# СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

*Огляд інтернет-ресурсів*
*(14–27.07)*

**2014 № 14**

# Соціальні мережі
## як чинник інформаційної безпеки

**Інформаційно-аналітичний бюлетень**
**Додаток до журналу «Україна: події, факти, коментарі»**
Огляд інтернет-ресурсів
(14–27.07)
№ 14

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

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

**Редакційна колегія:**
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць



Київ 2014

**ЗМІСТ**

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ ..... 4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА ..... 20
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ ..... 24
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ ..... 33
Інформаційно-психологічний вплив мережевого спілкування на особистість ..... 33
Маніпулятивні технології ..... 35
Зарубіжні спецслужби і технології «соціального контролю» ..... 38
Проблема захисту даних. DDOS та вірусні атаки ..... 45

# РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

В последнее время в уанете стало модно запускать социальные сети. Только в апреле текущего года украинские разработчики анонсировали сразу пять национальных соцсетей, которые должны были составить серьезную конкуренцию ресурсам М. Цукерберга и П. Дурова. Из них до сегодняшнего дня дожили две с половиной. Это не остановило новых «золотоискателей» – на подходе троица свежих украинских соцсетей. Правда, конкурировать с «гигантами» они собираются уже не патриотизмом, а кое-чем другим, пишет AIN.UA (ttp://ain.ua/2014/07/14/532674?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed %3A+ainua+ %28AIN.UA %29).

Socialface

Социальная сеть уже запущена в бете, однако с регистрацией у пользователей возникают проблемы – авторизация по e-mail не проходит. По словам основателя Socialface Александра, проблема была на уровне провайдера и ее уже устранили. Проект находится на финальной стадии тестирования.

О том, что Socialface предназначена строго для украинцев, речь не идет – конкурировать с большими соцсетями команда рассчитывает за счет качества продукта. «Мы в своей сети объединили все фишки Facebook, “ВКонтакте”, Twitter, “Одноклассников” и даже торговой площадки Slando. Сеть построена на CMS – для комфорта управления ею», – рассказал AIN.UA Александр.

Интерфейс Socialface очень напоминает Facebook – он выполнен в похожей цветовой гамме и почти идентичен по расположению элементов управления. «Скажем так, это версия 1.0 сети, а дальше развитие только hand made», – пояснил основатель. Он также уточнил, что сервера у команды свои собственные и находятся в Украине.

Zine

В скором времени запустится социальная сеть Zine, которая, по словам создателей, представляет собой сетевой цитатник. Здесь пользователи будут публиковать цитаты великих людей, глубокие мысли, правила жизни и тому подобный контент.

Интерфейс будет разбит на так называемые квоты, в которых можно будет размещать текст, фотографии или файлы. Квоты будут отображаться в формате, похожем на публикации в других соцсетях. Если пользователь подпишется на чьи-то квоты, они начнут появляться в его хронике так же, как это происходит в Facebook или Twitter.

«Аналогичным путем ваши квоты отображаются в ленте подписчиков. Чтобы получать интересные квоты, подписывайтесь на интересных вам людей: друзей, знаменитостей, близких», – говорится в описании Zine. CEO и

основатель проекта В. Сердюк рассказал AIN.UA, что квоты должны рассказывать подписчикам пользователя Zine о его характере.

В своем профиле пользователь может добавлять обложку, которая отображается на всю ширину экрана, написать свою любимую цитату или другую информацию. В правом верхнем углу есть две кнопки: «написать квот» и «стена». В Zine также можно будет ставить ссылки на свои аккаунты в других соцсетях – Facebook, «ВКонтакте», Twitter, Instagram.

«Українці»

Еще одна социальная сеть для украинцев должна запуститься в ближайшее время, однако ранее ее запуск уже откладывали почти на месяц. Во «ВКонтакте» есть группа «Українців», на которую подписано более 3 тыс. пользователей, однако их активность незначительна, несмотря на то что паблик постоянно обновляется. Преимущественно, это записи патриотического характера.

Команда социальной сети пообещала рассказать подробнее о своем детище уже после запуска. По словам администраторов ресурса, конкурировать с «гигантами» «Українці» планируют не патриотичностью, а качеством. Хотя «желто-голубую» составляющую тоже никто не отменял.

Прежде всего, в команде «Українців» раскритиковали уже запущенные отечественные социальные сети, очевидно, имея ввиду WEUA.info и «Друзі». «Все соцсети, которые были созданы, – на самом деле ужасны по функционалу и интерфейсу. Даже при наличии крутых аналогов, разработчики не видят, что им надо сделать. Мы надеемся, что сможем сделать хорошую и конкурентную соцсеть. Постараемся, чтобы соцсеть была только для украинцев», – рассказали AIN.UA создатели социальной сети.

По их словам, сайт будет на украинском языке. А, может быть, и русский тоже ***(Яровая М. Еще три новых украинских соцсети. Теперь не о патриотизме // AIN.UA (ttp://ain.ua/2014/07/14/532674?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed %3A+ainua+ %28AIN.UA %29). – 2014. – 14.07).***

***

Компания «МТС Украина» создала для своих сотрудников корпоративную социальную сеть «Простор». Об этом IT Expert сообщила пресс-служба компании.

Это универсальное рабочее пространство, которое объединяет в себе функционал Интранета, социальных сетей Facebook, LinkedIn, а также инструменты проектного менеджмента. Социальная сеть призвана создать единую базу знаний и благоприятные условия для коворкинга сотрудникам компании независимо от города или подразделения, в котором они работают.

Структура «Простора» содержит информационный, учебный блоки, а также группы и сообщества для проектной работы и досуга. Страница обратной связи продолжает традицию открытого общения, начатую в формате регулярных онлайн-чатами с руководством компании. На этой

странице каждый сотрудник может вести диалог с топ-менеджером, задать вопрос или поделиться опытом.

Каждый сотрудник имеет собственную страницу, возможность общаться в личных сообщениях, вести блог, добавляться в группы и сообщества, подписываться на страницы топ-менеджмента, любых дирекций и департаментов. Для удобства использования социальная сеть поддерживает три языка – украинский, английский и русский. Сайт создан на базе Jive.

В социальной сети реализована программа лояльности с элементами геймификации – активные пользователи получают баллы, которые можно обменять на приятные бонусы.

Социальная сеть «Простор» постоянно совершенствуется. Так, в планах компании создать мобильные приложения для iOS и Android; интегрировать с системой Cisco Jabber для аудио- и видеозвонков. Также социальный портал будет подключен к системам электронного документооборота и аналитических систем, таких как SAP HR. Все это значительно облегчит взаимодействие сотрудников и повысит эффективность бизнес-процессов на всех уровнях в любом подразделении ***(МТС Украина запустила собственную социальную сеть // IT Expert (http://itexpert.org.ua/rubrikator/item/36991-mts-ukraina-zapustila-sobstvennuyu-sotsialnuyu-set.html). – 2014. – 15.07).***

***

Крупнейшая социальная сеть – Facebook, вероятно, уже достигла пика своей популярности, и в скором времени интерес пользователей к ней начнет угасать. К такому выводу пришли ученые из немецкого Института программного анализа и информационных систем (IAIS) при Обществе имени Фраунгофера (объединение 67 немецких институтов прикладных исследований), пишет Marketing Media Review (http://mmr.ua/news/id/issledovateli-predrekli-skoryj-zakat-facebook-40406/).

Это не первое подобное исследование, которое предрекает проекту М. Цукерберга скорое забвение. На этот раз эксперты проанализировали динамику пользовательского интереса к 175 различным сервисам в Интернете и подтвердили циклическую природу социальных сетей: они быстро набирают популярность, но так же быстро теряют ее.

Исследование К. Керстинга и К. Баукхаге основывается на данных сервиса «Google Тренды», который считает, сколько раз пользователи в той или иной стране «гуглили» какую-либо тему. В поле зрения ученых попали социальные сети, такие как Twitter, «ВКонтакте», Google+, LinkedIn и др., и прочие интернет-сервисы – AirBnB, Amazon, Groupon, Spotify, eBay и т. д. Поисковые данные собирались по 45 странам. Большая часть социальных сервисов подчиняется одному и тому же закону: в какой-то момент все они переживают бум популярности, а затем сталкиваются с необратимым снижением интереса.

Facebook – не исключение, и коллективное внимание к нему следует все той же «холмообразной» схеме, утверждают К. Керстинг и К. Баукхаге. Различные модели анализа поисковых данных расходятся в оценке скорости, с которой будет снижаться популярность Facebook, но самая нейтральная предполагает, что к 2017 г. интерес к соцсети сократится на 50 % относительно текущего уровня.

Авторы оговариваются, что их анализ не позволяет делать прогнозы о снижении количества пользователей Facebook в абсолютных величинах.

Похожее исследование, основанное на статистике поисковых запросов в «Google Трендах», в начале 2014 г. провели ученые Д. Канарелла и Д. Шпехлер из Принстонского университета. Они подсчитали, что число пользователей Facebook сократится на 80 % в период с 2015 по 2017 г. Публикация работы вызвала не только повышенное внимание прессы, но и живую реакцию самого Facebook. Команда М. Цукерберга ответила собственным «исследованием»: аналитик М. Дэвелин проследил динамику «лайков» на страницах Facebook Принстонского, Гарвардского и Йельского университетов и заключил, что университет Принстона находится под угрозой исчезновения. А снижение частоты запросов в Google по слову «воздух» еще более пугающее: воздух на Земле может исчезнуть из-за спада интереса к нему со стороны интернет-аудитории, съязвил представитель Facebook.

Впрочем, данные самой компании намекают на то, что Facebook действительно испытывает некоторые трудности с поддержанием внимания существующих пользователей и привлечением новых. Если к концу III квартала 2013 г. прирост ежемесячной аудитории соцсети составлял 18 % (в годовом выражении), то в конце 2013 г. – 16 %, а к концу I квартала 2014 г. – уже 14 %.

Помимо замедления роста аудитории, одним из главных вызовов для Facebook является старение аудитории: все больше тинейджеров выбирают более простые и приспособленные для общения мессенджеры. В октябре 2013 г. о снижении количества часов, которые подростки проводят в соцсети, заявлял финансовый директор Facebook Д. Эберсман. Способом борьбы с этой проблемой стала покупка быстрорастущего мессенджера WhatsApp за рекордную для технологической отрасли сумму – 19 млрд дол.

В последнее время Facebook также подвергается критике за использование персональных данных своих пользователей в рекламных интересах, а также психологические эксперименты с отображением постов в пользовательских лентах новостей. Недавняя новость о том, что соцсеть проводила «эксперимент с эмоциями» почти 700 тыс. своих юзеров, фильтруя их «френд-ленты» по параметру позитивности или негативности постов, вызвал острую реакцию интернет-сообщества ***(Исследователи предрекли скорый закат Facebook // Marketing Media Review (http://mmr.ua/news/id/issledovateli-predrekli-skoryj-zakat-facebook-40406/). – 2014. – 14.07).***

***

Facebook продолжает заботиться об удобстве пользователей. На этот раз социальная сеть озадачилась просмотром видео. Теперь, когда пользователи мобильных устройств на платформе iOS и Android будут просматривать видео, в плеере им будут предлагаться другие релевантные видео (Нечто подобное мы постоянно видим на YouTube). Так что больше у пользователей не будет необходимости возвращаться в ленту, чтобы найти продолжение любимого сериала.

Эта новая опция может поспособствовать увеличению количества просмотров видео и, следовательно, лайков.

Сами представители Facebook на вопрос об этом нововведении ответили, что: «Это новая функция, которую мы тестируем на мобильных устройствах, чтобы помочь пользователям находить еще больше интересных для них видео».

Пока это обновление распространяется только на органический видеоконтент и охватывает лишь часть пользователей соцсети.

Новый видеоплеер появляется только при просмотре видео, добавленных непосредственно на Facebook (с YouTube и другими платформами это уже не работает). Видео в ленте проигрывается автоматически, но при нажатии открывается в полноэкранном режиме. После окончания просмотра видео сворачивается, и появляются рекомендации «Больше видео [имя друга] и других» в нижней части экрана.

Идея основана на том, что раз уж вы осилили развернуть видео на весь экран, то, вероятно, захотите посмотреть еще больше.

Изменения видеоплеера могут принести Facebook пользу в нескольких направлениях:

1. Чем чаще люди смотрят видео, тем больше вероятность, что они будут его размещать. А ведь именно сейчас Facebook борется с YouTube и Vine за владение пользовательским видео и его монетизацию.

2. Просмотры видео позволят Facebook захватить еще больше пользовательского внимания и времени. Это поможет социальной сети расширить влияние на жизнь пользователей, ограничить их вовлеченность в проекты конкурентов, а также накопить новые данные о людях и их предпочтениях.

