считают В. Титушко виновным.

Кроме того, была создана заставка, на которой есть фото самого В. Титушко, а внизу нарисованы наручники, которые перечеркнули линиями красным цветом.

Другая группа, где намного меньше участников, является более активной. Там сообщения появляются часто и их активно комментируют. Так, администратор группы пишет: «Я не знаком, но я могу понять. Не то, что неприятно, а просто живешь себе и живешь, а тут бац! И весь Интернет о тебе говорит, как о преступнике, который вынашивал спецоперацию несколько лет».

Другой респондент отметил: «Жаль парня, из-за уродов сверху испортили несколько лет спокойной жизни».

Однако есть и те, кто осуждает поступок В. Титушко. «На зону гопника Титушко», – написал один из пользователей.

Напомним, подозреваемого в избиении журналистов во время субботних акций в Киеве выпустили под залог. За В. Титушко внесли почти 23 тыс. грн. Правоохранители объясняли, что его поведение общественно опасно, и он может влиять на потерпевшую. Потому что и ранее привлекался к уголовной ответственности.

Как известно, 18 мая 2013 г. группа спортивных молодых людей из Европейской площади устроила драку с националистами на ул. Большая Житомирская во время митингов ***(Вадик «Румын» стал героем соцсетей: одни оправдывают, а другие называют «гопником» // ru.tsn.ua (http://internetua.com/vadik--rumin--stal-geroem-socsetei--odni-opravdivauat--a-drugie-nazivauat--gopnikom). – 2013. – 24.05).***

Зарубіжні спецслужби і технології «соціального контролю»

В связи с терактом на Бостонском марафоне, помимо предполагаемого организатора Д. Царнаева и студентов из Казахстана, которые якобы препятствовали следствию, задержали еще одного человека – студента из Массачусетса К. Дамброзио. Правда, к взрывам он не имеет никакого отношения, но грозился устроить подобные и даже мощнее, пишет Eagle Tribune.

Полиция г. Метуэн штата Массачусетс задержала 18-летнего студента старших классов К. Дамброзио по подозрению в террористических угрозах. Юношу подвели опасные записи на стене в Facebook. «Он требовал людей замолчать, иначе он кого-нибудь убьет. Говорил, что сорвется, и о нем заговорят в новостях, что нечего плакать после того, что он сделает, потому что люди заслужили это», – раскрыл содержание записей начальник полиции Д. Соломон.

Самые тревожные сообщения касались теракта в Бостоне, в результате которого погибли трое и более 200 пострадали. «Забудьте о взрыве в Бостоне, подождите, что я сделаю! Я стану знаменитым», – обещал студент. При этом, как подчеркнули в полиции, угрозы не касались никого лично, но это не помешало воспринять их со всей серьезностью.

«Мы не можем такого допустить», – сказал Д. Соломон, при этом похвалив однокурсников К. Дамброзио, которые сообщили об опасных сообщениях. «Как говорится, если ты видишь что-то, скажи об этом», – цитирует полицейского My Fox Boston.

В доме у подозреваемого прошли обыски, в ходе которых были изъяты компьютер и игровая приставка Xbox. В ходе изучения страницы студента в Facebook, детективы нашли угрозы, касающиеся Белого дома, в связи с чем дело К. Дамброзио было передано ФБР.

В случае если вина студента будет доказана, ему грозит до 20 лет лишения свободы. На время следствия его обещают выпустить лишь в том случае, если будет внесен залог в 1 млн дол., сообщает Eagle Tribune.

Напомним, что в организации теракта на марафоне в Бостоне 15 апреля обвиняются братья Тамерлан и Джохар Царнаевы. Джохар был задержан в ходе спецоперации 20 апреля. Тамерлан 19 апреля скончался от ранений, полученных в перестрелке с полицией. Накануне также был задержаны уроженцы Казахстана А. Тажаяков и Д. Кадырбаев и гражданин США Р. Филлипос, которые по данным следствия, пытались уничтожить улики в комнате Джохара ***(18-летний студент может получить до 20 лет тюрьмы за провокационные записи в Facebook // InternetUA (http://internetua.com/18-letnii-student-mojet-polucsit-do-20-let-tuarmi-za-provokacionnie-zapisi-v-Facebook). – 2013. – 3.05).***

***

Министерство внутренних дел инициировало законопроект, обязующий провайдеров устанавливать у себя системы оперативно-розыскных мероприятий с целью контроля над деятельностью пользователей. Необходимые технические средства силовики предлагают закупать за счет операторов и провайдеров телекоммуникационных услуг.

На сегодняшний день законопроект, предлагающий внести изменения в статью 39 Закона «О телекоммуникациях», находиться на рассмотрении в Госкомпредпринимательстве. Официальные источники информацию о данном законопроекте не афишируют. К государственному регулятору отрасли телекоммуникаций законопроект также не поступал.

«Это выходит далеко за рамки здравого смысла, дошли до игнорирования не только телекомобщественности, но и НКРСИ. Считаю, что все документы подобного рода должны проходить через НКРСИ, как регулятора телеком-рынка. Не исключаю, что в данном случае НКРСИ может стать на сторону операторов. В любом случае, им не помешает знать о существовании такого законопроекта», – сообщает директор по обеспечению лицензионной деятельности и строительству компании «Фринет» А. Олексиенко.

«Насколько мы понимаем – в МВД хотят протолкнуть это как нерегуляторный акт. Поэтому его нигде не опубликовали. И в НКРСИ не прислали», – говорит Глава Правления ИнАУ Т. Попова.

К чему же такая конфиденциальность?

В соответствии с положениями, предложенных МВД изменений, операторы и провайдеры не только будут обязаны способствовать силовым структурам в раскрытии конфиденциальной информации о пользователях. Их также обяжут брать на себя все расходы по внедрению, необходимых для слежки за пользователями, технических средств.

Из текста самого законопроекта:

«Операторы телекоммуникаций обязаны за собственные средства устанавливать на своих телекоммуникационных сетях технические средства,

необходимые для осуществления уполномоченными органами оперативно-розыскных мероприятий; проведение негласных следственных (розыскных) действий и обеспечения временного доступа к вещам и документам, которые содержат информацию о связи, абонента, а также информацию о предоставлении телекоммуникационных услуг. В том числе получение информации об их длительности, содержании, маршрутов передачи и т. д.

Кроме этого, субъекты телекоммуникаций обязаны обеспечивать функционирование этих технических средств, а также в пределах своих полномочий содействовать проведению оперативно-розыскных мероприятий, негласных следственных действий и временному доступу к указанной информации с использованием информационно-телекоммуникационных систем и недопущению разглашения организационных и тактических приемов их проведения».

В прошлом году парламентарии уже рассматривали схожий законопроект, и отклонили его. Инициатором законопроекта был «регионал» В. Олейник. Мотивируя необходимость принятия изменений статью 39 Закона «О телекоммуникациях», депутат сообщал, что сегодня законодательством еще не в полной мере определен спектр обязательств провайдеров.

«По сути, при таких изменениях нам придется не только предоставлять информацию по возбуждённому уголовному делу, а и отвечать на каждый “чих” участкового инспектора. Нас обяжут строить новые каналы связи, и создавать дополнительные отделы по удовлетворению массовых запросив силовиков. В качестве примера приведу последний случай: к секретарю компании обратился представитель одного из райотделов УВД и срочно требовал предоставить исчерпывающую информацию по айпишнику (компания юридически ответить на запрос не могла), иначе его шеф рассердится. Теперь я так понимаю, таких “нетерпеливых” будет намного больше. Возмущает, то что данный законопроект тихо проходит без всяких согласований с общественностью!», – рассказывает Председатель комиссии УСПП по вопросам науки и информационных технологий И. Петухов.

Представители рынка, надеяться на благоразумие законодателей, которые не допустят создания новых коллизий в действующем законодательстве. «Эти изменения не смогут повлиять на процедуры распространения информации о потребителе, так как данная информация в соответствии с КПК может передаваться правоохранительным органам в рамках уголовного дела на основании соответствующего решения суда и/или определения следственного судьи. Другой порядок содействия операторами правоохранительным органом не предусмотрен, а потому инициированные МВД изменения – не имеют смысла», – сообщает начальник отдела регуляторной работы компании «Киевстар», Л. Цейтлина.

«В условиях и так самых низких цен на услуги Интернет в Украине – требование любых дополнительных затрат для производства этих услуг вряд ли приведет к тому что этот сегмент будет активно развиваться», – говорит руководитель пресс-службы компании «Воля» А. Михаелян ***(МВД хочет***

обязать провайдеров следить за пользователями // InternetUA (http://internetua.com/mvd-hochet-obyazat-provaiderov-sledit-za-polzovatelyami). – 2013. – 21.05).

***

Агентов ЦРУ обязали использовать социальные сети, чтобы не выделяться. Об этом пишет The Wall Street Journal со ссылкой на слова бывшего сотрудника организации. По сообщению источника издания, в ЦРУ разработали подробное руководство по использованию социальных медиа.

Некоторые современные психологи считают активность человека в Facebook и других соцсетях нормальным отражением его здоровой общественной жизни. А вот отсутствие профиля в популярных социальных сетях, напротив, может быть тревожным признаком, указывающим на асоциальный характер личности.

Психологи апеллируют к тому факту, что у преступников, совершивших массовые убийства, – норвежца А. Брейвика и американца Д. Холмса – не было аккаунтов в Facebook. Конечно, с такими умозаключениями можно поспорить, но вполне очевидно, что присутствие в соцсетях сегодня уже является нормой.

Возвращаясь к деятельности агентов ЦРУ, их обязали использовать соцсети, чтобы не привлекать к себе лишнего внимания со стороны окружающих. Руководство по использованию социальных медиа позволяет сотрудникам ЦРУ регистрироваться под своими настоящими именами, делать записи личного характера, публиковать фотографии.

Разумеется, сотрудникам ЦРУ запрещено разглашать любую информацию, связанную с их работой. Кроме того, тайным агентам запрещается контактировать в соцсетях с сотрудниками ЦРУ. К слову, у предполагаемого агента ЦРУ Р. Фогля, который недавно был задержан в Москве и обвинен в шпионаже и попытке завербовать сотрудника российских спецслужб, была активно обновляемая страничка в Facebook, открытая для 243 друзей ***(Агентов ЦРУ обязали использовать соцсети // InternetUA (http://internetua.com/agentov-cru-obyazali-ispolzovat-socseti). – 2013. – 24.05).***

***

Служба связи при правительстве Таджикистана обязала местных интернет-провайдеров заблокировать доступ к популярному видеохостингу.

Официально ведомство не комментирует причины блокировки YouTube, однако известно, что 18 мая на ресурсе были опубликованы ролики из передачи оппозиционного телеканала К+, посвященной свадьбе старшего сына президента Таджикистана Р. Эмомали. На видео запечатлен поющий и танцующий президент страны Р. Эмомали. На сегодняшний день ролики собрали более 50 тыс. просмотров.

