СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(18.02–3.03)

2013 № 5

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(18.02–3.03)
№ 5

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

Головний редактор
О. Онищенко, академік НАН України

Редакційна колегія:
В. Горовий (заступник головного редактора, науковий керівник проекту),
В. Касаткін, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2013

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Социальная сеть Facebook намерена ввести систему фильтрации в поисковую систему сайта, которая будет скрывать профили подростков, если поиск производится взрослым пользователем.

Владельцы ресурса рассчитывают, что новые ограничения помогут оградить несовершеннолетних пользователей от педофилов и злоумышленников, пишет Comments.UA.

Фильтр в ближайшее время может появиться в новом «социальном поисковике» Facebook Social Graph, который в начале этого года запустил американский интернет-гигант.

Social Graph, по словам основателя ресурса М. Цукерберга, обещает стать третьим, вслед за новостной лентой и разделом Timeline, ключевым элементом крупнейшей соцсети мира.

Эта функция позволяет совмещать традиционный онлайн-поиск с социальными данными от друзей и «друзей друзей».

«Думаю, эта система поможет расширить связи между пользователями соцсети и компаниями, – рассказал в интервью Би-би-си аналитик компании Ovum М. Литтл. – Чем больше контактов, тем проще рекламодателям находить свою целевую аудиторию».

Однако вскоре внимание пользователей и правозащитников привлек один ключевой элемент этой системы: новый алгоритм позволяет совмещать социальные, географические и многие другие данные о пользователях.

Например, по ключевым словам «бадминтон» и «Санкт-Петербург» можно найти список петербуржцев, увлекающихся бадминтоном. Но точно также любой желающий может получить список «17-летних девушек», находящихся по соседству.

Руководство компании, однако, заверило, что они очень серьезно относятся к всему, что касается возраста пользователей. Если возникнут подозрения, что возраст пользователя указан неверно, аккаунт будет заблокирован до тех пор, пока его владелец не предоставит официальный документ с датой рождения.

Проведенный по просьбе Би-би-си проверочный поиск учащихся одной из британских школ показал, что фильтр выполняет свою функцию: в результатах отобразились лишь взрослые выпускники школы и совершеннолетние школьники ***(Facebook сделает так, чтобы взрослые не смогли найти подростков // From-UA (http://www.from-ua.com/news/016e8cc92d86c.html). – 2013. – 18.02).***

***

Yahoo! может стать социальной сетью.

В интервью Bloomberg News М. Майер, гендиректор Yahoo!, рассказала о стратегических планах компании. В частности, сказала она следующее: «Обмен информацией (между пользователями) должен быть встроен в наши продукты в качестве базового компонента. Желание делиться своими

интересами с друзьями – это одна из тех вещей, которые люди действительно хотят делать».

Эксперты из Wired тут же решили, что речь идет о фундаментальных переменах в стратегии Yahoo!. Понять слова М. Майер иначе, чем «мы собираемся стать социальной сетью», довольно трудно. Каким образом функционал, позволяющий «делиться интересами с друзьями», тогда станет базовым компонентом?

Пока что компания укрепляет связи с Facebook. После судебного иска в начале прошлого года (Yahoo! хотела отсудить у Facebook кнопку Like), при М. Майер два интернет-гиганта перешли к разговорам о сотрудничестве. Обмен пользовательскими данными между аккаунтами в Yahoo! и Facebook теперь довольно сильно развит, и М. Майер собирается и дальше действовать в том же направлении. В планах – создание общей поисковой системы. А ведь в 2006 г. Yahoo! чуть не купила Facebook, предложив стартапу 1 млрд дол., но получила отказ.

Другой попыткой стать социальной сетью, которую теперь можно смело признать неудачной, стала покупка Flickr. Теперь фотосайт тонет вместе с Yahoo!, а его ниша занята Instagram и другими приложениями, ориентированными в первую очередь на мобильный рынок.

А основное стратегическое направление, по М. Майер, это как раз «мобилизация» основного портала Yahoo!. На сегодняшний день почта и другие сервисы недостаточно хорошо адаптированы к мобильной среде. М. Майер собирается сократить количество онлайн-приложений для пользователей, но сделать работу с почтой удобной для пользователей смартфонов ***(Yahoo! может стать социальной сетью // InternetUA (http://internetua.com/Yahoo--mojet-stat-socialnoi-setua). – 2013. – 17.02).***

***

Facebook анонсував вихід нового, повністю переписаного Like Box plugin – який завантажується в чотири рази швидше. Така швидкість завантаження досягатиметься за рахунок меншої кількості компонентів, менше CSS та асинхронного завантаження JavaScript.

Так, Like Box plugin у найпростішому варіанті без стрічки новин та без аватарок прихильників завантажуватиметься за 0,51 с. порівняно з приблизно 2,3 с. для старої версії, кількість завантажуваних джерел при цьому зменшиться з 15 до 4.

Якщо ж плагін відображатиме аватарки прихильників, швидкість завантаження становитиме 0,75 с. проти 2,4 с., кількість завантажуваних джерел зменшиться з 25 до 13 ***(Лайкати тепер можна буде значно швидше // UkrainianWatcher (http://watcher.com.ua/2013/02/27/laykaty-teper-mozhna-bude-znachno-shvydshe/). – 2013. – 27.02).***

***

Google+ запустив свою систему логінення для сайтів та мобільних додатків.

При логіні через Google+ Sign-in ви зможете вказувати які дані із соціальної мережі сторонній сервіс може отримувати і хто з ваших друзів буде бачити вашу активність у цьому сервісі. Також підтримується дворівнева верифікація.

Керувати сервісами, до яких ви залогінились через Google+ Sign-in, та їхніми дозволами ви можете на сторінці plus.google.com/apps або в мобільному додатку Google Settings на Android. Якщо ви залогінитеся на якись сайт за допомогою Google+ Sign-in, ви зможете встановити собі його мобільний додаток в один клік ***(Google+ запустив свою систему логінення для сайтів та мобільних додатків // UkrainianWatcher (http://watcher.com.ua/2013/02/27/google-zapustyv-svoyu-systemu-lohinennya-dlya-saytiv-ta-dodatkiv/). – 2013. – 27.02).***

***

Керівники груп «ВКонтакте» матимуть різні рівні доступу.Соціальна мережа «ВКонтакте» оновила адмінпанель для пабліків – публічних сторінок, які набули популярності за останні два роки.

Відтепер власники пабліків можуть змінювати ролі тих користувачів, що мають доступ до керування сторінкою – їх тепер три: Модератор, Редактор і Адміністратор. Модератор може видаляти додані користувачами матеріали, керувати чорним списком спільноти, Редактор – писати від імені спільноти, додавати, видаляти і редагувати контент, оновлювати головну фотографію, а Адміністратор – може призначати і знімати адміністраторів, змінювати назву та адресу спільноти. Окрім того, існує єдиний статус Творця сторінки, який неможливо змінити.

Нагадаємо, за кілька місяців почне свою роботу офіційна біржа рекламних постів на «ВКонтакте», яка зведе інтереси пабліків та рекламодавців і дозволить офіційно продавати рекламу в спільнотах ***(Google+ запустив свою систему логінення для сайтів та мобільних додатків // UkrainianWatcher (http://watcher.com.ua/2013/02/26/vkontakti-onovyv-adminku-publichnyh-storinok/). – 2013. – 26.02).***

***

Сооснователь Facebook Э. Саверин назвал главным риском социального гиганта стремительные темпы ее роста вместе с потребностью объяснять нормы приватности ресурса пользователям и регуляторам, передают РИА Новости.

Отмечается, что аудитория Facebook превысила миллиард пользователей. Новые правила приватности и нормы использования соцсети, как правило, негативно воспринимаются подписчиками сервиса. Последние зачастую опасаются утечки своей персональной информации маркетологам.

Аналогичные претензии к Facebook есть у и регуляторов рынка. Так, в минувшем году соцсеть обещала запрашивать согласие юзеров на изменения в настройках приватности, а также согласилась на проверки регуляторов на протяжении 20 лет.

Несмотря на то, что рост компании является «крупным активом», он может спровоцировать недопонимание, подчеркнул Э. Саверин на конференции The Wall Street Journal в Сингапуре. «Расти слишком быстро – это большой риск. Когда вы растете слишком активно, сложно взаимодействовать (с пользователями), обучать», – убежден он.

«Facebook регулярно сталкивается с разнообразными угрозами. На рынке есть много технологических компаний с выдающимися ресурсами, разработками, талантливыми и опытными сотрудниками, которые стараются занять свою нишу», – отметил Э. Саверин.

Напомним, что до этого глава соцсети М. Цукерберг сообщал о намерениях увеличить корпоративные расходы примерно на 50 % в 2013 г. для расширения штата и выпуска новых продуктов для рекламодателей.

Отметим, что Э. Саверин родился в Бразилии, но вырос и учился в США. В Гарвардском университете он познакомился с М. Цукербергом и оказался одним из сооснователей Facebook. Считается, что именно Э. Саверин предоставил стартовый капитал, нужный для создания соцсети, однако потом он перестал принимать активное участие в ее работе. По сведениям WSJ, Саверину изначально принадлежала треть соцсети, а после ряда формальных операций и первичного публичного размещения акций Facebook его доля уменьшилась до 2 % ***(Сооснователь Facebook назвал главный риск социальной сети // Минфин (http://minfin.com.ua/2013/02/22/723425/). – 2013. – 22.02).***

***

Месячная аудитория фотосервиса Instagram превысила отметку в 100 млн пользователей. Об этом сообщается 26 февраля в блоге Instagram, передает «Лента.ру».

Таким образом, за месяц активная аудитория Instagram возросла на 10 млн человек. В середине января фотосервис впервые раскрыл информацию о месячной аудитории, но ни тогда, ни позже не приводил информацию о том, как много людей пользуются Instagram ежедневно.

Как указано на странице пресс-центра Instagram, каждый день пользователи сервиса загружают по 40 млн фотографий. Кроме того, каждую секунду они оставляют тысячу комментариев и ставят по 8500 «лайков».

Instagram был куплен социальной сетью Facebook в апреле 2012 г. Спустя несколько месяцев фотосервис, существовавший только в виде мобильного приложения, запустил собственную веб-версию и отказался от интеграции в Twitter.

Приложение позволяет обрабатывать снимки с помощью встроенных фотофильтров и выкладывать их в соцсети. По состоянию на март 2012 г.

Instagram скачали 30 млн человек. 100-миллионную аудиторию фотосервис набрал примерно за 2,5 года: первая версия приложения появилась в октябре 2010 г.

Как сообщал «Обозреватель», Instagram впервые раскрыл месячную аудиторию сервиса в 20-х числах января 2013 г. ***(Аудитория Instagram увеличилась до 100 млн в месяц // Обозреватель (http://finance.obozrevatel.com/advertising/52869-auditoriya-instagram-uvelichilas-do-100-mln-v-mesyats.htm). – 2013. – 27.02).***

***

Операторы мобильной связи отдельных стран упрощают доступ абонентов с мобильных устройств к Facebook Messenger.

Около 20 операторов мобильной связи из 14 стран будут предоставлять своим абонентам доступ к сервису обмена сообщениями Facebook Messenger с мобильных устройств бесплатно или со значительными скидками.

В рамках соглашения, о котором объявила соцсеть, пользователи смогут бесплатно или со скидками на трафик обмениваться сообщениями через приложения Facebook Messenger для платформ Android и iOS, а также через приложение Facebook для бюджетных телефонов, оптимизированное для чатов.

Предложение будет действительно у 18 операторов в 14 странах мира, включая Three в Ирландии, Smart на Филиппинах, Oi в Бразилии, Airtel и Reliance в Индии, Tre в Италии и др. В Facebook не уточняют о планы расширения программы партнерства на другие страны и с другими операторами.

Число пользователей крупнейшей в мире соцсети Facebook превышает 1 млрд, более 600 млн пользуются мобильными сервисами компании. По данным компании, функция обмена сообщениями доступна сегодня на более чем 6 тыс. моделей мобильных телефонов, как через специально разработанные приложения, так и через мобильную версию соцсети.

Напомним, что Facebook занялся тестированием возможности обмена голосовыми сообщениями. Новая функция уже доступна американским и канадским пользователям клиентов под iOS и Android. Для отправки голосовых сообщений используется интернет-протокол VoIP. Впрочём, общение происходит не в реальном времени как при разговоре по телефону. Процедура куда больше напоминает функцию Voice Mail. Предположительно, возможность обычного разговора появится позднее. Так же как и функция отправки SMS на обычные номера ***(Facebook Messenger в отдельных странах станет бесплатным // InternetUA (http://internetua.com/Facebook-Messenger-v-otdelnih-stranah-stanet-besplatnim). – 2013. – 28.02).***

***

Шесть новых социальных сетей.

Предложение превышает спрос. Социальная сеть стала неотъемлемой частью жизни для многих людей. Именно поэтому, разработчиков и стартаперов не покидают мысли о создании новых платформ, которые смогли бы обогнать вездесущий Facebook и собрать под своим крылом тысячи, а то и миллионы пользователей. Как сообщает AIN.UA, каждый год появляется что-то новое: социальные сети для мам, домохозяек, любителей книг или музыки. Мы решили отобрать шесть наиболее интересных социальных сетей, на которые стоит обратить внимание в этом году.

Bookish

Это социальная сеть, созданная специально для обсуждения и покупки книг. Bookish была профинансирована такими крупными издательствами, как Simon & Schuster, Hachette Book Group and Penguin Group, которые поставили перед собой цель создать виртуальное пространство, объединяющее читателя и автора книги. В свою очередь для издательских домов появилась возможность увеличить присутствие в Интернете. Пользователям социальной сети предлагаются интервью с писателями, отрывки книг, отзывы и рекомендации. Кроме того, понравившееся издания можно приобрести, так как социальная сеть генерирует ссылки на Amazon и локальные магазины. Bookish предельно удобен, он позволяет искать новых авторов всеми необходимыми способами. Им действительно приятно пользоваться. Следует отметить, что социальная сеть нацелена на англоязычную аудитории или на людей, хорошо владеющих иностранным языком. В настоящее время база Bookish насчитывает более 2 млн экземпляров книг с информацией о каждом наименовании и около 400 тыс. страниц с данными об авторах. По словам руководителя социальной сети А. Хазэй, главная цель проекта – предоставить «энтузиастам чтения» как можно больше информации о книгах и максимально удобный доступ к ним.

Fancy

Fancy пока малоизвестна за пределами США. «Находите уникальные вещи, коллекционируйте любимые предметы, покупайте все в одном месте», – говорится в сообщении социальной сети. Это быстрорастущий социальный сервис электронной коммерции, основанный создателями Twitter и Facebook. Кроме того, Fancy – соцсеть, блог и магазин, а также сообщество людей, которые любят покупать одежду высокой моды, дизайнерские аксессуары и коллекционировать фотографии экзотических мест. Эксперты сравнивают Fancy с Pinterest. Пользователь может не просто поделиться интересной картинкой, но и приобрести то, что на ней изображено. Аудитория социальной сети – 60 % мужчины, которые любят покупать интересные вещи. На сегодняшний день насчитывается 250 тыс. зарегистрированных пользователей, а ежедневная посещаемость колеблется от 100 тыс. до 200 тыс. уникальных посетителей. Социальная сеть располагает как веб-интерфейсом, так и мобильными приложениями для платформ iOS и Android. Крупнейший инвестор Fancy – французская компания PPR, которая вложила

в стартап 10 млн дол. Ранее сообщалось, что компания Apple планировала приобрести Fancy, однако слухи не подтвердились.

Icebergs

Icebergs – социальная сеть, которая позволяет собирать все, что понравилось пользователю в Интернете: фотографии, тексты, видеозаписи, целые веб-сайты, а также загружать собственные файлы. «Это прекрасное место в облаке для вашего ежедневного исследования, проектов или поиска вдохновения», – говорится в сообщении Icebergs. Сервис позволяет собрать все вещи в кучу и организовать их, как угодно пользователю. Можно выделить какой-то объект визуально или создать группу объектов. После того как необходимый контент собран, пользователь может рассказать о своем «информационном айсберге» друзьям в других социальных сетях. Сервис еще официально не запущен, и для того чтобы им воспользоваться, необходимо отправить запрос на тестирование. Точная дата запуска проекта не сообщается. Icebergs создан двумя испанцами А. Переттой и Ц. Изерном. Среди консультантов фигурирует вице-президент компании Adobe MAX, обеспечивающей продукцию Adobe, М. Гоф.

Medium

Основатели сервиса микроблогов Twitter Э. Уильямс и Б. Стоун решили открыть новую социальную сеть. Medium предназначен для того, чтобы люди могли выбирать уровень своего информационного вклада. То есть социальная сеть берет предлагаемый пользователем контент (текст или фотографии) и подбирает похожую информацию у других пользователей. Просматривать и добавлять информацию могут все. Сообщения при этом располагаются не в традиционном хронологическом порядке, а по рейтингу популярности. Вся информация разбита на коллекции, у каждой из которых есть свои темы и шаблоны для загрузки материалов. Авторизация социальной сети происходит через Twitter. Таким образом, любой пользователь сервиса микроблогов сможет опубликовать пост, определяя его в нужную коллекцию. «Мы знаем, что большинство людей в большинстве случаев предпочитают просто просматривать контент, и это неплохо. По собственному желанию они могут одним кликом обозначить, что какой-то материал им понравился, таким образом создавая обратную связьс автором и распространяя информацию», – говорит основатель проекта Э. Уильямс.

Vine

Vine трудно назвать социальной сетью в классическом понимании этого слова. Тем не менее, у приложения есть все предпосылки стать полноценной социальной сетью с веб-интерфейсом, профилем пользователя и новостной лентой. Пока, это мобильное приложение, позволяющее создавать короткие видеоролики длительностью не более 6 с. Сервис принадлежит компании Twitter, которая купила его в октябре 2012 г., а его запуск состоялся в январе этого года. В данный момент оно доступно владельцам смартфонов на операционной системе iOS. Количество зарегистрированных пользователей превысило 100 тыс. человек. Следует

отметить, что социальная сеть получила признание не только со стороны пользователей, но и со стороны корпоративных клиентов. В частности, бренды начинают осваивать Vine. Эксперты говорят, что это новый вид контента, который только начинают осваивать. Как и у всего нового, у него есть определенный wow-эффект, который повышает количество вовлеченной аудитории.

Zeen

Сооснователи популярного сервиса YouTube Ч. Херли и С. Чен создали новый стартап – социальную сеть Zeen, позволяющую создавать и читать электронные журналы. Фактически это агрегатор информации. Собирая разную информацию в сети (тексты, фото и видео), пользователь получает возможность создать цифровой журнал из этого контента. Также для журнала можно придумать обложку, сверстать его на свое усмотрение или сделать верстку по шаблону, создать превью страниц и сформировать содержание номера. Автора понравившегося журнала можно добавить в друзья, а контентом поделиться в других социальных сетях. Сервис Zeen может стать очень удобным инструментов для небольших издательств или онлайн-СМИ, которые рассматривают возможность запуска журналов. В настоящее время Zeen находится на стадии бета-тестирования, хоть и принимает новых пользователей. Новые функции добавляются постоянно ***(6 новых социальных сетей // AIN.UA (http://ain.ua/2013/02/27/114048). – 2013. – 27.02).***

***

Во «ВКонтакте» переосмыслили принцип управления публичными сообществами.

Как сообщает AIN.UA, в «ВКонтакте» изменили принцип управления публичными страницами – усовершенствования значительны. Раздел редактирования информации о сообществе был полностью переработан. Кроме того, разработчики «ВКонтакте» добавили в сообщества новые уровни полномочий руководителей, изменили порядок блоков на странице и усовершенствовали поиск по участникам.

Интерфейс сообществ претерпел визуальные изменения. Теперь структура редактирования информации на странице публичного сообщества по дизайну приближена к группам. Управление вынесли на отдельную страницу с разделами: «Информация», «Участники», «Чёрный список» и «Ссылки».

Во вкладке «Информация» можно заполнять и редактировать сведения о публичной странице, управлять разделами под главной фотографией и делать другие настройки.

Раздел «Участники» делится на участников и руководство страницы. Теперь в поиске по участникам можно искать людей по прямой ссылке на профиль. Поиск стал мгновенным: когда пользователь начинает вводить имя

участника, поиск сразу выдаст результаты. Однако это работает только с теми сообществами, в которых состоит не более 1000 человек.

Удалять участников стало проще – ранее их приходилось заносить в чёрный список. Теперь такая необходимость отпала, вы можете удалять нежелательных участников без лишних манипуляций быстро и безболезненно.

Настройка уровней доступа в публичных страницах теперь такая же, как в группах и мероприятиях. Тип сообщества не имеет значения.

Во вкладке «Руководители» вы можете управлять полномочиями руководства страницы – выдать соответствующие права каждому руководителю, а также настроить их отображение в блоке «Контакты».