3. Обеспечение более удобного способа просмотра видео может пригодиться Facebook при покорении мира Smart-TV. Если чтение статусов с дивана кажется некоторым пользователям слишком трудной работой, то просмотры видео или слайд-шоу фотографий друзей точно станет для них приятным и непринужденным опытом ***(Facebook тестирует изменения в видеоплеере // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_testiruet_izmeneniya_v_videopleere). – 2014. – 16.07).***

***

Украинские пользователи Интернета отказываются от российских интернет-ресурсов. Украинцы все больше пренебрегают поисковиками yandex.ua, почтовым сервисом mail.ru и российскими социальными сетями − «Одноклассники» и «ВКонтакте». Об этом свидетельствуют последние данные украинского представительства компании Gemius, которая занимается онлайн-исследованиями в Центральной и Восточной Европе.

Так, по данным Gemius, рекорд падения посещаемости установил российский поисковик «Яндекс». За полгода сервис потерял более 800 тыс. уникальных пользователей из Украины − посещаемость сайта упала с 8,9 млн в январе до 8,1 млн в мае. В результате «Яндекс» уступил свое стабильное 4-е место в списке рейтинговых сайтов Украины видеосервису YouTube. Наряду с этим количество уникальных пользователей главного конкурента− Google − за этот же период возросло на миллион− с 12,2 млн до 13,2 млн. Потери понес и российский почтовый сервис mail.ru, его аудитория уменьшилась на 400 тыс. − с 10,4 млн в январе до 10 млн в мае.

Растеряла украинскую аудиторию и российская социальная сеть «Одноклассники» − с 5,2 млн в январе до 5 млн в мае, хотя до этого несколько лет этот показатель был стабильным. Для сравнения, американская соцсеть Facebook нарастила аудиторию с 5,6 млн в январе до 6 млн в мае, что позволило сервису впервые превзойти по популярности «Одноклассники» и занять седьмое место в рейтинге самых популярных ресурсов в Украине. А соцсеть «ВКонтакте» хотя и показала прирост, с 11,1 млн пользователей в январе до 11,5 млн в мае, но динамика роста сайта намного скромнее, чем в прошлом году.

В падении популярности российских сервисов есть политическая подоплека, уверен А. Мась, руководитель «Украинской баннерной сети». С началом аннексии Крыма на российские сервисы распространился бойкот продуктов и услуг made in Russia. Бойкот набрал обороты после обострения ситуации на Донбассе. «Поисковики − это сервисы, построенные на доверии. Поскольку среди украинцев доверие к России снизилось, российские поисковики потеряли лояльную аудиторию», − отметил А. Мась.

В апреле сервис попал под шквал критики, когда для российских пользователей на своих онлайн-картах начал отражать Крым как часть России. Еще один скандал, связанный с политической ситуацией в Украине, – увольнение С. Петренко, генерального директора украинского филиала, который некорректно высказался в Facebook о смерти активистов Антимайдана в Одессе. Как результат, менеджер был вынужден покинуть компанию и уйти в бессрочный отпуск. В «Яндексе» объяснили, что высказывание С. Петренко не является официальной позицией компании.

При этом причины снижения показателей «Яндекс» А. Мась не сводит только к патриотизму украинцев, но и объясняет более прозаичными факторами – конкуренцией со стороны Google. «Когда у сервиса меньшая доля – за нее постоянно нужно бороться. Большой шар надувается быстрее,

чем маленький. Соответственно, Google, у которого доля больше, проще удерживать свою аудиторию», − добавил А. Мась.

В украинском офисе «Яндекс» падение по причине «национальной идентификации» отвергают, так как сервис зарегистрирован в Украине и здесь платит налоги. Поэтому снижение посещаемости связывают с несовершенным исследованием аудитории.

«Системы измерения доли поисковых систем достаточно несовершенны, а колебания доли из-за технических изменений могут быть разными − и положительными, и отрицательными. Они могут быть вызваны различными причинами. Сейчас мы анализируем, что происходит с долей. Пока точно не можем сказать, какова причина на самом деле», − констатирует Д. Ткалич, аналитик компании «Яндекс.Украина», отмечая, что связывать негативные тенденции с бойкотом российских товаров в Украине не стоит. «Мы не видим по своим внутренним приборам такого влияния. По нашей внутренней статистике, ни пользователей, ни запросов не стало меньше», − говорит он.

В качестве примера возможного технического падения Д. Ткалич приводит историю с реферер-параметрами, которые идентифицируют, с какой из поисковых систем на сайт пришел трафик. «Довольно часто поисковые системы, в частности, Google, экспериментируют с этим параметром. Иногда, как результат, системы сбора статистики не могут корректно распознать поисковую систему, с которой пришел трафик, и часть переходов с поиска становятся “невидимими” для них. Визуально доля будто падает, тогда как у конкурентов растет», − добавляет аналитик «Яндекса».

Контролируемые соцсети

Падение российских социальных сетей может быть вызвано сезонностью, поскольку летом интернет-сервисы обычно теряют аудиторию. В этом Forbes заверили в украинском офисе «ВКонтакте»: «Никаких негативных тенденций в пользовании сервисом в Украине нет. Есть традиционный сезонный спад, характерный едва ли не для всех интернет-ресурсов. К концу лета количество посещений обычно возвращается к норме и снова продолжает расти».

А вот причина падения «Одноклассников» может скрываться в консервативности аудитории, которая пользуется этим ресурсом. «Одноклассники» имеют стабильную аудиторию постарше. Уровень ее общения носит доисторический характер. Тогда как аудитория Facebook более активная, ей национальные интересы важнее, чем фото семьи или отдыха, поэтому сервис работает больше как новостной ресурс», − объясняет А. Мась.

По его мнению, то, что Facebook превзошел «Одноклассников», может быть вызвано цитируемостью пользователей сервиса − они комментируют ту или иную тему. «И уже через несколько минут этот комментарий появляется в новостных лентах информационных агентств», − констатирует он.

Украина начинает становиться частью глобального Интернета, а не российского, отмечает М. Саваневский, управляющий партнер цифрового агенства PlusOne DA. «Сейчас наблюдается очень четкий тренд относительно быстрого роста украинской аудитории Twitter, YouTube, Facebook и многих других популярных международных сервисов. Его уже нельзя изменить, – говорит М. Саваневский. – И это означает, что уже через 2–3 года Facebook может стать соцсетью № 1 для украинских пользователей».

Однако не следует также исключать, что возможное влияние на популярность российских социальных сетей опять-таки имели политические скандалы. Напомним, основатель «ВКонтакте» П. Дуров в апреле, после своего ухода из компании, заявлял о давлении со стороны ФСБ России, которая обращалась к нему с требованием предоставить личные данные организаторов групп Евромайдана. В свою очередь, «Одноклассники» в июне оказались в эпицентре скандала из-за мгновенного удаления постов с критикой В. Путина.

«Люди начали переживать за сохранение конфеденциальности своих данных. Конечно, это почти не влияет на людей – “хардюзеров” (пользуются соцсетью пять и более раз в неделю), но для тех, кто заходил в соцсеть редко, это стало дополнительным стимулом вообще не заходить туда», – отмечает М. Саваневский.

Рекламный оптимизм

Несмотря на потерю аудитории, вышеперечисленные сервисы продолжают входить в топ-10 самых популярных украинских ресурсов.

Поэтому, как отмечают эксперты на рекламном рынке, падение аудитории пока не отразилось на рекламных доходах ресурсов – едва ли не единственной статье дохода российских сервисов в Украине.

Но общее проседание рынка рекламы в Интернете ощутили на себе все игроки, в том числе и российские. «Поток рекламного инвентаря в Интернете уменьшился, поскольку компании не знают, какие направления им развивать сейчас, когда прошла революция и идет война на Донбассе. Поэтому они чувствуют себя неуверенно», − объяснил А. Мась.

В серьезность падения популярности сервисов не очень верят и в рекламных агентствах, которые непосредственно работают с российскими сервисами. «Мы не видим, чтобы наши клиенты отказывались от размещения на таких ресурсах. Вряд ли произойдет значительное падение рекламных доходов российских ресурсов в Украине. Речь о тенденции пока не идет. Станет ли она такой, можно будет оценить только через год», − заключает И. Скикевич, директор рекламного агентства Mindshare (входит в рекламный холдинг GroupM), обслуживающего Orimi, Kimberly Clark, SC Johnson, Roshen, «Эпицентр», Delta Medical и др. ***(Почему российские интернет-сервисы теряют популярность в Украине // InternetUA (http://internetua.com/pocsemu-rossiiskie-internet-servisi-teryauat-populyarnost-v-ukraine). – 2014. – 16.07).***

***

Необычные социальные сети: для самых умных, самых красивых, для животных и роботов

Оглушительный успех социальных сетей во многом определило тщеславие: кто же устоит перед тем, чтобы похвастаться перед миллионами отпуском на Мальдивах, рождением ребенка или очередной ступенькой в карьере? Но еще больше пользователю польстит членство в эксклюзивном онлайн-клубе, где собраны самые умные (успешные, красивые, обеспеченные). Многие социальные сервисы пытаются на этом сыграть и запускают необычные фильтры для членов сообществ. Редакция AIN.UA подготовила подборку таких оригинальных проектов (http://ain.ua/2014/07/16/532855).

Для самых умных

Smart is the new sexy, считают создатели популярного сериала о гиках «Теория большого взрыва». Это мнение разделяют и огранизаторы движения для интеллектуалов Mensa, которые в июне этого года объединили усилия с крупнейшим в США сайтом знакомств Match.com. Результатом стал запуск сайта знакомств для людей, которые по уровню своего IQ могут претендовать на статус самых умных – Mensa Match. Чтобы попасть на этот сайт знакомств, нужно доказать, что ваш IQ выше 130. Чтобы доказать это, нужно либо состоять в организации Mensa, либо пройти онлайн-тест на IQ за 1 дол.

Закрытые соцсети «для своих» часто запускают и крупные вузы. Собственно, с закрытой сети для Гарварда и начинался Facebook. По слухам, в 2000-х один из известных украинских интернет-предпринимателей, тогда еще студент, делал социальную сеть для своего вуза. Но после того как в нее просочились данные об одном из преподавателей-чиновников, проект быстро свернулся.

Для самых красивых

Один из самых известных проектов такого рода – международная сеть Beautiful People. Это онлайн-дейтинг с элементами соцсети только для самых красивых. Сами создатели описывают ее, как «элитный онлайн-клуб, вход в который охраняют сами члены клуба». Это означает, что для регистрации здесь нужно выслать свои фото, и пользователи сервиса сами определят, достоин ли кандидат попасть в сеть. По утверждению администрации, с помощью сервиса уже поженилось 700 пар красивых людей.

Украина не остается на обочине мировых трендов: в мае украинская команда запустила закрытую социальную сеть только для красавцев и красавиц Simpotki.net.

Для самых богатых

Если нашлись люди, купившие приложение I am rich для iPhone, стоившее 1000 дол. и состоявшее из заставки для смартфона, то, очевидно, найдутся люди, готовые платить за принадлежность к «самым богатым» в социальных сетях. Показательный пример такой сети – Affluence (в переводе

с английского «достаток»). Регистрация там бесплатная, но вас туда пустят, только если ваше состояние превышает 1 млн дол., либо же ваш годовой доход – выше 200 тыс. дол. Впрочем, миллиардеры таким не заморачиваются: их проще искать на Twitter или Facebook, главное, чтобы аккаунт был верифицирован.

Для животных

У любимой собаки М. Цукерберга по кличке Бист есть свой аккаунт на Facebook. Но есть сети, созданные специально для того, чтобы счастливые владельцы могли постить фото, видео и тексты о своих питомцах или от их имени. В мире очень много примеров таких сообществ – Youpet.com, Dogster.com и другие.

Украинцы и здесь не отстают. В 2011 г. группа энтузиастов из Харькова запустила проект «Мордашки.com» (сейчас он недоступен). В этом году один из самых известных украинских стартапов Petcube запустил iOS-приложение, где можно публиковать фотографии своего питомца, добавлять в друзья и следить за обновлениями других любителей животных, оставаться на связи с помощью push-уведомлений и делиться фотографиями в Facebook и Twitter.

Для роботов

Приход Skynet уже близко: недавно искусственный интеллект в образе подростка из Одессы прошел тест Тьюринга. Кроме того, роботы всего мира смогут «общаться» во всемирной сети для роботов RoboEarth, хранить и получать там информацию ***(Карпенко О. Необычные социальные сети: для самых умных, самых красивых, для животных и роботов // AIN.UA (http://ain.ua/2014/07/16/532855). – 2014. – 16.07).***

***

Американець Д. Грінфілд створив додаток Hashtack, що дає змогу об’єднати контент із Facebook, Twitter та Instagram.

Hashtack – це додаток, який збирає фото та відео із соціальних мереж Facebook, Instagram та Twitter в одному медіумі. Користувачі можуть «лайкати», коментувати, масштабувати зображення, а також перемощувати їх.