В Таджикистане нередко блокируют популярные сайты. Так, YouTube в стране блокируется уже третий раз с июля 2012 г. В разное время таджикских пользователей также лишали доступа к сайтам Facebook, Twitter, «ВКонтакте»,

«Радио Свобода» ***(В Таджикистане из-за видео с пляшущим президентом заблокировали YouTube // InternetUA (http://internetua.com/v-tadjikistane-iz-za-video-s-plyashusxim-prezidentom-zablokirovali-YouTube). – 2013. – 25.05).***

***

Пользователи Ирана столкнулись с блокировкой доступа к некоторым веб-ресурсам и замедлением скорости Интернета. Об этом 24 мая сообщило информационное агентство Reuters.

Западные СМИ и многие пользователи связывают перебои в работе глобальной сети с президентскими выборами, которые состоятся 14 июня и станут для Ирана первыми с 2009 г. Тем не менее, правительство Ирана отрицает любую связь между нарушениями в работе Интернета и предстоящими выборами.

Для работы в Интернете многие иранские пользователи используют технологию частных виртуальных сетей VPN, однако с марта этого года Тегеран запретил работу «нелицензионных» VPN-сетей, заблокировав им доступ к внутренним иранским ресурсам.

Пользователи заявили, что замедление скорости Интернета началось примерно с марта этого года, однако на этой неделе падение скорости стало совсем очевидным. На некоторых иранских форумах появляются сообщения о том, что уже почти три недели пользователи не могут войти в учетные записи в почтовых сервисах Yahoo, Microsoft и Google. В феврале 2012 г., когда в Иране были парламентские выборы, наблюдалась похожая ситуация ***(Накануне выборов иранские пользователи столкнулись с блокировкой Интернета // Securitylab (http://www.securitylab.ru/news/440670.php). – 2013. – 24.05).***

***

Следственный комитет (СК) России объявил тендер «на оказание услуг доступа к системе мониторинга и прогнозирования противоправных действий на основе информации из соцсетей, блогов и СМИ». Поиск будет проводиться по встроенному электронному архиву.

Систему должны разработать до конца года. Максимальная цена контракта составляет около 1,2 млн руб.

Для того чтобы осуществлять мониторинг программистам будет необходимо разработать систему, способную анализировать сообщения пользователей «ВКонтакте», Facebook, Twitter, Livejournal, «Одноклассники», YouTube, RuTube, Instagram и Foursquare.

Аналогичными системами давно пользуются в администрации президента. Программа позволяет чиновникам обрабатывать сообщения более 40 млн русскоязычных блогов, микроблогов, форумов и социальных сетей.

Разработчики системы утверждают, что она позволяет отслеживать рост социальной напряженности в Интернете, протестные настроения, экстремизм; обсуждение уровня цен, зарплат, пенсий, инфраструктуры, медицины и пр.

Эксперты СК объясняют необходимость создание данного механизма тем, что он предоставит возможность оперативного реагирования на возникающие угрозы и средство предотвращать преступления.

Кроме того, система должна автоматически собирать все сообщения о работе СК из «значимых открытых и закрытых источников» ***(Эксперты СК России будут следить за СМИ и соцсетями // Securitylab (http://www.securitylab.ru/news/440616.php). – 2013. – 24.05).***

Проблема захисту даних. DOS та вірусні атаки

У соціальній мережі «ВКонтакте» виявили вразливість, яка дозволяє у статус будь-якого користувача без його відома додати будь-які «прослухані» ним пісні.

Користувач, який виявив уразливість, продемонстрував її на акаунті засновника соціальної мережі П. Дурова. Невдовзі до акаунта прем'єр-міністра Росії Д. Медвєдєва додали «прослухані» пісні з нецензурною лексикою та dubstep-обробку виступу О. Навального на мітингу.

Адміністрація «ВКонтакте» запевняє, що вразливість уже усунули, а акаунти, яким додавали «прослухані» пісні, зламані не були ***(Вразливість «ВКонтакте» дозволяла додати будь-які «прослухані» пісні користувачам // UkrainianWatcher (http://watcher.com.ua/2013/04/29/vrazlyvist-vkontakte-dozvolyala-dodaty-bud-yaki-prosluhani-pisni-korystuvacham/). – 2013. – 29.04).***

***

Создан «черный Google» – самый страшный поисковик Интернета

«Если люди не могут найти что-то в Google, они думают, что это не сможет найти никто. Это не так», – утверждает Д. Мэзерли, создатель Shodan, самого страшного поискового движка Интернета. В отличие от Google, который ищет в сети простые сайты, Shodan работает с теневыми каналами Интернета. Это своего рода «черный» Google, позволяющий искать серверы, веб-камеры, принтеры, роутеры и самую разную технику, которая подключена к Интернету и составляет его часть. Об этом сообщает nanonewsnet.ru.

Shodan работает 24 часа в сутки семь дней в неделю, собирая информацию о 500 млн подключенных устройствах и услугах ежемесячно.

Просто невероятно, чту можно найти в Shodan с помощью простого запроса. Бесчисленные светофоры, камеры безопасности, домашние системы автоматизации, системы отопления – все это подключено к Интернету и легко обнаруживается.

Пользователи Shodan нашли системы управления аквапарка, газовой станцией, охладителя вина в отеле и крематория. Специалисты по кибербезопасности с помощью Shodan даже обнаружили командно-контрольные системы ядерных электростанций и ускорителя атомных частиц.

И особенно примечателен в Shodan с его пугающими возможностями тот факт, что очень немногие из упомянутых систем имеют хоть какую-то систему безопасности.

«Это гигантское фиаско в безопасности», – говорит Х. Д. Мур, директор по безопасности в Rapid 7. Эта компания имеет частную базу данных типа Shodan для собственных исследовательских задач.

Если сделать простой поиск по запросу default password, можно найти бесконечное число принтеров, серверов и систем управления с логином admin и паролем «1234». Еще больше подключенных систем вообще не имеют реквизитов доступа – к ним можно подключиться с помощью любого браузера.

Независимый специалист по проникновению в системы Д. Тентлер в прошлом году на конференции по кибербезопасности Defcon продемонстрировал, как он с помощью Shodan нашел системы управления испарительными охладителями, нагревателями воды с давлением и гаражными воротами.

Он нашел автомойку, которую можно включать и выключать, и ледовую арену в Дании, которую можно разморозить одним нажатием кнопки. В одном городе к Интернету была подключена целая система управления дорожно-транспортной сетью, и всего одной командой ее можно было перевести в «тестовый режим». А во Франции он нашел систему управления гидроэлектростанцией с двумя турбинами, каждая из которых генерирует по 3 МВт.

«Этим можно нанести серьезный вред», – сказал Д. Тентлер, и он еще мягко выразился.

Так почему же все эти устройства подключены к сети и почти не защищены? В некоторых случаях, таких как дверные замки с управлением через iPhone, принято считать, что их очень сложно найти. И тогда о безопасности думают по остаточному принципу.

Более серьезной проблемой является то, что многие такие устройства вообще не должны быть в онлайне. Фирмы часто покупают устройства, которые позволяют с помощью компьютера управлять, скажем, системой нагревания. Как подключить компьютер к системе нагревания? Вместо прямого подключения во многих ИТ-отделах просто подключают и то, и другое к веб-серверу, тем самым неосознанно раскрывая их всему миру.

«Конечно, на таких вещах просто нет безопасности, – говорит Д. Мэзерли. – Но в первую очередь им не место в Интернете».

Но хорошо то, что Shodan почти полностью используется для благих целей. Сам Д. Мэзерли, который три года назад создал Shodan просто забавы ради, ограничил число запросов до 10 без учетной записи и 50 с учетной записью. Если вы хотите задействовать больше возможностей Shodan, Д. Мэзерли запросит у вас дополнительную информацию о ваших целях – и оплату.

Испытатели проникновения, специалисты по безопасности, научные исследователи и правоохранительные органы – вот основные пользователи

Shodan. Д. Мэзерли согласен с тем, что Shodan могут воспользоваться как отправной точкой и плохие ребята. Но он при этом добавляет, что киберпреступники обычно имеют доступ к ботнетам – большим коллекциям инфицированных компьютеров, которые могут делать то же самое, но скрытно.

Сегодня большинство кибератак сосредоточены на краже денег и интеллектуальной собственности. Плохие ребята пока еще не пытались навредить кому-то, взорвав здание или отключив светофоры.

Специалисты по безопасности надеются предотвратить подобные сценарии, выявляя эти незащищенные подключенные устройства и услуги с помощью Shodan и предупреждая их владельцев об уязвимостях. А тем временем масса вещей в Интернете без всякой безопасности просто сидят и ждут атаки ***Создан «черный Google» – самый страшный поисковик Интернета // IT Expert (http://itexpert.in.ua/rubrikator/item/25959-sozdan-chernyj-google-samyj-strashnyj-poiskovik-interneta.html). – 2013. – 6.05).***

***

Пароли в ближайшем будущем будут вытеснены другими, более простыми и надежными средствами аутентификации, считает М. Барретт, директор PayPal по вопросам безопасности.

Выступая на конференции Interop, которая проходила с 6 по 10 мая в Лас-Вегасе, М. Барретт раскритиковал распространенные в современном мире методы аутентификации. По его словам, они небезопасны и неудобны: чтобы не держать в памяти множество аутентификаторов, пользователи либо используют везде один и тот же пароль, либо создают простые пароли, которые легко подобрать – 12345 или password (англ. «пароль»), сообщает Лента.Ру.

Двухэтапные системы аутентификации (когда помимо логина и пароля нужно ввести, например, присланный в SMS код подтверждения), применяемые многими интернет-компаниями, М. Барретт назвал «мечтой для регулятора, но кошмаром для пользователя».

Вместо паролей М. Барретт предложил использовать биометрические «устройства аутентификации» – сканеры отпечатков пальцев или сетчатки глаза (хотя возможно и применение USB-токенов). Один раз привязав аккаунт к системе, пользователь сможет авторизовываться на сайте, отсканировав палец или сетчатку глаза.

Систему аутентификации, описанную М. Барреттом, разрабатывает альянс Fast IdentityOnline (FIDO). В него входят компании, занимающиеся вопросами компьютерной безопасности, системные интеграторы и интернет-компании. М. Барретт – президент альянса.

В основе системы, подчеркивают разработчики, будут лежать открытые стандарты, благодаря чему она сможет использоваться в сети повсеместно.

М. Барретт предсказал, что «устройства аутентификации», поддерживающие систему FIDO, появятся уже в 2013 г. – в том числе и в мобильных телефонах. Полностью система вытеснит традиционные пароли, по

его оценке, через несколько лет. М. Барретт уточнил, что внедрить у себя FIDO планирует и PayPal.

Электронная платежная система PayPal является подразделением компании eBay, владеющей одноименным интернет-аукционом. В PayPal зарегистрированы 128 млн активных аккаунтов; система работает более чем в 190 странах.

На рынке уже имеются устройства – в частности, ноутбуки – со встроенными сканерами отпечатков пальцев, однако повсеместного распространения такие приборы пока не получили. Сканеры, как правило, используются в качестве одного из этапов многофакторной аутентификации ***(Пароли в Интернете могут заменить отпечатками пальцев // Vlasti.net (http://vlasti.net/news/166263). – 2013. – 13.05).***

***

В Интернете распространяется новая вредоносная программа, способная воровать данные учетных записей пользователей в социальной сети Facebook. Маскируется вирус под расширение для популярных браузеров.