Блок с контактами на главной странице теперь находится в самом низу, а блок со ссылками поднялся выше. В мероприятиях контакты теперь не привязаны к руководству. Как и в пабликах с группами, вы можете указывать на странице сообщества контакты любых людей.

Собственная рекламная сеть «ВКонтакте» – проект SocialTank – запустила размещение рекламы на сайтах партнеров, но не для всех. Новый функционал уже доступен, и сеть находится в активной стадии запуска системы в ограниченное тестирование – в сеть принимаются партнеры, но только по инвайтам ***(Во «ВКонтакте» переосмыслили принцип управления публичными сообществами // AIN.UA (http://ain.ua/2013/02/27/114285). – 2013. – 27.02).***

***

«Третья волна» социальных сетей.

Когда появляется новая социальная сеть, вы заводите в ней профиль – для интереса или из других каких бы то ни было побуждений? Если да, и если во всех – то у нас для вас плохие новости.

Впрочем, иногда новые сервисы, даже совершенно бессмысленные на первый взгляд, выстреливают. Э. Файзуллин (CEO соцсети про эмоции Fixfeel) написал для нас пост о том, почему тематические социальные сети – это будущее.

Все мы знаем о социальных сетях, о том, какую роль они играют в жизни людей и какой популярностью пользуются (если говорить о гигантах, вроде Facebook или «ВКонтакте»). Социальная сеть – это отличный инструмент для общения, поддержки личных связей, обмена информацией. Это такое идеальное описание, и когда-то социальные сети полностью под это подходили.

Сейчас все иначе, сейчас социальная сеть – это медийный «журнал», дикая смесь из информационно-развлекательного контента и рекламы. Сейчас пользователь в основном не создает контент, он его потребляет в этом «журнальном» формате. Есть еще и огромное количество «рубрик» – групп по интересам, где можно найти информацию на любой вкус и цвет. В связи с этим личное общение уходит на второй план, и, с молчаливого

согласия самого пользователя, он превращается в «подписчика». В отличие от того, какой контент ему интереснее, он выбирает Facebook или «ВКонтакте», либо любую другую социальную сеть.

Люди по прежнему общаются посредством личных сообщений, и этого не отнять у социальных сетей. Это их «фишка» – удобная, бесплатная, быстрая связь. Но этого стало недостаточно, желания самовыражаться никто не отменял, поэтому и пришла «вторая волна» новых социальных сетей.

Кто бы мог подумать, что сервисы по обмену твитами и фото станут популярными, ведь это все есть в «ВКонтакте» и Facebook, – но получилось именно так, как получилось. Ко второй волне относятся Instagram, Twitter, Foursquare. Кстати, мы эту волну с успехом прозевали, и не сделали ни одного конкурентноспособного продукта. Здесь весь фокус снова возвращается к пользователю, к личному общению и к его способности генерировать контент. Теперь можно спокойно что-то написать, сфотографировать – и это увидят, как минимум, друзья, прокомментируют, залайкают. Это не затеряется в тоннах статей, новостей, репостов, шуток, музыки. Поэтому и количество лайков под фотками в Инстаграме больше, и вероятность того, что твой статус прочтут в Twitter – значительно выше. «Подписчик» снова стал «пользователем», доказал свое желание генерировать контент (овации).

А теперь приходит «третья волна» социальных сетей – тематических, пользователи сами генерируют контент, его стало достаточно много, и он уже вполне может объединяться по темам или интересам. Появляются геолокационные сервисы для соседей, инстаграмы для животных, соцсети для автолюбителей и программистов, и т. д. Самым лакомым куском в этой сфере является тема эмоций. Это та тематика, которая ясна и понятна всем: ты можешь не быть программистом, ты можешь не иметь автомобиля или десятка кошек, но в жизни у тебя происходят события, которые вызывают эмоции.

За счет простоты идеи и ее понятности всем можно набрать огромную аудиторию. Тем более, проблема действительно существует – «пользователям некуда писать про свои эмоции». Каждый выкручивается, как может, кто-то делает принтскрин заметок и выкладывает в Инстаграм, кто-то капслоком пишет в Twitter. У таких сервисов большое будущее. Поэтому наши заокеанские друзья уже вовсю работают над этим (moodpanda.com; placesapp.me; nikoniko.com) ***(«Третья волна» социальных сетей // InternetUA (http://internetua.com/tretya-volna--socialnih-setei). – 2013. – 3.03).***

***

Facebook тестирует новую Хронику.

Разработчики социальной сети Facebook приступили к тестированию видоизмененного формата пользовательских страниц под названием

Хроника. В новой версии слегка изменено местоположение некоторых элементов интерфейса, а рекламные блоки «переехали» вниз страницы.

Видоизмененная Хроника пока что доступна только пользователям Facebook из Новой Зеландии. Эта страна уже давно имеет славу «тестового полигона» для крупнейшей социальной сети мира. После «обкатки» новой Хроники в Новой Зеландии и внесения в нее изменений, если это понадобится, разработчики начнут применять новый формат пользовательских страниц во всем остальном мире ***(Facebook тестирует новую Хронику // InternetUA (http://internetua.com/tretya-volna--socialnih-setei). – 2013. – 3.03).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

В соцсетях выставляют свидания за деньги, чтобы помочь выжить знакомым людям.

В Украине на пике популярности голливудская фишка – парни и девушки продают всем желающим свидания с собой, чтобы перечислить вырученные деньги на лечение тяжелобольных. Желающие поучаствовать в таком аукционе (многие лично знают человека, которому нужна помощь), выставляют свое фото в специальной группе в соцсетях, после чего начинаются торги, стартующие от 5–20 грн за встречу. Иногда покупатели так входят в азарт, что в итоге предлагают сумму в 10 раз больше начальной.

«Сегодня» разыскала украинцев, которые “продавались” ради благородной цели. «Мы собираем деньги на лечение человека, у которого серьезная болезнь печени. Наш аукцион мы создали 4 года назад по типу голливудского, где продаются свидания со звездами. У нас на продажу пошли свидания с местными криворожскими звездами – телеведущими, диджеями, фотографами. Сейчас этих людей на торгах меньше, но вместо них пришли обычные горожане, – рассказала нам одна из организаторов аукциона И. Дан, которая и сама «продается». – Важно понять, что продается не человек, а возможность пообщаться. Ничего интимнее рукопожатия нет! Например, за свидание со мной незнакомый тогда мне парень заплатил около 200 грн, но так получилось, что и я выбрала свидание с ним, заплатив всего лишь 90 грн. Теперь он один из моих лучших друзей, мы открыли с ним экстрим-клуб, прыгали с моста и скал. Несмотря на то что я замужем, я продолжаю участвовать в аукционе – продаю консультации по астрологии».

По ее словам, благодаря аукциону удалось собрать около 10 тыс. грн на первую операцию парню с больной печенью, сейчас рассчитывают выручить около 16 тыс. – на очередную операцию.

А вот киевлянин Игорь, свидание с которым за 120 грн купила брюнетка, о своей встрече вспоминает с юмором. «Выставить фото на аукцион меня попросила моя подруга из КПИ, которая помогала собирать

деньги на лечение какой-то девушке. Цена на меня стартовала от 5 грн, всего свидание хотели купить 24 девушки, но одна из них заплатила наибольшую сумму, после чего лот был продан.

Некоторые из участников таких сообществ часто вообще отказываются идти на свидание, после того как оно уже проплачено. «Как-то проконтролировать, что человек точно придет на свидание – нереально, ведь все происходит на добровольных началах, к тому же в Интернете. Фото таких "отказников" мы планируем вывесить на доску позора в нашем интернет-сообществе», – рассказали нам организаторы благотворительного аукциона в Черновцах.

Популярны свидания с брюнетками и парнями-блондинами. Так, если за блондинку парни поочередно предлагают на 5 грн больше, а максимум дают 200 грн, то на брюнеток цену повышают на 50 грн каждый. Организаторы говорят: максимум давали около 2 тыс. грн за девушку и 1,5 тыс. за парня ***(В соцсетях выставляют свидания за деньги, чтобы помочь выжить знакомым людям // InternetUA (http://internetua.com/v-socsetyah-vistavlyauat-svidaniya-za-dengi--cstobi-pomocs-vijit-znakomim-luadyam). – 2013. – 18.02).***

***

Секретарь Донецкого горсовета С. Богачев использует социальные сети для решения проблем горожан. Об этом он пишет в своем блоге на «Новости Донбасса».

«Существует определенный бюрократизм и волокита в решении насущных проблем дончан, которые, порой требуют оперативного вмешательства. Пока жалоба жильцов пройдет несколько инстанций и попадет ко мне на стол, уже и проблема может стать не столь актуальной, а может и наоборот, вырасти как снежный ком. При этом у людей складывается впечатление, что чиновники просто не хотят решать их личные, но очень важные для каждого человека проблемы. Обдумывая возможную альтернативу, я принял решение завести свою страничку на Facebook.com. И следует отметить, что это сразу же начало давать положительные результаты», – сообщает С. Богачев.

В частности, по его словам, благодаря обращениям людей с помощью Facebook.com, была ликвидирована свалка строительного мусора на остановке общественного транспорта в Петровском районе города.

«Справедливости ради следует отметить, что хорошим помощником в обратной связи с жителями Донецка является и сайт "Новости Донбасса". В комментариях к моему блогу простые жители города рассказывают о своих проблемах, которые я также беру на заметку. Например, 6 февраля "Ника" сообщила, что в Кировском районе на поселке "Победа" к трамвайной остановке нет дорожки: «Толпы людей "ломают" ноги, в грязь, снег, не могут подойти к остановке. А вы говорите, что вопрос благоустройства – приоритетный! Куда смотрят чиновники…». На мой запрос Главное

управление благоустройства и коммунального обслуживания Донецкого горсовета сообщило, что “объемы работ по ремонту дороги от ДК Абакумова до ул. Ахматовой, дорожки к трамваю (поселок Победа) будут включены в план работ по текущему ремонту автодорог Кировского района на 2013 г.”. Другими словами, уже в этом году к данной остановке заасфальтируют дорожку», – пишет С. Богачев.

В то же время, он отмечает, что не все обращения через средства массовой информации и социальные сети находят свое подтверждение. Для проверки таких ложных сообщений были задействованы люди, которые потратили свое рабочее время впустую.

«Очень хотелось бы, чтобы даже в комментариях под блогами и на Facebook ко мне обращались реальные люди, которым действительно нужна моя помощь. Давайте ценить наше драгоценное время и не тратить его попусту», – резюмировал С. Богачев ***(Социальные сети помогают секретарю Донецкого горсовета решать проблемы горожан // НОВОСТИ.dn.ua (http://novosti.dn.ua/details/196635/). – 2013. – 19.02).***

***

Тернополяни масово втікають з «Однокласників» та «ВКонтакте».

Шалена популярність соціальних мереж починає лякати молодь. Тепер стає модно видаляти свої особисті сторінки, щоб мати час на творчість й інші захоплення.

Молоді тернополяни видаляють свої аккаунти із соцмереж, щоб мати час на навчання і хобі. Вони стверджують, що всю корисну інформацію можна знайти в інтернет-просторі поза межами соціальних мереж.

Наразі найбільшою соціальною мережею в Рунеті є сайт «ВКонтакте». Згідно з даними «Вікіпедії», на 2013 р. на цьому ресурсі щодня перебуває понад 43 млн осіб, що майже дорівнює населенню України. Більша частина молодих людей має свою сторінку на цьому ресурсі, а ті, хто не має, – швидше винятки.

Звичайно, що вільний час затрачається на віртуальне спілкування. Саме через це тернопільський студент Т. Ємільянов вирішив видалити свій аккаунт.

«Майже весь вільний час після навчання я проводив “ВКонтакте”, – розповідає Т. Ємільянов. – Мені здається, що найрозповсюдженіший наркотик сучасної молоді – соціальні мережі. Спілкування є дуже корисним, а нібито “ВКонтакте” це можна найкраще реалізувати через те, що там величезна кількість людей онлайн. Я мав популярну сторінку, де було багато друзів. З часом я помітив, що наше з ними спілкування дуже поверхневе. Кожен створює собі образ, який не відповідає дійсності. І люди починають йому присвячувати своє життя. Вони ходять на вечірки заради статусів і нових фото, якими потім хизуються “ВКонтакте”. Я вирішив, що таке “пластмасове” спілкування мені не потрібне, адже це марна трата часу».

Хлопець говорить, що помітив тенденцію серед своїх товаришів – вони почали видалятись із контакту. До речі, це стало можливим тільки із середини 2011 р. Він вважає, що тепер має багато вільного часу і проводить його з користю. «Проглядаючи нескінченні відео і коментуючи різні фотографії, у мене не було часу навіть підготуватись до занять, – розповідає хлопець. – Зараз такої проблеми немає. Я купив плівковий фотоапарат і витрачаю вільний час на фотознімки. Також почав читати книжки».

За його словами, «ВКонтакте» бачить і багато позитивних моментів, з якими було важко розлучатись.

Фотограф М. Купленко підтримує ініціативу видалення із сайту «ВКонтакте». Він скаржиться на низькоякісний контент. «“ВКонтакте” доводиться переглядати безліч відеороликів, які не мають жодного змісту, а також низькоякісні знімки, – говорить М. Купленко. – А справді гарні фотографії немає з ким обсудити. Свої знімки я завантажую на flickr.com. Вони – під ніком difuzion».

Також свої фото можна завантажити на сайт panoramio.com або на picassa.google.com. Причому залиті на Panoramio світлини щомісяця відбирають для наповнення служби Google Earth.

П. Попов спробував знайти альтернативу «ВКонтакте» на найпопулярнішій у світі за кількістю відвідувачів соціальній мережі Facebook. «На цьому ресурсі я також довго не затримався, – говорить він. – Цей сайт дуже перевантажений рекламою. І сконцентруватись на спілкуванні я там не зміг. А також набридає його пафос. Цим він від “ВКонтакте” не дуже відрізняється, та й спілкування проходить у режимі – подивись, який я крутий!» ***(Тернополяни масово втікають з «Однокласників» та «ВКонтакте» // Новинний портал за Збручем (http://zz.te.ua/ternopolyany-masovo-vtikayut-z-odnoklasnykiv-ta-vkontakti/). – 2013. – 19.02).***

***

Украинцы смогут вызвать «скорую» по SMS и через Facebook.

Автомобили скорой помощи оснастят GPS-навигаторами, планшетными компьютерами и принтерами. Это предусмотрено планом модернизации системы скорой медицинской помощи, которое 20 февраля представило Государственное агентство по инвестициям и управлению национальными проектами.

Как сообщает «КоммерсантЪ-Украина», вызов скорой станет доступен не только по телефону, но и с помощью SMS, электронной почты или через социальные сети – Twitter и Facebook.

По словам руководителя проекта А. Навроцкого, запланированные мероприятия призваны модернизировать отечественную систему скорой медицинской помощи и привести ее к европейским стандартам.

В частности, обратившийся за помощью человек должен ждать ответа диспетчера на линии не более 5 с.; на определение того, какому врачу адресовать вызов, будет уходить не более 45 с. Всего же от приема звонка до

направления бригады по адресу диспетчер должен будет тратить не более 3 мин. Скорая помощь в сельской местности обязана прибывать к пациенту максимум за 20 мин., а в городе – за 10. Время оказания реанимационной помощи должно составлять не более 8 мин.

Проект предусматривает оснащение машин скорой GPS-навигаторами и рациями нового поколения. Врачи получат в распоряжение мини-принтеры и планшетные компьютеры на базе операционной системы Android, с выходом в Интернет и функцией Wi-Fi.

«GPS-навигатор позволит отслеживать местоположение автомобиля, и водитель уже не сможет ездить за картошкой, используя государственное имущество»,– заявил глава Госинвестпроекта В. Каськив.

Сами же врачи от технологических новшеств не отказываются, но сомневаются, что пациенты и медики старшего поколения смогут ими эффективно воспользоваться.

«Не все врачи старшего возраста умеют пользоваться компьютерной техникой. Кроме того, у нас компьютеризированы далеко не все поликлиники и не везде есть интернет, особенно в сельской местности»,– отметил заведующий отделением неотложной скорой помощи клиники «Борис» М. Омельчук.

Ранее Премьер Н. Азаров потребовал найти ресурсы для ежегодного обновления парка автомобилей скорой помощи на 1000 машин, а также потребовал, чтобы «скорая» выезжала на все вызовы ***(Украинцы смогут вызвать «скорую» по SMS и через Facebook // Обозреватель (http://obozrevatel.com/society/82190-ukraintsyi-smogut-vyizvat-skoruyu-po-sms-i-cherez-facebook.htm). – 2013. – 21.02).***

***

Facebook протесты становятся все более популярными в Украине. Дать клич среди множества людей одномоментно одним нажатием кнопки – прекрасная техническая возможность для молодых революционеров. Нам запомнились российские протесты и их интернет-лидеры, собирающие толпу с социальных сетях. Даже более – обсуждая в группах и событиях возможных лидеров и выступающих на митингах. В Украине движение только набирает обороты, наступая как на американские, так и на русские грабли. Забегая немного наперед скажу, что политические лозунги зарождаются и умирают в социальных сетях. Реальная нужда и экономические вопросы сейчас выводят молодежь и так называемый «креативный класс» на улицы.

Опыт отечественной организации движений в Интернет, особенно сбор людей на акции, пока что не радует их инициаторов. Из 1000 откликнувшихся на призыв прийти может и сотня, и полсотни. В чем же причина столь высокой поддержки в Интернете, и столь низкой явки и уличной активности? Социологи и психологи сетуют на природу человека: комплексы, страхи, лень. И они отчасти правы. Но лишь отчасти.

Объяснять такой классической теорией можно и акции против застройки пейзажной аллеи в Киеве, и акции против других застроек, и недавнюю акцию против укравтодора. Во всех из перечисленных акциях предварительное участие подтверждали тысячи человек. В то время как реально приходили от силы сотни. Можно ли побороть такую проблему? Оказывается да, возможно.

Уже порядка двух лет Институт PolitPR проводит публичные дискуссии и политические лекции, куда приглашает всех желающих к диалогу, к обучению. Зачастую приходят молодые люди и все тот же креативный класс. Последнее время, правда, стали приходить люди старше 50 лет. Такая тенденция безумно радует.

Каждое из мероприятий, будь это дискуссия по экономике или политике, приходит не менее 200–300 человек. Не раскрывая всех технологических секретов, расскажу несколько наших важных правил, которые могут помочь общественно-политическим движениям.

Первое. Личности – важный элемент встреч. К нам на дискуссии приходят политики, эксперты, активисты. Всегда есть несколько спец гостей, к которым будут вопросы. Можно как угодно называть акцию или дискуссию, но без доверия она не состоится. На первых порах кредит доверия могут дать лишь авторитеты в обществе. Далее вы сами станете авторитетной площадкой (группой людей), доверие к которой будет выше, чем к отдельно взятым ее VIP участникам.

Второе. Не увлекаться страницами, сообществами и группами в социальных сетях. Когда мы приглашаем на очередную дискуссию, люди идут не в Raimov discussion court, а к Д. Раимову и его команде. Наши страницы в социальных сетях стали главными активами: их посещают более, чем те же группы и страницы, которые нам принадлежат.

Третье. Не бегите за качеством подачи информации. Куда более интересна фотография с события, сделанная на обычный телефон, чем фото, сделанное на профессиональную камеру. Мы обычно во время дискуссий и встреч делаем фото и видео, быстро размещая их в Интернет. Такая оперативность заменяет камеры телевидения и не дешёвую прямую трансляцию в Интернет

Четвертое. Сбор людей необходимо проводить в несколько этапов. Вначале мы собираем сторонников на наших страницах, событиях и группах. Обязательно просим всех регистрироваться: оставлять телефон, почту, ссылки на страницы в социальных сетях. Далее вступают в силу технологии маркетинга: рассылки на почту, рассылки smscообщений, письма на страницы в социальные сети. И, ближе к событию, звонки. Человек чувствует и свою необходимость, и свою включенность в процесс, и персональную ответственность. Не прийти после всего этого, как не прийти на день рождения, предварительно подтвердив свой приход имениннику.

Итог, пятое. Всегда оставаться на волне и быть максимально инновационным. Классические газеты интересны только бабушкам, в то

время как на акции ходит молодежь и прогрессивные городские интеллектуалы. У них достаточно своеобразное восприятие мира через монитор компьютера и новейший девайс.

За годы нашей работы мы сумели разработать алгоритм вытягивания из виртуального мира интернета реальных людей. Сейчас у нас собрались базы сторонников, которые интересуются общественными проблемами, экономическими вопросами, правовыми вопросами и вопросами города. Все это помогает ускорить процесс, но, все же, те пять правил лежат в основе ***(Facebook протест // Marketing Media Review (http://mmr.ua/news/id/facebook-protest-33682/). – 2013. – 20.02).***

***

Створили програму, яка буде вести блог після смерті користувача.