Hashtack робить користування соціальними мережами більш зручним. Приміром, в Instagram не можна без згоди автора публікувати скріншот його повідомлення. Натомість Hashtack дає можливість користувачам забирати собі фото, які їм подобаються (завантажуючи при цьому інформацію про ім’я автора та іншу додаткову інформацію). На запозиченому зображенні водночас з’являється маркування, яке позначає, що пост неоригінальний.

Додаток також дає змогу створювати окремі потоки хештегів. Якщо, наприклад, створити потік #WorldCup, то можна побачити будь-яке фото чи відео з використанням цього хештегу.

За словами Д. Грінфілда, нині він намагається вивести свій проект на ринок. Він вважає, що цей додаток буде корисним не лише для пересічного

користувача, а й для працівників сфери SMM, контент-менеджерів, бізнесменів та ін.

Hashtack відкриває перший етап пошуку фінансування. Донині проект спонсорував особисто Д. Грінфілд. Спершу продукт мав назву Divyy, однак у березні відбувся його ребрединг. Наразі Hashtack доступний лише для iOS, однак очікується також вихід Android-версії ***(Американець створив додаток, що об'єднує в собі фото та відео із трьох соцмереж // MediaSapiens (http://osvita.mediasapiens.ua/material/32731). – 2014. – 16.07).***

***

Google+ скасував заборони довкола імен у профілях своїх користувачів. Відтепер можна зазначати будь-яке, у тому числі фейкове, ім'я в соціальній мережі, пише mashable.com.

Ще з часу появи мережі Google+ у 2011 р., у ній було заборонено створювати фейкові імена. Приміром, користувачі мусили зазначати таке ж ім'я, як в YouTube. Це відбувалося, незалежно від того, легко було ідентифікувати людину таким чином чи ні.

Відтепер, як повідомляється в офіційному блозі Google+, їхня платформа відкрита для будь-яких нікнеймів. Google заохочує користувачів зазначати свої справжні імена, однак креатив людей обмежувати також не збирається.

«Ми знаємо, що наша політика використання імен була незрозумілою і призводила до деяких непотрібних труднощів у деяких наших користувачів, – ідеться в повідомленні компанії. – Просимо вибачення за це та сподіваємося, що нинішні зміни є кроком до того, що Google+ стане гостинним та безбар'єрним місцем, таким, яким ми хочемо його бачити».

Нова функція соцмережі не означає, що користувачі не матимуть жодних обмежень. Якщо особа один раз змінила ім'я, то Google+ зможе закрити для неї цю можливість на термін до трьох місяців. Це залежатиме від того, як давно профіль зареєстрований у мережі, та як часто його власник міняє свою ідентифікацію ***(Google+ дозволив користувачам зазначати у профілі фейкові імена // MediaSapiens (http://osvita.mediasapiens.ua/material/32749). – 2014. – 16.07).***

***

Українська соціальна мережа WEUA.info змінила дизайн, удосконалила функціонал та виправила технічні проблеми. Про це повідомляє AIN.UA.

У новому дизайні сайту залишилися попередні кольори (зелений, білий та чорний). Однак вони стали менш насиченими, пастельними. Крім того, в оформленні з'явився сірий колір.

За словами засновника WeUA.info Б. Оліярчука, редизайн соцмережі є лише першим кроком до повного оновлення ресурсу. Раніше він розповідав, що команда планує перезапустивши сайт на новому движку.

Нині розробники працюють над створенням нового ядра ресурсу, намагаючись оптимізувати його роботу. Зокрема, намагаються сайт більш швидким.

Через чотири місяці мають з'явитися мобільні додатки WEUA для платформ iOS та Android ***(Українська соціальна мережа WeUA змінила дизайн та працює над повним оновленням // MediaSapiens (http://osvita.mediasapiens.ua/material/32763). – 2014. – 17.07).***

***

В App Store появилось приложение Mentions, разработанное в Facebook Creative Labs специально и исключительно для знаменитых людей, у которых есть верифицированный аккаунт на Facebook. С его помощью они могут отслеживать упоминания своего имени в соцсети, оперативно реагировать и вступать в беседу с фанатами или хейтерами. По данным Facebook, люди, которым предоставлен доступ к приложению, уже генерирую в два раза больше контента, чем раньше.

Среди первых пользователей Mentions: В. Голдберг, Э. Ширан, М. Кэри. Потенциальная аудитория, на которую приложение может оказать влияние, составляет 800 млн человек, именно столько людей подписаны на верифицированные аккаунты. Помимо экстренного реагирования в топиках, звезды могут следить за трендовыми темами и высказывать свое отношение к ним, формируя сознание масс (либо негативное отношение к себе) ***(Facebook выпустил приложение для знаменитостей // InternetUA (http://internetua.com/Facebook-vipustil-prilojenie-dlya-znamenitostei). – 2014. – 18.07).***

***

Киевская команда, выпустившаяся из акселератора EastLabs, создала сервис социальных закладок, коллекционирования и шаринга контента из социальных сетей Likeastore. На этом сайте можно найти абсолютно все страницы, которые пользователь когда-либо лайкал в любой из популярных социальных сетей – сервис синхронизирован с Twitter, Facebook и еще десятком социальных сетей, кроме «ВКонтакте» и «Одноклассников», пишет AIN.UA (http://ain.ua/2014/07/20/533377).

Зарегистрировать в Likeastore можно по e-mail, через Facebook, Twitter или GitHub. Добавить в ленту другие соцсети можно в специальном разделе.

Отсутствие синхронизации с двумя российскими соцсетями не имеет под собой политической подоплеки. «Во "ВКонтакте" есть проблема серверного доступа к API – мы технически не можем сделать нормальную поддержку этой социальной сети. А "Одноклассники" даже не смотрели – мы все-таки ориентируемся больше на мир, нежели СНГ, плюс за все время существования сервиса не поступило ни единого запроса на "Одноклассники"», – пояснил CEO команды Likeastore А. Белецкий.

Likeastore синхронизирует данные с частотой не менее чем раз в полчаса. То есть, как только пользователь отметил страницу в соцсети как понравившуюся, ссылка на статью, клип или твит появится в его инбоксе Likeastore в течение 30 мин.

Пользователи могут вести открытие и закрытые коллекции. Открытые коллекции будут видны для других пользователей Likeastore, которые могут подписываться на чужие коллекции и получать результаты у себя в ленте. А закрытые будут видны только самому пользователю.

Недавно в Likeastore появилось браузерное расширение. По словам А. Белецкого, многие пользователи используют Likeastore как сервис отложенного чтения – нечто вроде Pocket, но по социальным сетям. Однако, в отличие от западного аналога, в украинском сервисе сохраняются только понравившися Facebook-страницы и собственные записи, в которых есть ссылки. Остальные типы контента, такие как фото, видео и т. д. пока недоступны, но возможность синхронизировать их появятся в ближайшем будущем, обещает А. Белецкий. Зато в Pocket, в отличие от Likeastore, нет интеграции с Twitter и другими соцсетями, помимо Facebook.

Модели монетизации у украинцев пока как таковой нет. «Сейчас тестируем различные гипотезы и ищем способы монетизации через эффективное продвижение контента», – говорит А. Белецкий ***(Яровая М. Pocket для соцсетей: Украинцы создали сервис отложенного чтения Facebook, Twitter, GitHub и других // AIN.UA (http://ain.ua/2014/07/20/533377). – 2014. – 20.07).***

***

Мобильное приложение «ВКонтакте» вернулось в магазин приложений AppStore от Apple – впервые с 26 апреля.

По сравнению с прошлой версией приложения в нем осталось намного меньше возможностей для прослушивания музыки, пишет РБК Daily. Например, пользователи теперь не могут через приложение искать записи песен, которые в соцсети разместили другие пользователи, информирует news.eizvestia.com.

Эти записи они все же могут прослушивать, но для этого им сначала нужно найти чужие песни в соцсети через браузер и добавить в свой список воспроизведения. Если пользователь в приложении находит ссылки на чужие аудиозаписи, он может прослушать только 30 с. – потом приложение предложит ему купить песню через музыкальный магазин iTunes, принадлежащий Apple.

В Android таких ограничений пока нет – там музыкальные плейеры «ВКонтакте» стали одними из самых популярных приложений в разделе «Музыка».

«ВКонтакте» также сделала в мобильном приложении специальную заглушку-предупреждение – она появляется, когда пользователь заходит на страницы соцсети с контентом для взрослых.

Программисты соцсети с апреля несколько раз выпускали новые версии приложения, но их отклоняли в Apple из−за доступа через приложение к эротическому контенту, рассказал РБК источник, близкий к руководству соцсети.

В российском разделе App-Store «ВКонтакте» было одним из самых популярных по числу загрузок в 2013 г. – больше скачивали только самые популярные игры, свидетельствует статистика AppAnnie ***(Для прослушивания музыки «ВКонтакте» появились ограничения // Экономические известия (http://news.eizvestia.com/news_technology/full/336-dlya-proslushivaniya-muzyki-vkontakte-poyavilis-ogranicheniya). – 2014. – 21.07).***

***

Компания Facebook, владелец крупнейшей в мире социальной сети, ввела новую функцию «Сохранить». Об этом в официальном блоге Facebook рассказал один из разработчиков компании Д. Джамбальво.

Как следует из названия, новая функция позволяет пользователям сохранять различные материалы для дальнейшего просмотра. Это может быть как ссылка с текстом, который пользователь собирается прочитать позднее, так и страницы людей, компаний и групп на самом Facebook.

Новая функция будет доступна через несколько дней на самом сайте Facebook и через мобильные приложения для Google Android и iOS ***(Компания Facebook, владелец крупнейшей в мире социальной сети, ввела новую функцию «Сохранить» // Lenta-ua (http://lenta-ua.net/novosti/obschestvo/66792-facebook-podarit-polzovatelyam-novuyu-opciyu.html). – 2014. – 22.07).***

***

У Таджикистані запустили місцеву соціальну мережу vipnet.tj. Її створили як альтернативу заблокованому днями російському ресурсу «Одноклассники». Про це журналістам повідомив засновник сайту Г. Саломзод.

За словами засновника мережі, у ній діє заборона на розміщення екстремістських матеріалів і використання нецензурних виразів. Про це йдеться в тексті користувацької угоди, розміщеній на сайті.

Як зазначив засновник таджицької соцмережі vipnet.tj, вона має функцію фільтрації нецензурних та лайливих слів. «Такі слова, спрямовані від одного користувача до іншого не доходять до адресата», – пояснив він.

Окрім нецензурних виразів та «екстремізму», у таджицькій соцмережі забороняється завантаження матеріалів «що заперечують підвалини Республіки Таджикистан», суперечать «законодавству ісламської релігії», а також порушують авторське право.

Що саме мається на увазі під «законодавством ісламської релігії» та про які «підвалини республіки» йдеться – на сайті не зазначено ***(У***

***Таджикистані створили соцмережу-аналог «Однокласників» // MediaSapiens (http://osvita.mediasapiens.ua/material/32962). – 2014. – 23.07).***

***

Facebook и LinkedIn получили наиболее низкие оценки среди социальных сетей в индексе удовлетворенности американских потребителей. Об этом свидетельствует отчет American Customer Satisfaction Index за 2014 г.

Хотя ресурсы прибавили в баллах относительно прошлого года (по 5 баллов каждый, до 67), они замыкают рейтинг соцсетей, которыми остались довольны пользователи в США. Примечательно, что исследование проводилось до того, как Facebook организовала неоднозначный эксперимент над пользователями с целью исследования возможности управлять их эмоциями с помощью целенаправленной фильтрации сообщений друзей.

Лидером рейтинга стала соцсеть Pinterest, которая прибавила за год 4 балла до 76, вслед за ней идет Wikipedia с 74 баллами, ее показатель снизился на 4 пункта. Видеохостинг YouTube набрал 73 балла по шкале удовлетворенности пользователей, Google+ осталась на прежнем уровне с 71 баллами. Twitter прибавил 4 пункта, но недалеко ушел от Facebook и LinkedIn, набрав 69 баллов.

В среднем индекс удовлетворенности работой соцсетей в США прибавил три пункта за год до 71 балла.

Среди интернет-поисковиков пользователи остались наиболее удовлетворены работой Google (83 балла), далее идут Bing и MSN (по 73 балла), а замыкают рейтинг Yahoo (71 балл) и AOL (70 баллов). Средний индекс удовлетворенности американских пользователей работой поисковиков оценен в 80 баллов ***(Американцы остались недовольны Facebook и LinkedIn // InternetUA (http://internetua.com/amerikanci-ostalis-nedovolni-Facebook-i-LinkedIn). – 2014. – 24.07).***

***

Геолокационная соцсеть Foursquare представила новую версию своего мобильного приложения: у него полностью изменится дизайн и пропадут чекины. О предстоящих нововведениях компания сообщила в своём официальном блоге, пишет Marketing Media Review (http://mmr.ua/news/id/foursquare-predstavil-prilozhenie-bez-chekinov-i-v-novom-dizajne-40546/).