В связи с этим, активным пользователям Mozilla Firefox и Google Crome лучше не стоит соглашаться ни на какие дополнения к обновления к браузерам. Именно в них и обнаружена вредоносная троянская программа Trojan:JS/Febipos.

Попадая на компьютер вирус сразу же отслеживает подключение к Facebook, а также загружает файл конфигурации, который позволяет ему передавать команды браузеру незаметно для пользователя. Данное вредоносное программное обеспечение может выкладывать в Facebook пользователя ссылки на страницы, делиться контентом, присоединяться к группам и даже общаться в чате с друзьями владельца учетной записи.

Кроме того, благодаря обновляемым файлам конфигурации, троян может менять свою активность, размещать другие сообщения или затихать на время, передает РИА Новости. При этом приложение не осуществляет никакой деятельности на компьютере, где не были обнаружены данные для входа в аккаунт Facebook.

Следует отметить, что изначально Trojan:JS/Febipos был ориентирован на бразильскую аудиторию и «разговаривал» только на португальском. Сейчас специалисты подтверждают, что злонамеренная программа может быть легко адаптирована к любому другому языку.

В связи с этим компания Microsoft рекомендует регулярно проверять свою активность в социальных сетях. При необходимости надо менять реквизиты доступа и сканировать компьютер на предмет наличия вредоносного программного обеспечения ***(Вирус похищает учетные данные в Facebook // Utro.ua (http://www.utro.ua/ru/zhizn/virus_pohishchaet_uchetnye_dannye_v_facebook1368519887). – 2013. – 14.05).***

***

Украинцев просят не «светиться» в социальных сетях

Современные злоумышленники активно пользуются технологиями. Чаще всего при совершении краж квартирные воры пользуются информацией, которую сами того не зная предоставляют им будущие жертвы. Об этом во время пресс-конференции заявила начальник отдела ГСО МВД Украины С. Павловская.

По ее словам, воры очень часто используют сообщения из статусов в соцсетях, из которых можно почерпнуть информацию о местонахождении владельца квартиры. Неплохую помощь домушникам оказывают и фото, на которых очень часто видны дорогие интерьеры и ценные вещи ***(Украинцев просят не «светиться» в социальных сетях // InternetUA (http://internetua.com/ukraincev-prosyat-ne--svetitsya--v-socialnih-setyah). – 2013. – 16.05).***

***

Компания «Доктор Веб» обнаружила неизвестный ранее функционал в новой вредоносной программе для Facebook. Trojan.Facebook.311 может не только публиковать от имени пользователя новые статусы, вступать в группы, оставлять комментарии, но и рассылать спам в социальных сетях Facebook, Twitter и Google+.

Троянская программа Trojan.Facebook.311 представляет собой написанные на языке JavaScript надстройки для популярных браузеров Google Chrome и Mozilla Firefox. Злоумышленники распространяют троянца с использованием методов социальной инженерии – вредоносные программы попадают в систему при помощи специального приложения-установщика, маскирующегося под «обновление безопасности для просмотра видео». Примечательно, что установщик имеет цифровую подпись компании Updates LTD, принадлежащей Comodo. Надстройки называются Chrome Service Pack и Mozilla Service Pack соответственно. С целью распространения троянца злоумышленники создали специальную страницу на португальском языке, ориентированную, по всей видимости, на бразильских пользователей Facebook.

После завершения установки в момент запуска браузера Trojan.Facebook.311 пытается загрузить с сервера злоумышленников файл с набором команд. Затем встроенные в браузеры вредоносные плагины ожидают момента, когда жертва выполнит авторизацию в социальной сети Facebook. После этого троянец может выполнять от имени пользователя различные действия, обусловленные содержащимися в конфигурационном файле командами злоумышленников: поставить «лайк», опубликовать статус, разместить на стене пользователя сообщение, вступить в группу, прокомментировать сообщение, пригласить пользователей из списка контактов жертвы в группу или отправить им сообщение. Помимо этого троянец может по команде злоумышленников периодически загружать и устанавливать новые

версии плагинов, а также взаимодействовать с социальными сетями Twitter и Google+, в частности, рассылать спам.

В последнее время Trojan.Facebook.311 был замечен за распространением в сети Facebook сообщений, содержащих изображение, которое имитирует встроенный в браузер медиаплеер. При щелчке мышью по нему пользователь перенаправляется на различные мошеннические ресурсы. Аналогичным образом с помощью личных сообщений и статусов троянец рекламирует мошеннические викторины, в которых якобы можно выиграть различные ценные призы ***(Новый троянец охотится на пользователей Facebook, Twitter и Google+ // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2013/05/17/social-trn.html). – 2013. – 17.05).***

***

Хакеры группы Anonymous взломали 52 сайта Израиля, сообщает «Обозреватель». Взломанные сайты принадлежали полугосударственным и частным компаниям, а также больницам, аптекам и транспортным фирмам.

Напомним, несколькими днями ранее группа Anonymous взломала сайт радиостанции «Голос Кореи». Хакеры также сообщили об атаках на северокорейский сайт пропаганды и на страницу информационного агентства ЦТАК, однако неизвестно, были ли они успешными ***(Anonymous взломали 52 сайта Израиля // Обозреватель (http://tech.obozrevatel.com/news/87912-anonymous-vzlomali-52-sajta-izrailya.htm). – 2013. – 18.05).***

***

Американский хакер П. Томпсон разработал приложение Bunny.py, с помощью которого можно эффективно скрывать трафик в пакетах 802.11. Эта программа позволяет поднять собственную беспроводную сеть между устройствами, при этом сеть будет невидима для постороннего наблюдателя (darknet), поскольку ее трафик замаскирован в посторонних WiFi-пакетах. Другими словами, Bunny создает инфраструктуру уровня 1/2 по сетевой модели OSI.

Для маскировки маленьких фрагментов данных Bunny использует некоторые фрагменты пакетов, которые плохо определены в стандарте 802.11, в том числе поле с указанием производителя, зашифрованные пакеты и некоторые поля в пакетах. Другой узел подпольной сети способен обнаруживать фрагменты информации, внедренные Bunny. Доступ посторонних в сеть предотвращается криптографическими методами.

Для тестирования программы нужна карта, способная отслеживать и изменять WiFi-трафик.

На практике Bunny можно использовать для проникновения в чужую локальную сеть, маскируя управляющие команды к устройству-жучку по WiFi непосредственно в пакетах 802.11 данной беспроводной сети. То есть после установки шпионского устройства в сети жертвы нам не нужно поднимать собственную сеть WiFi, а можно пользоваться имеющейся сетью ***(Скрытие***

трафика в шуме WiFi // InternetUA (http://internetua.com/skritie-trafika-v-shume-WiFi). – 2013. – 20.05).

***

Японское подразделение портала Yahoo! заявило о возможной утечке данных 22 млн своих пользователей. Об этом сообщает «Обозреватель».

Как пояснили представители компании, они обнаружили попытку взлома системы администрирования порталом.

Какие именно данные могли похитить, в Yahoo! не уточнили. В компании отметили, что пароли пользователей, а также данные, необходимые для изменения паролей, остались в сохранности.

При этом Yahoo! рекомендовал всем пользователям сменить на всякий случай свои пароли ***(Японский Yahoo! потерял данные 22 млн аккаунтов // Обозреватель (http://tech.obozrevatel.com/news/93467-yaponskij-yahoo-poteryal-dannyie-22-mln-akkauntov.htm). – 2013. – 20.05).***

***

Эксперты «Лаборатории Касперского» подвели итоги активности вирусописателей за I квартал 2013 г., передает корреспондент ProIT со ссылкой на пресс-службу компании.

Основные цифры за I квартал 2013 г.:

• 49 % украинских пользователей подверглись заражению через веб-ресурсы в I квартале 2013 г.;

• Украина находится на 5-м месте среди стран на веб-ресурсах которых, размещены вредоносные программы;

• Украина заняла 8-м место в списке стран, жители которых подвергаются наибольшему риску заражения в Интернете.

Главными событиями I квартала оказались целевые атаки и хорошо спланированные кампании по кибершпионажу.

Счет инцидентам в области информационной безопасности открыла рассекреченная «Лабораторией Касперского» глобальная операция «Красный октябрь», проводимая киберпреступниками с целью шпионажа за дипломатическими, правительственными и научными организациями в различных странах мира. На протяжении пяти лет злоумышленники осуществляли сбор конфиденциальной информации как с персональных компьютеров, так и с мобильных устройств, сетевого оборудования, USB-дисков, почтовых баз данных, локальных и удаленных серверов.

Следом за «Красным октябрем», в феврале этого года, были обнаружены еще две кибершпионские сети. Первая из них – MiniDuke – отличается необычайно малыми (всего 20 Кб) размерами бэкдора, уникального для каждой зараженной системы. Бэкдор проникал на компьютеры пользователей через уязвимости в приложении Adobe Reader. Другая серия атак, о которой стало известно из отчета компании Mandiant в феврале 2013 г., была организована группой китайских хакеров, получившей название APT1. Предположительно,

жертвами этой масштабной операции, продолжающейся с 2006 г., стали уже более 140 компаний.

Наконец, под занавес I квартала – в марте – была обнародована информация еще о двух инцидентах: исследование о наиболее ранней из известных версий червя Stuxnet и об операции TeamSpy, организаторы которой избрали в качестве своей цели высокопоставленных политиков и борцов за права человека в странах СНГ и Восточной Европы.

Помимо кибершпионажа, начало 2013 г. ознаменовалось также масштабными целевыми атаками, жертвами которых стали как политические деятели (тибетские и уйгурские активисты), так и крупные коммерческие компании – в частности, от взлома корпоративных сетей пострадали Apple, Twitter, Facebook, Evernote и др.

Всего же в I квартале 2013 г. продукты «Лаборатории Касперского» обнаружили и обезвредили более 1,3 млн вредоносных объектов. При этом наиболее часто встречающейся угрозой в Интернете вновь стали вредоносные ссылки, ведущие на взломанные или созданные злоумышленниками сайты. По сравнению с VI кварталом 2012 г. их доля возросла на 0,5 %, и в итоге в I квартале 2013 г. на такие ссылки пришлось 91,4 % всех срабатываний веб-антивируса «Лаборатории Касперского».

В Украине количество зафиксированных «Лабораторией Касперского» интернет-угроз превысило 47 млн образцов, а заражению через веб-ресурсы в I квартале 2013 г. подверглись 49 % украинских пользователей. С такими показателями Украина заняла 8-е место в списке стран, жители которых подвергаются наибольшему риску заражения в Интернете.

По итогам I квартала эксперты «Лаборатории Касперского» отметили также особенный рост зловредов среди мобильных угроз: за три месяца в начале года было зафиксировано более 20 тыс. новых образцов вредоносного ПО для мобильных устройств. Для сравнения: за весь 2012 г. было обнаружено чуть более 40 тыс. подобных угроз ***(49 % украинцев подверглись интернет-атакам в I кв 2013 г. // ProIT (http://proit.com.ua/news/internet/2013/05/15/143551.html). – 2013. – 15.05).***

***

Незалежна асоціація банків України (НАБУ) запустила проект «Протидія кіберзлочинності», покликаний підвищити обізнаність клієнтів банків про безпечну поведінку.