У Лондоні написали програму, яка вивчатиме особистість користувача Twitter і продовжить вести мікроблог після його смерті.

Британські програмісти створили програму, яка дасть можливість мерцям продовжити своє ативне життя в соціальних мережах.

Як повідомляє The Daily Mail, програма буде доступна для завантаження вже в березні. Вона має назву LivesOn.

Розробка вивчатиме смаки свого користувача, його лексику і переконання, і продовжить писати замість нього повідомлення в мікроблозі Twitter після його смерті.

Автори програми обіцяють, що програма буде абсолютно безкоштовною.

На їхню думку, це чудовий спосіб залишити свою особистість в історії. Однак готуються до осуду з боку суспільства.

«Треба бути готовим до того, що ця розробка зачепить багатьох людей, не зважаючи на всі філософські і етичні аргументи. Одних наша програма образить, інші будуть у захваті. Але тільки уявіть, якщо люди зможуть побачити в цьому маленький і точний спосіб, як продовжити своє життя», – переконаний автор програми Д. Бедвуд ***(Створили програму, яка буде вести блог після смерті користувача // Вголос (http://vgolos.com.ua/zhyttya/news/12695.html). – 2013. – 20.02).***

***

Facebook и Google учредили премию для ученых.

Одиннадцать ученых стали миллионерами – после того, как впервые получили премию за прорыв в естественных науках. Ученые получат по 3 млн дол. – это более чем вдвое превышает сумму выплат за Нобелевскую премию.

Новую премию учредили несколько самых известных в мире технологических магнатов, в частности один из основателей Google С. Брин, основатель Facebook М. Цукерберг и др.

Эти финансовые ресурсы помогут ученым проводить исследования стволовых клеток, новых методов лечения рака и генетических заболеваний и т. д.

Учредители премии говорят, что хотят создать ажиотаж вокруг научных достижений, которые могут продлить человеческую жизнь.

В будущем учредители премии планируют ежегодно присуждать пять наград по 3 млн дол. ***(Facebook и Google учредили премию для ученых // «Газета «Донбасс» (http://donbass.ua/news/technology/internet/2013/02/21/facebook-i-google-uchredili-premiju-dlja-uchenyh.html). – 2013. – 21.02).***

***

В 2013 г. ЮНИСЕФ Украина начинает сотрудничество с социальной сетью «ВКонтакте» и открывает свою собственную страницу. Об этом сообщили в пресс-службе организации.

По состоянию на январь 2013 г. среднее суточное количество уникальных пользователей «ВКонтакте» с Украиной составляет 8,9 млн человек.

Почти все дети в крупных городах Украины (96 %) имеют дома персональный компьютер, из них 92 % имеют возможность выхода в Интернет. И 80 % таких детей зарегистрированы в популярной сети «ВКонтакте». Влияние социальных сетей на детей и молодежь очень большое. Однако в основном характер этого влияния имеет развлекательный характер.

Детский Фонд ООН (ЮНИСЕФ) стремится изменить стереотипы о несерьезности и невозможность доносить важные темы в таких сетях. «Мы будем информировать о принципах, что в первую очередь касаются прав детей. Социальные сети могут иметь позитивное влияние, если их правильно использовать», – говорится в сообщении.

Контент страницы ЮНИСЕФ Украины в «ВКонтакте» – это ключевые сообщения о правах и интересах детей раскрыты в доступной форме. Мы надеемся, что благодаря этому молодежь и подростки станут ближе к ценностям развитого общества, а родители найдут для себя полезную информацию и советы.

Справка: Детский фонд ООН (ЮНИСЕФ) является мировым лидером по защите прав и интересов детей. Фонд работает в более 190 странах мира ради защиты и поддержки детей. В этом году ЮНИСЕФ в Украине празднует 15-ти своей деятельности ***(ЮНИСЕФ открыл страницу в социальной сети // УНН (http://vchaspik.ua/zhizn/112038yunisef-otkryl-stranicu-v-socialnoy-seti). – 2013. – 1.03).***

Facebook будет показывать видеорекламу.

Крупнейшая в мире социальная сеть планирует увеличить доходы за счет введения нового типа рекламы. Уже в ближайшее время в ленте новостей пользователей могут появиться автоматически проигрываемые видеоролики, продвигающие различные товары.

Вице-президент по бизнесу и маркетингу Facebook Д. Фишер согласился, что автоматически проигрываемая видеореклама может быть раздражающей, но подчеркнул, что специалисты Facebook «смогут найти способ реализовать ее правильно». На конференции в Стэнфордском университете Д. Фишер отметил, что он восхищен системой рекламы на YouTube, из чего можно сделать вывод, что видеореклама на Facebook может быть построена по схожему принципу.

Д. Фишер отметил, что видеообъявления уже успешно действуют на Facebook. Рекламодатель может запостить ролик, а затем заплатить, чтобы его показали большому количеству людей, вот только выбор открывать видео или нет, пока что остается за пользователем.

«Я уверен, что есть множество различных способов введения в Facebook видеорекламы. Некоторые из них могут быть раздражающими, но есть и те, которые потенциально могут удовлетворить и интересы пользователя, и интересы рекламодателя. Мы все еще не ввели в соцсеть видеорекламу, потому что не отыскали этого баланса. Но, когда мы решим эту проблему, видеореклама появится», – заявил Д. Фишер.

В декабре уже сообщалось, что Facebook планирует запустить автоматически проигрываемую видеорекламу. По информации сайта, новый рекламный продукт будет запущен к апрелю 2013 г. Социальная сеть будет работать с короткими 15-секундными роликами. По всей видимости, аудио будет запускаться вместе с видео, так что каждое посещение соцсети будет сопровождаться неожиданными звуковыми «спецэффектами» коммерческого содержания.

Большинство людей неохотно кликают по ссылкам для просмотра рекламных видео. Но если ролик запускается автоматически и при этом он интересный, многие согласятся просмотреть его до конца. Это хорошо соотносится со стратегией Facebook в области рекламы. В идеале соцсеть хочет, чтобы продвижение товаров выглядело не как навязчивая реклама, а как дополнительный источник информации и в конечном счете как развлечение для пользователей. Facebook не хочет, чтобы люди закрывали сайт, чтобы скрыть рекламу.

Вероятнее всего, как и YouTube, соцсеть позволит через несколько секунд пропускать ролик. По словам Д. Фишера, рынок телерекламы оценивается в 70 млрд дол. Учитывая это, логично, что рекламные ролики пытаются освоить и самый популярный в мире инструмент сетевой коммуникации. По телевидению среднестатистический американец

потребляет около 16 мин. рекламы каждый час. Тот же средний американец 6,5 часов в месяц проводит в Facebook.

Если бы Facebook показывал столько же рекламы, сколько сегодня показывает телевидение, он мог бы демонстрировать пользователю более 400 15-секундных роликов в месяц. Правда, в Интернете люди куда менее терпимы к рекламе, чем аудитория традиционных СМИ. Скорее всего, Facebook будет демонстрировать не более десятой части от этого количества.

При таком раскладе соцсеть сможет отвоевать значительную долю рекламных бюджетов у телекомпаний, до некоторой степени пожертвовав лояльностью пользователей. Конечно, большинство людей, зарегистрированных в Facebook, совсем не обрадуются нововведениям. Как бы то ни было, Facebook – это бесплатная платформа, а, значит, пользователи должны быть готовы к рекламной монетизации ***(ЮНИСЕФ открыл страницу в социальной сети // InternetUA (http://internetua.com/Facebook-budet-pokazivat-videoreklamu). – 2013. – 20.02).***

***

«ВКонтакте» тестує власну контекстну рекламу на сайтах.

Минулого тижня в тестовому режимі почала свою роботу рекламна мережа «ВКонтакте», яка дасть змогу розміщувати оголошення на сайтах-учасниках мережі.

Протягом найближчого часу новинка стане доступною для всіх рекламодавців, які вирішили спробувати її на практиці. Як пояснили в авторизованому центрі обслуговування партнерів мережі, оголошення від «ВКонтакте» поки не використовують тематику сайту, на якому розміщені, та його контент, проте в майбутньому планується залучити і ці параметри.

Водночас, за словами прес-секретаря соцмережі Г. Лобушкіна, «ВКонтакте» не має наміру конкурувати з Яндексом та Google в галузі контекстної реклами.

За відгуками перших користувачів рекламної мережі «ВКонтакте», наразі в її оголошеннях низькі показники CTR і CPM. Рекламодавці, у свою чергу незадоволені тим, що рекомендовані ціни за клік набагато вищі від реальних.

С. Полецький, керівник центру обслуговування мережі, пояснив, що транслювання оголошень на сайти партнерів поки доступне не всім рекламодавцям, і як тільки це трапиться, вартість за клік зросте. Окрім того, адміністрація має намір покращити дизайн оголошень: збільшити шрифт та видимість для користувачів ***(«ВКонтакті» тестує власну контекстну рекламу на сайтах // UkrainianWatcher (http://watcher.com.ua/2013/02/18/vkontakti-testuye-vlasnu-kontekstnu-reklamu-na-saytah/). – 2013. – 18.02).***

***

Большинству пользователей (51 %) не нравится, когда бренды вмешиваются в их беседы в социальных сетях, даже когда речь идет о продукции данного бренда, сообщает towave.ru

Единственный случай, когда, по мнению пользователей (58 %), брендам все же уместно вступать в общение с потребителями – ответ на жалобы.

Это результаты исследования, проведённого совместно двумя компаниями – JD Power Panel и Netbase.

Другие интересные результаты исследования:

– 32 % потребителей не понимают, что бренды подслушивают их разговоры в социальных медиа;

– 43 % полагают, что прослушивание разговоров – это вмешательство в частную жизнь пользователей;

– 48 % думают, что брендам все же нужно слушать разговоры, с целью улучшить свои товары;

– 64 % считают, что компаниям следует отвечать на комменты в социальных сетях только в том случае, если они непосредственно адресуются данной компании ***(Пользователи не хотят, чтобы бренды подслушивали их в социальных сетях // IT Expert (http://itexpert.in.ua/rubrikator/item/22974-polzovateli-ne-chotyat-chtobi-brendi-podslushivali-ich-v-sotsialnich-setyach.html). – 2013. – 19.02).***

***

Twitter упростил закупку рекламы в ответ на инициативы Facebook.

Сеть микроблогинга анонсировала новую рекламную платформу, которая, с одной стороны, должна облегчить для рекламодателей закупку рекламы, а с другой – сделать сам ресурс более интересным для производителей товаров и поставщиков услуг. Об этом сообщает CyberSecurity.ru.

Также в Twitter сообщили, что заключили с компаниями Adobe и Salesforce соглашения о сотрудничестве в области ряда аспектов, связанных с работой трех сервисов, а также с продажей рекламных объявлений в объединенных пакетах, позволяющих рекламодателям самим охватывать большую аудиторию. Финансовые детали соглашения стороны не разглашают.

Следует отметить, что соглашение Twitter и ее рекламные инициативы следуют вскоре после того, как похожие инициативы презентовала соцсеть Facebook, также обновившая свою рекламную платформу и API для нее.

В совместном заявлении Twitter, Adobe и Salesforce сказано, что рекламодатели, приобретающие рекламу в Twitter, также могут для своих нужд использовать маркетинговые инструменты Adobe Media Optimizer и Salesforce Marketing Cloud.

Напомним, что ранее в Twitter заявляли, что намерены в 2014 г. достичь рекламного оборота в 1 млрд дол., тогда как в этом году он составит порядка 545, 2 млн дол. В прошлом Twitter уже заключила рекламные соглашения с баинговыми агентствами Omnicom и Razorfish для продажи спонсорских сообщений и продвигаемых твитов ***(Twitter упростил закупку рекламы в ответ на инициативы Facebook // IT Expert (http://itexpert.in.ua/rubrikator/item/23044-twitter-uprostil-zakupku-reklami-v-otvet-na-initsiativi-facebook.html). – 2013. – 21.02).***

***

Pinterest оцінили у 2,5 млрд дол.

Соціальна мережа Pinterest провела черговий раунд фінансування, у рамках якого всю компанію було оцінено у 2,5 млрд дол.

Як пише Bloomberg, новий раунд інвестицій був проведений фондами Valiant Capital Management, Andreessen Horowitz, Bessemer Venture Partners і FirstMark Capital. У травні 2012 р., коли Pinterest закрив перший раунд фінансування, проект оцінювали в 1,5 млрд дол., таким чином, менше ніж за рік компанія подорожчала на мільярд.

Таким чином, нові інвестиції вводять Pinterest в клуб найцікавіших інтернет-сервісів, в які інвестори охоче вкладають свої кошти: Twitter (оціночна вартість 9 млрд дол.), Dropbox (4 млрд дол.), Airbnb (2,5 млрд дол.) та ін.

За даними осіннього дослідження маркетологів, Pinterest більше мотивує людей робити покупки онлайн, ніж Facebook ***(Pinterest оцінили в 2,5 млрд дол. // UkrainianWatcher (http://watcher.com.ua/2013/02/21/pinterest-otsinyly-v-2-5-mlrd/). – 2013. – 22.02).***

***

В Китае началось повальное увлечение аналогом Twitter.

Число пользователей китайского интернет-блога «Сина вэйбо» – weibo.com – аналога сервиса Twitter, по последним данным, достигло 500 млн человек, сообщает tasstelecom.ru.

Как сообщило накануне агентство Синьхуа со ссылкой на заявление компании «Сина Корп», число активных пользователей, ежедневно размещающих информацию в микроблоге, за прошлый год возросло до 46,2 млн человек.

Совокупный доход микроблога «Сина вэйбо» в 2012 г. составил 66 млн дол. 77 % дохода принесло размещение рекламы, остальные 23 % прибыли составил доход от предоставления различных дополнительных услуг.

«Компания планирует расширять спектр предоставляемых сервисов и в первую очередь сосредоточится на развитии приложений для мобильных устройств, – приводит агентство слова исполнительного директора “Сина

Корп” Ц. Говэя. – Более 75 % пользователей заходят в микроблог через телефоны и планшеты».

В минувшую среду компания опубликовала годовой финансовый отчет за 2012 г. Согласно данным отчета, за этот период ее чистая прибыль составила 529,3 млн дол., увеличившись на 10 % в годовом исчислении ***(В Китае началось повальное увлечение аналогом Twitter // IT Expert (http://itexpert.in.ua/rubrikator/item/23111-v-kitae-stremitelno-rastet-chislo-polzovateley-mikrobloga-sina-veybo.html). – 2013. – 22.02).***

***

Спільнота MDK на «ВКонтакте» заробляє до 1 млн дол. на рік.

На сайті Hopes&Fears вийшло інтервю з авторами спільноти MDK (vk.com/mudakoff), яка налічує майже 2 млн учасників та є одним з найчисленніших пабліків у соціальній мережі «ВКонтакте».

Автори побажали залишитися неназваними, щоб уникнути помсти незадоволених користувачів – таке, за їхніми словами, уже відбувалось. «На вигляд це звичайні інтелігентні люди за 20 років», – пише H&F. Паблік MDK відкрився у травні 2011 р. і сконцентрував свою увагу на висміюванні популярних тем, публікації демотиваторів, троллфейсів та інших прикольних картинок.

Рекламу хлопці почали розміщувати після того як кількість підписників пабліка перевалила за 80 тис. На сьогодні в MDK є три типи рекламних постів – за 8 тис. руб. (видаляється через годину), а також варіанти за 15 тис., 20 тис. і 30 тис. руб. (закріплення на весь день у шапці сторінки). Разом зі спільнотами-супутниками реклама в пабліках приносить їм до 1 млн дол. на рік.

За словами авторів, вони тісно співпрацюють з техпідтримкою «ВКонтакте», а також мають цілий пул модераторів, які стежать за обговореннями, чистять коментарі та модерують контент від користувачів. Нова рекламна біржа від «ВКонтакте» їх не лякає – навпаки, вони вважають, що обмеження до одного рекламного поста на день може торкнутись лише маленьких спільнот. MDK запустило власний додаток, який увійшов у топ завантажень App Store, і тепер має намір розвиватись поза межами «ВКонтакте» – автори розуміють, що бути залежним від когось шкодить їхньому бізнесу ***(Спільнота MDK на ВКонтакті заробляє до 1 млн дол. на рік // UkrainianWatcher (http://watcher.com.ua/2013/02/27/spilnota-mdk-na-vkontakti-zaroblyaye-do-1-mln-na-rik/). – 2013. – 27.02).***

***

Facebook сможет узнавать о покупках своих пользователей в оффлайн магазинах благодаря партнерству с Acxiom и Epsilon.

Как сообщает издание Ad Age, социальная сеть тестирует новый вид таргетинга, который позволит рекламодателям нацеливать свои объявления

на тех пользователей соцсети, которые покупали определенные товары в обычных магазинах

Работает вся схема так: пользователь соцсети в обычной жизни участвует в программе лояльности какого-то магазина, в ходе которого ему выдается дисконтная карта. При дальнейших покупках информация о них вместе с e-mail и телефонным номером покупателя (при выдаче дисконтной карты всегда запрашиваются контактные данные) заносится в базу. Подобные базы есть у таких гигантов рынка данных, как Epsilon, Acxiom и Datalogix. Благодаря партнерству с этими компаниями, социальная сеть сможет получить доступ к этим данным и, соответственно, сопоставить e-mail адреса и номера телефонов с теми, что пользователи Facebook использовали при регистрации и заполнении своего профиля.

Гипотетически такой метод таргетинга может позволить, к примеру, компании Coca-Cola нацеливать рекламу на тинейджеров, которые покупали газировку в прошлом месяце, а Pampers сможет показывать рекламу жителям Северной Каролины, которые недавно приобретали товары для детей – благо сам Facebook обладает просто огромным количеством данных о демографии и пристрастиях своих пользователей.

Новая функция, похоже, нацелена на CPG-маркетологов (Consumer Packaged Goods – потребительские товары в упаковке), которых Facebook старательно обхаживает в последнее время – соцсеть даже организовала первый CPG Саммит в Нью-Йорке в прошлом месяце. В ходе этого событие всеобщее внимание было приковано к обсуждению так называемых «пользовательских аудиторий» – технология, при использовании которых бренды загружают e-mail адреса, номера телефоны и адреса проживания пользователей из баз данных своих CRM-систем, что позволяет показывать рекламу на Facebook четко своим имеющимся клиентам. Рекламный таргетинг, основанный на данных о покупках, использует ту же самую технологию (под названием хеширование – «hashing») для того, чтобы найти совпадение данных, не позволяя при этом контрагентам Facebook видеть информацию о пользователях соцсети и наоборот.

Это уже далеко не первая попытка таргетинга рекламных объявлений на основе данных о совершенных пользователями покупках. К примеру, компания Datalogix работала над подобным средством в партнерстве с несколькими технологическими компаниями, включая AppNexus, Invite Media и MediaMath. Ключевое отличие от нынешней попытки Facebook заключается в том, что раньше возможно было лишь приобрести агрегированные данные cookies, что делало нетривиальным задачу определения того, как много пользователей из пула видели рекламу, или же многим из них она была показана по два раза, а кто-то так и не увидел объявления.

Ad Age обратился за разъяснениями относительно нового продукта в Epsilon, которая перенаправила запрос в Facebook, а социальная сеть отказалась от комментариев ***(Facebook сможет узнавать о покупках своих***

пользователей в оффлайн магазинах благодаря партнерству с Acxiom и Epsilon // Marketing Media Review (http://mmr.ua/news/id/facebook-smozhet-uznavat-o-pokupkah-svoih-polzovatelej-v-offlajn-magazinah-blagodarja-partnerstvu-s-acxiom-i-epsilon-33770/). – 2013. – 26.02).

***

Facebook купує у Microsoft рекламну платформу.

Соціальна мережа Facebook оголосила про свої наміри придбати у Microsoft її дочірньої компанії Atlas Advertiser Suite, яка надає рекламні рішення для digital media.

За допомогою цієї угоди Facebook планує посилити свої позиції в сегменті графічної реклами і посилити конкуренцію з Google.

Згідно з умовами угоди, команда Atlas залишиться в Сіетлі, де до цього часу і базувався її бізнес.

У блозі Facebook ідеться, що інструменти Atlas допоможуть компаніям більш гнучко вибирати і розміщувати власну рекламу на сайті, а також відстежувати її ефективність.

Facebook повідомляє, що за допомогою інструментів Atlas кінцеві рекламодавці й рекламні агентства зможуть точніше витрачати рекламні гроші і отримати велику віддачу від розміщення реклами на сторінках найбільшої світової соцмережі.

Вартість угоди з купівлі Atlas не розголошується, проте відомо, що Microsoft продає цей актив у рамках ліквідації бізнесу, пов'язаного з раннім придбанням компанії Aquantive, за який у 2007 р. софтверний гігант віддав 6,3 млрд дол.