«Мы разработали символ, который сочетает в себе булавку, приколотую к карте, и эмблему супергероя. Мы всегда думали о Foursquare как о сервисе, который даёт вам суперсилу для исследования своего города, и наше новое лого отражает это видение», – прокомментировали редизайн приложения в компании. Теперь для его оформления используется розово-голубая цветовая схема и новый набор шрифтов.

Вместе с оформлением меняется и принцип работы Foursquare. Теперь сервис превратится в рекомендательную систему, которая будет

анализировать предыдущую активность пользователя и на основании полученных данных советовать ему посетить то или иное место. Вся информация, связанная с чекинами, и сама эта функция теперь доступна в другом приложении Foursquare – Swarm.

Предполагается, что обновлённый Foursquare появится в магазинах приложений в ближайшие две недели ***(Foursquare представил приложение без чекинов и в новом дизайне // Marketing Media Review (http://mmr.ua/news/id/foursquare-predstavil-prilozhenie-bez-chekinov-i-v-novom-dizajne-40546/). – 2014. – 24.07).***

***

Мобильное приложение соцсети Secret, где можно публиковать посты анонимно, получило 25 млн дол. в новом раунде инвестиций. Об этом сообщается в корпоративном блоге компании.

Среди инвесторов названы Index Ventures, Redpoint Ventures, Garry Tan and Alexis Ohanian, SV Angel, Fuel Capital, Ceyuan Ventures, но полный список вложившихся держат в секрете. Как пишет New York Times, в настоящее время компания оценивается более чем в 100 млн дол.

Также компания представила новую версию приложения: теперь войти в Secret можно через Facebook. Соответственно, приложение свяжет пользователя с его «друзьями» из этой социальной сети. Раньше Secret показывал посты тех, кто есть в телефонной книге или почте клиента.

В одном из предыдущих обновлений Secret, выпущенном 10 июня, появилась опция доступа через социальную сеть «ВКонтакте». Как рассказал пресс-секретарь «ВКонтакте» Г. Лобушкин РБК, благодаря интеграции с «ВКонтакте», пользователь Secret знает, что тот или иной пост написал кто-то из их друзей, но не будут понимать, кто именно.

Приложение Secret основано бывшими сотрудниками Google в начале 2014 г. Оно доступно на Android и iOS и позволяет анонимно делиться с друзьями своими инсайдами, мыслями – любыми сообщениями. Текст можно сопроводить картинкой или фотографией, добавить смайл. При регистрации Secret импортирует контакты из телефонной книги и почтового клиента. После этого те из них, которые тоже установили Secret, образуют группу «друзей». Но все же понять, кто именно из друзей написал конкретное сообщение, пользователь не может.

За шесть месяцев своего существования приложение обрело международную известность. Изначально приложение было доступно только пользователям в США, позднее его география расширилась. На родине популярность приложение завоевало благодаря публикации там инсайдов крупных IT-компаний и СМИ ***(В анонимную соцсеть Secret вложили $25 млн // Sostav.ua (http://sostav.ua/publication/v-anonimnuyu-sotsset-secret-vlozhili-25-mln-62331.html). – 2014. – 15.07).***

***

На днях компании Facebook и Oculus VR выпустили совместное заявление, в котором говорится, что подписанная ранее между ними сделка завершена, пишут «Комментарии» (http://comments.ua/ht/479137-facebook-zavershila-pogloshchenie-oculus-vr.html).

Несмотря на то, что о покупке Oculus VR компанией Facebook сообщалось еще в конце марта, с приобретением тех или иных активов связано множество необходимых формальностей. Таким образом, оформление зачастую требует много времени, сообщает «ITC».

В опубликованном по поводу завершения сделки заявлении говорится, что теперь Facebook и Oculus VR с волнением смотрят в совместное будущее, планируют создать вычислительную платформу нового поколения и совершить революцию в способах общения людей.

Что касается оснований для заключения сделки, основатель Oculus VR П. Лаки ранее сообщил, что план заключается в «способствовании принятию виртуальной реальности в долгосрочной перспективе, а не в стремлении к получению быстрой прибыли» и что партнерство является «прозрачным и очевидным путем к предоставлению виртуальной реальности для каждого».

Стоит отметить, что во время решения всех вопросов, связанных с закрытием сделки, Oculus VR не сбавляла темпы развития проекта очков виртуальной реальности Oculus Rift. Не так давно Oculus VR купила известную в сфере индустриальной разработки и дизайна компанию Carbon Design Group.

Сроки выхода потребительской версии очков пока не называются, но в недавнем интервью генеральный директор Oculus VR Б. Ирибе заявил, что они будут продаваться по цене, граничащей с себестоимостью ***(Facebook завершила поглощение Oculus VR // Комментарии (http://comments.ua/ht/479137-facebook-zavershila-pogloshchenie-oculus-vr.html). – 2014. – 22.07).***

# СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

П. Порошенко завел страницу в соцсети «ВКонтакте». Пресс-служба «ВКонтакте» подтвердила подлинность его страницы, сообщает ТСН.

Официальное представительство Президента Украины доступно по адресу: vk.com/poroshenko.petro. Достоверность публичной страницы подтверждает галочка возле названия, а также надпись «Официальная страница».

Как сообщается на самой странице П. Порошенко, здесь «все неравнодушные будут иметь возможность обмениваться мыслями и идеями, делать все возможное для того, чтобы Украина жила по-новому».

Планируется публикация новостей, фотоальбомов и видеообращений, также ожидается информация от первого лица «из-за кулис». Кроме того, пользователям доступны специальные приложения – с графиком Президента, формой обратной связи, предвыборной программой П. Порошенко. Дополнительно существует возможность стать волонтером, заполнив специальную анкету ***(Президент завел страницу во «ВКонтакте» // IT Expert (http://itexpert.org.ua/rubrikator/item/36994-prezident-zavel-stranitsu-vo-vkontakte.html). – 2014. – 15.07).***

***

Министерство иностранных дел Украины запустило свое представительство в социальной сети «ВКонтакте». Официальная страница государственного органа доступна по адресу vk.com/mfa_ukraine, передает корреспондент «proIT» со ссылкой на пресс-службу соцсети.

«МИД наращивает усилия в сфере коммуникаций. Наша цель состоит в том, чтобы объективная информация об Украине доходила до как можно большего количества людей. Мы создали страницу МИД “ВКонтакте”», – говорит министр иностранных дел П. Климкин.

Представители министерства подчеркивают: открывая официальную страницу во «ВКонтакте», они надеются, что она станет источником непредубежденной, интересной и полезной информации о деятельности МИД и о внешней политике Украины.

«Ежесуточно социальную сеть “ВКонтакте” открывают около 11 млн уникальных посетителей из Украины. И есть положительная тенденция, когда политики и государственные органы пытаются наладить связь с обществом, используя именно те интернет-ресурсы, которые действительно успели стать для пользователей и средством получения информации, и местом для обсуждения и генерации новых идей», – прокомментировал В. Леготкин, пресс-секретарь «ВКонтакте» в Украине ***(МИД Украины вышло в соцсеть «ВКонтакте» // InternetUA (http://internetua.com/mid-ukraini-vishlo-v-socset--vkontakte). – 2014. – 14.07).***

***

Политик и соцсети: «услышать каждого» по-индийски

…Наряду с простыми смертными в соцсетях засветились и десятки первых лиц различных государств. Отличный PR или просто дань времени?..

Как показывает почти годичная подобная практика новоизбранного премьера Индии Н. Моди (избран на пост 14 мая 2014 г.), онлайн-присутствие первого лица государства несет в себе достаточно большое количество сугубо прагматичных дивидендов для этого самого лица. Это и отмечают многие психологи.

Во-первых, наличие человека в той или иной соцсети его коллегами по онлайну расценивается как статус себе равного. Пусть в реальной жизни люди, общающиеся в одном чате, занимают разные социальные ниши (депутат и водитель, к примеру), но в онлайн-сущности они равны. Не существует классовых, социальных и материальных преград. Регистрация в 2–3 клика – и ты там, «где все друзья». Именно такую позицию занял тогдашний (по состоянию на декабрь 2012 г.) губернатор индийского штата Гуджарат. Конечно же, он знал, что будет баллотироваться на пост премьера на майские выборы 2014 г. И сделал очень прогрессивный шаг: стал ближе к десяткам миллионов своих соотечественников. Аккаунт в Facebook в настоящее время собрал будущему лидеру Индии более 19 млн подписчиков от множества индийцев, сделав его самым читаемым в Facebook жителем страны. О НаМо (аббревиатура имени политика) узнал мир. В этом плане Н. Моди значительно опередил других коллег по цеху – П. Порошенко (0,18 млн читателей), В. Путина (0,3 млн читателей), А. Меркель (0,6 млн читателей), Д. Кэмерона (0,25 млн читателей). Уступает индиец президенту США Б. Обаме, страничку которого читают в два раза больше подписчиков (41 млн читателей).

Во-вторых, уже с первых дней своего пребывания в соцсети индийский политик очень четко подошел к реализации стратегии «услышать каждого». Кроме десятков рабочих визитов по Гуджарату и всей Индии, политик находил время отвечать на сотни тысяч самых разных сообщений и постов на своей страничке. Разумеется, что в такой полиэтничной стране, как Индия, вопрос языка и веры всегда стоит на первом месте, и каждый политик должен принимать это во внимание. НаМо так и сделал. Со своего аккаунта он отвечал жителям Facebook на самых разных языках – английском, хинди, гуджарати, урду. Этот прием позволял разноязычным индийцам понимать слова политика и делало их общение с ним легким и комфортным. Публика была в восторге от реплик и реляций НаМо. Его рейтинг рос.

И в-третьих, пунктуальность и открытость этого индийского политика, проявленная наряду с поступками в реальной жизни в Facebook, создала НаМо особый имидж. Ведь уже немолодой человек (сейчас ему 63), а нашел общий язык с многомилионной индийской молодежью. Отвечая на их вопросы вовремя и по делу, Н. Моди приобрел себе сотни тысяч (!) новых поклонников и укрепил веру в него старых. В свою очередь, в режиме онлайн-диалогов политик смог не понаслышке узнать, чем живут люди в различных регионах страны, понять их проблемы, подумать о решениях этих самых проблем.

Показательно, что этого политик добился всего лишь за полтора года присутствия в соцсети. При этом, в отличие от многих других мировых известностей, Facebook обозначил его страницу специальным символом, обозначающим, что это – автентичная страница пользователя, а не его пресс-секретаря.

Украинским политикам есть чему поучится у своего индийского коллеги. Надо отдать им должное – они неплохо используют соцсети – пока не занимают высокие посты. Будем надеяться, что в век информации они не забудут о новых приемах связи со своими гражданами ***(Бхат А., историк, путешественник: Политик и соцсети: «услышать каждого» по-индийски // 112.ua (http://112.ua/mnenie/politik-i-socseti-uslyshat-kazhdogo-po-indiyski-89521.html). – 2014. – 18.07).***

***

В Facebook жителями города создана страница под названием «Луганск-Белая книга».

«Группа создана, чтобы отслеживать информацию о раненных и погибших в городе Луганске, сообщать о местах очередной трагедии, давать консультации о том, куда и в каких случаях необходимо обращаться, для поиска людей. Всё что связано с вопросом жизни и смерти в Луганске – это тема группы, – говорится в описании.

Участники группы намерены составить поименный список погибших луганчан и просят помощи у всех, кто обладает данными об этих людях. Пока известны имена только двух человек, погибших в Луганске 18 июля ***(В Фейсбуке создана группа «Луганск-Белая книга», участники которой хотят составить список погиблих // City News (http://www.citynews.net.ua/news/35268-v-feysbuke-sozdana-gruppa-lugansk-belaya-kniga-uchastniki-kotoroy-hotyat-sostavit-spisok-pogibshih.html). – 2014. – 19.07).***

***

Кам’янець-Подільське комунальне підприємство «Міськтепловоденергія» запустило свою офіційну сторінку у Facebook.

Як повідомляє прес-служба відомства, найближчим часом планується відкриття таких сторінок і в інших соціальних мережах. Скарги, які надходитимуть через соціальні мережі, розглядатимуться на рівні з іншими офіційними зверненнями від споживачів за умови, що буде вказана точна адреса, ім’я заявника та бажано його номер телефону.