Сайт проекту anticyber.com.ua має стати джерелом отримання інформації про:

– боротьбу з кіберзлочинністю в Україні та світі;

– основні види та загрози кібершахрайства у фінансовій сфері;

– превентивні заходи, що допоможуть Вам не стати жертвою кіберзлочинців;

– правила поведінки у випадку виявлення шахрайських дій, Ваші права та можливості.

Наразі ви можете прочитати на сайті про три великі групи шахрайств: шахрайства з телефоном та Інтернетом, шахрайство з банкоматом та шахрайство з платіжними картками. Партнерами проекту виступили НБУ, МВС та 19 комерційних банків ***(В Україні запустили сайт, який допоможе боротись з кіберзлочинністю // UkrainianWatcher (http://watcher.com.ua/2013/05/17/v-ukrayini-zapustyly-sayt-scho-dopomozhe-borotys-z-kiberzlochynnistyu/). – 2013. – 17.05).***

***

Хакер создал ботнет, с помощью которого взломал 420 тыс. компьютеров и, управляя ими, составил одну из самых полных и подробных карт Интернета. Зараженные компьютеры отпинговали 460 млн IPv4-адресов (то есть в исследование не вошли IPv6, но их пока гораздо меньше, чем первых).

Картина получилась вполне предсказуемая: наиболее освещенные светочем веба части мира – Европа и восточная часть США. Интересно, конечно, что Германия и южная Англия целиком на порядок более интернетизированы, чем остальная Европа. В Азии – мощные центры и киберпустота вокруг, если присмотреться, даже в суперпродвинутых Японии и Южной Корее. Уровень проникновения Интернета, конечно, может запросто служить маркером высокоэффективной экономики.

Анонимный хакер, кроме того, исследовал уровень интернет-трафика в зависимости от времени суток и на основе данных создал эту красивую gif-карту. Тут хорошо видно, как ночью веб-активность падает в разы.

«Зачем я это сделал? – задается риторическим вопросом анонимный исследователь и отвечает, – да просто, чтобы не задаваться дурацким вопросом, почему я этого не сделал, хотя мог» ***(Хакер взломал 420 тыс. компьютеров, чтобы создать карту Интернета // IT Expert (http://itexpert.in.ua/rubrikator/item/26185-khaker-vzlomal-420-tys-kompyuterov-chtoby-sozdat-kartu-interneta.html). – 2013. – 15.05).***

***

Українці втрачають власні гроші через неуважність та невміння користуватися фінансовою інформацією. На цьому наголошують представники Національної асоціації банків України, які нині намагаються підвищити обізнаність банківських клієнтів завдяки спеціальному проекту «Протидія кіберзлочинності у банківській сфері». Тим часом правоохоронці наголошують, що рятувати громадян від кібершахраїв треба шляхом створення умов, які б дозволяли зловмисникам «заробляти гроші законно».

Лише за три перші місяці цього року через злочини у сфері комп’ютерних технологій українці втратили близько 62 млн грн. На цьому наголошує начальник відділу міжнародної діяльності Національної академії внутрішніх справ М. Акімов. При цьому загальні світові прибутки від таких незаконних дій, за його словами, щорічно сягають трильйона доларів. А це перевищує

сукупні доходи від незаконної торгівлі наркотиками, зброєю та людьми, каже він.

«Якщо раніше злочинці обмежувалися тим, що могли підробляти пластикові картки, змінювати магнітні стрічки, накладати спеціальні накладки на банкомати, щоб копіювати інформацію, пін-коди, які вводив власних пластикової картки, то тепер відбувається злам комп'ютерної мережі і швидке переведення коштів з одного рахунку на інший, з однієї країни до іншої, а потім – відмивання через мережу фіктивних фірм», – наголошує він.

За словами М. Акімова, боротьба з кіберзлочинністю в Україні розпочалася лише кілька років тому і наразі серед її пріоритетів не тільки виявлення таких злочинів, але і запобігання їм. Головним чином через створення умов, які б «дозволяли потенційним кіберзлочинцям заробляти гроші законно».

Поінформований значить озброєний

Тим часом колишній співробітник ФБР, а нині начальник управління інформаційної безпеки SWIFT Exchange Д. Кодлінг зауважує: ефективність боротьби з кіберзлочинністю багато у чому залежить від досвідченості експертів, наявності необхідних ресурсів та, головним чином, достатнього фінансування. Відтак Великобританія, Канада та США, за його словами, нині є найбільш прогресивними країнами у цій сфері.

Утім, Д. Колдінг переконаний, що попередити кіберзлочини можуть і самі громадяни. Головне – бути достатньо поінформованим, пояснює він.

«Багато залежить від освіченості. Щоб уберегтися від кіберзлочинності, ви маєте володіти інформацією про свого провайдера, тих, хто встановлює ваше технічне обладнання чи захисне устаткування на нього. Краще користуватися послугами відомих компаній, адже тоді у якості послуг можна бути впевненим. Натомість співпрацювати з маловідомими фірмами, навіть якщо вони пропонують знижки, не варто», – говорить фахівець.

Наразі ж експерти наголошують: щонайменше 70 % витоків інформації нині відбувається саме через вірусне програмне забезпечення.

SMS про стан банківського рахунку допоможе врятувати гроші

Тим часом статистика Незалежної асоціації банків показує: у 2012 р. кількість випадків незаконного зняття сторонніми особами грошей з банківських карток, у порівнянні з 2011 р., зросла утричі.

Відтак цього року представники організації розпочали підвищувати обізнаність клієнтів банків завдяки проекту «Протидія кіберзлочинності у банківській сфері». Зокрема у його рамках діє спеціальний сайт, який знайомить користувачів з основними видами фінансового кібершахрайства, боротьбою з кіберзлочинністю в Україні та світі, превентивними заходами, а також правилами поведінки у разі виявлення шахрайських дій.

«Ми боремося насамперед з тим, щоби наші громадяни були уважнішими. Бо багато шахрайських операцій, які відбуваються в Україні, пов'язані не з використанням високих технологій, а, насамперед, з неуважністю громадян стосовно фінансової інформації. Наприклад, як треба зберігати пін-

код і чи потрібно його запам'ятовувати, чи ні», – пояснює керівник проекту «Протидія кіберзлочинності у банківській сфері» Т. Самсонюк.

Між тим, щоб уберегти власні кошти, експерти радять, зокрема, не називати нікому пін-коду від своєї банківської картки, не передавати її іншим, лишати зразок власного підпису на її зворотному боці, а також підключити опцію смс-повідомлень про стан банківського рахунку і операціях, проведених платіжною карткою ***(Кібершахраї обкрадають українців: 62 млн грн за три місяці // InternetUA (http://internetua.com/k-bershahra--obkradauat-ukra-nc-v--62-m-lioni-griven-za-tri-m-syac). – 2013. – 20.05).***

***

Антивирусная лаборатория PandaLabs компании Panda Security предупреждает о вспышке новых случаев интернет-мошенничества. Последние аферы используют удобства, предоставляемые электронной почтой, а также ее уязвимостью. Преступники получают доступ к какому-либо реальному email-аккаунту и рассылают сообщения по всему списку контактов жертвы с целью вымогательства денег у людей.

Например, в письме с темой Very Urgent («Очень срочно»), пришедшем от человека из списка контактов, сообщается, что отправитель находится в отпуске, но у него украли кошелек с кредитной картой и авиабилетами, поэтому ему срочно требуются деньги, чтобы вернуться домой. Если получатель поверит и перечислит деньги указанным в письме способом, то они поступят на банковский счет киберпреступников.

«Существует множество вариаций данного типа мошенничества. В данном конкретном случае сообщение циркулирует в Интернете несколько месяцев, а затем его активность начинает постепенно угасать», – отмечает Л. Корронс, технический директор PandaLabs.

Подобные мошеннические сообщения позволяют киберпреступникам не только получать деньги от своих жертв, но и собирать адреса личных и корпоративных почтовых аккаунтов.

«Одной из главных проблем, с которой сталкивается жертва подобного мошенничества, является то, что киберпреступники меняют пароль к аккаунту, в результате чего законный владелец не может получить к нему доступ, – объясняет Л. Корронс. – Эта проблема усугубляется, если человек использует одинаковый пароль для своих аккаунтов в Facebook или Twitter, что позволяет киберпреступникам контролировать их и выдавать себя за жертву обстоятельств».

«Будьте особенно осторожны при получении подобного сообщения. В этом случае свяжитесь непосредственно с отправителем, например, по телефону, и выясните степень подлинности данного письма», – советует Л. Корронс ***(PandaLabs предупреждает о вымогательстве денег по email // InternetUA (http://internetua.com/PandaLabs-preduprejdaet-o-vimogatelstve-deneg-po-email). – 2013. – 19.05).***

***

Эксперты Symantec предупреждают европейские организации о новой волне хакерских атак. Известно, что в ходе атаки злоумышленники применяют сложные приёмы социальной инженерии. По имеющейся информации, жертвами киберпреступников стали, по крайней мере, 14 французских компаний. Кроме того, аналогичные атаки зафиксированы в Румынии и Люксембурге.

Эксперты из Symantec утверждают, что атаки начинаются с телефонного звонка одному из сотрудников компании. В разговоре ему сообщают о счете-фактуре, который будет ему выслан по электронной почте.

На самом деле отправленный файл является модификацией RAT-трояна Shadesrat. Оказавшись на компьютере жертвы, вирус открывает злоумышленникам доступ к конфиденциальным данным, которые позволят им подключиться к банковским счетам компании.

Информация, собранная Shadesrat, может также использоваться кибермошенниками для новых атак с применением приёмов социальной инженерии ***(Хакеры атакуют компании, используя троян Shadesrat // InternetUA (http://internetua.com/hakeri-atakuuat-kompanii--ispolzuya-troyan-Shadesrat). – 2013. – 19.05).***

***

Антивирусная компания Trend Micro сообщила об обнаружении новой кибершпионской операции, направленной на компрометацию компьютеров в различных государственных министерствах, технологических компаниях, исследовательских организациях и неправительственных организациях в более чем сотне стран.

Trend Micro называет новую операцию SafeNet и заявляет, что в ее рамках жертвы получают мошеннические электронные сообщения, различными способами принуждаются к посещению вредоносных ресурсов и получают файлы с вредоносными кодами, направленными на кражу персональных данных. В рамках исследования деятельности кампании SafeNet, Trend Micro выявила два типа командно-контрольных серверов, указывающих на то, что как минимум две независимые группы хакеров проводят параллельные атаки и имеют разные цели, но используют один и тот же арсенал вредоносов.

Первая кампания использует арсенал мошеннических писем с содержимым, связанным с Тибетом и Монголией. Данные письма имеют приложенные .doc-файлы, эксплуатирующие уязвимость, устраненную Microsoft в Word ровно год назад. Журналы доступа от этой кампании собираются на C&C-серверах, связанных с 243 уникальными IP-адресами из 11 стран. Однако на момент исследования лишь три сервера были активными в рамках этого направления.