Сторони домовилися про те, що навіть після угоди з Facebook Microsoft буде продовжувати користуватися технологіями Atlas.

За даними компанії Emarketer, на сьогодні частка Google на американському ринку графічної інтернет-реклами становить 18 %, проти 15 % у Facebook ***(Facebook купує у Microsoft рекламну платформу // real-economy.com.ua (http://real-economy.com.ua/news/34871.html). – 2013. – 1.03).***

***

Російський мільярдер продає акції Mail.ru на 550 млн дол.

Підконтрольна російському мільярдеру А. Усманову USM Holdings Ltd. заробить на продажі акцій Mail.ru близько 559 млн дол.

Як повідомляється, USM продає 15,5 млн акцій за 34,25–36 дол. за одну акцію, що становить частку приблизно в 7,4 % у капіталі Mail.ru Group Ltd.

За даними Bloomberg, після продажу цього пакета USM буде володіти 17,9 % у Mail.ru, організатором угоди є Morgan Stanley.

На сьогодні частка USM у капіталі Mail.ru Group Ltd. становить 25,3 %, але загальна частка голосуючих акцій становить 60,6 %. Після завершення операції частка голосуючих акцій становитиме 58,1 %, тобто компанія збереже контроль.

Крім того, Mail.ru планує виплатити додаткові дивіденди в обсязі 899 дол. млн у зв'язку зі зменшенням своєї частки у Facebook і продажем пакетів акцій Groupon і Zynga.

Зазначимо, що за підсумками 2012 р. неаудований чистий прибуток Mail.Ru Group збільшився на 37 % у річному вираженні до 8,499 млрд руб., виручка – зросла на 39 % до 21,151 млрд руб.

Тим часом, у зв'язку з новиною про продаж частки А. Усманова, розписки Mail.ru Group впали на 9 % до 34 дол.

Прискорений продаж 7 % пакета Mail.ru А. Усмановим до дивідендних виплат наводить аналітиків Sberbank CIB на думку про можливість вивільнення грошових коштів для придбання соціальної мережі «ВКонтакте».

«...Такий розвиток подій, на нашу думку, може бути сприйнятий як негативне для Mail.ru Group – з'явиться ризик, що згодом соціальна мережа буде перепродана останній», – йдеться в аналітичній записці Sberbank CIB.

Раніше повідомлялося, що провідний російський інтернет-ресурс збільшив прибуток до 280 млн дол. ***(Російський мільярдер продає акції Mail.ru на 550 млн дол. // ua.korrespondent.net (http://ua.korrespondent.net/business/rynki/1514159-rosijskij-milyarder-prodae-akciyi-mail-ru-na-550-miljoniv-dolariv). – 2013. – 28.02).***

***

«ВКонтакте» взяла под контроль рекламу в приложениях.

Социальная сеть «ВКонтакте» взяла под контроль размещение рекламы в приложениях, которые включают в себя, в частности, игры, викторины, автоматические поздравления друзей с праздниками. Об этом сообщается в правилах работы ресурса. С 1 марта 2013 г. интеграционная реклама в приложениях соцсети будет размещаться централизованно через руководство «ВКонтакте».

Необходимость изменений в соцсети объяснили тем, что в настоящее время системы продаж интеграций в приложениях «выстраиваются в длинные цепочки, которые могут включать одно или несколько рекламных агентств, в результате чего доход разработчиков может составлять лишь небольшой процент от стоимости рекламы». Поэтому продажа интеграций и выплаты разработчикам будут проходить только через «ВКонтакте», что, на взгляд соцсети, «значительно упростит взаиморасчеты между разработчиками и рекламодателями». При этом разработчики приложений смогут привлекать рекламодателей самостоятельно.

В приложениях соцсети останутся два возможных формата интеграций: офферные и медийные. При офферных интеграциях пользователь получает вознаграждение за некую последовательность действий, определенную рекламодателем – например, игровой объект за вступление в сообщество бренда. Медийная интеграция – это временное брендирование элементов

приложения, стоимость ее определяется среднесуточной посещаемостью приложения.

Как сообщает «Коммерсантъ» со ссылкой на заместителя генерального директора «ВКонтакте» И. Перекопского, объем рынка интеграций в 2013 г. соцсеть оценивает примерно в 500–700 млн руб., а комиссия «ВКонтакте» за размещение составляет около трети от этой суммы.

С 1 марта 2013 г. в приложениях «ВКонтакте» также нельзя будет размещать баннеры и другие медийные форматы. Единственно возможными форматами останутся рекламные интеграции и размещение таргетированной рекламы через рекламную систему «ВКонтакте». О запуске рекламной сети «ВКонтакте» было объявлено в ноябре 2012 г. В тестовом режиме она была запущена в феврале 2013 г. В течение месяца система должна заработать в полную силу ***(«ВКонтакте» взяла под контроль рекламу в приложениях // InternetUA (http://internetua.com/vkontakte--vzyala-pod-kontrol-reklamu-v-prilojeniyah). – 2013. – 28.02).***

***

Видеохостинг YouTube тестирует функцию, позволяющую пользователям выбирать между просмотром «длинной» рекламы перед роликом и «рекламной паузой» в процессе просмотра видео. Об этом сообщает The Next Web.

При попытке открыть некоторые видео пользователям предлагают выбрать между двумя схемами просмотра рекламы. В ряде случаев он также может указать, какой из предложенных рекламных роликов он хочет посмотреть перед самим видео. The Next Web отмечает, что длительность предложенной «длинной» рекламы варьируется от 30 с. до двух минут.

В случае, если пользователь выберет «рекламную паузу», либо не выберет ничего в отведенный отрезок времени, в процессе просмотра ему покажут несколько рекламных роликов. Их количество зависит от длительности самого видео.

Представители YouTube не стали уточнять, когда новый механизм выбора рекламы будет введен окончательно. Они сообщили изданию, что видеохостинг постоянно проводит эксперименты и изучает реакцию пользователей.

Возможность размещения видеорекламы на YouTube появилась в 2010 г. Рекламные ролики обычно запускаются перед самим видео и могут быть «пропущены» только спустя несколько секунд, либо должны быть проиграны до конца. Помимо видеорекламы на YouTube есть и баннеры, появляющиеся поверх видео в процессе просмотра ***(На YouTube появятся «рекламные паузы» // InternetUA (http://internetua.com/na-YouTube-poyavyatsya--reklamnie-pauzi). – 2013. – 26.02).***

***

Google «зганяє» користувачів у глобальне інтернет-гетто. Пошуковик піднявся на вершину гори даних користувачів, де кожен крок записаний, вивчений і проданий тим, хто більше заплатить.

У вас немає акаунта в Google+? Більшість тих, хто там не реєструвався, теж так думає. Насправді ж, якщо ви недавно зареєструвалися на Gmail, YouTube або будь-якому іншому сервісі пошукового гіганта, ви стали власником «єдиного облікового запису Google», який містить у собі і публічну сторінку на Google+.

Найбільш активні користувачі вже встигли відчути на собі, як далеко просунулася інтеграція різних сервісів, що належать Google, у межах єдиного акаунта. Наприклад, відгук, залишений на сайті ресторанної критики Zagat, або користувальницький огляд додатка на Google Play вже сьогодні «лінкуються» – вельми несподівано для багатьох – з публічним профілем на Google+, який містить персональні дані, включаючи справжні ім'я та прізвище.

Топ-менеджмент Google заявляє, що все ще тільки починається. «Google+ це частина Google, – говорить Б. Хоровітц, віце-президент компанії. – Існує безліч точок входу в Google+, і з кожним днем інтеграція просувається». У той самий час у Google+ не відзначається помітної соціальної активності між користувачами. Онлайн-паспортом людини в мережі де-факто, як і раніше, є Facebook, і справа тут навіть не в кількості зареєстрованих акаунтів. Google+ виглядає настільки нетипово-безлюдним для соцмережі, що кілька західних видань уже встигли охрестити цей проект найбільшим провалом у історії пошукового гіганта.

Незважаючи на думку преси, керівництво Google завжди розуміється на тому, коли продукт вийшов дійсно невдалим. І знаходить мужність відкрито заявити про це – досить згадати гучні закриття багатообіцяючих проектів Wave і Buzz. Очевидно, що Google+ виконує не тільки функцію чергової соцмережі. Про те, що ще входить до «великого плану» Google, сьогодні запекло сперечаються західні соціологи і маркетологи.

Згідно з найбільш поширеним трактуванням, запустивши Google+, керівництво пошукача намагається запобігти гегемонії Facebook у сегменті персоналізованої реклами, причому найважчим шляхом – вступивши з останнім у пряму конкуренцію. Адже Google+ було запущено в той час, коли кількість користувачів Facebook уже перевалила за півмільярда.

Як Facebook, так і Google отримують більшу частину свого прибутку від продажу реклами. Однак у Facebook є те, про що Google завжди міг тільки мріяти – прив'язка онлайн-активності покупців до їхніх реальних імен і соціального оточення. На думку маркетологів, уніфікація Google+ з іншими сервісами пошукового гіганта дасть Google можливість зібрати власне «досьє» на користувача і пропонувати їм більш персоналізовану (а, виходить, і більш дорогу) рекламу.

Крім того, запустивши функцію Google+ Sign-In, що дає змогу реєструватися на сторонніх сервісах з використанням даних із Google+ (аналог Facebook Connect), пошукач отримує можливість накопичувати гори інформації про відвідувані користувачами онлайн-сервіси, сфери їхніх інтересів, їхні пошукові звички тощо. Така можливість – манна небесна для пошукового бізнесу Google, що приносить 95 % від усієї виручки корпорації.

«Google сидить на вершині гори даних користувачів», – пояснює А. Остек, президент агентства Resolution Media, який виступає посередником між Google і рекламодавцями. За його словами, показник CTR (click-through rates, відсоток клікабельності. – Ред.) зріс на рекламі тих клієнтів, які на сторінці своїх брендів у Google+ додали дані користувача – наприклад, кількість користувачів, що рекомендували продукт, натискуючи на «+1». «Залежно від конкретного випадку, показник CTR може вирости від 2 до 15 %», – пояснює А. Остек.

Єдиний акаунт уже приніс компанії свої плоди. Наприкінці року Google відзвітував про 235 млн користувачів, які тією чи іншою мірою використовували функції Google+, наприклад, кнопку «+1» – аналог кнопки Like на Facebook. Для порівняння, у середині 2012 р. ішлося про 150 млн користувачів. Використовуючи всі свої сервіси для «допомоги» Google+, компанія демонструє всю серйозність намірів у протистоянні з Facebook за можливість бути головним «медіатором» між користувачами та бізнесом.

Але боротьба з Facebook не єдина версія, яка пояснює особливі зусилля, докладені Google для розвитку своєї «нетипової соцмережі». Нещодавно «хід конем» зробив найбільший онлайн-магазин Amazon, запустивши власну рекламну мережу і ставши тим самим третім серйозним претендентом на панування в сегменті таргетованої реклами. Нехай, на відміну від того самого Facebook, Amazon нічого не знає про друзів і соціальну активність своїх покупців. Але велика історія покупок дасть змогу інтернет-магазину по-своєму точно таргетувати рекламу. Адже суть всієї реклами, у кінцевому рахунку, зводиться до покупок.

З появою третього великого гравця баланс сил на ринку таргетованої онлайн-реклами виглядає таким чином:

• Google. Традиційно домінує у сфері відстеження купівельних намірів. Тобто якщо користувач шукає інформацію про товар, то в більшості випадків він до нього прицінюється.

• Facebook. Володіє найбільшою базою даних персональної інформації – більше ніж 1 млрд користувачів, включаючи їхні інтереси і друзів. Така інформація надзвичайно важлива для маркетологів, які вивчають попит і купівельні переваги.

• Amazon. Володіє найактуальнішою базою даних з пошуку товарів і здійснених покупок. Ця інформація – на вагу золота для рекламодавців.

Донедавна дані Google про покупців, їхні покупки і демографію не були настільки повними і доречними, як у Facebook або Amazon. У міру

інтеграції сервісів Google в рамках єдиного акаунта збирані дані становитимуть дедалі більший інтерес для рекламодавців. У цьому сенсі саме Google зможе зібрати більш вичерпне досьє на потенційного покупця, ніж Facebook і Amazon кожен окремо.

Д. Едвардс, редактор Business Insider, вважає ситуацію, що склалася, вельми спірною з позиції приватності інтернет-користувачів: «Персональні дані – це актив, який має свою цінність. І Google, так само, як Facebook з Amazon, збираючи дані користувачів і заробляючи з їхньою допомогою мільярди, ніяк не компенсують користувачам цей актив. А разом із персональними даними користувачі втрачають і анонімність».

«Тепер, коли на сцену виходить Amazon, заступаючи шлях рекламного бізнесу Google, захист цього "друкарського верстата" стане для пошукача головним пріоритетом», – резюмує Д. Едвардс ***(Google «зганяє» користувачів у глобальне інтернет-гетто // Ua.comments.ua (http://ua.comments.ua/ht/196786-google-zganyaie-koristuvachiv-u-globalne.html). – 2013. – 1.03).***

***

Вам не нравилось, что вездесущий Facebook следит за вашими действиями даже на сторонних сайтах? Оказывается, это были цветочки: теперь Facebook сможет таргетировать рекламу, основываясь на нашем покупательском поведении даже в оффлайне. Такая возможность появится в ближайшие недели и поначалу будет доступна только американским компаниям.

Еще в сентябре 2012 г. соцсеть запустила специализированный инструмент Custom Audiences, который позволяет рекламодателям идентифицировать своих клиентов с их профилями в Facebook по учетным данным в соцсети, телефонному номеру или адресу электронной почты.

Это значит, что информацию о клиентах, которой владеют компании, можно соотнести с данными о пользователях Facebook. Другими словами, каждого, кто оставлял компании данные о себе даже в оффлайне (к примеру, заполнял анкету для получения карты лояльности), можно легко найти в Facebook. Разумеется, для того, чтобы показывать ему таргетированную рекламу.

На днях Facebook сообщил о заключении соответствующих соглашений с фирмами Datalogix, Acxiom, Epsilon и BlueKai. Теперь возможности Custom Audiences расширятся за счет данных этих компаний. В результате рекламодатели смогут таргетировать рекламу на покупателей конкретных товаров или услуг, например, на любителей прохладительных напитков или на тех, кто планирует покупку автомобиля.

Безусловно, эта новость порадует рекламодателей, которые смогут демонстрировать рекламу именно тем, кому она будет наиболее интересна. Да и самим пользователям Facebook это на руку: они будут видеть более релевантную рекламу, которая действительно может их заинтересовать.

В то же время у тех, кто обеспокоен «слежкой» компаний и протестует против использования своих персональных данных в рекламных целях, появился новый повод для тревоги. Впрочем, представители соцсети поспешили успокоить пользователей, подчеркнув, что Facebook не собирается делиться их персональными данными с другими компаниями ***(Facebook будет следить за пользователями даже в оффлайне // InternetUA (http://internetua.com/Facebook-budet-sledit-za-polzovatelyami-daje-v-offlaine). – 2013. – 2.03).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Несмотря на то, что социальные сети могут вызвать депрессию, их влияние на здоровье может быть и положительным. Исследователи из Университета Аризоны выяснили, что использование Facebook способствует умственной деятельности пожилых людей и улучшает их настроение.

Необычное исследование провела Ж. Волтман, аспирант психологического факультета в Университете Аризоны. Ее работа показала, что пожилые люди, умеющие пользоваться популярными социальными сетями, чувствуют себя менее одинокими. Кроме того, у них улучшается память и другие навыки. Пожилые пользователи Facebook на 25 % лучше справлялись с тестами на запоминание, чем их менее продвинутые сверстники.

Правда, вряд ли эти цифры являются по-настоящему точными, учитывая маленький размер фокус-групп. Ученые привлекли к исследованию 28 человек в возрасте от 68 до 91 года. До начала исследования все эти люди не пользовались соцсетями. Первую группу из 14 пожилых людей научили пользоваться Facebook и попросили писать посты в соцсеть не реже раза в день. Вторую группу попросили освоить платформу онлайн-дневников Penzu. На этом ресурсе записи приватны, синхронизации с соцсетями нет.

Пожилые американцы ежедневно пользовались соцсетями в течение двух месяцев, после чего ученые провели ряд исследований, чтобы выяснить, как эти ресурсы на них влияют. Если показатели пользователей Penzu практически не изменились, то пожилые пользователи Facebook почувствовали себя счастливее, их мозговая деятельность активизировалась.

Ж. Волтман предполагает, что положительный эффект достигается благодаря постоянному обновлению ленты в Facebook, которое заставляет мозг концентрироваться на новой информации. Более того, соцсеть позволяет старикам восполнить крайний недостаток общения, от которого страдают многие пожилые люди.

«Facebook – это великий феномен в нашей культуре», – пишет Ж. Волтман, – Уже проведено множество исследований о том, как пользуются Facebook молодые, но мы практически ничего не знаем о том, как активность в соцсетях сказывается на пожилых. Людей старшего возраста на Facebook становится все больше и больше, вот почему было так важно провести это исследование».

Однако регистрация в сети имела возрастные ограничения. Те, кому исполнилось более 100 лет, не могли стать пользователями соцсети. Так, 104-летняя жительница США М. Джозеф не смогла указать дату рождения, так как интерфейс сайта позволяет указывать возраст лишь до 99 лет ***(Исследователи: Facebook делает пожилых людей счастливыми // Utro.ua (http://www.utro.ua/ru/zhizn/issledovateli_facebook_delaet_pozhilyh_lyudey_schastlivymi1361522738). – 2013. – 22.02).***

***

С каждым годом количество времени, которое мы проводим в социальных сетях, увеличивается; именно здесь мы общаемся с друзьями, делимся своими мыслями и чувствами. VoIP-компания Rebtel провела исследование, целью которого было выяснить, насколько социальные сети влияют на эмоциональное состояние человека.

Как выяснилось, сильнее других соцсетей на наше настроение влияет Facebook. Хотя большинство респондентов сообщает, что ни одна социальная сеть не способна испортить им настроение, те, у кого соцсети все-таки вызывают негативные эмоции, чаще всего говорят именно о Facebook (19,4 %), реже – о Twitter (4,7 %) и LinkedIn (4,1 %).

В то же время Facebook лидирует и в списке соцсетей, повышающих настроение: почти 46 % опрошенных заявили, что Facebook дарит им положительные эмоции. Аналогичным эффектом, хотя и гораздо менее выраженным, обладает YouTube – 17,5 %, следом идет LinkedIn (6,5 %).

Особенное внимание авторы исследования уделили отметкам с помощью геолокационных сервисов. По данным опроса, большинство пользователей отмечают свое местоположение в Foursquare или Facebook для того, чтобы сообщить друзьям и семье, где они находятся (34,6 %) или получить специальные предложения от компаний (22,9 %). При этом почти каждому второму (45 %) не нравится, когда его местоположение отмечают другие люди ***(Facebook сильнее других соцсетей влияет на настроение // InternetUA (http://internetua.com/Facebook-silnee-drugih-socsetei-vliyaet-na-nastroenie). – 2013. – 22.02).***

***

В соцсетях набирает обороты новое развлечение: женщины выкладывают в Интернет свои «нормальные» фото – и рядом себя же, с лицом, искаженным до безобразия. Попросту говоря, строят рожи. И чем чуднее получается, тем лучше.

Началось все в июле прошлого года, когда симпатичная брюнетка по имени Кристен разместила в сети два своих фото – обычное и «уродливое». Народ лайкнул, а после этого началось – девчонки изгаляются, кто как может: закатывают и таращат глаза, надувают щеки, морщат нос, скалятся во весь рот. Об этом пишет ЭГ.

И весь этот «паноптикум» выкладывают в Интернет. Фишка в том, чтобы поставить два фото вместе, – важно видеть изображение до и после. На страничке под названием «Симпатичные девочки, делающие уродливые лица», уже больше 11 тыс. подписчиков.

Таким образом, считают администраторы сайта, дамы сбрасывают с себя обязанность все время хорошо выглядеть и не боятся быть смешными и глупыми. И призывают: «Расслабьтесь и станьте дикими. Покажите, насколько ужасным может быть ваше лицо. Чем уродливее вы выглядите, тем лучше у вас будет карма и тем счастливее станут люди на планете!»

Пользователей просят только об одном: не оставлять под фото вредные или уничижительные замечания. Начинание подхватили и мужчины. Но пока смельчаков мало – в «мужском» разделе всего около 200 подписчиков ***(Молодые женщины уродуют себя в соцсетях // From-UA (http://www.from-ua.com/news/3b69a60d18a32.html). – 2013. – 20.02).***

***

Министерство внутренних дел принимает меры по блокированию интернет-игры, которая послужила причиной гибели 12 детей в Черкасской области. Об этом сообщил председатель Нацкомиссии Украины по вопросам защиты общественной морали В. Костицкий во время онлайн-конференции в Киеве.