«Я хочу, щоб люди знали про абсолютно все, що робиться на нашому підприємстві, які труби і де ремонтуються, скільки поривів у нас, з якими проблемами ми зустрічаємося щодня. Саме тому ми вирішили займатися не лише тепловими чи водяними мережами, а й долучитися до соціальних. Сподіваюся на конструктивний діалог з громадою», – заявив гендиректор КП В. Гордійчук ***(В Кам’янці комунальне підприємство спілкуватиметься з клієнтами через соцмережі // Незалежний громадський портал (http://ngp-ua.info/2014/07/15321). – 2014. – 16.07).***

# БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Профессиональная соцсеть LinkedIn приобрела новостной агрегатор Newsle. Об этом сообщает the-village.ru

Сумма и условия сделки не разглашаются. Известно лишь, что Newsle пока что продолжит свою работу, хотя его команда уже присоединилась к LinkedIn и начала интегрировать свои функции в соцсеть.

Новостной агрегатор Newsle был основан в 2011 г. Он позволяет отслеживать упоминания контактов пользователя из соцсетей в различных блогах и онлайн-изданиях. Предполагается, что такие инсайты помогут профессионалам совершенствоваться в своей работе и находить новые точки для карьерного роста.

Для LinkedIn эта сделка продолжает серию инвестиций в продукты, нацеленные на обмен бизнес-информацией. Ранее соцсеть уже приобрела новостной сервис Pulse, а также разрешила пользователям публиковать длинные посты и добавлять на свою страницу различный медиаконтент ***(Соцсеть LinkedIn приобрела новостной агрегатор Newsle // Media бізнес (http://www.mediabusiness.com.ua/content/view/40020/118/lang,ru/). – 2014. – 15.07).***

***

Социальная сеть Facebook, начиная с этой осени, начнет отслеживать телешоу, которые пользователи в США смотрят на мобильном телефоне или планшете. Об этом сообщает lenta.ru

Информацию о ТВ-предпочтениях Facebook будет сопоставлять со своими базами данных о пользователях, после чего сообщит о возрасте и поле зрителей рейтинговому агентству Nielsen. В результате рекламодатели, размещающие рекламу в телепрограммах, смогут больше узнать об аудитории, смотрящей телешоу онлайн.

Раньше данные для исследований Nielsen предоставляли зрители, которые добровольно согласились подключаться к аналитической системе во время просмотра телевизора. Однако с помощью Facebook и других агрегаторов данных Nielsen теперь стремится изучить предпочтения более широкой аудитории, в том числе, смотрящей телепрограммы только в онлайн-режиме.

Вопрос о том, будет ли Facebook спрашивать согласия пользователей, прежде чем сообщать ТВ-аналитикам информацию о них, остается открытым. По словам представителей Nielsen, Facebook будет предоставлять анонимную агрегированную информацию для таргетинга, не связанную напрямую с конкретными аккаунтами.

Однако тот факт, что Facebook отслеживает поведение пользователя на стороннем сайте и сообщает о его привычках своему партнеру, может вызвать недовольство у аудитории соцсети. Один из вариантов исключить

себя из процесса сбора данных: не использовать регистрационные данные Facebook для захода на видеохостинги.

Онлайн-видеореклама является одним из наиболее быстрорастущих сегментов рекламного рынка. По прогнозу eMarketer, она вырастет на 40 % в этом году до 6 млрд дол.

Возможность точнее таргетировать рекламу является ключевым конкурентным преимуществом для площадок, а Facebook может обеспечить рекламодателей данными о своей аудитории, размер которой превышает 1,23 млрд пользователей. Ранее в этом месяце Facebook заявила о покупке платформы LiveRail, которая специализируется на размещении таргетированной онлайн-видеорекламы ***(Facebook отследит телевизионные предпочтения пользователей // Media бізнес (http://www.mediabusiness.com.ua/content/view/40025/118/lang,ru/). – 2014. – 16.07).***

***

Facebook анонсировал обновление для десктопных объявлений игровых приложений – теперь компании могут включать в них рекламу виртуальных товаров и игровой валюты, чтобы вовлекать больше пользователей и увеличивать число игроков.

Новый формат объявлений доступен как для «Новостной ленты», так и для правой колонки. Создавать такие объявления можно во всех рекламных инструментах социальной сети.

Компания Kixeye уже успела протестировать новый рекламный формат для игры Battle Pirates. Цель, которую ставила перед собой компания, была следующей – привлечь внимание и вовлечь в игру пользователей, которые ранее уже покупали что-то в игре, а также активных юзеров, которые еще не успели ничего купить. Kixeye предложили пользователям скидку на покупку «золота» в игре, что дало увеличение CTR на 10 %, конверсии – на 50 % для тех пользователей, которые ранее уже что-то покупали, и увеличение конверсии на 14 % для пользователей, которые не покупали ничего ранее ***(Facebook расширил формат объявлений для игровых приложений // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_rasshiril_format_obyavleniy_dlya_igrovyh_prilozheniy). – 2014. – 16.07).***

***

Twitter запускает новый инструмент для отслеживания упоминаний брендов, который покажет, какую роль может сыграть повседневная деятельность компании в маркетинговой политике, пишет Marketing Media Review (http://mmr.ua/news/id/twitter-provedet-monitoring-upominanij-brendov-40454/).

Новый инструмент появится уже в ближайшее время. Он позволит маркетологам узнать, как и сколько говорят о компании в соцсети. Для этого

нужно будет выделить ключевые слова, относящиеся к бренду, и инструмент проанализирует разговоры, в которых они использовались.

Инструмент классифицирует разговоры по типам и категориям, а также показывает местоположение пользователей, обсуждающих бренд, на карте Великобритании. К примеру, вас интересует категория «Транспорт», и вы вводите в поиск такие слова, как «трафик», «поезд», «метро» и т. д. Затем на карте появляются упоминания этих слов в разговорах в Twitter, и таким образом можно увидеть, о чем и в каких районах говорят чаще. Инструмент также позволяет увеличивать масштаб карты. Среди предложенных категорий: музыка, эмоции, еда и напитки, животные.

Как сообщает MarketingWeek, инструмент был запущен по просьбе самих компаний, которые обратились к соцсетям, чтобы узнать, как постоянное взаимодействие с аудиторией влияет на развитие бренда.

В Twitter полагают, что запуск нового инструмента поможет маркетологам обратить внимание на повседневные возможности бренда, что простимулирует их тратить больше средств на рекламу в течение года ***(Twitter проведет мониторинг упоминаний брендов // Marketing Media Review (http://mmr.ua/news/id/twitter-provedet-monitoring-upominanij-brendov-40454/). – 2014. – 17.07).***

***

Крупнейшая в мире соцсеть Facebook начала тестирование кнопки Buy («Купить»), с помощью которой пользователи могут приобрести рекламируемые на сайте товары. Об этом говорится в сообщении Facebook, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-nachala-testirovanie-knopki-kupit-40467/).

Новый сервис тестируется с небольшим числом пользователей и партнеров Facebook из числа малого и среднего бизнеса в США.

«Пользователи компьютеров и мобильных устройств могут нажать кнопку «Купить» в рекламных блоках или записях на страницах брендов, что позволит им приобрести продукт напрямую у этого бренда, не покидая сайт Facebook», – поясняют в компании принцип работы сервиса.

В то же время Facebook подчеркивает, что данные банковских карт, используемых для покупки определенного продукта, соцсеть не будет передавать другим рекламодателям. Пользователи могут сами выбрать, сохранять ли данные банковской карты на сайте для будущих покупок.

В ходе тестирования Facebook не будет взимать комиссию с товаров, проданных с помощью кнопки «Купить», сообщает агентство Reuters со ссылкой на информированные источники. Денежные транзакции будут осуществляться сторонней процессинговой компанией, название которой не уточняется.

Напомним, что Facebook уже не первый год экспериментирует с продажей товаров на своем сайте. В 2012 г. соцсеть представила сервис Gifts,

позволявший отправить другу реальный подарок с доставкой – например, цветы или пирожные.

Однако спустя год Facebook отказалась от продажи «физических» подарков через сервис, ограничившись возможностью отправить лишь подарочную карту. В то же время комиссия с продажи товаров через сайт может разнообразить спектр источников дохода для Facebook, главным из которых сейчас является реклама ***(Facebook начала тестирование кнопки Купить // Marketing Media Review (http://mmr.ua/news/id/facebook-nachala-testirovanie-knopki-kupit-40467/). – 2014. – 20.07).***

***

Facebook пытается дать ответ на вопрос, занимающий каждого продавца: действительно ли реклама в социальной сети, насчитывающей 1,3 млрд пользователей, помогает увеличивать продажи? Пока мир с удовольствием «лайкает» и «фолловит», соцсеть начала концентрироваться на звоне кассовых аппаратов. Facebook проводит испытание кнопки «Купить» и выясняет, как онлайн-реклама влияет на продажи в реальных магазинах.

Нажми на кнопку

Привлечение на свою сторону розничных продавцов поможет Facebook решить следующую большую задачу – увеличить сумму, которую каждый рекламодатель тратит в сети. Однако после многолетних скандалов вокруг конфиденциальности ей нужно продвигаться осторожно, поскольку соцсеть сотрудничает с информационными брокерами и использует собственные клиентские базы данных ритейлеров.

По словам Э. Роса, генерального директора Datalogix, информационного брокера из Колорадо, сотрудничающего с Facebook, возможность подсчитать простые показатели, например рентабельность инвестиций, становится все более важной, с учетом роста опасений относительно мошенничества с онлайн-рекламой. «Бот не сможет купить товар в магазине», – говорит он.

Для измерения влияния рекламы на продажи Facebook сотрудничала с 20 ритейлерами. Отмечено повышение продаж в среднем на 2 % среди пользователей, которым показали рекламу, по сравнению с теми, кому ее не показывали. Средства, потраченные на рекламу, вернулись в среднем в восьмикратном размере. Согласно опубликованным недавно данным, реклама в сети так же эффективно убеждает людей покупать в реальных магазинах, как и совершать покупки онлайн.

В настоящее время Facebook находится в центре внимания – на следующей неделе компания должна опубликовать данные о доходах за II квартал. В прошлом году Facebook превзошла прогнозы аналитиков на волне подъема мобильной рекламы. Ключом к будущим успехам может стать розничная продажа, поскольку именно эта отрасль в настоящее время тратит больше всего на цифровую рекламу в США – по прогнозу исследовательской

компании eMarketer, в этом году ритейлеры потратят на онлайн-рекламу 11,2 млрд дол.

По словам Н. Франше, главы департамента розничной торговли и электронной коммерции в Facebook, он надеется, что по мере приближения следующего сезона покупок соцсеть будет занимать все больше места в кампаниях ритейлеров. «Мы абсолютно уверены, что это будет делаться безопасным для пользователей способом, однако гораздо более эффективными для рекламодателей методами», – сказал он.

Большой брат не смотрит

Facebook всячески подчеркивает, что не видит информации о том, что пользователи покупают в магазинах. Один из заметных радикальных шагов соцсети в вопросах конфиденциальности предполагал покупку данных на сайте, когда в 2007 г. компания запустила систему онлайн-рекламы Beacon, которая автоматически передавала данные о действиях пользователей сторонним сайтам – например Zappos.com.

Тогда сеть извинилась за эту систему и в нынешнем году попыталась исправиться, сосредоточившись на том, чтобы сделать установки конфиденциальности легкими для понимания – однако не избежала критики. Facebook обвинили в проведении психологического эксперимента по влиянию на пользователей.

Согласно опубликованным недавно данным, реклама в сети так же эффективно убеждает людей покупать в реальных магазинах, как и совершать покупки онлайн.

Сейчас не социальная сеть собирает еще больше данных, а ритейлеры загружают свои клиентские базы, содержащие сведения обо всем – от карт лояльности до адресов доставки. Данные анонимизированы и сопоставлены с профилями пользователей.

Facebook также сотрудничает с такими компаниями, как Datalogix and Acxiom, которые могут комбинировать тысячи источников данных, чтобы определить, что покупают люди, вплоть до марки зубной пасты.

Контора пишет

Например, Acxiom, отслеживающая более 700 млн людей по всему миру, создала «мастер-профили», в которых онлайн-деятельность объединяется с офлайн-информацией, такой как политические симпатии и уровень дохода.

Walmart связала свои рекламные объявления о приближении учебного года, направленные пользователям Facebook с детьми школьного возраста, с реальными продажами и заявила, что заработала в 16 раз больше, чем было потрачено на рекламу. А продавец одежды Banana Republic сообщил, что в прошлом сезоне продаж Facebook был его самым эффективным маркетинговым каналом. Компания использовала социальную сеть для поиска пользователей, похожих на своих молодых клиентов.

Аналогичный эффект получили компании потребительских товаров – реклама пива Bud Light подняла продажи на 3,3 %.