C&C-серверы в рамках второй атаки содержали в себе данные об атаках на 11 563 компьютера-жертвы из 116 стран. Здесь Trend Micro сообщила о том, что лишь 76 компьютеров-клиентов были связаны с коммандно-контрольными

серверами на момент исследования. Наибольшее количество жертв здесь было из таких стран, как США, Китай, Пакистан, Филиппины и Россия.

Размещаемое в рамках обеих атак вредоносное программное обеспечение направлено, главным образом, на кражу персональных данных, однако оно создано по модульному принципу и может иметь дополнительные возможности. Так, в Trend Micro нашли вспомогательные модули, которые позволяют получать сохраненные пароли из Internet Explorer, Mozilla Firefox и Remote Desktop Protocol в Windows ***(Trend Micro выявила следы новой кибершпионской операции // InternetUA (http://internetua.com/Trend-Micro-viyavila-sledi-novoi-kibershpionskoi-operacii). – 2013. – 20.05).***

***

Check Point объявила об обнаружении разворачивающихся атак фишинговых программ и ботов. В атаках использовались новые варианты эксплойтов уязвимости (CVE-2012-0158), нацеленные на компьютеры сотрудников ряда крупных мировых корпораций.

Атаки начались с фишинговых электронных сообщений якобы от Citibank или Bank of America. В самих письмах, в теме которых было указано Merchant Statement («Коммерческая выписка») или что-либо подобное, получателям предлагалось открыть зараженное вложение в формате Microsoft Word. Но вложение содержало не выписку, а вредоносное приложение, которое при открытии автоматически запускалось, заражая компьютер получателя и передавая крупной бот-сети контроль над ним. Уникальный аспект данных атак состоял в том, что вредоносное ПО оказалось способно открывать сетевые порты, красть регистрационные данные пользователей (логины и пароли), а также действовать как саморазмножающийся спам-бот, готовый к выполнению новых инструкций к атаке, а также к рассылке вредоносных электронных писем другим жертвам.

«Киберпреступники постоянно инициируют новые атаки, ежедневно распространяя тысячи вариантов вредоносных программ, – говорит Д. Дор, вице-президент по продуктам компании Check Point. – Традиционные антивирусные программы оказываются бессильны, когда речь идет о неизвестных ранее угрозах».

«Организациям необходима многоуровневая система защиты, включающая технологию эмуляции угроз, способную выявить и предотвратить новые атаки и справиться с вариантами существующих», – добавляет Д. Дор ***(Check Point сообщила об обнаружении новых фишинговых атак // InternetUA (http://internetua.com/Check-Point-soobsxila-ob-obnarujenii-novih-fishingovih-atak). – 2013. – 21.05).***

***

Власти США отключили на военно-морской базе США на Гуантанамо беспроводной Интернет и ограничили доступ к социальным сетям из-за угрозы взлома. Об этом сообщает 20 мая Associated Press.

В частности, отключен доступ к сети микроблогов Twitter, а также социальной сети Facebook, заявил официальный представитель расположенной на территории базы тюрьмы.

Причиной ограничения доступа в Интернет военные назвали угрозы со стороны группы хакеров Anonymous.

Ранее международная кибергруппировка начала кампанию солидарности «Операция Гуантанамо», приуроченную к сотому дню с начала голодовки, объявленной заключенными Гуантанамо, и призвала международное сообщество выступить против тюрьмы в течение трех дней после 17 мая. Продвигаемые в рамках кампании хэштеги попали 17 и 18 мая в американские и мировые топы Twitter, пишет International Business Times.

Согласно официальной информации, голодовка в знак протеста против бессрочного содержания в тюрьме проходит в тюрьме с 15 марта, 20 мая в ней участвуют 103 из 166 заключенных.

Американская тюрьма, расположенная на американской базе на территории Кубы, была создана в 2002 г. для содержания людей, подозреваемых в терроризме. Заведение неоднократно подвергалось критике со стороны правозащитных организаций в связи с применением пыток и содержанием заключенных без предъявления обвинения. Президент США Б. Обама заявлял о своем намерении закрыть тюрьму еще во время своей первой предвыборной кампании в 2008 г. ***(Из-за угроз Anonymous на Гуантанамо ограничили Интернет // InternetUA (http://internetua.com/iz-za-ugroz-Anonymous-na-guantanamo-ogranicsili-internet). – 2013. – 21.05).***

***

Румынский хакер, находящийся в заключении за кражу денег с банковских счетов и незаконную модификацию банкоматов, объявил об изобретении новой схемы защиты. Предполагается, что схема, созданная находящимся в неволе хакером, поможет сделать банкоматы практически неуязвимыми к так называемым «скиммерам» (устройствами, которые преступники устанавливают на гнездо приема карты в банкомате, чтобы считать с нее секретные данные банковского счета).

В. Боанта, гражданин Румынии, с 2009 г. находящийся в заключении по делу о мошенничестве с банковскими картами и банкоматами, обещает представить публике новаторское приспособление, которое можно установить на любой действующий банкомат. В этом случае необычно то, что сам В. Боанта как раз и занимался перехватом банковских карт с помощью скиммера, пока не был арестован по делу одной из местных преступных группировок.

Сейчас В. Боанта заявляет, что решил перейти на «светлую» сторону еще во время следствия. Якобы, он понял, что преступления для него были своего рода адреналиновой зависимостью, а теперь он хочет обратить свои навыки и знания на благо общества.

Изобретение В. Боанты носит название SRS (Secure Revolving System – защитная поворотная система). В системе SRS применяется остроумная механическая защита от скиммеров. Фактически, скиммер представляет собой замаскированное устройство для считывания пластиковых карт, тайно устанавливаемое за несколько секунд на основной приемник карт в банкомате. Скиммер сам по себе не выполняет опасных действий – он только похищает данные с карты ничего не подозревающего пользователя.

Механизм SRS, который придумал В. Боанта, резко меняет ситуацию с защитой банкоматов. Сначала клиент вставляет карту длинной стороной, так что магнитная полоса располагается параллельно стенке банкомата. Далее механизм поворачивает карту на 90°, чтобы считать информацию с магнитной полосы уже по стандартной схеме. После считывания карта поворачивается обратно и возвращается клиенту. Такая схема сильно осложняет задачу преступника, поскольку магнитная полоса нигде не проходит по прямой линии, пока не окажется внутри защищенного от махинаций картридера.

В ожидании выхода из тюрьмы В. Боанта передал свою идею двум специалистам из фирмы MB Telecom (Бухарест, Румыния): М. Тудору и А. Бизгару. Они помогли бывшему преступнику запатентовать свое изобретение и найти деньги на дальнейшую разработку механизма SRS.

Конструкция защитного механизма SRS выиграла первый приз на апрельской международной выставке изобретений в Женеве (Швейцария), правда сам изобретатель не смог появиться на вручении наград по уважительной причине. Сейчас В. Боанте отбыл всего шесть месяцев из назначенного судом пятилетнего срока: ему предстоит провести в тюрьме еще четыре с половиной года. Тем не менее, его партнеры из фирмы MB Telecom признают его полное право на технологию SRS как изобретателя. После доводки опытных образцов, MB Telecom планирует начать массовые поставки механизма SRS уже во второй половине текущего года. Кстати, представители MB Telecom считают, что распространение технологии SRS поможет улучшить имидж Румынии, которую часто считают пристанищем киберпреступности ***(Раскаявшийся хакер изобрел механизм защиты банкоматов // InternetUA (http://internetua.com/raskayavshiisya-haker-izobrel-mehanizm-zasxiti-bankomatov). – 2013. – 21.05).***

***

Компания Eset сообщила о раскрытии целенаправленной атаки, которая два года использовалась для хищения конфиденциальной информации в Пакистане и ряде других стран. При расследовании инцидента стало известно, что корни этой кибератаки берут начало в Индии. Целью кибератаки являлась кража конфиденциальной информации с зараженных компьютеров – для этого использовались различные способы, включая клавиатурный шпион, модуль снятия скриншотов рабочего стола, модуль передачи документов на внешний сервер и т. д. После успешной атаки все собранные данные отправлялись к злоумышленникам.

При организации атаки киберпреступники использовали действующий цифровой сертификат, которым подписывали вредоносные исполняемые файлы. Такая подпись придавала этим файлам большую легитимность. Упомянутый сертификат еще в 2011 г. был получен компанией, расположенной в Нью-Дели (Индия). Вредоносное ПО, которое подписывалось этим сертификатом, распространялось через электронную почту.

Киберпреступники маскировали вредоносные файлы под электронные документы с якобы важным содержанием. Специалистами Eset было обнаружено несколько подобных документов, которые, судя по всему, должны были заинтересовать потенциальных жертв. Так, в одном из них использовалась тема индийских вооруженных сил.

На сегодняшний день нет точной информации о том, на какие именно учреждения была направлена кибератака, однако можно с уверенностью сказать, что цели атаки располагались в Пакистане. Данные системы телеметрии наглядно демонстрируют, что именно в этой стране вредоносный код проявил наибольшую активность (79 % от общего количества обнаружений данной угрозы пришлось на Пакистан).

По информации экспертов Eset, для успешной установки вредоносного ПО злоумышленники применяли несколько векторов атаки. В одном случае использовался эксплойт для широко известной уязвимости CVE-2012-0158, которая может эксплуатироваться с помощью специально сформированного документа Microsoft Office – его открытие на уязвимой системе инициирует исполнение произвольного кода. Как упоминалось выше, такие документы доставлялись потенциальным жертвам по электронной почте. Открывая документ, пользователь незаметно для себя инициировал установку вредоносного ПО.

Другой вектор атаки заключался в рассылке по электронной почте исполняемых вредоносных файлов, которые маскировались под файлы Word или PDF-документы. Для дополнительной маскировки и усыпления бдительности пользователя, во время установки вредоносного ПО действительно отображался документ с определенным содержанием ***(Индийские хакеры воровали данные в Пакистане // InternetUA (http://internetua.com/indiiskie-hakeri-vorovali-dannie-v-pakistane). – 2013. – 21.05).***

***

Conpot позволяет вычислить киберпреступников, которые сканируют IP-адреса SCADA-систем, а затем отслеживают их деятельность.

IT-специалист Л. Рист разработал приманку на хакеров, которые осуществляют нападения на системы объектов критически важной инфраструктуры.

Conpot позволяет вычислить киберпреступников, которые сканируют IP-адреса SCADA-систем, а затем отслеживают их деятельность. Приманка имитирует систему Siemens SIMATIC S7-200, которая подключается к

Интернету через модуль ввода/вывода CP 443-1. Conpot поддерживает два сетевых протокола Modbus и SNMP, которые обычно используются SCADA-системами.

По словам разработчиков, Conpot также совместим с человеко-машинным интерфейсом и графическими пользовательскими интерфейсами, которые используются для контроля над системами управления.