По его словам, интернет-игра, распространяемая через социальные сети, «Собачий кайф» стала причиной 12 случаев суицида среди детей в Черкасской области. Этот вопиющий случай вынудил Нацкомиссию обратиться в Генпрокуратуру, МИД и МВД страны с требованием принять меры по недопущению распространения опасной игры на территории страны.

В. Костицкий сообщил, что МВД уже откликнулось на обращение комиссии и пообещало, что примет меры по блокированию интернет-игры, передает Gloss.ua.

«Собачий кайф» – игра с асфиксией (удушьем), когда умышленно перекрывается доступ кислорода к мозгу с целью вызвать кратковременный обморок и состояние эйфории. Участник игры садится на корточки у стенки и глубоко и быстро дышит в течение 35 с., потом встает, опираясь о стену. Второй участник должен передавить горло полотенцем и душить его около 5−7 с. – пока тот не потеряет сознание и как бы не переместиться в «параллельный» мир.

Игра стала довольно популярной среди подростков Украины, России и других постсоветских республик, которые много времени проводят в социальных сетях. В прессе в течение минимум четырех лет неоднократно

появлялась информация о попытках удушения, которые часто приводили к летальным последствиям ***(От «Собачьего кайфа» погибло уже 12 детей: МВД блокирует Интернет-игру // MIGnews.com.ua (http://mignews.com.ua/ru/articles/133035.html). – 2013. – 21.02).***

***

Сотрудники Технологического университета штата Джорджия в Атланте (США) провели исследование, в ходе которого ответили на вопрос – как стать суперпопулярным пользователем Twitter, если сам не являешься знаменитостью? По мнению учёных, сообщает NewScientist, для этого нужно быть общительным, грамотным, позитивным и не зацикленным на своей особе человеком.

Группа сотрудников Технологического университета штата Джорджия в Атланте, под управлением С. Д. Хатто, в течение 15 месяцев отслеживала 500 обычных микроблогов в Twitter, тщательно анализируя, появляющиеся там записи. Учёных интересовали употребляемые пользователями слова, их эмоциональная окраска, количество ругательств и сленга, а также популярных в сети сокращений, типа ЛОЛ (много смеха или громко смеяться).

В итоге американские учёные выяснили, что стать звездой Twitter, при удачных обстоятельствах, может каждый, чьи твиты несут позитивную информацию, написанную простым и понятным языком. Огромной популярностью при этом пользуются постоянные ретвиты занимательных новостей, а вот твитты о переживаниях и подробностях жизни пользователя внимания не привлекут.

«Twitter в основном используется для передачи новостей. Моих подписчиков не волнует, что я ел на завтрак, но они проявляют огромный интерес, если я раскопаю какую-нибудь интересную новость», – объясняет этот феномен сотрудник Технологический университет штата С. Д. Хатто.

Кроме того, для достижения успеха не стоит пренебрегать своими подписчиками. То есть нужно постоянно отвечать на их комментарии и как можно чаще ретвитить их записи и упоминать о них в своем микроблоге, так как в противном случае интерес подписчиков к микроблогу пользователя резко «охладевает».

Окончательные результаты этого исследования сотрудники Технологического университета штата Джорджия в Атланте (США) планируют огласить в апреле в Париже, где должна состояться конференция, посвящённая человеческим факторам в компьютерных системах ***(Учёные: звездой Twitter может стать любой интернет-пользователь // UkrNews24 (http://ukrnews24.com/uchyonye-zvezdoj-twitter-mozhet-stat-lyuboj-internet-polzovatel/). – 2013. – 1.03).***

***

Исследователи выяснили, что главной причиной, по которой социальные сети теряют популярность, является усложнение процесса ведения аккаунта. MIT Technology Review представляет в своем блоге результаты научной работы ученых из Швейцарской высшей технической школы Цюриха.

В качестве предмета для изучения группа ученых под руководством Д. Гарсии выбрала социальную сеть Friendster, которая после падения популярности была преобразована в социальный игровой портал. При помощи архива Интернета исследователи провели цифровое «вскрытие» успешной в прошлом социальной сети и выяснили, что главная причина ухода пользователей – увеличение количества времени и сил, которые необходимо тратить для ведения аккаунта.

Массовому уходу пользователей способствует их зависимость от друзей. Отказ одного пользователя от сети заставляет его друзей задуматься о том же, что в конечном итоге может привести к потере большого количества посетителей социального портала. Вместе с тем анализ топологии дружеских взаимосвязей в успешных и уже закрытых сетях показал, что у таких популярных ресурсов, как Facebook и Livejournal, устойчивость к обвальной потере пользователей меньше, чем у Friendster в лучшие годы.

Ученые пришли к выводу, что главной задачей, которую предстоит решать создателям социальных сетей, является оценка соотношения выгод и затрат, с которыми сталкивается пользователь. Пример Friendster, по мнению авторов научной работы, показал, что даже плотное переплетение дружеских связей не удержит посетителей в случае резкой негативной реакции на технические трудности или смену дизайна.

Friendster была создана в 2002 г. и считается одной из первых социальных сетей. После радикальной смены дизайна в 2009 г. портал столкнулся с потерей популярности и упал на 800 место в рейтинге посещаемости Alexa (ранее поднимался до 40). В 2011 г. сайт был перезапущен как игровой портал, который сегодня пользуется популярностью в юго-восточной Азии ***(Ученые установили причины смерти социальных сетей // Версии.com (http://versii.com/news/274177/). – 2013. – 1.03).***

Маніпулятивні технології

КНДР распространила на Youtube новый видеоколлаж, на котором президент США Б. Обама и американские солдаты сгорают в пламени ядерного взрыва. Ролик был размещен спустя две недели после того, как на этом же хостинге появилось видео с кадрами Нью-Йорка в огне после ракетного удара.

В тексте, сопровождающем новый видеоколлаж, говорится, что «США практически привели КНДР к проведению ядерного испытания, которое служит сдерживающей силой».

Прежний ролик был удален с хостинга после того, как выяснилось, что ряд кадров при его создании был взят из игры Call of Duty, из-за чего ее создатели пожаловались руководству YouTube.

Напомним, накануне КНДР провела очередные ядерные испытания, устроив подземный ядерный взрыв ***(КНДР распространила на Youtube новый видеоколлаж с горящим Обамой // Левый берег (http://world.lb.ua/news/2013/02/20/189913_kndr_rasprostranila_youtube_noviy.html). – 2013. – 20.02).***

***

Популярные в настоящее время социальные сети как Facebook и Twitter стали не только грозным оружием Скотланд-Ярда по поимке преступников, но и большой угрозой для обычных людей со стороны киберпреступников, среди которых особо опасны работорговцы. Об очередном случае похищения девочки в Индонезии сообщило агентство Ассошиэйтед-Пресс.

14-летняя индонезийка добавила в список своих друзей в соцсети Facebook незнакомого человека, после чего ему стал известен её домашний адрес, возраст и другая информация. Этих данных было достаточно для того, чтобы выследить и похитить ничего не подозревающую жертву и долгое время удерживать ее в неволе. Преступник планировал отвезти девочку на один из индонезийских островов и продать в рабство. Но у похитителя не оказалось денег на дорогу даже в один конец и он бросил свою жертву на первой же автобусной остановке. Его так и не нашли.

«Такова судьба не одной единственной девочки из Индонезии, а многих женщин в Юго-Восточной Азии. Например, на Филиппинах людей часто похищают с помощью уловок не только в соцсетях, но и при SMS-переписке, – сообщила Л. Клин, представительница в ЮВА некоммерческой организации Terre des Hommes Netherlands по вопросам похищения людей. – В основном, такие мошенники нацелены на молодежь, как самую уязвимую социальную группу, поэтому мы всегда должны думать о том, что выкладываем в сети, и какие могут быть последствия публикаций, а заодно и приучать к осторожности собственных детей» ***(Социальные сети стали опасным оружием в руках похитителей людей // ТАСС-Телеком (http://tasstelecom.ru/news/one/17125). – 2013. – 26.02).***

***

Facebook превращается в социальную ферму?

Как сообщает AIN.UA, контент-фермы, которые долгое время были бичом поисковика Google, выдавая бесполезный хлам за релевантные результаты, теперь мигрировали в Facebook. Из социальной сети постепенно высасывают, собственно, социум, делая ее скорее контентной сетью. А

точнее фермой. Возможно, вы не слышали о таком понятии, как контент-ферма, но в наверняка сталкивались с ними в Интернете.

Вот как они работают в Google: вы делаете поисковой запрос, переходите на результат в поисках ответов на свои вопросы, а вместо этого натыкаетесь на абсолютно бесполезный для вас контент. Под контент-фермами подразумевают сайты, которые платят копейки за дешевые статьи низкого качества, тем не менее соответствующие по оформлению всем требованиям поискового алгоритма Google. Несмотря на соблазнительные заголовки, эти статьи неизменно разочаровывают по содержанию.

Как вам такое руководство, обещающее сделать из вас актера?

Шаг 1: Решите, кем вы хотите стать – профессионалом или аматором. Шаг 2: Переезжайте в большой город.

Для контент-ферм качество не важно. Все, что имеет значение – это ваш клик в Google – краткий момент, когда ваши глаза выхватывают рекламу на их сайте. Фермы с их потоками контентного хлама – это просто новая форма спама, из-за которой Сеть постепенно теряет свое ключевое значение.

В 2011 г. Google представил твики для своего алгоритма, предназначенные урезать власть ферм над поисковой выдачей. И эти изменения какое-то время работали. Однако вместо того, чтобы сначала поблекнуть, а позже и вовсе исчезнуть, некоторые фермы просто переместились на еще более плодородную почву. На Facebook их засилье возможно благодаря распространению посредством «лайков» и «шеиров» одноразового визуального контента – дурацких ничего не значащих картинок.

Сайты вроде Stylish Eve добиваются успеха благодаря дьявольски простой формуле. Эта базирующаяся в Египте компания царствует в Facebook в виде набора чрезвычайно успешных аккаунтов, посвященных стилю и образу жизни под такими именами, как «Наряды», «Декор для дома» и «Каблуки». Каждая из этих «дочек» представляет собой поток из (в большинстве краденных) картинок на ряду со спамовыми ссылками, рекламирующими родственные сайты сети или родительский StylishEve.com. Качество контента уходит на второй план, на первом неизменно объем. Например, последний пост про идеи подарков ко Дню святого Валентина представляет собой коллекцию вырванных из контекста изображений из разнообразных онлайн-каталогов. Текст, разумеется, не лучше – складывается впечатление, что его писал ученик младших классов.

Более 5 млн людей уже подписаны на страничку Stylish Eve в Facebook. Каждый день подписчики жалуются на то, что сайт не предоставляет ссылок на источники информации. Но руководство сайта их игнорирует. Stylish Eve стремиться удержать пользователей на своих страницах, а их глаза – на своем контенте, а точнее, на рекламных объявлениях. Какое-то время Stylish Eve без разрешения эксплуатировал контент сайта Polyvore. На этом ресурсе пользователи могут объединять вещи из интернет-магазинов в комплекты в режиме онлайн.

Флагманская спам-страничка Stylish Eve в Facebook под названием «Наряды» существует и пользуется популярностью именно благодаря потоку этих картинок, сворованных прямиком из профайлов на Polyvore. Без разрешения, разумеется. Сообщество Polyvore было шокировано подобной наглостью. Пользователи, чьи комплекты были без разрешения опубликованы на страничке «Наряды», запустили протест под лозунгом: «Будьте оригинальны. Не копируйте чужие комплекты». Но это не помогло.

Через несколько дней после взрыва негодования в интернет-сообществе Polyvore, спам-империя Stylish Eve постаралась себя обелить. Со мной связался руководитель компании, 25-лентний египтянин по имени А. Хельми. Хвастаясь, что его страница получила 70 тыс. новых фоловеров в день, когда разгорелся скандал, А. Хельми заявил, что «не было никакой необходимости» в публикации моей истории. Он утверждал, что Stylish Eve не спам, а скорее «онлайн-журнал», который дает людям идеи для их собственных модных ансамблей. Он закончил свою речь странной угрозой послать мою статью Google, «чтобы они могли посмотреть, как вы оцениваете их работу».

А. Хельми сравнил Stylish Eve с такими сайтами как HGTV, которые также постят коллекции картинок, чтобы дать пользователям идеи дизайна без указания источника информации. «Многие люди хотят видеть на сайте ссылки на источники, но этот журнал их не публикует», – сказал А. Хельми. Он упустил из виду ключевой факт: фотографии на HGTV бесплатно присылают сами дизайнеры, чтобы получить отклик о своей работе.

Но и это еще не все. А. Хельми сказал, что извинился перед пользователям Polyvore, чей контент был сворован. Он сказал, что даже предлагал работу дизайнера одному из моих информаторов, и собирался платить ей за публикацию ее комплектов на страницах Stylish Eve в Facebook. Я спросил, извинился ли он перед каждым пользователем Polyvore, чей контент он украл. А. Хельми ответил «да». Однако это было лишь частично правдивое заявление. Я связался с несколькими людьми из пользователей Polyvore, чьи коллажи появлялись без их разрешения на страницах Stylish Eve в Facebook, и спросил, получали ли они подобные предложения. Некоторым действительно предлагали работу, но с большинством никто не связывался и извинений не приносил.

Но суть не в этом. Даже если бы Stylish Eve платил всем создателям украденных сетов, и даже если бы перестал воровать их, изменило бы это что-нибудь? В конце-концов, проблема не в морали бизнес-модели Stylish Eve, а в будущем, которое она прочит Facebook – социальная сеть превращается в имиджборд. Спам-сеть постит фотографии, вот и все. Множество фотографий без комментариев, без контекста, без указания источников – день за днем сплошным потоком. Это стало возможным потому, что в сентябре 2011 г. Facebook сделал одно знаковое изменение – в разы увеличил скорость загрузки изображений. Данное улучшение должно было сделать вашу визуальную связь с друзьями более быстрой и личной. Но

эффект оказался противоположным. Текстовые статусы сменились картинками и фото, которые отнюдь не были личными – сеть заполонили мемы и фото, взятые непойми откуда из интернета, и взорвали Facebook посредством вирусного распространения через «лайки» и «шеиры».

В сентябре 2012 г. компания изменила алгоритм, который определяет, какие посты будут отображаться в ленте новостей. Таким образом Facebook хотел ограничить количество информационного хлама, которым пользователей забрасывают их псевдо друзья. Но на деле идея состояла в том, чтобы резко сократить досягаемость их страниц для брендов. Злые SMM-менеджеры увидели, как стремительно сокращается их аудитория. Приходилось платить много денег, чтобы показать пользователям свои посты. Для многих, чьи потоки контента были достаточно велики, сумма проплат достигала порядка 700 тыс. дол. в год.

В ста метрах от собственного банкротства ради достижения своей же аудитории брендированным страницам осталось одно единственное решение. Новый алгоритм Facebook поощрял вовлечение – «лайки» и «шеиры». То есть успешному посту необходимо было только задать импульс, подобно снежному кому. Как доказывают Stylish Eve и другие ему подобные, в гонке за лайками картинки являются самым верным способом оставаться в топах. Еще один пример – это набор страниц для тинейджеров, негласно возглавляемый сообществом Teen Swag. Им управляют анонимные администраторы, которые, возможно, вовсе даже и не тинейджеры. Они постят предсказуемый поток дурацких фотографий и призывов «лайкать и делиться» всем подряд без разбору. Страницы пропагандируют идиотскую философию так называемого «письма счастья». И они завалены спамом.

Нельзя сказать, что Stylish Eve, тинейджерские страницы и другие контент-фермы имеют более низкую культурную значимость, чем все остальное, что сегодня присутствует на Facebook. Лайкнуть статус своего приятеля о том, как он всю ночь безудержно тусил на дне рождения – это тоже действие не особого эмоционального или интеллектуального характера. Но Facebook задумывался для настоящих людей – про их жизнь, про все те глупые, прекрасные, мерзкие, гениальные и скучные вещи, которые мы с вами совершаем каждый день.

Контент-спаму не место там, где живут настоящие люди. И тем не менее, все больше и больше места ему находится на Facebook ***(Facebook превращается в социальную ферму? // AIN.UA (http://ain.ua/2013/02/25/113969). – 2013. – 25.02).***

Зарубіжні спецслужби і технології «соціального контролю»

Сайт Лиги безопасности Интернета в ближайшее время пополнится собственной социальной сетью. Об этом сообщает smonews.ru.

Это будет закрытая сеть для своеобразной кибернетической дружины, целью которой является выявление распространителей детской порнографии

в Интернете. В настоящее время в дружине состоят около 20 тыс. добровольцев. Новая сеть поможет им координировать свои действия, а так же получать задания от старших групп. Все члены дружины распределены по группам, и в каждой группе есть старший. Это так называемые десятники, сотники и тысячники.

Добровольцы охотятся не только за педофилами, но также и за распространителями пропаганды наркотиков, насилия, алкоголизма и суицида. Все результаты поисков сначала аккумулируются у старших групп, а затем передаются в Лигу безопасности Интернета для последующей их передачи в правоохранительные органы.

Кроме того, Лига часто сама выдает задания группам или даже отдельным кибернетическим дружинникам с указанием конкретного адреса размещенного материала. Дружинники же принимают все возможные меры для того, чтобы выяснить физический адрес отправителя и его настоящее имя.

За прошлый год благодаря «кибердружинникам» было возбуждено 150 уголовных дел по факту распространения детской порнографии. Однако дружина является достаточно уязвимой структурой. Ведь те же распространители и потребители детской порнографии могут без труда внедриться в эту сеть. Так что не все так однозначно ***(У Лиги безопасности Интернета будет своя социальная сеть // IT Expert (http://itexpert.in.ua/rubrikator/item/22917-u-ligi-bezopasnosti-interneta-budet-svoya-sotsialnaya-set.html). – 2013. – 18.02).***

***

Страницы террористических организаций в социальных сетях Twitter и Facebook чаще всего удаляют. Но гражданских активистов беспокоит, как это может повлиять на свободу слова.

В конце января Twitter закрыл страницу террористической группировки «Аль-Шабааб», которая располагается в Сомали и имеет связи с «Аль-Каидой». Это произошло после того, как группировка разместила в социальной сети видео с угрозами убить двух кенийских заложников, если власти Кении не выполнят ее требования.

Twitter никак не прокомментировал закрытие страницы, но эксперты по социальным сетям пришли к выводу, что «Аль-Шабааб» нарушила правила использования сети Twitter, запрещающие прямые угрозы насилия.

Эта схема становится всё более распространенной. Страница в Twitter или Facebook, имеющая связи с террористической организацией или напрямую управляемая ею, попадает в центр внимания, активисты и пресса поднимают шум, социальная сеть удаляет страницу – а через некоторое время появляется новая.

С тех пор как террористические группировки начали искать доступ к более широкой аудитории в мире, их появление в социальных сетях стало вызовом для Twitter, Facebook и им подобным. Но в то время как власти

стран хотят, чтобы социальные сети пресекали появление аккаунтов таких группировок, интернет-активисты призывают к большей прозрачности правил социальных сетей.

Научный сотрудник Вашингтонского института по политике на Ближнем Востоке А. Зелин недавно опубликовал доклад о том, как джихадистские группировки используют социальные сети. Большинство группировок после удаления страницы, по словам А. Зелина, просто открывают новую.

«Это создает ситуацию, похожую на игру “поймай крота”, когда что-то уходит из сети, но потом создает новую страницу и находится какое-то время в сети, и потом ее снова удаляют из сети, так что это как игра в “кошки-мышки”», – говорит А. Зелин.

Именно это произошло в декабре прошлого года в Пакистане: Facebook закрыл страницу «Умар Медиа» – информационной ветки пакистанского «Талибана», поскольку посчитал, что она нарушает правила Facebook, будучи сторонником страниц, пропагандирующих терроризм. Две недели спустя появилась новая страница «Умар Медиа», но остается неясным, принадлежит ли она одной и той же группе.

Как частные компании, Facebook и Twitter могут допустить кого угодно на свои платформы. Однако, в связи с огромным количеством пользователей по всему миру, некоторые эксперты по теории Интернета называют их «общественным местом» – глобальной городской площадью в цифровую эру.

Многие считают Twitter лидером среди социальных сетей по приверженности свободе слова, однако некоторые активисты выражают обеспокоенность по поводу недостаточно четкой политики сети по отношению к экстремистским и террористическим организациям.

«У Twitter нет как таковой политики по отношению к террористическим организациям у себя на платформе. Если кто-то подстрекает кого-то или группу людей к насилию и эта угроза неотвратима, то они удалят страницу, как это произошло с “Аль-Шабааб”», – говорит А. Зелин.