«С точки зрения рекламодателей, информирование о новых продуктах, исследование и обмен мнениями клиентов происходит преимущественно в цифровом пространстве, однако почти все расчеты происходят офлайн, – рассказал Э. Роса. – Facebook – это новейший носитель. Он возник с нуля и вырос до десятков миллионов долларов, а сейчас начал привлекать внимание. Клиенты говорят: отлично, я могу сказать, что вышел в соцсеть, у меня есть страничка фанов, но я хочу знать, способствует ли это продажам».

То, что Facebook настаивает, чтобы люди использовали свои настоящие имена, отличает его от множества других издателей цифровой рекламы, включая конкурирующих Twitter и Pinterest. У него также широкие возможности таргетирования благодаря информации, которую пользователи предоставляют добровольно.

Р. Мальотра из группы измерений Facebook считает, что даже если реальные люди нажимают на ссылку или лайкают пост, это действие мало связано с их намерением купить продукт.

По словам Д. Белла, профессора из Уортонской школы бизнеса, который изучает электронную коммерцию, Facebook пытается решить «вековую проблему маркетинга», существующую до сих пор, потому что очень много транзакций осуществляется офлайн.

«Каким бы замечательным ни был Интернет, на него приходится всего лишь 10 % всей коммерции», – констатирует он.

Электронную коммерцию – в соцсети

На этой неделе социальные сети, включая Facebook, Twitter и Pinterest, еще на шаг приблизились к предложению электронной коммерции на своих платформах. Битва за ритейлеров разгорается с новой силой.

17 июля Facebook объявил, что проводит испытания кнопки «Купить», которая позволит людям приобретать продукт, не покидая приложение соцсети. По результатам начального тестирования с несколькими малыми и средними компаниями в США, возможно, больше компаний электронной коммерции станут покупать рекламу в этой соцсети.

На этой неделе компания Twitter приобрела CardSpring, разработчика прикладного программного интерфейса для мобильных платежных приложений, цена сделки не разглашается. CardSpring связывает детали платежа с картами лояльности и купонами для транзакций, осуществляемых онлайн и в магазине.

В прошлом году сервис микроблогов нанял Н. Хаббарда, бывшего генерального директора Ticketmaster, для разработки продукта электронной коммерции. Компания также сотрудничала с Amazon, позволяя добавлять товары в онлайн-корзины с помощью твитов, и со Starbucks, призывая людей твитить, чтобы купить кофе для друга.

Фотохостинг Pinterest ритейлеры рассматривают как совершенно естественное место для размещения рекламы, поскольку пользователи здесь на своих «досках» составляют списки пожеланий. Компания объединила усилия с Shopify, интернет-платформой из более чем 100 тыс. магазинов, и

теперь все «пины» их продуктов снабжены деталями – например, ценой ***(У Facebook появится больше возможностей зарабатывать на пользователях // InternetUA http://internetua.com/u-Facebook-poyavitsya-bolshe-vozmojnostei-zarabativat-na-polzovatelyah). – 2014. – 22.07).***

***

Чистий прибуток соціальної мережі Facebook за II квартал 2014 р. збільшився більше ніж у два рази (138 %) порівняно з показником за 2013 р. і досяг 791 млн дол., пише Корреспондент.net (http://ua.korrespondent.net/business/financial/3396508-prybutok-Facebook-za-druhyi-kvartal-2014-roku-zbilshyvsia-u-dva-razy).

Виручка за звітний період зросла на 61 % і становила 2,91 млрд дол. проти 1,81 млрд дол. на рік раніше. Більша частина квартальної виручки (92 %) припадає на доходи від реклами, які продемонстрували зростання порівняно з аналогічним періодом минулого року на 67 % до 2,68 млрд дол.

Нагадаємо, чистий прибуток компанії Facebook Inc. у I кварталі 2014 р. зріс у 2,9 раза – до 642 млн дол., порівняно із 219 млн дол. на рік раніше.

Facebook – найбільша у світі соціальна мережа з капіталізацією 182,9 млрд дол. (NASDAQ). Щомісячна аудиторія соцмережі становить 1,32 млрд користувачів ***(Прибуток Facebook за другий квартал 2014 року збільшився у два рази // Корреспондент.net (http://ua.korrespondent.net/business/financial/3396508-prybutok-Facebook-za-druhyi-kvartal-2014-roku-zbilshyvsia-u-dva-razy). – 2014. – 24.07).***

***

Акции американской социальной сети Facebook 23 июля прибавили в цене более 5 % на фоне опубликованной позитивной финансовой отчетности за II квартал 2014 г. После закрытия биржевых торгов в Нью-Йорке цена за бумагу составила рекордные для компании 75,30 дол. ***(Акции Facebook рекордно выросли // InternetUA (http://internetua.com/akcii-Facebook-rekordno-virosli). – 2014. – 24.07).***

***

У перспективі двох-трьох років основну конкуренцію для банків становитимуть IT-компанії, такі як Google, Facebook, Twitter, Amazon і PayPal, які самі вже стають банками.

Про це сказала в інтерв'ю Forbes О. Попова, голова ради директорів Дельта Банку.

Вона зазначила, що багато банків на сьогодні також рухаються шляхом перетворення на такі компанії, обирають своєю головною метою створення зручної системи платежів для клієнтів, яка ставала б інструментом оплати товарів і послуг.

«Банк – це сукупність IT-компанії, якісного маркетингу, який включає розуміння потреб клієнта та вміння працювати з аналітикою, також для банку

критично важливий ризик-менеджмент. Тобто сучасний банк – це симбіоз IT-компанії, маркетингового агентства та якісного ризик-менеджменту. Але це дуже непросте завдання з погляду платформи і технології, обсяг інвестицій у реалізацію якої з нашого боку обчислюється мільйонами доларів», – сказала О. Попова ***(Головним конкурентом банків стають соцмережі й онлайн-аукціони, – банкір // LB.ua (http://ukr.lb.ua/news/2014/07/25/274078_glavnim_konkurentom_bankov.html). – 2014. – 25.07).***

***

Facebook оттачивает таргетинг рекламы в мобильных приложениях, позволяя разработчикам ориентироваться на конкретные устройства, а не только на различные версии операционных систем, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapuskaet-novye-nastrojki-targetinga-dlja-reklamy-mobilnyh-prilozhenij-40537/).

В официальном блоге сказано, что таргетинг на мобильные устройства будет запущен в течение ближайших нескольких дней.

Реклама мобильных приложений в Facebook очень успешна, в основном благодаря таргетингу на мобильные устройства. Чтобы получить больше установок того или иного приложения, а также большую вовлеченность пользователей, очень важно привлечь правильную аудиторию, используя наиболее актуальные для этой аудитории рекламные предложения. Поэтому мы усиливаем акцент на мобильном таргетинге. В течение следующих нескольких дней вы сможете охватить пользователей таких мобильных устройств, как, например, Samsung Galaxy S5, iPhone 5s или HTC One. Ранее же вы могли взаимодействовать только с владельцами устройств на базе систем iOS или Android, с минимальной версией ОС и исключительно с помощью Wi-Fi.

Разработчик Facebook Ч. Ли также обозначил преимущества таргетинга на мобильные устройства:

Больший возврат инвестиций: вы сможете охватить наиболее заинтересованных пользователей и оптимизировать ваши объявления, ориентируясь на конкретное мобильное устройство.

С помощью App Insights вы сможете определить, на каком устройстве ваше приложение работает лучше всего, и нацелить вашу рекламную стратегию именно на владельцев этого гаджета. К примеру, маркетологи одного туристического агентства выяснили, что их услуги пользуются большим успехом у владельцев iPhone 5s, и дальше будут уже ориентироваться на них при создании рекламных объявлений.

Вы сможете сосредоточиться только на тех устройствах, которые наиболее подходят для ваших приложений, и не тратить время на гаджеты, где приложение не пользуется популярностью.

Также Ч. Ли напомнил о таргетинге на индивидуализированные и аналогичные аудитории в Facebook:

В добавление к таргетингу на мобильные устройства, вы можете охватить наиболее лояльных пользователей, создавая индивидуализированные аудитории, которые включают в себя людей, использующих ваши мобильные приложения. Например, если бы вы были разработчиком приложений, вы могли бы продвигать свои разработки среди людей, которые уже знакомы с другой вашей продукцией и любят ее. А также вы могли бы создать аналогичную аудиторию, круг людей, которые похожи на ваших постоянных клиентов, и которых возможно тоже заинтересуют ваши приложения.

С помощью индивидуализированных пользовательских аудиторий вы можете взаимодействовать с людьми, уже использующими ваши разработки, чтобы повысить уровень конверсии и вовлеченности. К примеру, приложение, специализирующееся на путешествиях может повысить лояльность уже имеющихся пользователей, предлагая более выгодные цены на авиаперелеты или рекламу, призывающую «прямо сей час» заказать билет.

Другое преимущество индивидуализированных аудиторий в Facebook – это возможность легко связаться с самыми активными юзерами. К примеру, одно из коммерческих приложений определило 25 % самых активных пользователей, которые возвращают приложению 56 % от его стоимости. В результате, были созданы рекламные объявления, ориентированные конкретно на этих пользователей, побуждая их совершать покупки и увеличивать рост доходов компании-разработчика.

Комбинация индивидуализированных и аналогичных аудиторий дает вам возможность обзавестись лояльными подписчиками и увеличить вовлеченность уже существующих пользователей.

И наконец, Ч. Ли привел несколько подсказок по управлению рекламой для мобильных приложений в Facebook:

Не сужайте свою аудиторию. Если нет четкой причины создавать разные рекламные кампании для разных мобильных устройств, то сгруппируйте их пользователей. Рекомендуемый размер группы для каждого рекламного объявления должен составлять хотя бы 500 тыс. человек.

Создавайте рекламные компании, которые вызовут отклик вашей аудитории. К примеру, для рекламы на iPad используйте фото iPad или упомяните в своем тексте App Store.

Оптимизируйте ваши ценовые предложения для каждой рекламной акции: создавайте разные рекламные кампании для каждого устройства в отдельности или для группы устройств, так как конкуренция также варьируется в зависимости от гаджета.

Используйте индивидуализированные и аналогичные аудитории, чтобы обратить на себя внимание большего количества лояльных пользователей ***(Facebook запускает новые настройки таргетинга для рекламы мобильных приложений // Marketing Media Review (http://mmr.ua/news/id/facebook-zapuskaet-novye-nastrojki-targetinga-dlja-reklamy-mobilnyh-prilozhenij-40537/). – 2014. – 23.07).***

***

Профессиональная социальная сеть LinkedIn сообщила о покупке маркетингового стартапа Bizo за 175 млн дол. Согласно условиям сделки, LinkedIn платит 10 % стоимости в своих акциях, остальное – наличными. Закрытие сделки ожидается в III квартале.

Еще до соглашения о покупке компания Bizo была партнером LinkedIn. Она занимается выпуском решений для маркетологов и продавцов. В заявлении LinkedIn говорится, что компания с поглощением Bizo расширяет спектр своих услуг за пределы кадровой сферы и получает возможности по интеграции своих решений с продуктами для бизнес-автоматизации.

В июне 2013 г. компания Bizo привлекла 30 млн дол. В IV квартале 2013 г. Bizo сообщила о выручке в размере 12,4 млн дол. ***(LinkedIn покупает компанию Bizo // InternetUA (http://internetua.com/LinkedIn-pokupaet-kompaniua-Bizo). – 2014. – 24.07).***

# СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

## Інформаційно-психологічний вплив мережевого спілкування на особистість

Голландське креативне агентство Just запустило проект 99 Days Of Freedom («99 Днів Свободи»), у рамках якого деякі юзери Facebook перестануть користуватися соцмережею протягом 99 днів.

Як повідомляє psfk, після завершення терміну дослідники зроблять висновок про те, як Facebook впливає на рівень щастя людини.

Раніше дослідження Just показали, що в середньому користувач проводить у Facebook 17 хвилин на день. Це означає, що учасники 99 Days Of Freedom звільнять 28 годин вільного часу.

При цьому автори проекту стверджують, що кількість днів було обрано не випадково. За цей період експеримент не встигне набриднути користувачам, а дослідники зможуть зібрати необхідну інформацію.

«Ми прогнозуємо, що експеримент принесе велику кількість позитивних емоцій, і через 99 днів ми будемо знати, чи правильна наша теорія», – говорить М. Стратхоф, арт-директор Just

Для участі в експерименті необхідно зареєструватися на сайті проекту, поставити у своєму профілі на Facebook аватар 99 Days Of Freedom, відмовитися від відвідування соцмережі і «насолоджуватися життям» ***(Юзери Facebook заради експерименту відмовились від соцмережі на 99 днів //***

***InternetUA (http://internetua.com/uazeri-Facebook-zaradi-eksperimentu-v-dmovilis-v-d-socmerej--na-99-dn-v). – 2014. – 16.07).***

***

Социальные сети – всемирная эпидемия для современного общества

Сегодня можно оглянуться назад на историю человечества и увидеть печальную закономерность – у каждого века была своя непобедимая и неизлечимая болезнь, которая разрушала и калечила не просто человеческие жизни, а и жизни целых семей, племен, народов...