«Главная цель – это сделать подобную технологию доступной для широкой аудитории. Не только для IT-специалистов, но для системных администраторов, работающих с ICS-системами, которые хотят предотвратить кибератаки на свои системы и не хотят подвергать их опасности», – заявил Л. Рист ***(Новая приманка обнаруживает хакеров, атакующих SCADA-системы // InternetUA (http://internetua.com/novaya-primanka-obnarujivaet-hakerov--atakuuasxih-SCADA-sistemi). – 2013. – 20.05).***

***

Как сообщил индийский хакер под ником Godzilla, ему удалось обнаружить несколько брешей в системе безопасности веб-сайта Совета Европы, эксплуатируя которые киберпреступнику удалось получить привилегированный доступ к административной панели сайта, а также к материалам сертификационных курсов, включая CEH v8, CHFI v4, ECSS и ECSA/LPT 4.

Godzilla отмечает, что в случае, если обнаруженным способом воспользуются злоумышленники, они легко смогут получить доступ к стратегически важным информационным системам ведущих стран мира, так как их использует минобороны США, АНБ, ЦРУ НАСА и т. д.

По словам хакера, он указал ведомству на существующие бреши для того чтобы специалисты пересмотрели систему безопасности информационных ресурсов ***(Обнаружены бреши в системе безопасности веб-ресурсов Совета Европы // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2013/05/21/website-flaws.html). – 2013. – 21.05).***

***

Правительство Японии приняло решение создать Войска кибербезопасности, которые будут сформированы из программистов и экспертов по компьютерным сетям.

21 мая 2013 г. Совет по мерам информационной безопасности под председательством генерального секретаря кабинета министров Ё. Суги принял решение создать в составе вооруженных сил Войска кибербезопасности, а также расширить рынок услуг, обеспечивающих защиту компьютерных систем от взлома.

Премьер-министр Японии С. Абэ заявил, что правительство должно создать зону кибернетической деятельности, которая будет совершенно безопасной и достойной страны с первоклассными информационными

стандартами, каковой является Япония. После общественного обсуждения программу планируется реализовать в июне текущего года.

Войска кибербезопасности будут сформированы из программистов и экспертов по компьютерным сетям, которые в первую очередь должны оградить от действий хакеров государственные и оборонные системы. В 2015 г. при правительстве будет также создан Центр кибернетической безопасности, координирующий политику в этой сфере, включая подготовку специалистов ***(Правительство Японии приняло решение создать Войска кибербезопасности // InternetUA (http://internetua.com/pravitelstvo-yaponii-prinyalo-reshenie-sozdat-voiska-kiberbezopasnosti). – 2013. – 22.05).***

***

Администрация социальной сети Twitter объявила о введении двухступенчатой системы проверки подлинности пользователей.

По данным представителей компании, «такой шаг продиктован недавними атаками хакеров на аккаунты агентства Associated Press, телеканалов CNN, Fox News и других известных корпоративных профайлов».

Взломав Twitter агентства Associated Press, хакеры разместили сообщения о том, что президент Б. Обама ранен в результате взрывов в Белом доме. Фондовый рынок США отреагировал на это резким падением. В феврале был взломан микроблог фотоподразделения агентства AFP. Еще больше повезло президенту Венесуэлы Н. Мадуро: его Twitter взломали дважды за месяц.

Отныне система предлагает владельцам страничек кроме логина и пароля вводить дополнительный код, который будет приходить в виде смс-сообщения. Пользователи Twitter могут выбрать новую функцию в настройках дневника, для активации которой следует ввести номер своего мобильного.

«Мы надеемся, что новшество существенно обезопасит наших пользователей», – заметили в компании.

Подобную схему защиты уже используют в Google, Facebook и Microsoft ***(Twitter будет бороться с хакерами // Интернет-обозрение Главное™ (http://glavnoe.ua/news/n137584). – 2013. – 23.05).***

***

Специалист по безопасности раскрыл заговор Facebook и «ВКонтакте»

Социальная сеть «ВКонтакте» изменила процедуру восстановления пароля, скрыв большую часть номера телефона пользователя, чтобы избежать возможного раскрытия личных данных, сообщает «Обозреватель» (http://tech.obozrevatel.com/news/48137-vkontakte-vyishla-iz-sgovora-s-facebook.htm).

Ранее, зная электронную почту пользователя, можно было узнать номер мобильного телефона человека через процедуру восстановления пароля в Facebook и «ВКонтакте». При восстановлении пароля «ВКонтакте» открывал

первые семь цифр номера, а Facebook – последнии четыре, что позволяет составить из них полный номер телефона пользователя.

«Мы изменили процедуру восстановления доступа к аккаунту таким образом, что впредь разбойники не смогут узнать номер телефона его владельца даже благодаря другим, менее защищенным западным сервисам», – заявил пресс-секретарь «ВКонтакте» Г. Лобушкин.

В настоящий момент «ВКонтакте» отображает только две последние цифры номера.

Представители Facebook заявили, что не намерены менять свою систему восстановления пароля.

Напомним, ранее российский специалист по безопасности Д. Евтеев в своем блоге обратил внимание на потенциальную проблему с утечкой личной информации через форму восстановления забытого пароля в Facebook и «ВКонтакте». Он отметил, что соцсети пребывают «в сговоре», показывая разные части номера пользователя, что дает возможность при использовании обеих соцсетей установить номер целиком ***(«ВКонтакте» вышла «из сговора» с Facebook // Обозреватель (http://tech.obozrevatel.com/news/48137-vkontakte-vyishla-iz-sgovora-s-facebook.htm). – 2013. – 23.05).***

***

Twitter-аккаунты одной из крупнейших британских газет Daily Telegraph 21 мая были взломаны активистами из так называемой Сирийской электронной армии, поддерживающей президента Сирии Б. Ассада. Также под каток хакеров попала и страница издателя на Facebook.

Напомним, что ранее аналогичные действия Сирийская электронная армия совершала и в адрес других СМИ, в частности в адрес Financial Times, The Guardian, Associated Press, CBS, Al Jazeera, BBC и сайта The Onion.

Взломанные Twitter-аккаунты содержали пропагандистские заявления в поддержку Б. Ассада, а также ссылки на якобы взломанные другие аккаунты Daily Telegraph в Twitter, в частности @TelegraphArt, @TelegraphFilm, @Tele_Comedy, @TelegraphSport и @TelegraphBooks.

Как сообщили в редакции Daily Telegraph, сейчас контроль над аккаунтами восстановлен ***(Хакеры взломали Twitter-аккаунт газеты Daily Telegraph // МediaБізнес (http://www.mediabusiness.com.ua/content/view/35034/118/lang,ru/). – 2013. – 22.05).***

***

Массовое распространение троянской программы среди пользователей Skype началось 23 мая в странах СНГ, пишет «Обозреватель» (http://tech.obozrevatel.com/news/83406-sng-atakoval-skype-virus.htm).

Распространение происходит путем спам-рассылки сообщения, предлагающего получившему его пользователю перейти по ссылке и посмотреть на фотографию в Facebook.

Переход по ссылке приводит к загрузке с файлообменных сервисов 4shared.com или dropbox.com архива facebook_profile.zip, содержащего вредоносную исполняемую программу под именем profile-facebook_23052013_img.exe.

Типичная фраза, сопровождающая вредоносную ссылку, выглядит как «это очень хорошая фотография вы http://bit.ly/10UCanc?id=XXX», где XXX – Skype-логин получателя. Сообщения с вредоносной ссылкой поступают от пользователей, состоящих в контакт-листе получателя.

По данным «Лаборатории Касперского», в архиве спам-рассылки распространяется вредоносная программа Backdoor.Win32.CPD.phy.

К 15:00 23 мая специалисты «Лаборатории Касперского» обнаружили около 30 разновидностей этого бэкдора и зафиксировали около 1700 его атак более чем в 70 странах мира. Такое число инцидентов позволяет назвать атаку широкомасштабной.

Распространяемый в ходе атаки бэкдор служит для загрузки на зараженный компьютер другого трояна – Trojan.Win32.Yakes.csli. Он, в свою очередь, служит для рассылки вредоносных ссылок по контакт-листам мессенджеров Skype, Windows Messenger, QIP, Google Talk и Digsby ***(СНГ атаковал Skype-вирус // Обозреватель (http://tech.obozrevatel.com/news/83406-sng-atakoval-skype-virus.htm). – 2013. – 24.05).***

***

Литовский портал сети DELFI (Delfi.lt) подвергся хакерской атаке из-за статьи, посвященной предполагаемой скупке голосов за российскую участницу конкурса «Евровидение». В результате он стал недоступен для читателей. Об этом сообщает портал DELFI в соседней Латвии (Delfi.lv).

По информации источника, во второй половине 22 мая, редакция Delfi.lt получила электронное письмо с угрозами. В письме (на русском языке) утверждалось, что на сайте размещена статья, которая «не отвечает действительности, порочит имидж России и нашей соотечественницы Д. Гариповой». Авторы письма требовали удалить данный материал в течение часа. В противном случае они угрожали «принять радикальные меры».

Через час после этого портал стал недоступным. Как заявил глава отдела ИТ К. Шяулис, «это явная DDoS-атака, подключались из разных стран – Турции, России, Японии, Бразилии. Эти компьютеры объединены в так называемый ботнет».

В этой ситуации Delfi.lt, как сообщается, обратился в кибернетическую полицию Литвы, а также в Службу регулирования связи.

На момент написания данной заметки портал оставался недоступным.

Указанная статья была опубликована на Delfi.lt несколько дней назад. В ней утверждалось, что некие русскоязычные мужчины проводили скупку голосов прибалтов в пользу конкурсантки «Евровидения» от России Д. Гариповой. По утверждению источника, схема заключалась в том, чтобы собрать группы людей, у каждого из которых будет по несколько мобильных

телефонов. После голосования участникам якобы обещали по 20 евро. Была опубликована также запись телефонного разговора, в ходе которого обсуждалась данная тема.

О том, что в Литве по аналогичной схеме проводилась скупка голосов в пользу другого участника «Евровидения» (представителя Азербайджана) сообщал портал 15min.lt. В подтверждение источник опубликовал видеозапись беседы со «скупщиками», сделанную скрытой камерой. Между тем прокуратура Литвы, изучив предоставленные журналистами материалы, заявила, что «оснований для досудебного расследования нет» ***(Хакеры отомстили за статью о «пророссийских» махинациях на «Евровидении» // InternetUA (http://internetua.com/hakeri-otomstili-za-statua-o--prorossiiskih--mahinaciyah-na--evrovidenii). – 2013. – 23.05).***

***

«Лаборатория Касперского» представила новый сервис по расследованию компьютерных инцидентов, призванный помочь компаниям вовремя выявить сам инцидент, локализовать его распространение, а также произвести пост-анализ для восстановления хронологии событий, выявления использованных инструментов и идентификации злоумышленников.

Создание вредоносного программного обеспечения давно превратилось из обычного хулиганства в многомиллионный преступный бизнес. Целевые атаки на компании, охота за ценной конфиденциальной информацией, DDoS-атаки, мошенничество в системах дистанционного банковского обслуживания приобрели повсеместный характер. Противостоять такого рода атакам, за которыми стоят преступники с продвинутыми техническими знаниями и сильной финансовой мотивацией, способные быстро менять стратегию и методы нападения, – непросто. Поэтому для того чтобы принять удар и устоять на ногах, предприятиям необходимо не только использовать превентивные средства защиты от инцидентов, но и иметь наготове эффективные механизмы реагирования на них.