Эксперт по цензуре в Интернете и старший научный сотрудник фонда «Новая Америка» Р. МакКиннон говорит, что помимо введения правил пользования сайтами, регулирующих поведение пользователей и самой платформы, социальные сети также должны подчиняться законам тех стран, в которых действуют.

В части требований властей Twitter, к примеру, действует в зависимости от страны.

«Надеюсь, их действия отвечают на юридически обязывающие запросы. Таким образом, если власти направляют юридически обязывающее требование и явно показывают, что содержание конкретного вопроса противозаконно, то сеть обязана его удалить или заблокировать», – говорит Р. МакКиннон.

В октябре 2012 г. Twitter заблокировал страницу неонацистов по просьбе немецких властей, посчитавших, что страница нарушает законодательство относительно разжигания ненависти.

В первых двух отчетах по прозрачности Twitter отметил устойчивое увеличение запросов властей на удаление содержания и уведомлений об авторских правах. В большинстве случаев, как сообщает Twitter, запросы на удаление не были удовлетворены.

Фонд «Электронная граница» – организация активистов в Интернете – также отметила увеличение запросов к Twitter со стороны властей США приостановить страницы предполагаемых террористических группировок.

По мнению Р. МакКиннон, Facebook является менее прозрачной в части получения запросов от официальных органов и того, каким образом эти запросы разрешаются.

Как отмечают некоторые эксперты, публикация информации на английском языке почти всегда активизирует системы фильтрования на Facebook и Twitter.

Писатель и антрополог С. Кендзиор говорит, что Facebook, возможно, не замечает присутствия некоторых террористических группировок потому, что они пишут не по-английски, и приводит в качестве примера «Союз исламского джихада», который пишет в основном по-узбекски.

А. Зелин также отмечает, что страницы группировки «Аль-Шабааб» на арабском и сомалийском языках никогда не закрывали, хотя они содержат почти ту же информацию, что и англоязычная версия.

Пока террористические группировки продолжают пользоваться социальными сетями, борцы за свободу слова, скорее всего, усилят свои требования по более прозрачной политике в отношении экстремистских группировок. Принимая во внимание также желание властей отрезать доступ таким группировкам, социальные сети должны будут решать, где провести границу ***(Клевцова А. Как социальные сети обращаются с террористами? // Радио Азаттык (http://rus.azattyq.org/content/terrorist-accounts-in-social-networks/24907251.html). – 2013. – 20.02).***

***

Английская судебная система собирается принять закон, позволяющий использовать данные электронной переписки. Судебные приставы не погнушаются прочитать личные сообщения, отправленные через социальные сети Facebook, LiveJournal, сервисы, созданные для общения. Принятый закон может коснуться отечественных предпринимателей, подписывающих контракты с иностранными партнерами. В случае судебных разбирательств, доказательствами окажутся неожиданные вещи, полученные путем взлома социальных сетей. Согласно внесенному предложению, арбитражным судом используются доказательства электронной почты, сообщения социальных сетей.

И. Тимчишин, являющаяся экспертом международного арбитража, объяснила возможные последствия принятого законопроекта. Электронные документы легко фальсифицировать, в случае выявления факта подделки подобных доказательств, решение окажется негативным для стороны, решившейся на фальсификацию электронных данных ***(Социальные сети и электронные письма станут доказательством в суде // Delate.info (http://delate.info/2272-socialnye-seti-i-elektronnye-pisma-stanut-dokazatelstvom-v-sude.html). – 2013. – 26.02).***

***

В последние годы в Нью-Йорке (США) уровень тяжких преступлений, таких как убийства, постоянно уменьшается. В прошлом году было зафиксировано рекордно низкое их число – 414. И темпы продолжают падать.

Как оказалось, не последнюю роль в столь радостной статистике играют социальные сети наподобие Facebook и Twitter. Нью-йоркские полицейские приноровились постоянно мониторить новые сообщения в популярных сетях и блогах, выявляя письменные потенциальные угрозы от членов мелких банд.

По данным полиции, именно на небольших преступных группировках лежит вина в почти трети всех перестрелок в городе. Специальные команды защитников правопорядка SET (Strategy Enforcement Teams), созданные во всех округах мегаполиса, просеивают тонны твитов и постов, авторство которых принадлежит известным полиции личностям. В результате полученной информации было проведено несколько успешных операций по задержанию гангстеров, по размаху напомнивших события по зачистке мафиозных структур в 70–80-х годах прошлого века.

Остается только порадоваться за стражей порядка, которые сумели обратить на благо общества болтливость и развязанность людей с криминальной историей ***(Полиция Нью-Йорка использует социальные сети для предотвращения убийств // InternetUA (http://internetua.com/policiya-nua-iorka-ispolzuet-socialnie-seti-dlya-predotvrasxeniya-ubiistv). – 2013. – 3.03).***

Проблема захисту даних. DOS та вірусні атаки

Мошенники внедряют новую технологию кражи денег с пластиковых карт – «шимминг». Она позволяет абсолютно незаметно похитить номер банковской карты, ее PIN-код и другие данные через банкомат.

Мошенники изобрели новый способ кражи данных и денег с банковских карт. В отличие от «традиционных» методов, новое устройство, которое тоньше человеческого волоса, клиент не видит, что и делает его практически беспомощным перед преступниками.

Мошенники, специализирующиеся на кредитных картах, разработали новую технологию – «шимминг», позволяющую похитить номер банковской карты, ее PIN-код и другие данные через банкомат. Об этом сообщил специалист Cisco Systems Д. Хири в блоге Cisco Security Expert со ссылкой на компанию-производителя бакноматов Diebold. По оценкам последней, из-за шимминга финансовые организации и частные лица теряют миллиарды долларов в год.

Устройства для кражи данных прошлого поколения, получившие название «скиммеры», представляли собой накладки на банкоматы. Шиммеры, в отличие от них, незаметны: тонкая гибкая плата вставляется через щель картридера (устройство для приема карт) и считывает данные введенных карт. «Такой тип мошенничества нетривиален с технической точки зрения, – чуть ли не восхищается ловкостью злоумышленников эксперт из Cisco Systems. – Прокладка должна быть очень гибкой и тонкой. Фактически, она должна быть тоньше 0,1 мм в большинстве случаев, чтобы уместиться в картридере и не мешать введению кредитных карт».

Чтобы более зримо представить, какое мастерство нужно для изготовления мошеннического устройства, эксперт приводит сравнения: толщина кредитки – примерно 0,76 мм, крупицы соли – 0,5 мм. Толщина человеческого волоса – около 0,18 мм. То есть плата для шимминга должна быть почти в два раза тоньше волоса.

По данным эксперта, такие устройства недавно начали массово выпускаться и уже «широко используется в некоторых частях Европы». В компании Diebold BFM.ru заявили, что знают о существовании этой разновидности мошенничества. «Однако о случаях ее применения в России нам пока ничего не известно, – сказал BFM.ru системный инженер компании Diebold в России и СНГ И. Стригин. – Для борьбы со всеми известными способами скимминговых атак на банкоматы (и в том числе с шиммингом) у нас уже есть портфель антискимминговых решений и сервис удаленного мониторинга Diebold ATM Security Protection Suite.

В портфель входит специальное устройство, создающее электромагнитное поле вокруг банкомата и мешающее скиммеру или шиммеру считывать информацию с магнитной полосы банковской карты в картридерах, так что данные владельца карты оказываются надежно защищены».

Российские банки пока не сталкивались с шиммингом. «Классикой» российских карточных мошенников остается скимминг, то есть получение доступа к данным карты путем установки устройств на картридер в банкомате с последующей подделкой карты. «Злоумышленники любят использовать и механические устройства. Например, преступники устанавливают в картридер крючки и щупы, карточки застревают в банкомате, и становится возможной их кража. Этот вид мошенничества называется фишингом», – говорит представитель Diebold.

Для кражи PIN-кодов и персональной информации клиентов преступники подсматривают, как люди пользуются банкоматом, для чего рядом с банкоматом устанавливают миниатюрные видеокамеры. «Кроме того, преступники могут перехватывать PIN-коды, когда они пересылаются с клавиатуры во внутренний компьютер. Для этих целей используются проводные отводы в банкоматах или осуществляется удаленная запись электромагнитного излучения электропроводки банкомата, – говорит И. Стригин. – Распространены и различные способы захвата и извлечения банкнот из презентера банкомата».

Еще более изощренным способом мошенничества являются манипуляции с операционной системой банкоматов: преступники вторгаются в компьютерную сеть банкоматов для кражи денег и получения информации о счетах. «Кроме того, хакеры создают небольшие программы, называемые вирусами и червями, которые самостоятельно распространяются через Интернет и могут нанести серьезный ущерб компьютеру внутри банкомата», – перечисляет эксперт.

Рекомендации экспертов по тому, как обезопасить себя и свои банковские карты от скимминга, традиционны: не сообщать никому PIN-код, подключить SMS-оповещение о состоянии счета, использовать банкомат, находящийся под видеонаблюдением и в людном месте, и обращать внимание на его внешний вид. «Кроме того, может быть полезно просто прикрыть ладонью клавиатуру во время ввода PIN-кода и обратить внимание на людей позади. Не стоит оставлять квитанцию в банкомате», – напоминает И. Стригин из Diebold.

Однако против такого способа мошенничества как шимминг клиенты ничего сделать не смогут, вынуждены констатировать эксперты. «В случае шимминга никаких внешних устройств увидеть не удастся», – говорит А. Друкер из Москоммерцбанка.

«Главная рекомендация – обзаводиться чиповыми картами, которые защищены от такого типа мошенничества. Это в данном случае самый надежный способ, и не случайно наш банк в этом году переходит на чиповые карты», – заявил А. Вишняков из Unicredit. «Это, конечно, не сможет предотвратить считывание магнитной полосы карты и последующее ее копирование, но поможет клиенту впоследствии вернуть свои деньги, – добавляет эксперт Москоммерцбанка. – Дело в том, что скопировать информацию с чипа невозможно, по крайней мере, на данный момент таких фактов зафиксировано не было.

При использовании такой карты клиент банкомат обязан производить авторизацию по данным чипа, а не магнитной полосы, а в случае невозможности авторизации по чипу создавать транзакцию типа Fallback». Тогда практически в 100 % случаев мошеннических транзакций ответственность ляжет на банк-эквайер, которому принадлежит банкомат. Поэтому если кто-то скопирует данные магнитной полосы такой карты,

сделает ее дубликат и попытается снять деньги, у клиента будет намного больше шансов опротестовать подобную операцию, говорит А. Друкер.

Впрочем, как правило, мошенники предпочитают не связываться с подделкой таких карт, так как это слишком сложно и дорого, отмечает вице-президент банка «Интеркоммерц» Д. Хренов.

«Честно говоря, несмотря на стремление максимально защитить клиента, его карту и внедрение новых технологических решений, уровень мошенничества не снижается, – заключает вице-президент Первого республиканского банка Д. Орлов. – В качестве основной рекомендации, наверное, стоит посоветовать клиентам чаще использовать карту как платежный инструмент, а не как средство для получения наличных» ***(Осторожно новая разновидность скимминга – Шимминг // Центр исследования компьютерной преступности (http://www.crime-research.ru/news/16.02.2013/7472/). – 2013. – 18.02).***

***

Хакеры из Бангладеша взломали сайт Одесской областной организации КИУ. На главной странице сервера они разместили угрозы о наказании от Аллаха.

Возможной причиной хакерского взлома может быть освещение местных выборов, проходивших в Болградском и Фрунзенском районах. Наблюдатели КИУ активно освещали ход голосования. «Пока нельзя утверждать ничего однозначно, но я не могу исключать, что такое совпадение неслучайно», – говорит глава Одесской облорганизации КИУ А. Бойко.

На сайте отображается обращение: «Все братья-мусульмане, помните о судном дне». Также взломщики разместили на сайте КИУ угрожающую фразу: «Мы идем» ***(Одесских избирателей атаковали террористы из Бангладеша // ИА «Репортер» (http://www.reporter.com.ua/news/unr/). – 2013. – 18.02).***

***

Серия хакерских атак была проведена на корпоративные системы Apple. Сценарий атаки выглядел так же, как и недавние события, связанные со взломом Facebook. На одном из сайтов разработчиков приложений были поражены ряд программ. После скачивания программ сотрудники компании занесли к себе на ПК вредоносное ПО, которое сразу же начало распространяться по всей сети. К счастью, компании удалось изолировать заражённые компьютеры, тем самым предотвратив утечку данных. Основная атака была направлена на слабо защищённые Java-плагины. (NovostiUA.net (http://novostiua.net/techniks/31347-hakery-dobralis-i-do-apple.html). – 2013. – 20.02).

В официальном сообщении руководства компании говорится о том, что хакеры, которые провели кибератаки на Facebook и Apple, относятся к одной

и той же группировке. Ещё ранее представители социальной сети заявили о том, что недавние события являются только частью массированных хакерских атак на крупные ресурсы американских компаний.

Эксперты говорят о том, что полностью обезопасить всю корпоративную систему почти невозможно. Ярким примером тому является последняя хакерская атака, следствием которой могла устать утечка данных. Об уязвимости платформы Java ещё месяц назад говорили представители Министерства внутренней безопасности США, которые настоятельно рекомендую отказаться от этого ПО ***(Хакеры добрались и до Apple // NovostiUA.net (http://novostiua.net/techniks/31347-hakery-dobralis-i-do-apple.html). – 2013. – 20.02).***

***

В атаке хакеров на серверы почти 40 американских компаний, включая Apple, Facebook и Twitter, подозревается группировка, которая базируется в Восточной Европе или России. Об этом сообщило агентство Bloomberg.

Хакеры, похоже, стремились получить секретную информацию Apple, покушаясь на ее интеллектуальную собственность, приводит агентство мнение представителей спецслужб США. Такие же атаки были предприняты в последнее время против социальных сетей Facebook и Twitter. По словам источников, хакеры использовали по крайней мере один сервер компании, которая базируется в Украине ***(В хакерской атаке на Apple, Facebook и Twitter заподозрили украинцев // Соціальна країна (http://sockraina.com/content/в_хакерской_атаке_на_apple_facebook_и_twitter_заподозрили_украинцев). – 2013. – 20.02).***

***

Антивирусная лаборатория PandaLabs опубликовала отчет о вирусной активности, включающий анализ мероприятий и происшествий в сфере IT-безопасности за прошедший год. Согласно отчету, 31,98 % всех проверенных компьютеров в мире содержали вредоносные программы. Общее количество всех образцов вредоносных программ в базе данных PandaLabs достигло примерно 125 млн, а исследователи PandaLabs подсчитали, что как минимум 27 млн новых образцов вредоносных программ было создано только в 2012 г. Три четверти новых образцов вредоносных программ, созданных в 2012 г., были троянами.

Эти цифры показывают возможности киберпреступников по автоматизации процесса создания новых вариантов вредоносных программ, а также свидетельствуют о том, что в среднем в сутки создавалось 74 тыс. новых угроз.

В 2012 г. трояны доминировали среди всех прочих угроз больше, чем когда-либо ранее. Три четверти вредоносных инфекций были вызваны троянами (76,56 %), что более чем на 3 % больше по сравнению с 2011 г. Одна из причин такого роста заключается в росте «популярности» наборов

эксплойтов, таких как Black Hole, которые способны использовать различные системные уязвимости для автоматического заражения компьютеров без вмешательства пользователя. Вирусы занимают второе место (8 %), в то время как черви опустились на третье место с 6,44 % от числа всех инфекций.

Среди самых инфицированных стран лидируют Китай, Южная Корея и Тайвань с 54,89 %, 54,15 % и 42,14 % зараженных компьютеров соответственно. Но есть и положительные новости: доля зараженных компьютеров во всем мире значительно снизилась. Например, количество инфицированных компьютеров в Китае упало с 56 % в 2011 г. до 54,89 % в 2012 г., а в Тайвани это снижение было еще более заметным – с 52 % до 42,14 %.

Страны с наименьшим уровнем заражения – Швеция (20,25 % инфицированных ПК), Швейцария (20,35 %) и Норвегия (21,03 %).

Помимо обзора наиболее значимых событий в сфере компьютерной безопасности в 2012 г., отчет также содержит прогнозы будущих тенденций на 2013 г. Киберпреступления и атаки на сайты социальных сетей 2012 г. останутся актуальными и в 2013 г. Особое внимание необходимо будет уделить защите сетей от уязвимостей операционных систем и приложений, использование которых становится все более распространенным со стороны киберпреступников и национальных спецслужб с целью скрытого взлома систем. Пользователи Android столкнутся с возрастающим числом атак со стороны киберпреступников. Кибершпионаж и кибервойны все чаще будут заявлять о себе в 2013 г., усугубляя проблему в мире компьютерной безопасности ***(Panda: почти каждый третий ПК – заражен вредоносным ПО // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2013/02/19/every-third-pc-infected.html). – 2013. – 19.02).***

***

Анонимусы вслед за взломом сайтов управления юстиции Киевской и Тернопольской областей «скрутили голову» сайту Главного управления юстиции в Хмельницкой области.

На этот раз хакеры не обошлись лаконичной фразой «Лавринович, мы пришли за тобой!», а оставили после себя емкую «угрозу».

Так, хакерская «новость» предостерегает министра юстиции: «Лавринович, храните деньги в сберегательной кассе. Мы начинаем внутреннее расследование финансовых потоков вашей семьи. По нашим данным, за 2012 г. касса семейной взаимопомощи Лавриновичей потолстела на более чем 18,4 млн дол. Следствие переходит в фазу сбора доказательной базы. Без уважения, Восточно-Европейское крыло группы Анонимус».

Напомним, 4 февраля под стенами управления прошла акция протеста под лозунгом «Ломанём Лавриновича», во время которой группа молодых людей в узнаваемых масках Гая Фокса пыталась заблокировать вход в

учреждение, протестуя против очередного запрета Интернет Партии Украины.

Как заявил глава ИПУ Д. Голубов в интервью «proIT»: «Если кто-то наступает на свободу слова в Интернете или на любые интернет-ресурсы – мы всегда приходим на помощь и заставляем чиновников любого уровня нас услышать» ***(Анонимусы взломали еще один сайт управления юстиции: теперь они считают деньги Лавриновичей // Думская.net (http://dumskaya.net/news/lavrinovich-hranite-dengi-v-sberegatelnoj-kasse-024542/). – 2013. – 20.02).***

***

Более миллиона человек по всему миру ежедневно становятся жертвой киберпреступлений. В общей сложности это обходится в сумму более 100 млрд дол. в год. На это с тревогой указывают специалисты американской компании по защите всемирной сети от электронных взломщиков Symantec, выводы которой опубликованы сегодня в европейской печати.

Внимание преступников все чаще привлекает операционная система Android, которой оснащена половина мобильных телефонов. Аналитики считают, что количество киберпреступлений, связанных с этими устройствами, возрастет в 2013 г., так как люди все чаще проводят банковские операции, используя мобильные устройства. Например в Австралии и США, по данным Sophos – разработчика средств защиты информации для компьютеров – происходит больше взломов мобильных телефонов нежели программ для работы в Интернете.

Не прибавляет уверенности и развитие мобильного интернета 3G и 4G, так как это, по словам экспертов, увеличивает шанс злоумышленника совершить взлом устройства, находясь на борту самолета.

Излюбленный метод взломщиков – это предложение пройти по ссылке или выслать сообщение на указанный номер. Обычно опытные пользователи скептически относятся к таким предложениям, но новички принимают их. Мотивы таких преступлений могут быть весьма разнообразными, причем не все они связаны с деньгами. Для кого-то это является средством наживы, а для кого-то – проверкой своих компьютерных способностей.

Власти многих стран предпринимают попытки борьбы с подобными преступлениями. Ведь каждый обманутый пользователь – это определенная сумма денег для злоумышленника. К борьбе с киберпреступностью подключился и Интерпол. Государства усилили давление на компании, которые хранят в базах данные о своих пользователях. Например, в Великобритании за утечку информации о счетах предусмотрен крупный штраф. Подобный случай произошел с компанией Sony PlayStation Network в 2011 г. Из-за взлома, она была оштрафована на 250 тыс. фунтов ***(Более миллиона человек по всему миру ежедневно становятся жертвой киберпреступлений // Центр исследования компьютерной преступности (http://www.crime-research.ru/news/19.02.2013/7477/). – 2013. – 19.02).***

***

Неизвестные хакеры взломали официальный Twitter-канал автомобильного бренда Jeep, разместив на нем несколько фальшивых сообщений, в том числе и сообщения о том, что бренд продан концерну Cadillac и теперь Jeep останавливает работу собственного производства, сообщает cybersecurity.ru.

Примечательно, что точно такая же история, но днем ранее, произошла с сетью закусочных Burger King. В пресс-службе Jeep говорят, что они не имеют понятия о том, кто может стоять за взломом их Twitter-аккаунта, а также не знают, связан ли их инцидент с происшествием в Burger King. В Twitter инцидент с Jeep также оставили без комментариев.