К таким недугам многие активисты сегодня относят социальные сети. Именно провождение большого количества времени людьми в соцсетях беспокоит ученых по всему миру. Конечно, интернет-серфинг принес нам немало полезных вещей. Информация, которую мы находим на различных сайтах, часто нужна нам для работы, учебы, выполнения дел по хозяйству. Например, многие ищут гороскоп на неделю или рецепты народной медицины в сети, где такая полезная информация находится в широком доступе.

Но вовсе не секрет, что только стоит нам посетить социальные сети, как мы теряем счет времени. Причем проводим время в социальных сетях мы, как правило, не с пользой. Работник забывает о своем деле, домохозяйка забрасывает свои хлопоты, дети пропадают в соцсетях вместо активного проведения досуга, а зачастую и жертвуют своим временем, которое отведено на учебу. Некоторые ученые окрестили такую зависимость «массовой эпидемией».

Сегодня даже представители старшего поколения освоили соцсети. Создаются также специализированные соцсети для людей одной профессии или общих интересов.

Как мы убиваем время

Было установлено, что хоть социальные сети изначально были придуманы для более легкого и простого способа установить связь, общаться с друзьями и родственниками, с которыми Вы не можете увидеться лично из-за географического местонахождения, общение – это не основное наше занятие в «социалках».

Оказывается, что большую часть времени мы тратим на рассматривание чужих фото и страничек, посещение различных публичных групп и браузерные игры.

Люди, которые имеют различные комплексы, только обостряют их, посещая странички более успешных или привлекательных внешне знакомых и незнакомых людей.

Также различные коммерческие проекты нередко обогащаются за счет пользователей.

Что в итоге?

В итоге мы получили расшатанную нервную систему, недосыпание, плохую успеваемость на учебе и в работе, а главное – стали отдаляться от

тех, кто находится рядом с нами по эту сторону монитора ***(Социальные сети – всемирная эпидемия для современного общества // Novostiua.net (http://novostiua.net/stati/58492-socialnye-seti-vsemirnaya-epidemiya-dlya-sovremennogo-obschestva.html). – 2014. – 17.07).***

## Маніпулятивні технології

14 липня у користувачів соцмереж викликало обурення заява речника Федерального уряду Німеччини про необхідність вести перемовини з представниками так званої «ДНР» та «ЛНР», яка була зроблена після зустрічі німецького канцлера з російським президентом.

Інформація про те, що ця заява є нібито результатом домовленостей між В. Путіним та А. Меркель щодо України, спричинила резонансну дискусію в українських ЗМІ і соцмережах. Деякі повідомлення та вислови обурення супроводжувала фотографія теплого привітання німецького та російського лідерів, яка, щоправда, була зроблена 1 червня 2012 р. під час візиту В. Путіна до Берліна.

Хвиля невдоволення інтернет-користувачів перетворилася у флеш-моб коментарів Danke Frau Ribbentrop («Дякую, пані Ріббентроп») на сторінці А. Меркель у Facebook, натякаючи на таємні домовленості між СРСР та Німеччиною напередодні Другої світової війни щодо розподілу територій інших країн.

Згадана фотографія А. Меркель та В. Путіна в контексті 2014 р. була також показана в сюжеті ТСН про флеш-моб «Дякую, пані Ріббентроп».

Адміністрація сторінки німецького канцлера назвала такі коментарі спам-атакою та висловила сподівання, що дискусія повернеться в конструктивне русло. Однак онлайн-редакція залишила за собою право видаляти коментарі, які «порушують чинне право або містять образи, наклепи, є расистського або політико-екстремістського характеру».

На думку українського журналіста В. Портникова, акція проти А. Меркель була організована російською пропагандою. «Я вважаю, що мета російської пропаганди – посварити Україну з Німеччиною як дуже впливовою країною в ЄС. У Німеччині є чимало видань, які безпосередньо або опосередковано пов’язані з російською пропагандистською машиною. Завдяки цьому флешмобу такі видання отримають непоганий ілюстративний матеріал, щоб репрезентувати українців як одну зі сторін конфлікту в їхній власній країні. А це якраз і є метою російської пропаганди!» – сказав В. Портников у коментарі «Німецькій хвилі» ***(Тролинг Меркель у соцмережах супроводжувало фото дворічної давності // MediaSapiens (http://osvita.mediasapiens.ua/material/32729). – 2014. – 16.07).***

***

Пользователи Facebook начали «троллинг» президента Франции, который не находит в себе сил отказать в продаже России военных судов.

Разделяющие проукраинскую позицию пользователи соцсети призывают писать президенту Франции Ф. Олланду в Facebook о возмущении продажей военных судов России, развязавшей войну против Украины.

«Спасибо за “Мистраль” для России, господин президент! Вы поможете украинцам умереть!» – пишут на странице Ф. Олланда ***(Украинцы начали «мочить» в Facebook Франсуа Олланда // IT Expert (http://itexpert.org.ua/rubrikator/item/37019-ukraintsy-nachali-mochit-v-facebook-fransua-ollanda.html). – 2014. – 16.07).***

***

Акции социальной сети Introbiz за два месяца поднялись в цене в 360 раз! Такой невероятный скачок объясняется просто. Социальная сеть Introbiz два месяца назад практически не имела никакой популярности. Одна ее акция стоила 6 центов, сегодня же она составляет 21,96 дол. То есть рост составил 36 тыс. процентов! Правда, на самых последних торгах зафиксирован спад цены до уровня 13,9 дол., тем не менее, если сравнивать с изначальной ценой акций, то рост составил 22 тыс. процентов!

Социальная сеть нашла для себя «золотую жилу». Она продает за полсотни долларов контактную информацию самых известных людей мира. Пользователем социальной сети является один единственный человек. Это некто М. Сынчез, который является директором этой сети, ее главным финансистом и акционером. Этому человеку принадлежит 72 % акций его странной компании.

На этом странности компании Cynk Technology Corp не заканчиваются. Так, в финансовом отчете за 2013 г. было указано, что компания имеет убыток в сумме 1,5 млрд дол. При этом FT во время проверки работы компании зафиксировала факт, что 78 покупателей информации заплатили по 50 дол. через ЭДС PayPal. То есть выручка несоизмерима с заявленным убытком. Все эти люди якобы купили контактную информацию популярного актера Л. ДиКаприо.

Выглядит странным и список известных личностей. К примеру, там есть никому не известный знаток фитнесса, называющий себя «Лепщиком тела». Наладить с ним контакт сеть предлагает за 1,5 тыс. дол.! Странно выглядит и то, что ни у одного аккаунта в сети нет ни единого подписчика. При этом сайт Introbiz.com появился в сети еще в 2009 г. и тогда же зарегистрировался в компании Domains By Proxy из штата Аризона. Эта компания отвечает за сохранность личных данных пользователей тех порталов, которые имеют с ней соответствующий договор.

Наконец, компания Cynk Technology Corp на своем сайте разместила ложный адрес своего местонахождения. Те люди, которые мало-мальски

имеют хоть какое-то представление в работе интернет-компаний, недоумевают, ибо выглядит все это едва ли не как насмешка над системой контроля и людьми. В так называемой деятельности Cynk Technology Corp не прослеживается даже намека на какую-то логику.

Остается лишь удивляться тому, что соответствующие контролирующие органы до сих пор не предприняли к этой компании ни каких мер. Ведь судя по всему, мы видим одну из схем по отмыванию грязных денег ***(Социальная сеть Introbiz без пользователей подорожала в 360 раз // IT Expert (http://itexpert.org.ua/rubrikator/item/36988-sotsialnaya-set-introbiz-bez-polzovatelej-podorozhala-v-360-raz.html). – 2014. – 14.07).***

***

У соцмережах та проросійських інтернет-виданнях поширюють відео нічного бою під заголовком «Ополченцы разбили нацгвардию Мариновка». 11 липня зйомку було опубліковано на YouTube-каналі Ukraine News TV 2014.

Відео нічного обстрілу із систем залпового вогню поширили видання infoodessa.com, anti-maidan.com, novorosinform.org та в низці соцмереж, видаючи це за обстріл у Маринівці Донецької області.

Водночас у коментарях до відео користувачі поширили посилання на ці ж кадри, зняті два роки тому. Насправді, відео нічного обстрілу було зняте на Кавказі під час масштабних навчань російської армії, які стартували 17 вересня 2012 р. На полігоні Капустин Яр проходили навчання з бойовою стрільбою за участі ракетних військ та артилерії 58-армії. Відео опубліковане 19 вересня 2012 р.

Як відомо, у ніч на 12 липня відбувся мінометний обстріл пропускного прикордонного пункту Маринівка. За повідомленням МЗС України, обстріл вівся зі сторони Російської Федерації ***(У мережі поширюють фейкове відео нічного бою під маринівкою // MediaSapiens (http://osvita.mediasapiens.ua/material/32709). – 2014. – 15.07).***

***

У Донецьку поширюється новий вид вимагання грошей від місцевих жителів через соціальні мережі.

Невідомі відсилають приватні повідомлення власникам акаунтів соціальних мереж з вимогою перерахувати гроші на потреби Новоросії, інформує «Сиргис Информ».

У випадку відмови обіцяють розправу, а як доказ серйозності своїх намірів вказують у повідомленні адресу жертви, яку, ймовірно, дізнаються через місцевих співробітників міліції.

Гроші терористи вимагають перераховувати на рахунок у Webmoney, а також на карту «Приватбанку». Шантаж терористи проводять з фейкових, анонімних акаунтів.

«Допоможи Новоросії. З тебе 3 тис. гривень на карту Приватбанку 5211 5374 5187 3256 чи Webmoney. Якщо не допоможеш – будеш інвалідом. Це не жарт. Ти живеш за адресою ..», – от такі повідомлення отримують донеччани ***(Терористи вимагають від донеччан гроші для Новоросії: якщо не допоможеш – будеш інвалідом // Ipress.ua (http://ipress.ua/news/terorysty_vymagayut_vid_donechchan_groshi_dlya_novorosii_yakshcho_ne_dopomozhesh__budesh_invalidom__foto_74836.html). – 2014. – 16.07).***

***

На странице «ВКонтакте» лидера вооруженных формирований «ДНР» И. Гиркина (Стрелкова) зафиксирована подмена сообщения о сбитом якобы украинском АН-26.

Об этом свидетельствует разное время первого сообщения и нового, которым заменили предыдущее, передают «Комментарии».

В первом сообщении было зафиксировано московское время 17:50.

«В районе Тореза только что сбили самолет Ан-26, валяется где-то за шахтой “Прогресс”. Предупреждали же – не летать в “нашем небе”. А вот и видео-подтверждение очередного “птичкопада”. Птичка упала за террикон, жилой сектор не зацепила. Мирные люди не пострадали», – тогда написал И. Гиркин.

Свои слова он подкрепил двумя ссылками на видео.

В замененном – 17:37, в котором говорится о сбитом АН-26 в районе Снежного и якобы отступлении, по словам И. Гиркина, «укров»..

Также о подмене свидетельствует то обстоятельство, что замененное сообщение невозможно открыть в новом окне из-за смены времени. Браузер предупреждает об ошибке ***(Гиркин подменил свое сообщение о сбитом самолете // Комментарии: Харьков (http://kharkov.comments.ua/news/2014/07/17/213916.html). – 2014. – 17.07).***

## Зарубіжні спецслужби і технології «соціального контролю»

В Россию на прошлой неделе приезжали представители социальной сети Facebook для переговоров с Роскомнадзором, сообщает газета «Известия» со ссылкой на три источника в госструктурах. Встреча состоялась в условиях секретности по просьбе Facebook.

Facebook представлял директор по общественной политике Facebook в Центральной и Восточной Европе Т. Кристенсен. Он обсудил с руководством Роскомнадзор вопросы законодательного регулирования интернета в России. Итоги встречи неизвестны.

23 июня состоялся визит вице-президента Twitter К. Кроуэлла в Москву. Он тоже общался с руководством Роскомнадзора по поводу законодательного регулирования Интернета в России. Ранее, в мае, замглавы

Роскомнадзора М. Ксензов пригрозил Twitter блокировкой, если сервис не будет удалять аккаунты, признанные в России экстремистскими.

После встречи руководитель Роскомнадзора А. Жаров заявил, что Twitter удалит микроблоги по требованию российских властей, в том числе аккаунт Правого сектора. В тот же день представители соцсети опровергли эту информацию ***(Представители Facebook секретно встретились с руководством Роскомнадзора // IT Expert (http://itexpert.org.ua/rubrikator/item/36977-predstaviteli-facebook-sekretno-vstretilis-s-rukovodstvom-roskomnadzora.html). – 2014. – 14.07).***

***

Кировским районным судом за посягательство на территориальную целостность и неприкосновенность Украины (ч.1 ст. 110 Уголовного кодекса Украины) к трем годам лишения свободы (с испытательным сроком в один год) приговорен житель Днепропетровска, уроженец Магдалиновского района.