Как говорится в заявлении компании, сервис «Лаборатории Касперского» предусматривает три последовательных этапа выполнения необходимых работ для устранения рисков, связанных с компьютерным инцидентом: оперативный анализ компьютерного инцидента, расследование его и экспертное сопровождение уголовного дела.

На первом этапе специалисты «Лаборатории Касперского» проводят оперативный анализ происшествия, помогая пострадавшей компании понять ситуацию и взять ее под контроль. Эксперты восстанавливают возможную картину произошедшего, устанавливают, какие именно узлы IT-инфраструктуры были вовлечены в инцидент, фиксируют цифровые свидетельства. В ходе дальнейшего анализа проводятся исследование первичной информации об инциденте и полный анализ вредоносного ПО. На основе этих данных компания получает отчет, содержащий результаты исследования, а также рекомендации по устранению последствий случившегося

инцидента. Документ может служить достаточным основанием для обращения в правоохранительные органы с целью проведения необходимых проверок по данному направлению.

Следующий этап предусматривает расследование, которое позволяет получить, а также проанализировать все технические и финансовые аспекты произошедшего инцидента, установить схему преступления, определить лиц, причастных к инциденту, и подготовить данные, подтверждающие эти факты. По итогам расследования, проводимого силами специалистов «Лаборатории Касперского», компания получает подробный отчет о компьютерном инциденте, который может быть использован правоохранительными органами для проведения доследственной проверки и расследования в рамках уже возбужденного уголовного дела.

В случае возбуждения уголовного дела «Лаборатория Касперского» готова оказывать экспертную поддержку пострадавшей от преступления компании. На этом этапе специалисты «Лаборатории Касперского» могут выступать в качестве представителя пострадавшей организации, оказывают всю необходимую информационную и техническую поддержку расследованию уголовного дела, а также проводят консультации правоохранительным органам по результатам расследования, проведенного ранее «Лабораторией Касперского» ***(«Лаборатория Касперского» открыла сервис по расследованию компьютерных инцидентов // InternetUA (http://internetua.com/laboratoriya-kasperskogo--otkrila-servis-po-rassledovaniua-kompuaternih-incidentov). – 2013. – 23.05).***

***

Компания «Доктор Веб» обнаружила новую вредоносную программу для платформы Android, способную перехватывать входящие СМС-сообщения и перенаправлять их злоумышленникам. Троянец Android.Pincer.2.origin представляет весьма серьезную опасность для пользователей, т. к. в украденных им сообщениях могут находиться в том числе и проверочные mTAN-коды, которые используются различными финансовыми системами типа «Банк-Клиент» для подтверждения денежных операций, а также другая конфиденциальная пользовательская информация.

Троянец, обнаруженный специалистами несколько дней назад, является вторым известным представителем семейства Android.Pincer. Как и ее предшественник, обновленная вредоносная программа распространяется под видом сертификата безопасности, который якобы требуется установить на мобильное Android-устройство. В случае если неосторожный пользователь выполнит установку и попытается запустить троянца, Android.Pincer.2.origin продемонстрирует ложное сообщение об успешной установке сертификата, после чего до поры до времени не будет проявлять сколько-нибудь заметной активности.

Чтобы загружаться вместе с операционной системой, троянец регистрирует системный сервис CheckCommandServices, который в

дальнейшем работает в качестве фоновой службы. В случае успешного старта при очередном включении мобильного устройства Android.Pincer.2.origin подключается к удаленному серверу злоумышленников и загружает на него ряд сведений о мобильном устройстве. Среди них:

– название модели;

– серийный номер устройства;

– IMEI-идентификатор;

– название используемого оператора связи;

– номер сотового телефона;

– язык, использующийся по умолчанию в системе;

– версия операционной системы;

– информация о том, имеется ли root-доступ.

Далее вредоносная программа ждет поступления от злоумышленников управляющего СМС-сообщения с текстом вида «command: [название команды]», содержащего указание к дальнейшим действиям. Киберпреступниками предусмотрены следующие директивы:

– start_sms_forwarding [номер телефона] – начать перехват сообщений с указанного номера;

– stop_sms_forwarding – завершить перехват сообщений;

– send_sms [номер телефона и текст] – отправить СМС с указанными параметрами;

– simple_execute_ussd – выполнить USSD-запрос;

– stop_program – прекратить работу;

– show_message – вывести сообщение на экран мобильного устройства;

– set_urls – изменить адрес управляющего сервера;

– ping – отправить СМС с текстом pong на заранее указанный номер;

– set_sms_number – изменить номер, на который уходит сообщение с текстом pong.

Команда start_sms_forwarding представляет особенный интерес, т. к. позволяет злоумышленникам указывать троянцу, сообщения с какого номера ему необходимо перехватить. Данная функция дает возможность использовать вредоносную программу как инструмент для проведения таргетированных атак и красть, таким образом, специфические СМС-сообщения, например сообщения от систем «Банк-Клиент», содержащие проверочные mTAN-коды, либо конфиденциальные СМС, предназначенные для самых разных категорий лиц: от простых пользователей до руководителей компаний и государственных структур ***(Новый Android-вредонос ворует SMS // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2013/05/23/sms-stealing-malware.html). – 2013. – 23.05).***

***

Журналисты американского издания Scripps News провели настоящее расследование и обнаружили на серверах телекоммуникационных компаний TerraCom и YourTel America персональные данные более чем 170 тыс. граждан,

получавших государственные субсидии на мобильную связь, в том числе бесплатные мобильные телефоны. В открытом доступе лежали их имена, номера социального страхования, даты рождения и информация об участии в программе.

Результаты своего расследования журналисты опубликовали в статье на сайте Scripps News. Статья вызвала большой резонанс. Вместо благодарности за обнаруженную уязвимость, издание получило угрозы со стороны телекоммуникационных компаний, которые обвиняют их в несанкционированном доступе к информации и нарушении закона Computer Fraud and Abuse Act. Теперь журналисты могут пойти под суд.

Самое смешное, что репортеры нашли персональные данные пользователей через поиск в Google, они не использовали каких-то специальных методов для взлома. В письме от телекоммуникационных компаний сказано, что злоумышленники использовали «хакерскую» программу Wget – стандартную утилиту для массового скачивания файлов ***(Журналисты обнаружили уязвимость, теперь пойдут под суд как хакеры // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2013/05/23/reporters-use-google-find-breach-get-branded-as-hackers.html). – 2013. – 23.05).***

***

Компания Bitdefender, известная своими антивирусными решениями, представила новый бесплатный продукт для мобильной платформы Android под названием Clueful («Осведомленность»). Главная функция пакета Clueful заключается в защите пользователей от посягательств на тайну частной жизни. В частности, технология Clueful позволяет предупредить пользователя о подозрительном или некорректном поведении приложений. В частности, утилита Clueful помогает отследить раскрытие личных данных в свободный доступ, доставку спама и несанкционированный доступ к сугубо личной информации.

Совершенно бесплатно утилита Bitdefender Clueful для Android обеспечивает мониторинг и анализ Android-приложений, обнаруживая несанкционированный доступ личной информации или отправку личных данных наружу. Также отслеживаются попытки отправки спама, доступ к фотографиям, отправка личных паролей в незашифрованном виде, отправка календарей на посторонние ресурсы, прерывание телефонных разговоров звуковой рекламой и другие виды вмешательства в жизнь пользователя.

Разработчики утилиты Clueful утверждают, что их продукт содержит уникальные алгоритмы для анализа поведения приложений. Например, утилита Clueful сопоставляет действия приложения с фирменной постоянно обновляемой базой данных Bitdefender Cloud, чтобы понять, в каком случае личные данные могут оказаться под угрозой. Кроме того, утилита Clueful выполняет проверку при установке каждого нового приложения. С каждым

новым анализом обновляется общий рейтинг безопасности устройства (Privacy Score) с точки зрения уязвимости личной информации.

Значение утилиты Clueful трудно переоценить в современном мире, где утечка любых частных данных может в итоге привести к серьезным рискам – от финансовых потерь до нарушения тайны частной жизни. Отдельную ценность этому продукту придает тот факт, что его выпустила та же компания, что разработала одну из лучших систем безопасности для Android: Bitdefender Mobile Security. Официальное представление утилиты Bitdefender Clueful для Android состоялось 21 мая – с этого дня продукт официально доступен в магазине приложений Play Маркет ***(Clueful от BitDefender – защита приватности пользователей на платформе Android // InternetUA (http://internetua.com/Clueful-ot-BitDefender---zasxita-privatnosti-polzovatelei-na-platforme-Android). – 2013. – 24.05).***

***

Эксперты мира IT всё чаще склоняются к мысли, что в последнее время DDoS-атаки из средства нападения на сайты и сервера превращаются в распространителя вирусов.

К такому выводу эксперты компании Prolexic, занимающейся изучением современных методов хакерской войны и разработкой мер противостояния им пришли, проанализировав крупные DDoS-атаки, которым в этом году подверглись многие СМИ.

Кроме того, изучив ряд нападений на финансовые структуры США, эксперты пришли к выводу, что вместе с проведением крупных атак, хакеры, использующие DDoS всё чаще рассылают в спам-сообщениях отдельные вредоносные программы.

Таким образом, DDoS-атака сопровождается не только перегрузкой трафика, но и распространением вредоносного программного обеспечения. Согласно мнению экспертов, такое решение выглядит весьма разумным для хакеров. Пока компании пытаются противостоять DDoS, куда больше хаоса в работу вносят вирусные нападения, засоряющие сервера и провоцирующие отказ в работе. В ходе такой атаки IT-специалисту сложнее противостоять злоумышленникам.

Согласно выводам отчёта Prolexic, современные компании должны озаботиться мерами по изоляции атакованных компонентов. Это обеспечит защиту от попадания в систему вредоносных программ, скрывающихся в спам-данных ***(DDoS-атаки превращаются в инструмент для распространения вирусов // InternetUA (http://internetua.com/DDoS-ataki-prevrasxauatsya-v-instrument-dlya-rasprostraneniya-virusov). – 2013. – 24.05).***

***

Выступая на конференции AusCERT 2013, HD Moore, разработчик Metasploit, обвинил в халатности поставщиков встроенных систем. По его

мнению, именно они ставят под угрозу кибербезопасность компьютерных сетей.

HD Moore заявил, что в то время, как системные администраторы достойно выполняют свою работу по защите систем, они не могут справиться с угрозами, которые несут в себе модемы, маршрутизаторы, телефоны и прочее, потому что производители встроенных систем «в целом не заботятся о кибербезопасности».

На конференции Moore представил результаты масштабного сканирования адресного пространства IPv4, учитывая TCP и UDP-сервисы, что позволило ему обнаружить большое количество уязвимостей.

Разработчик заявил, что он возмущен тем фактом, как производители незащищенных встроенных систем предоставляют их пользователям, и даже при наличии известных уязвимостей отказываются исправлять их.