В медиа-агентстве, оказывающем PR-поддержку General Motors, заявили, что смогли восстановить контроль над Twitter-аккаунтом Jeep примерно через час после его взлома. Еще примерно через час после этого поддельные сообщения были удалены из ленты. В PR-агентстве Ignite Social Media говорят, что «могут лишь догадываться», кто реально стоял за взломом ***(Взломан Twitter автопроизводителя Jeep // IT Expert (http://itexpert.in.ua/rubrikator/item/23016-chakeri-vzlomali-twitter-lentu-avtoproizvoditelya-jeep.html). – 2013. – 20.02).***

***

Как сообщает BBC News, учетная запись хакерской группировки Anonymous в сети микроблогов Twitter – @Anon_Central, – за обновлениями которой следят более 160 тыс. пользователей, была взломана малоизвестными киберпреступниками из Rustle League, сообщает securitylab.ru

По мнению экспертов, взлом произошел из-за «человеческого фактора» – а именно использования ненадежного пароля.

«Причиной того, что Anonymous стали жертвой взлома, скорее всего, является человеческая слабость, – отмечает эксперт по информационной безопасности компании Sophos Г. Клули. – Скорее всего, они использовали слабый пароль, или практику применения одного и того же пароля для доступа к разным ресурсам» ***(Хакеры взломали микроблог Anonymous в Twitter // IT Expert (http://itexpert.in.ua/rubrikator/item/23101-chakeri-vzlomali-mikroblog-anonymous-v-twitter.html). – 2013. – 22.02).***

***

Поддельное расширение для Chrome взламывает учетные данные пользователей в Facebook. Используемая злоумышленниками вредоносная программа позволяет им заполучить полный контроль над учетной записью потенциальной жертвы. сообщает securitylab.ru.

IT-специалисты из компании Bitdefender обнаружили в сети новую фишинговую атаку на пользователей социальной сети Facebook. Мошенники отправляют потенциальным жертвам спам письма, содержащие ссылку на

вредоносный ресурс, на котором якобы можно скачать бизнес версию Flash Player – расширение для браузера Chrome.

После установки на компьютер пользователя вредоносная версия Flash Player начинает отслеживать его интернет-деятельность. При посещении учетной записи в Facebook вредоносная программа осуществляет поиск cookie-файлов для того, чтобы определить, находится ли пользователь сейчас в соцсети. Если учетная запись активна, то злоумышленники встраивают Javascript-код в веб-страницу и осуществляют вредоносную деятельность. К примеру, мошенники могут рассылать спам-сообщения, или размещать ссылки на вредоносные страницы в учетной записи пользователя.

Помимо этого, злоумышленники также могут похитить cookie-файлы, связанные с учетной записью пользователя в Facebook, и получить к ней доступ с другого компьютера.

Вредоносный код позволяет увеличивать количество отметок «нравится» на конкретных страницах. Впоследствии такие страницы продаются на подпольных форумах. Дело в том, что страницы с большим количество отметок «нравится» получают высокий рейтинг и заинтересовывают других пользователей. С их помощью злоумышленники могут распространять какой-либо контент и любое вредоносное ПО. На черном рынке учетные записи с большим количеством отметок «нравится» продаются за 150–200 дол.

Аналитик компании BitDefender Б. Ботезату отметил, что обнаружить эту инфекцию могут только антивирусные программы с активированными веб-фильтрами. В связи с этим зафиксированная исследователями угроза может сохраняться в браузере в течение достаточно длительного времени ***(Поддельное расширение для Chrome взламывает учетные данные пользователей в Facebook // IT Expert (http://itexpert.in.ua/rubrikator/item/23105-poddelnoe-rasshirenie-dlya-chrome-vzlamivaet-uchetnie-dannie-polzovateley-v-facebook.html). – 2013. – 22.02).***

***

Правительство США начало проводить индивидуальные контратаки на китайских хакеров, обвиняемых в промышленном шпионаже и хищении конфиденциальных данных, в том числе в краже государственных тайн. Как предполагается, вслед за атаками последует обнародование имен подозреваемых, а также проведение судебных исков.

Следует отметить, что решение правительства было принято после того, как исследователи компании Mandiant опубликовали отчет о масштабной хакерской кампании против США, в ходе которой компьютерное подразделение китайской армии, базирующееся в Шанхае, похитило сотни терабайт информации у более чем 140 различных организаций.

В то же время китайская сторона по-прежнему отрицает свою причастность к подобным инцидентам. Как следует из заявления

Министерства обороны Китая, в докладе Mandiant слишком мало «технических доказательств», а наличие китайских IP-адресов ни о чем не говорит.

«Пекин ведет против всех нас войну, и мы обязаны объединиться, чтобы прекратить это. Совместными усилиями США и наши союзники в Европе и Азии смогут использовать усиленные дипломатические и экономические рычаги давления на Китай», – прокомментировал американский сенатор М. Роджерс ***(США инициировали беспрецедентную атаку на китайских хакеров // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2013/02/25/us-attaks-china.html). – 2013. – 25.02).***

***

Не так давно руководство США обвиняло власти Китая в организации широкомасштабных шпионских атак на веб-серверы гражданских и военных учреждений Соединённых Штатов. Теперь пришла очередь Китая предъявить свои претензии США. Министерство обороны Китая обвиняет американских хакеров в шпионских атаках на два своих военных веб-сайта.

Согласно заявлению Министерства обороны этой страны, на протяжении прошлого года подведомственные сайты подвергались приблизительно 144 тыс. хакерским атакам ежемесячно, две трети из которых были из Соединённых Штатов.

В последнее время вопрос кибер-шпионажа вбивает большой клин в отношения между двумя странами. Белый дом считает, что высшее руководство Китая поощряет хакерские атаки со своей стороны. Китай же отвергает все обвинения и объявляет себя жертвой кибер-войны. Американское правительство пока никак не отреагировало на предъявленное обвинение китайской стороны ***(Кибер война США и Китая набирает обороты // americaru.com (http://www.americaru.com/news/62359). – 2013. – 1.03).***

***

В Украине кибер-преступления входят в топ-5 самых распространенных экономических преступлений. Каждая пятая украинская компания в 2012 г. подверглась кибер-атаке.

Сегодня уровень компьютерной преступности еще не достигает оборотов, сравнимых с торговлей наркотиками, но уже заставляет всерьез задуматься об обеспечении безопасности. В мире ситуация выглядит следующим образом: 411 млрд дол. составили убытки от компьютерных преступлений в 2011 г. Примерно 1 млн пострадавших за один день. (http://www.investgazeta.net/praktika/kiber-ataka-na-biznes-nuzhno-a-chto-163782/).

Реальность наших дней такова, что работа мало-мальски крупного хозяйства невозможна без компьютерной составляющей. Чаще всего

устанавливается система «банк-клиент», через которую и производятся финансовые операции. Делается это с простой и понятной целью – чтобы не ездить каждый раз в банк – нередко это получаются десятки километров.

Это, как показывает анализ и опыт последних лет, и есть та потенциальная «дыра», через которую могут уйти и нередко уходят деньги.

Откуда берутся эти дыры? Как ни прискорбно, но в большинстве случаев на компьютерах стоит нелицензионное программное обеспечение. Нелицензионное – это значит, уже кем-то взломанное. Значит, в той же системе Windows – наиболее распространенной на компьютерах в Украине – уже есть дыры, или, иначе говоря, «бек-доры» (back door – задняя дверь) или троянские программы – специальное программное обеспечение, используемое хакерами в работе.

Поэтому практически каждая такая связь уже изначально уязвима. Жертвами могут стать все.

Охотники за вашими деньгами

Условно, охотников за деньгами в сети можно разделить на несколько групп.

Есть хакеры высшего класса – они способны взломать любую защиту. От них практически невозможно защититься. Радует одно – их интересуют фирмы с громкими именами и фантастическим состоянием банковского счета, а значит, и суммы порядка десятков миллионов долларов. Они, скорее всего, просто не будут заниматься одной отдельно взятой локальной фирмой.

Наиболее опасны две другие категории. Одни – это те, кто пишет программы-отмычки для учебы или развлечения – например, студенты. Пишутся такие отмычки нередко по просьбе серьезных людей за относительно небольшие деньги. Сам программист, скорее всего, не будет никуда лезть, но вот вор посерьезнее его работу использует по полной программе. Но и эта категория еще не самая страшная.

А вот третья – самая опасная категория. Эти хакеры пишут специальные программы, работающие наподобие трала или сети – забрасывают ее по Интернету. Они заражают компьютеры и потом за ними следят. Причем следят не сами, а с помощью той же программы. Из сотни зараженных компьютеров вычленяются десяток-другой, на которых есть необходимая информация для снятия денег через Интернет, потом перехватывают управление машиной и – прощай, деньги, а нередко и сама информация, лежащая на диске.

Основные причины потерь

Почему это происходит? Чаще всего – из-за несоблюдения элементарных норм безопасности, отсутствия на компьютере антивирусных программ, или установленных дешевых – или того хуже – ломанных антивирусов. Итог один – потери денег, информации, времени.

Теперь нужно рассмотреть другие распространенные ошибки. Как показывает анализ хищений денег, ключи к банк-клиенту нередко лежат на

рабочем столе компьютера в папке с названием КЛЮЧИ. Это нечто сродни ключу под ковриком у входной двери.

Еще один уязвимый путь к компьютерам – применение Wi-Fi или мобильного Интернета. Очень часто установленные Wi-Fi роутеры ставятся с одними и теми же словами-паролями. И вот у очень многих пользователей стоят роутеры с одинаковыми паролями. Стоят просто потому, что инженеру-настройщику удобно так ставить. Для сравнения – представьте, что в многоквартирном доме во всех дверях – одинаковые личинки в замках.

Некоторые продвинутые пользователи предпринимают попытки шифрования сети, но тут подстерегает иная ошибка – использование самых элементарных систем шифрования, которые не представляют сложности ни для кого из опытных хакеров. Сеть таким образом становится открытой. Поэтому лучше всего сделать так, чтобы Wi-Fi сеть не была видна. Самый простой пример – на любом планшете или ноутбуке при попытке доступа к Wi-Fi сетям обычно высвечиваются несколько сетей. И злоумышленник может подъехать с ноутбуком к офису и взломать эту сеть, получив доступ к работе с компьютерами в сети.

Есть и более простые способы доступа – через мобильные телефоны. Смартфоны являют собой по сути тот же компьютер, с теми же «дырами» в защите. Очень часто такие смартфоны подключены к внутренней компьютерной сети и, соответственно, являют собой великолепную дыру. Причина – отсутствие элементарных антивирусов, которые, несмотря на некоторое замедление работы телефона, препятствуют доступу к содержимому сети.

Еще одна причина потерь – работа на устаревшем программном обеспечении. Большинство компьютеров в Украине работают под Windows, в которой сама компания разработчик периодически находит «дыры», «латая» их. Но если эти заплатки не ставить, то получаем открытую дверь.

Как с этим бороться?

В свое время начальник одной из контрразведок вывел железное правило – даже простые меры безопасности бывают гораздо эффективнее, чем их полное отсутствие. Поэтому установка лицензионного программного обеспечения и антивируса позволит избежать очень многих проблем.

Еще один очень простой, но очень действенный способ – любую банковскую операцию проводить с двумя электронными подписями. Например, подпись главного бухгалтера и подпись директора должны быть произведены с определенным интервалом. Соответственно, они должны находиться на разных компьютерах и уж никак не лежать в одной папке.

Еще один вариант – правильно выбранный банк-клиент. В Украине используются распространенные системы от BIFIT и iFOBS. На основании программного обеспечения этих компаний банки Украины создают банк – клиенты. Последней разработкой BIFIT стала передовая комплексная система электронного банкинга iBank 2 UA. Такие банки как Укрсиббанк, Укрсоцбанк, Райффайзен Банк Аваль, Брок бизнес банк и другие пользуются

этой системой в качестве своих банк клиентов. Каждый пользователь может выбрать наиболее защищенную версию.

Что делать при ограблении?

Допустим, случилось самое неприятное – компьютер взломан. Соответственно, счет открыт и с него начали уходить деньги. Вы это заметили. Деньги могут уходить как сразу, так и частями, несколькими платежами. Что делать в такой ситуации?

Частая и самая распространенная ошибка – пытаться что-то делать самостоятельно, если нет достаточных знаний в этой области.

Что обычно пытаются делать? Обычно пытаются через тот же банк-клиент отменить платеж, иногда считают, что это ошибка и решают разобраться позже, пытаются нажимать всякие кнопки отмены. Итог таких хаотичных шатаний один – денег на счету нет.

Что нужно делать? Правило общее для всех электросистем – обесточить компьютер. Мгновенно, не закрывая его через штатный режим закрытия. В случае стационарного компьютера – вилку сетевого из сети, в случае ноутбука – отключить батарею.

Зачем это делать? Дело в том, что очень часто программа-вор заметает следы – и тогда разобраться, что же произошло становится очень сложно. Если же компьютер был выключен, то специалист сможет восстановить последовательность операций и выяснить, что же происходило.

Следующий шаг – сделать звонок в банк и попытаться отменить транзакцию. Если банк работает в нормальном режиме – то до конца рабочего дня время есть. Иногда есть сутки, но лучше не затягивать.

После того как с банком все действия были проведены, необходимо обратиться в правоохранительные органы. К сожалению, у большинства пользователей сама идея обращения в милицию по такому виду преступлений вызывает скептические улыбки. Будем откровенны – весьма обоснованные.

Конечно, в структуре МВД есть отдел по борьбе с киберпреступностью, и там работают профессионалы высокого уровня, но, скорее всего, приедут по вызову не они, а обычный наряд патрульно-постовой службы. Несмотря на наличие автомата и вездехода, они едва ли смогут задержать ушедшие деньги и выяснить, кто их увел.

Поэтому нужно очень четко знать, к кому можно и нужно обращаться – нередко простое включение компьютера уничтожает все следы взлома. Поэтому специалисты будут включать машину при помощи различных ухищрений – например, вытащив жесткий диск и сделав с него копию – со всеми следами взлома. Подключая этот скопированный диск к уже работающей машине в качестве носителя информации, а не запускаясь с него, можно отследить, что и как было сделано злоумышленниками. После того как ИТ-специалисты смогли увидеть полную картину, и выдать свое заключение – наступает время работы милиции.

Как рассказал представитель отдела по борьбе с киберперступностью, «самое трудное – поменять психологию наших людей. Многие сотрудники МВД привыкли смотреть в глаза преступнику, а не на монитор с его IP-адресом. Точно также большинство пострадавших не понимают, как его могут ограбить сидя где-то на другом конце Украины или даже другой стороне планеты» ***(Кибер-атака на бизнес: что нужно, а что нельзя // investgazeta.net (http://www.investgazeta.net/praktika/kiber-ataka-na-biznes-nuzhno-a-chto-163782/). – 2013. – 1.03).***

***

Хакеры международного движения Anonymous выложили в свободный доступ информацию о высокопоставленных сотрудниках Bank of America.

Об этом участники движения сообщили на своем сайте, передает Associated Press. Вместе с этим подразделение Anonymous опубликовало более 14 гигабайт данных, которые, согласно их заявлениям, являются доказательством того, что целый ряд крупных новостных агентств, в том числе Bloomberg, Thomson Reuters и другие, занимаются сбором личной информации о своих пользователях.

Среди документов, опубликованных группой, отчеты ряда компаний о потенциальных угрозах, в том числе о самих Anonymous. Хакеры назвали собранную о них информацию «бесполезной». Bank of America и другие организации комментировать заявления Anonymous отказались ***(Хакеры выложили в свободный доступ информацию о сотрудниках Bank of America // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2013/03/01/boa-data-compromised.html). – 2013. – 1.03).***

***

Как сообщили эксперты компании Symantec, они обнаружили, что злоумышленники используют поддельные обновления для Adobe Flash-плеера, под видом которых распространяют вирусы.

По словам исследователей, хакеры используют Flash-плеер в качестве приманки, поскольку приложение является очень популярным среди интернет-пользователей, и ни о чем не подозревающие жертвы могут загружать вирусы под видом обновлений.

Эксперты установили, что хакеры создали довольно убедительное подобие страницы загрузки обновлений плеера, однако в нем было обнаружено несколько несоответствий.

Большинство ссылок отправляют обратно на атакованный домен, а все ссылки внутри страницы, кроме тех, которые ведут на вредоносные ресурсы, перенаправляют в корневую директорию сайта, в результате чего система выдает предупреждение об ошибке 404.

Кроме того, для большей убедительности злоумышленники разработали два варианта подтверждения установки обновлений, которая

якобы происходит: в первом – появляется всплывающее окно, которое предлагает пользователю загрузить установочный файл под названием flash_player_updater.exe. Во втором – кнопка «Download Now» якобы позволяет загрузить файл под названием update_flash_player.exe.

Исследователи отмечают, что кроме хищения паролей, эти файлы, судя по всему, осуществляют поиск учетных данных к FTP/telnet/SSH сервисам для всех популярных клиентов. Они также способны перехватывать учетные данные, передаваемые по SMTP, IMAP и POP3 протоколам ***(Symantec: Мошенники распространяют вирусы под видом обновлений для Adobe Flash // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2013/03/01/fake-adobe-flash-update-installs-ransomware-performs-click-fraud.html). – 2013. – 1.03).***

***

Вице-президент компании Google В. Серф призвал всех производителей электроники, которую можно подключить к Интернету, ввести строгую систему аутентификации для повышения безопасности своих пользователей. Об этом В. Серф заявил на конференции RSA 2013.

В. Серф признался, что он откровенно удивлен тем количеством устройств, которые в настоящее время можно подключить к Интернету. В прошлом люди шутили по поводу возможного подключения тостеров к сети. Сегодня же соединение с Интернетом могут установить кондиционеры, лампы накаливания и даже холодильники.

Эксперт обеспокоен тем, что системы управления такими устройствами недостаточно защищены, и их взлом может привести к настоящей катастрофе. В качестве примера В. Серф приводит соединение с Интернетом систем кондиционирования воздуха. Если хакер получит контроль над ними, то он может нарушить корректную работу электроэнергетической системы государства.

В. Серф заявляет, что об обеспечении безопасности устройств, подключаемых к Интернету, нужно подумать сегодня для того, чтобы избежать инцидентов в будущем ***(В. Серв: Бытовые устройства, подключаемые к Интернету, несут в себе реальную угрозу // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2013/03/01/internet-of-things-danger.html). – 2013. – 1.03).***

***

«Лаборатория Касперского» опубликовала отчёт об исследовании ряда инцидентов, связанных с очередным примером кибершпионажа против правительственных учреждений и научных организаций по всему миру. В ходе атаки злоумышленники применили сочетание сложных вредоносных кодов «старой школы» вирусописательства и новых продвинутых технологий использования уязвимостей в Adobe Reader – и всё это для того, чтобы

получить данные геополитического характера из соответствующих организаций.

Вредоносная программа MiniDuke распространялась при помощи недавно обнаруженного эксплойта для Adobe Reader (CVE-2013-6040). По данным исследования, проведенного «Лабораторией Касперского» совместно с венгерской компанией CrySys Lab, среди жертв кибершпионской программы MiniDuke оказались государственные учреждения Украины, Бельгии, Португалии, Румынии, Чехии и Ирландии. Кроме того, от действий киберпреступников пострадали исследовательский институт, два научно-исследовательских центра и медицинское учреждение в США, а также исследовательский фонд в Венгрии.

«Это очень необычная кибератака, – поясняет Е. Касперский, генеральный директор "Лаборатории Касперского". – Я хорошо помню, что подобный стиль программирования в вредоносном ПО использовался в конце 1990-х – начале 2000-х. Пока не очень понятно, почему эти вирусописатели "проснулись" через 10 лет и присоединились к "продвинутым" киберпреступникам. Эти элитные писатели вредоносных программ старой закалки успешные в создании сложных вирусов сегодня совмещают свои способности с новыми методами ухода от защитных технологий для того, чтобы атаковать государственные учреждения и научные организации в разных странах».

«Созданный специально для этих атак бэкдор MiniDuke написан на Ассемблере и чрезвычайно мал – всего 20 Кб, – добавляет Е. Касперский. – Сочетание опыта "олдскульных" вирусописателей с новейшими эксплойтами и хитрыми приёмами социальной инженерии – крайне опасная смесь».

В отчете антивирусной компании говорится, что авторы MiniDuke до сих пор продолжают свою активность, последний раз они модифицировали вредоносную программу 20 февраля 2013 г. Для проникновения в системы жертв киберпреступники использовали эффективные приёмы социальной инженерии, с помощью которых рассылали вредоносные PDF-документы. Эти документы представляли собой актуальный и хорошо подобранный набор сфабрикованного контента. В частности, они содержали информацию о семинаре по правам человека (ASEM), данные о внешней политике Украины, а также планы стран-участниц НАТО. Все эти документы содержали эксплойты, атакующие 9, 10 и 11 версии программы Adobe Reader. Для создания этих эксплойтов был использован тот же инструментарий, что и при недавних атаках, о которых сообщала компания FireEye. Однако в составе MiniDuke эти эксплойты использовались для других целей и содержали собственный вредоносный код.

При заражении системы на диск жертвы попадал небольшой загрузчик, размером всего 20 Кб. Он уникален для каждой системы и содержит бэкдор, написанный на Ассемблере. Кроме того, он умеет ускользать от инструментов анализа системы, встроенных в некоторые среды, в частности в VMWare. В случае обнаружения одного из них бэкдор приостанавливал

свою деятельность с тем, чтобы скрыть своё присутствие в системе. Это говорит о том, что авторы вредоносной программы имеют четкое представление о том методах работы антивирусных компаний.

Если атакуемая система соответствует заданным требованиям, вредоносная программа будет (втайне от пользователя) использовать Twitter для поиска специальных твитов от заранее созданных акаунтов. Эти аккаунты были созданы операторами бэкдора MiniDuke, а твиты от них поддерживают специфические тэги, маркирующие зашифрованные URL-адреса для бэкдора. Эти URL-адреса предоставляют доступ к серверам управления, которые, в свою очередь, обеспечивают выполнение команд и установку бэкдоров на заражённую систему через GIF-файлы.

По результатам анализа стало известно, что создатели MiniDuke используют динамическую резервную систему коммуникации, которая также может ускользать от антивирусных средств защиты – если Twitter не работает или аккаунты неактивны, вредоносная программа может использовать Google Search для того чтобы найти зашифрованные ссылки к новым серверам управления.

Как только заражённая система устанавливает соединение с сервером управления, она начинает получать зашифрованные бэкдоры через GIF-файлы, которые маскируются под картинки на компьютере жертвы. После загрузки на машину, эти бэкдоры могут выполнять несколько базовых действий: копировать, перемещать или удалять файлы, создавать каталоги, останавливать процессы и, конечно, загружать и исполнять новые вредоносные программы.

Сегодня бэкдор выходит на связь с двумя серверами – в Панаме и Турции – для того чтобы получить инструкции от киберпреступников ***(MiniDuke – новый инструмент кибершпионажа // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2013/02/28/MiniDuke.html). – 2013. – 28.02).***

***

Microsoft в своем блоге сообщила, что компания пополнила список недавно атакованных американских ИТ-производителей, затронутых недавно волной хакерских атак, связанных с уязвимостью в Java. В блоге корпорации говорится, что Microsoft не выявила случаев хищения клиентских данных.

В сообщении ИТ-производителя приводится совсем немного данных о вторжении, кроме того, пресс-служба компании не дает дополнительных комментариев по факту взлома, за исключением заявлений, что изложены в блоге. В компании заявляют, что атака по методу проведения была похожа на те, что были использованы в отношении Facebook, Twitter и ряда других.

Также на выходных корпорация заявила, что по недосмотру ИТ-персонала были просрочены несколько сертификатов безопасности, связанных с онлайновой платформой Azure, в результате чего с ней не

смогли работать многие программы и это вызвало сбои по всему миру у пользователей Azure.

Просроченные сертификаты не позволяли установить HTTPS-соединения и получить или отправить данные с/на Azure. Согласно сообщению Microsoft, проблема возникла примерно в 4:00 мск 23 февраля, но она была полностью ликвидирована примерно через четыре часа. «Мы приносим извинения нашим клиентам», – заявили в компании.

Критики Azure и облачных сервисов в целом уже заявили, что данный пример – лишь один из немногих, показывающих, что хранение важных данных опасно в удаленных облаках ***(Microsoft подверглась хакерской атаке // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2013/02/25/Microsoft-hacked.html). – 2013. – 25.02).***

***

В Украине вновь заявили о себе хакеры, оппозиционно настроенные по отношению к властям страны. Кто они такие и какие преследуют цели, выяснял корреспондент DW.

Уже в течение года в Украине ведутся «кибервойны», направленные против органов государственной власти. Все началось 31 января прошлого года, когда представители Министерства внутренних дел Украины решили закрыть один из крупнейших файлообменников EX.ua. за нарушение прав интеллектуальной собственности.

В ответ на обыски и изъятие серверов EX.ua, веб-сайты Президента страны, правительства, СБУ и МВД, Национального банка, Конституционного Суда, Налоговой администрации, правящей Партии регионов подверглись хакерским DDoS-атакам. В течение двух недель доступ к этим ресурсам был проблематичен и для внешних пользователей, и для сотрудников ведомств.

Веб-сайты Верховной Рады, Партии регионов периодически были также недоступны в течение июня и июля прошлого года. Тогда хакеры своими атаками проявляли солидарность с защитниками украинского языка. В то время народные депутаты Украины обсуждали и принимали Закон «Об основах языковой политики», который расширяет сферы использования региональных языков, в том числе русского, наряду с государственным украинским.

И последняя акция протеста хакеров пришлась на начало февраля. Трехдневным DDoS-атакам и дефейс-атакам (от англ. deface – уродовать, искажать; атака, при которой происходит «подмена лица» сайта) были подвергнуты сайты Киевского и Тернопольского управления Министерства юстиции Украины. Они были заблокированы и содержали послание: «Лавринович (министр юстиции Украины. – Ред.), до свидания!». Это был ответ хакеров на судебное решение о запрете Интернет партии Украины,

принятое по ходатайству Министерства юстиции из-за отсутствия у партии необходимого количества партийных ячеек в регионах.

Anonymous или обычные оппозиционеры?

Судя по сообщениям в социальных сетях и по видеообращениям в YouTube, «за свободу украинцев в Интернете и за украинский язык» боролись хакеры восточноевропейского крыла международной группы Anonymous. Лидер Интернет партии Украины Д. Голубов подтверждает причастность Anonymous к атакам, призванным защитить файлообменник EX.ua и его партию, которую он, не скрывая, называет «партией пиратов».

«Хакеры не любят, когда кто-то лезет в их среду и рассказывает, что здесь можно делать, а что нет. Хакеры не любят, когда людям запрещают скачивать пиратскую музыку и фильмы, и всячески пытаются уничтожить свободу в Интернете. Они всегда отвечают, действуя из разных уголков планеты», – заявил Д. Голубов DW. А вот участие Anonymous в акциях в защиту украинского языка он категорически отрицает: «Anonymous никогда не будут атаковать сайты из-за языковых вопросов, вопросов религии или истории. Это делают обычные люди, оппозиционно настроенные».

Таких «оппозиционно настроенных людей», причем с техническим образованием, в условиях недостаточного контроля над распространением разного рода хакерских программ, в Украине много. И, как подчеркнул в интервью DW ведущий эксперт по антивирусным программам российской «Лаборатории Касперского» В. Камлюк, «в этом смысле Украина, как и многие другие страны мира, не осталась в стороне от антиглобалистского движения хакеров-активистов, яркими представителями которого является группа Anonymous».

И если 99 % киберпреступников заинтересованы исключительно в краже денег или продаже украденной информации, то 1 % хакеров-активистов руководствуется иными принципами. «У них есть твердая политическая позиция. Они заинтересованы в том, чтобы достать ценную информацию, опубликовать ее вместе с политическим сообщением, либо выразить протест в виде атаки, которая выводит из строя оборудование серверов, опять-таки, с политическим подтекстом», – говорит эксперт «Лаборатории Касперского».

«Виртуальные неприятности» у власти только начинаются?

Оппозиционные политические партии Украины, как заявил DW народный депутат партии Ю. Тимошенко «Батькивщина» А. Шевченко, хотя и поддерживают всех, кто отстаивает свое право на свободу в сети, к «интернет-неприятностям» властей отношения не имеют. «Интернет в Украине оппозиционный по определению. Здесь следует понимать, что власти противостоит не какая-то отдельная оппозиционная партия, а большое количество разношерстных людей, чьи права и интересы постоянно нарушают», – сказал депутат. Он также не исключает, что число «виртуальных реакций на действия власти» будет только возрастать.

Эта проблема всерьез беспокоит и правоохранительные органы Украины, которые не готовы противостоять любым видам киберугроз, исходящих из разных стран мира. Один из технических консультантов МВД сообщил DW на условиях анонимности, что имевшие место атаки на государственные веб-ресурсы всего лишь «ребячество» по сравнению с происходящими серьезными киберпреступлениями, о которых общественности мало что известно ***(Кто создает украинским властям Интернет-неприятности // Polittech.org (http://polittech.org/2013/02/25/kto-sozdaet-ukrainskim-vlastyam-internet-nepriyatnosti/). – 2013. – 25.02).***

***

Британский антивирусный вендор Sophos надеется, что в предстоящие месяцы внимание мирового сообщества будет отвлечено от деятельности госхакеров и организуемых ими атак в сторону борьбы с традиционными вредоносными кодами. Ч. Висниевски, старший консультант по безопасности Sophos, говорит, что тема APT-атак в последнее время стала «ужасно отвлекать», так как на нее тратится слишком много ресурсов, тогда как сами эти атаки по своей природе носят практически единичный характер.

«Я нахожу это неправильным. Если государственные ведомства борются с ориентированными на них вредоносами, то это их дело. Мы предлагаем подумать об ИТ-безопасности миллионов простых пользователей. Мы перестали думать об этом, и это позволило киберпреступникам вырасти до невиданных ранее масштабов», – говорит Ч. Висниевски.

По его словам, APT-атаки на сегодня чрезвычайно редки, можно сказать уникальны, тогда как в повседневной жизни приходится иметь дело с совершенно другими программами. Злоумышленники создают «миллионы» образцов вредоносных кодов на базе разных семейств вредоносных кодов, полиморфных атак и других технологий.

По данным Sophos, за последнее время самым популярным и массово-опасным видом вредоносных кодов стал программы-вымогатели, которые под разными предлогами попадают на компьютеры пользователей и начинают требовать с них деньги. Ч. Висниевски говорит, что ранее секьюрити-компании настояли на том, чтобы поставщики платежных систем блокировали перевод денег в пользу создателей поддельных программ и это привело к тому, что последние изменили тактику получения платежей

«Программы-шантажисты работают быстро и решительно, полагаясь на то, что пользователь оказывается в безвыходной ситуации. Даже если вы знаете, что ваш компьютер был заблокирован не правоохранительными органами или провайдером, вы все равно можете заплатить. Sophos рекомендует использовать встроенные в операционные системы средства безопасности, такие как Microsoft Enhaced Mitigation Experience Toolkit (EMET), для создания первичного эшелона защиты», – говорит Ч. Висниевски ***(Пользователям не нужно бояться кибероружия, оно не***

для них // InternetUA (http://internetua.com/polzovatelyam-ne-nujno-boyatsya-kiberorujiya--ono-ne-dlya-nih). – 2013. – 1.03).

***

Киберпреступники, профессионально занимающиеся DDoS-атаками, все реже используют огромные бот-сети из зараженных компьютеров для проведения атак, предпочитая более эффективные и простые в управлении веб-серверы. Эксперты по информационной безопасности из «Лаборатории Касперского» и компании Highload Lab рассказали о том, почему это происходит, а также о некоторых других изменениях, произошедших в сфере DDoS-атак и борьбы с ними за последние годы.

Российские эксперты в области борьбы с DDoS-атаками согласны с западными коллегами: количество таких инцидентов растет, и они становятся более изощренными. Руководитель проекта Kaspersky DDoS Prevention «Лаборатории Касперского» А. Афанасьев и генеральный директор компании Highload Lab (защита от DDoS-атак) А. Лямин рассказали, как атаки на «отказ в обслуживании» эволюционируют, кто является главными мишениями и чего ждать от данной угрозы в будущем.

Серверы вместо обычных ПК

До недавнего времени для проведения мощных DDoS-атак киберпреступники использовали в основном крупные бот-сети (сети из зараженных компьютеров). Чем больше компьютеров заражено, тем более мощную атаку можно организовать – таким был основной мотив для строительства многомиллионной бот-сети. Однако поддерживать работоспособность достаточно крупной для мощных атак бот-сети – тяжелая задача, ведь злоумышленникам постоянно необходимо следить за тем, чтобы в онлайн-доступе было нужное количество зараженных компьютеров.

Это, в свою очередь, означает, что потребуются постоянные траты на покупку новых «загрузок», то есть новых зараженных компьютеров взамен тех, что по каким-либо причинам выпали из бот-сети. В условиях постоянного роста числа компьютеров, на которых установлены коммерческие антивирусные продукты, эта задача становится все более хлопотной. В ответ на эту тенденцию хакеры ищут новые инструменты для атак, отмечает А. Афанасьев.

«Если дорого и некомфортно иметь гигантский ботнет, его постоянно пополнять и поддерживать, то злоумышленник ищет более простые способы расположить источники своего нападения. Все чаще это выделенные серверы», – сказал эксперт.

По словам А. Афанасьева, рост числа программного обеспечения для виртуализации серверов (создания виртуальной копии реального компьютера или сервера) и относительная простота его использования привели к появлению большого числа плохо сконфигурированных серверов, а также серверов, содержащих незакрытые уязвимости. Злоумышленники находят

такие серверы, встраивают в них средства для осуществления DDoS-атак, и просто ждут «заказа».

«Принципы организации таких атак изменились. Вместо сотен тысяч рабочих станций – несколько серверов. Они производительнее, их быстрее и проще активировать», – отметил эксперт.

С А. Афанасьевым согласен А. Лямин, генеральный директор компании Highload Lab, занимающейся защитой от DDoS-атак. Он добавил, что распространение практики использования серверов в качестве источника вредоносного трафика связано с появлением новых инструментов анонимизации, которые ранее не были доступны.

«Действительно, серверы используют все чаще, в том числе потому, что появился инструментарий, позволяющий генерировать пакеты с поддельными IP-адресами на высоких скоростях», – рассказал А. Лямин.

Теоретически отразить DDoS-атаку можно, имея информацию об источниках вредоносного трафика – то есть, IP-адресах, с которых к атакуемому сайту идет паразитный трафик. Однако использование инструментария для анонимизации затрудняет выявление таких источников и – как следствие – устранение самой атаки.

При этом даже при наличии информации об источниках вредоносного трафика далеко не всегда удается отключить серверы, с которых он идет, отмечает А. Афанасьев. Злоумышленники территориально распределяют инфраструктуру для осуществления атак так, чтобы их было максимально трудно прекратить через обращение к провайдеру или дата-центру, в котором расположен атакующий сервер.

«Наши партнеры рассказывали нам об атаке, в которой серверы управления бот-сетью находились в одной из стран Центральной Азии, сами серверы, с которых велись атаки – в Турции и Европе, а цели атак – в США. Быстро закрыть такую бот-сеть или центр управления через прямое обращение к правоохранительным органам невозможно, поскольку злоумышленники выбрали страны, руководство которых крайне неохотно взаимодействует друг с другом. При этом преступники, как известно, границ не имеют», – рассказал А. Афанасьев.

Высокие сезоны

Как и прежде, больше всего атак происходит в периоды наибольшей бизнес-активности – в «высокие» сезоны в сфере торговли товарами и услугами. В году таких сезона два – с конца осени и до новогодних праздников, а также примерно с середины весны и до начала лета, в сезон отпусков. В предновогодний сезон под атаками оказываются интернет-магазины и сайты, предоставляющие востребованные в это время года услуги (замена и продажа зимней резины для автомобилей, например); в весенне-летний сезон хакеры переключают внимание на сайты туристических агентств, сервисов по продаже билетов, бронированию гостиниц и интернет-магазины с товарами, которые актуальны в этот период. Чаще всего причиной атак становится недобросовестная конкуренция.

Бывают, впрочем, и сферы бизнеса, которые находятся под угрозой DDoS круглый год ***(Хакеры меняют стратегию // InternetUA (http://internetua.com/hakeri-menyauat-strategiua). – 2013. – 26.02).***

***

Как сообщает AIN.UA, среди украинских пользователей социальной сети Facebook начал распространяться вирус. В частности, пользователю предлагается перейти по ссылке и установить расширение для браузеров Chrome и Firefox. По словам В. Вальдмана, который заметил брешь в системе безопасности социальной сети, при переходе по ссылке, весь таймлайн будет заполнен постами, в которых уже от имени пользователя будут отмечены все друзья. Для заражения профиля необходимо лишь перейти по ссылке ***(Среди украинских пользователей Facebook начал распространяться вирус // AIN.UA (http://ain.ua/2013/02/28/114599). – 2013. – 28.02).***

***

Команда безопасного поиска «Яндекса» в своем блоге сообщила о том, что теперь обнаружение сайтов, распространяющих вредоносный код для Java-приложений, станет более эффективным, благодаря запуску в поисковой системе специального поведенческого детектора.

Заражение компьютеров пользователей более чем в 2/3 случаях происходит через опасные сайты, когда в браузер загружаются вредоносные Java-апплеты. При отсутствии на компьютере виртуальной машины Java пользователю предлагается установка ее версии с уязвимостью, после чего зараженный сайт вновь атакует компьютер пользователя.

Зашифрованный вредоносный код, в котором применены самые популярные сегодня уязвимости JRE, определяется детектором и защищает компьютеры пользователей. Результатом его работы стало обнаружение более 4000 зараженных сайтов, посещаемость которых до заражения в сумме достигала 1,5 млн пользователей.

Рекомендации команды безопасного поиска Яндекса, защищающие от заражения, состоят в следующем:

– использование актуальных версий ПО, обязательное регулярное обновление Java и других плагинов;

– отключение запуска Java-апплетов, установленных по умолчанию, в браузере, и подтверждение их только для доверенных сайтов;

– использование обычных антивирусов, отслеживание регулярности их обновления;

– следование рекомендациям Яндекса по безопасности в сети ***(Команда безопасного поиска Яндекса объявила о запуске поведенческого детектора // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/internet_dlya_chaynikov/novosti/komanda_bezopasnogo_poiska_yandeksa_obyavila_o_zapuske_povedencheskogo_detektora?utm_source=ukrnet&utm_medium=rss). – 2013. – 1.03).***

***

В 2013 г. интенсивность кибератак – от криминального программного обеспечения (ПО) до социально-политического хакерства – возрастет. И коснется всех организаций – от крупных до самых малых. Таковы выводы исследования «Отчет по безопасности-2013», обнародованного компанией Check Point® Software Technologies Ltd.

Результаты исследования показали, что корпоративные сети 63 % предприятий подвергались атакам ботов, а более половины – воздействию вредоносного ПО не реже одного раза в день. Стремительное распространение приложений web 2.0 раскрыло перед хакерами беспрецедентные возможности проникновения в корпоративные сети. В 54 % случаев в компаниях наблюдались утечки конфиденциальной либо персональной информации.

При этом многие компании не воспринимают киберугрозы всерьез – 91 % организаций до сих пор использует потенциально небезопасные приложения.

«Организации руководствуются простой бизнес-логикой: если приложения эффективно помогают бизнесу, и их польза для бизнеса выше угроз потери и утечки информации – решение принимают в сторону использования этих приложений», – пояснил «РГ» вице-президент по работе с ключевыми клиентами MAYKOR А. Панагушин.

«При оценке угроз информационной безопасности всегда рассматриваются два фактора: критичность угрозы для бизнеса (стоимость возможного ущерба) и вероятность реализации угрозы, – считает R&D директор Veeam Software А. Ширманов. – Иными словами, первое – это как много конкуренты или иные лица могут заплатить за конфиденциальную информацию компании, а второе – это комбинация таких факторов, как стоимость взлома корпоративной системы защиты, известность и публичность компании, наличие подключения критических ресурсов сети к Интернету и т. д. В общем, злоумышленники проникают в корпоративные сети только тогда, когда стоимость получаемой ими информации выше стоимости взлома защиты. Но у большинства компаний в сети просто нет сколько-нибудь ценной информации с точки зрения злоумышленников. Поэтому такие компании полагают, что вряд ли станут объектом атаки, и не уделяют должного внимания вопросам информационной безопасности».

«Невнимание к вопросам информационной безопасности действительно присуще многим российским компаниям, но в большей степени предприятиям среднего и малого бизнеса, – добавляет начальник отдела продуктов для унифицированных коммуникаций Orange Business Services в России и СНГ Д. Дородных. – Они ошибочно считают, что атакам подвергаются только крупные компании. Не представляя реальный масштаб угроз, компании считают, что затраты на системы безопасности превышают возможный ущерб от деятельности кибер-злоумышленников. При этом зачастую атаки на корпоративные ресурсы остаются незамеченными, и

многие даже не осознают, что была утеряна важная информация, а компании был нанесен ущерб» ***(В 2013 году количество кибератак возрастет // InternetUA (http://internetua.com/v-2013-godu-kolicsestvo-kiberatak-vozrastet). – 2013. – 2.03).***