Наборы сетевых протоколов UPnP, которые пользуются популярностью, также очень уязвимы, и 63 % устройств, работающих с UPnP, общедоступны, что также ставит их под угрозу.

Moore заявил, что большие проблемы существуют в цепочке поставок встроенных систем: их отправляет один поставщик, модуль настраивается другой компанией, интеграция в готовую версию системы проводится третьей, а маркируется – четвертой. При этом, ни одна из компаний не намерена защищать своих конечных пользователей.

«Пока не случится действительно неприятный инцидент безопасности, ничего исправлено не будет», – подытожил Moore ***(Поставщики встроенных систем ставят под угрозу кибербезопасность // InternetUA (http://internetua.com/postavsxiki-vstroennih-sistem-stavyat-pod-ugrozu-kiberbezopasnost). – 2013. – 24.05).***

***

Как сообщил изданию the Washington Post один из бывших американских чиновников, пожелавший остаться неизвестным, атака на серверы интернет-компании Google в 2010 г., получившая название Aurora, спровоцировала утечку важных конфиденциальных данных.

Китайские хакеры, причастные к нападению, получили несанкционированный доступ к списку целей, за которыми на протяжении нескольких лет наблюдали спецслужбы США.

Более того, источник издания отмечает, что за проведением атаки могли стоять лица, находящиеся под наблюдением американских силовых структур.

По словам чиновника, до сих пор остается неизвестным, какой объем данных удалось заполучить киберпреступникам, однако он отмечает, что хакеры получили ценную информацию, включая базу данных судебных ордеров и постановлений, необходимых для организации наблюдения, в результате которого спецслужбы США могли бы обвинить в промышленном шпионаже китайских агентов, использующих электронную почту Gmail от Google.

«Знание того, что они являются субъектами расследования, позволило подозреваемым предпринять необходимые шаги, уничтожить компрометирующие данные, или даже уехать из страны», – отмечает собеседник the Washington Post ***(Взлом серверов Google в 2010 г. спровоцировал потерю важных данных американской разведки // InternetUA (http://internetua.com/vzlom-serverov-Google-v-2010-godu-sprovociroval-poterua-vajnih-dannih-amerikanskoi-razvedki). – 2013. – 24.05).***

***

Компания «Доктор Веб» сообщила о появлении в бот-сети Rmnet двух новых вредоносных модулей. Один из них позволяет злоумышленникам отключать установленные на инфицированном компьютере антивирусные программы. Кроме того, специалистам «Доктор Веб» удалось перехватить управление одной из подсетей Rmnet, в которой действуют эти вредоносные компоненты.

Вредоносные программы семейства Win32.Rmnet представляют собой многокомпонентные файловые вирусы, обладающие возможностью самостоятельного распространения. Вирус состоит из нескольких модулей, его основной вредоносный функционал позволяет встраивать в просматриваемые веб-страницы посторонний контент, перенаправлять пользователя на указанные злоумышленниками сайты, а также передавать на удаленные узлы содержимое заполняемых жертвой форм. Кроме того, вирусы семейства Rmnet способны красть пароли от популярных FTP-клиентов, таких как Ghisler, WS FTP, CuteFTP, FlashFXP, FileZilla и Bullet Proof FTP.

Специалистам «Доктор Веб» удалось перехватить еще одну подсеть Win32.Rmnet с использованием известного метода sinkhole. В этой подсети был установлен факт распространения двух новых вредоносных модулей, получивших общее обозначение Trojan.Rmnet.19. Один из них предназначен для детектирования на инфицированном компьютере виртуальных машин, зато второй представляет значительно больший интерес. Эмулируя действия пользователей (а именно нажатия на соответствующие значки мышью), данный компонент отключает на инфицированной машине антивирусы Microsoft Security Essential, Norton Antivisus, Eset NOD32, Avast, Bitdefender, AVG.

Если на компьютере используется антивирусное ПО Dr.Web, пользователю ничто не угрожает: для выгрузки компонентов антивируса требуется ввести капчу, а с этой задачей Trojan.Rmnet.19 справиться не в состоянии.

Всего в данной подсети вирус загружает с управляющего сервера на инфицированный компьютер семь вредоносных модулей:

– новый модуль, позволяющий отключать антивирусные программы;
– модуль для кражи файлов Cookies;
– локальный FTP-сервер;
– модуль для выполнения веб-инжектов;
– модуль для кражи паролей от FTP-клиентов;

– новый модуль, позволяющий детектировать наличие виртуальных машин;

– модуль для организации удаленного доступа к инфицированной системе.

Помимо этого, файловые вирусы семейства Rmnet содержат компонент для загрузки других модулей в память, модуль бэкдора, модуль для удаления антивирусных программ ***(Обнаружен новый компонент бот-сети Rmnet, отключающий антивирусные программы // InternetUA (http://internetua.com/obnarujen-novii-komponent-bot-seti-Rmnet--otkluacsauasxii-antivirusnie-programmi). – 2013. – 26.05).***

***

24 мая некоторые пользователи популярной соцсети Instagram запускали приложение и с прискорбием обнаруживали, что их аккаунты были удалены по причине «нарушений правил сервиса». При этом никто не потрудился им объяснить, какие конкретно правила были нарушены.

Вряд ли проблема связана с тем, что пользователи публиковали слишком много снимков (к примеру, в Twitter могут временно заблокировать аккаунт, если публиковать слишком много твитов в единицу времени). Скорее всего, проблема имела техническую природу и обладала произвольным характером: удалялись даже те аккаунты, которыми не пользовались уже достаточно давно.

Тем не менее несколько часов спустя инцидент был разрешен, аккаунты были восстановлены и пользователи вновь получили доступ к ним. Интересно, что сам Instagram никак не прокомментировал эту ситуацию и не извинился перед теми, у кого удалялись аккаунты ***(Instagram ненадолго сошел с ума // InternetUA (http://internetua.com/Instagram-nenadolgo-soshel-s-uma). – 2013. – 26.05).***

***

Новый информационный бюллетень от eScan посвящен новым тенденциям и сферам интересов в хакерской среде. На сей раз речь идет об атаках на гостиничный бизнес. Хакеров, ищущих способы быстрой наживы, все больше привлекает гостиничная индустрия – в последнее время на отели стали нападать даже чаще, чем на кафе и рестораны, которые долгое время были излюбленной мишенью киберпреступников. Это смещение акцентов показывает более целенаправленный подход хакеров, а не просто использование ими незапланированных и случайных атак.

По данным экспертов eScan, 40 % всех успешных атак приходится на отели и курорты, что говорит о их недостаточной защищенности. Как следствие, добычей злоумышленников могут стать персональные данные гостей отеля, номера их кредитных карт, а также другая конфиденциальная информация. Последствия утечки информации могут быть очень серьезными: значительные финансовые потери, утрата доверия клиентов, критически важной информацией могут завладеть конкуренты.

В качестве примера можно привести известную сеть отелей Marriott International Inc., которой потребовался 1 млн дол. для покрытия расходов, связанных со взломом информационной системы. Помимо понесенных финансовых потерь, компании Marriott International пришлось потратить немало усилий для того, чтобы восстановить испорченную репутацию, которая в индустрии гостеприимства порой дороже денег.

Метод, который наиболее часто применяется при взломе информационных систем отелей – это атака на приложения с использованием удаленного доступа, сообщают аналитики компании eScan MicroWorld. Во время таких атак часто задействуются веб-каналы, созданные внутренними ИТ-специалистами или ИТ-аутсорсерами. Такие системы бывают слабо защищены от внешних атак и доступ в них предоставляется без применения политики паролей, либо по легко угадываемым паролям. Другие часто используемые хакерские методы включают SQL-инъекции и атаки типа «человек посередине» (MITM, Man-In-the-Middle).

Последствиями угроз могут быть не только поврежденные файлы и компьютеры, выступающие в качестве вирусных агентов, но также потери производительности, уменьшение дискового пространства, излишне потраченное время и финансовые ресурсы. По иронии судьбы, как раз в то время, когда были разработаны методы защиты контента, угрозы информационной безопасности стали еще более серьезными, приводя иногда и к уничтожению данных. Однако системы, используемые для обнаружения этих угроз, по-прежнему страдают рядом недостатков.

«Лечение, предоставляемое некоторыми продуктами, заключается в сканировании данных после их сохранения на жестком диске, но к этому времени ущерб уже нанесен. В отличие от них, технология MicroWorld-WinSock Layer (MWL), реализованная в продуктах eScan, нейтрализует угрозы на сетевом уровне, когда они еще не могут достичь приложений на компьютере. Эту концепцию сканирования интернет-трафика можно назвать революционной», – заявил Г. Раммурти, генеральный и управляющий директор компании eScan MicroWorld ***(Отели становятся легкой добычей для хакеров // InternetUA (http://internetua.com/oteli-stanovyatsya-legkoi-dobicsei-dlya-hakerov). – 2013. – 25.05).***

***

Эксперты антивирусной компании Sophos сообщили об обнаружении нового интернет-мошенничества, в результате которого злоумышленники похищают учетные данные для доступа жертв в Twitter, историю браузера и другие важные данные.

Оказалось, что киберперступники решили использовать механические опечатки пользователей, которые пытаются авторизоваться в российской соцсети «ВКонтакте», а также используют невнимательность тех, кто пытается найти в крупнейшей российской соцсети европейских и американских знаменитостей.

Хакеры создали поддельный ресурс с адресом Vikontakte.net, который открывает страницу входа в другую популярную соцсеть – Twitter.

Внешний вид страницы оказался полностью идентичным странице авторизации в Twitter, однако адресная строка утверждает, что пользователь пытается зайти на сайт Vikontakte.net.

Если жертва все-таки упустила из виду такое несоответствие, она перенаправляется на ресурс в доменной зоне .SU, которая принадлежала распавшемуся в 1991 г. Советскому Союзу ***(Фишеры используют адрес Vikontakte для кражи учетных данных пользователей Twitter // Securitylab (http://www.securitylab.ru/news/440632.php). – 2013. – 24.05).***

***

Согласно данным отчета, который представила компания IP Commission, ежегодно хищение интеллектуальной собственности наносит США ущерб в размере 300 млрд дол. Как утверждают эксперты организации, 50–80 % от общего объема пиратства приходится на Китай.

В IP Commission говорят, что необходимо принять жесткие меры, чтобы сделать кражу интеллектуальной собственности экономически непривлекательной.

Эксперты организации также подчеркивают, что кроме Китая в число государств, ответственных за пиратство, осуществляемое в США, входят Россия, Индия и Украина. Аналитики объясняют, что в этих странах даже в крупных компаниях зачастую используется краденная интеллектуальная собственность, в том числе пиратское программное обеспечение.

В основном, пиратство осуществляется через подкуп сотрудников и обратную разработку. Кроме того, активно используется кибершпионаж.

Ранее власти США неоднократно называли кибершпионаж со стороны Китая одной из основных угроз национальной безопасности государства. А в мае 2013 г. Торговое представительство США назвало Украину наиболее опасной страной с точки зрения пиратства ***(Ежегодно интернет-пиратство наносит США ущерб в размере 300 млрд дол. // Securitylab (http://www.securitylab.ru/news/440614.php). – 2013. – 24.05).***