Осужденный агитировал пользователей соцсетей за создание «Украинской автономной республики» в составе Российской Федерации ***(Интернет-сепаратиста осудили на 3 года // DNEPR.INFO (http://dnepr.info/news/region/67617-internet-separatista-osudili-na-3-goda). – 2014. – 15.07).***

***

Іранський суд засудив вісьмох молодих громадян країни в цілому до 127 років тюрьми за антиурядові повідомлення у Facebook, повідомляє агентство AFP.

Як уточнює агентство, кожен з них засуджений до позбавлення волі строком від 11 до 21 року.

Імена засуджених не розголошуються, проте, згідно з постановою суду, вони отримали тюремні строки за «дії, що загрожують національній безпеці, антиурядову пропаганду і осквернення релігійних святинь та іранських лідерів».

В Ірані з 2009 р. заборонено доступ до Facebook, Twitter і YouTube. 23 травня 2014 р. влада країни також заблокувала Instagram, посилаючись на те, що соціальна мережа обмежує право громадян країни на недоторканність особистого життя.

Понад те, віртуальний простір країни контролює відділ з боротьби з інтернет-злочинністю, а з 2012 р. функціонує також спеціальне агентство з нагляду за Інтернетом ***(Суд засудив 8 іранців до 127 років в'язниці за пости в Facebook // LB.ua (http://ukr.lb.ua/news/2014/07/14/272823_sud_prigovoril_8_irantsev_127_godam.html). – 2014. – 14.07).***

***

Мобильные устройства Apple содержат закладки – скрытые механизмы, предназначенные для сбора сведений о пользователе спецслужбами. Об этом сообщает Cnews со ссылкой на отчет эксперта в области компьютерной безопасности Д. Здзиарски, подготовленного им к конференции Hackers On Planet Earth в Нью-Йорке.

Д. Здзиарски, также известный как NerveGas, принимал активное участие в разработке джейлбрейков для первых моделей iPhone и автор нескольких книг по разработке приложений для iOS. По его словам, 600 млн мобильных устройствах Apple, находящиеся в эксплуатации по всему миру, содержат «недокументированные службы, работающие в фоновом режиме», а также «подозрительные упущения в дизайне iOS, которые облегчают сбор данных». В презентации, в частности, упоминаются службы com.apple.pcapd и com.apple.mobile.file_relay.

Служба com.apple.pcapd при включении iOS-устройства немедленно запускает библиотеку libpcap, предназначенную для захвата сетевых пакетов. Д. Здзиарски указывает на то, что данная служба предназначена для анализа сетевого трафика, однако недоумевает, почему эта отладочная функция работает по умолчанию на всех iOS-устройствах подряд, никак не сигнализирует о своем присутствии и не требует активации режима отладки.

Вторая служба – com.apple.mobile.file_relay (File Relay), – по словам эксперта, вызывает еще больше вопросов. «Эта служба помещена в iOS с явным умыслом для того, чтобы извлекать данные с устройства по запросу», – пишет Д. Здзиарски.

При этом эксперт указывает на то, что служба способна извлекать данные минуя функцию шифрования данных на iOS-устройстве, предназначенную для защиты пользовательского контента. Наконец, в наиболее свежей версии iOS – iOS 7 – возможности службы были существенно расширены, отмечает он.

Если в предыдущих версиях платформы источниками File Relay были приложений AppleSupport, Network, WiFi, UserDatabases, CrashReporter и SystemConfiguration, то в iOS 7 список уже включает 43 источника, в том числе Accounts, AddressBook, Caches, CoreLocation, FindMyiPhone, MapsLogs, Photos, Voicemail и пр.

Accounts хранит информацию обо всех аккаунтах пользователя, введенных в устройство (включая Twitter, iCloud, Facebook и др); AddressBook – копия файла базы данных SQLite книги контактов пользователя (включая удаленные контакты, которые можно восстановить); Caches – пользовательская кэш-папка, содержащая ненужные скриншоты, различные полученные по сети изображения, оффлайновый контент и т. д., CoreLocation – журналы GPS, а Photos – дамп всех изображений, хранящихся на устройстве.

Особого внимания Д. Здзиарски заслужил источник под названием HFSMeta, который появился в iOS 7 также впервые. Он содержит время

изменения, название, размер и дату создания каждого файла на iOS-устройстве, включая все имена пользовательских файлов в Dropbox и т. п.

«По какой причине анализатор сетевых пакетов запущен на 600 млн персональных iOS-устройствах?», «Почему в устройстве запущены недокументированные службы, которые обходят функцию шифрования пользовательских данных и извлекают из памяти массивные объемы персональных данных?» – на эти и другие вопросы, по словам Д. Здзиарски, Apple не захотела ему ответить, оставив его запросы без внимания ***(Эксперт: Apple установила «жучки» на каждое устройство с iOS // InternetUA (http://internetua.com/ekspert--Apple-ustanovila--jucski--na-kajdoe-ustroistvo-s-iOS). – 2014. – 22.07).***

***

Абонентам в ряде городов России предлагают перейти на «чистый» Интернет, который больше напоминает кабельное телевидение. Это особое подключение, при котором уже нет доступа к популярным социальным сетям, а также многим другим популярным зарубежным ресурсам, например YouTube. Данный пакет предлагается для постоянного кабельного подключения.

При этом сразу указывается перечень доступных интернет-ресурсов в отдельном списке.

«Мы предлагаем вам оказаться в абсолютно чистом Интернете, где невозможно даже случайно наткнуться на сомнительную информацию.

Теперь вам не нужно ждать, пока органы правопорядка обнаружат страницы с противоправным содержимым и добавят их в реестр запрещённых сайтов.

Если вы выберете тариф “Чистый Интернет”, у вас будет уникальная возможность посещать только сайты с гарантированно благопристойным содержимым» ***(В России запустили «чистый интернет» – без соцсетей и заграничных сайтов // Весь Харьков (http://all.kharkov.ua/news/state/v-rossii-zapystili-chistyi-internet-bez-socsetei-i-zagranichnyh-saitov.html). – 2014. – 24.07).***

***

У Держдуму Росії внесли законопроект про запровадження механізму блокування або видалення фейкових акаунтів у соціальних мережах. Автором ініціативи є депутат О.Чепа від фракції «Справедлива Росія», пише tjournal.ru.

Згідно з цим документом, пропонується надати російським користувачам право подавати скарги на фальшиві сторінки в соцмережах, що ведуться від їхнього імені. Розглядом таких звернень має займатися Роскомнагляд.

До скарги особі необхідно буде додати документи, що посвідчують особу, а також заяву з чітким обґрунтуванням, чому певна сторінка має бути заблокована.

Роскомнагляд, розглянувши звернення громадянина, зможе вимагати блокування фейкового акаунту або повного видалення із соціальної мережі (якщо заблокувати його виявиться неможливо з технічних причин).

Як пише tjournal.ru, поки що невідомо, коли саме відбудеться розгляд законопроекту ***(Російський депутат запропонував примусово видаляти із соцмереж фейкові аккаунти // MediaSapiens (http://osvita.mediasapiens.ua/material/33020). – 2014. – 25.07).***

***

Исследователи из Принстонского университета (США) и Левенского католического университета (Бельгия) обнаружили ранее неизвестный механизм для отслеживания посещения пользователями определенных сайтов. В отчете «Сеть никогда не забывает: Постоянные механизмы отслеживания» (The Web never forgets: Persistent tracking mechanisms in the wild) они описали приложение AddThis, внедренное без ведома пользователей в 5 тыс. сайтов, входящих в топ-100 самых посещаемых ресурсов по статистике Alexa.

Пользователи, отслеживаемые приложением, не могут обезопасить себя ни с помощью обычной функции очистки браузера, ни применяя защитные решения наподобие AdBlock Plus. Среди сайтов, использующих AddThis, значатся ресурсы Министерства иностранных дел и торговли Австралии, Министерства охраны здоровья, Министерства юстиции, королевской семьи Великобритании, а также ряда правительственных организаций США, в том числе, Белого дома.

Главным разработчиком AddThis является Р. Харрис. В своем интервью изданию ProPublica он сообщил, что в нынешнем году начал эксперимент по внедрению технологии Canvas fingerprinting, которая должна стать альтернативой привычным текстовым файлам cookie. Она заключается в том, что с помощью Canvas API браузер пользователя создает уникальные невидимые изображения, которые потом конвертируются в идентификационные номера.

Пока механизмов, блокирующих эту технологию, не существует, поэтому эксперты советуют использовать анонимную сеть Tor, экспериментальный браузер Chameleon или добавить приложение AddThis в черные списки NoScript или NotScript ***(Обнаружен новый механизм для отслеживания пользователей в Сети // InternetUA (http://internetua.com/obnarujen-novii-mehanizm-dlya-otslejivaniya-polzovatelei-v-seti). – 2014. – 18.07).***

***

Верховный комиссар ООН по правам человека Н. Пиллэй выразила обеспокоенность по поводу опасной практики слежки за людьми в онлайновой среде, которая приводит к серьезным нарушениям основных свобод, в том числе права на неприкосновенность частной жизни. Н. Пиллэй сообщила, что ее офис подготовил доклад о защите права на неприкосновенность личной жизни в контексте национального экстерриториального слежения за цифровыми сообщениями и/или их перехвата и сбора личных данных.

В ходе его подготовки было установлено, что практика многих государств, касающаяся слежения, покрыта тайной. Зачастую она сопряжена с тем, что частные кампании, в частности провайдеры услуг в сфере цифровых технологий, предоставляют соответствующим органам полный доступ к информации и данным своих клиентов, без уведомления последних.

Верховный комиссар ООН отметила, что ее офис более года изучал сложное переплетение вопросов, связанных с правом на неприкосновенность частной жизни в условиях современных цифровых технологий. Эксперты проанализировали международное законодательство и нормативные акты многих государств, в том числе недавние судебные решения. Они провели опрос широкого круга лиц, в том числе побеседовали с представителями международных и региональных организаций, национальных учреждений, неправительственных организации и частного сектора.

Результаты этой работы они изложили в новом докладе. Его главный вывод сводится к тому, что массовая слежка правительств за электронной перепиской «становится уже не исключением, а опасной привычкой». Во многих государствах деятельность по отслеживанию коммуникаций не регулируется должным образом, она не подкреплена надлежащим национальным законодательством и механизмами контроля.

Авторы нового доклада напомнили, что конфиденциальность и свобода выражения мнений являются взаимозависимыми правами. Без надлежащей защиты конфиденциальности, безопасности и анонимности связи никто не может быть уверен, что его личные сообщения не находятся под надзором государств.

Верховный комиссар отметила, что слежка в Интернете за электронной перепиской, ее перехват или сбор личных данных должны стать предметом независимой проверки.

Н. Пиллэй отметила, что никто не может подвергаться произвольному вмешательству в его личную жизнь, а также произвольным посягательствам на тайну его корреспонденции.

Опасения по поводу национальной безопасности могут оправдывать исключительные и строго индивидуальные программы наблюдения, но наблюдения без адекватных гарантий защиты права на частную жизнь могут привести к негативным последствиям для системы прав человека и основоположных свобод.

Н. Пиллэй напомнила, что ст. 12 Всеобщей декларации прав человека и ст. 17 Пакта по гражданским и политическим правам гласят, что «никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств».

Генеральная Ассамблея ООН в своей резолюции, принятой в 2013 г., подтвердила, что права, которые человек имеет в офлайновой среде, должны также защищаться и в онлайновой среде, особенно право на неприкосновенность личной жизни ***(ООН: Слежка государств за людьми в онлайн-среде превращается в опасную привичку // InternetUA (http://internetua.com/oon--slejka-gosudarstv-za-luadmi-v-onlain-srede-prevrasxaetsya-v-opasnuua-privicsku). – 2014. – 18.07).***

***

С 1 августа в Российской Федерации вступает в силу антитеррористический закон, предоставляющий полное право на получение Федеральной службе безопасности РФ практически всех личных данных пользователей интернет-ресурсов, зарегистрированных в РФ, пишет «Обозреватель» (http://tech.obozrevatel.com/news/50468-sbu-sovetuet-ukraintsam-ubiratsya-iz-rossijskih-sotsialnyih-setej.htm

Таким образом ФСБ на законодательном уровне получает полное право вмешиваться в личную жизнь не только граждан России, но и иностранцев, сообщает «Пресса Украины».

Данные по всем логинам и электронным адресам своих пользователей, списки их контактов, сведения о количестве, объеме и адресатах передаваемых сообщений владельцы почтовых серверов, блог-хостингов, форумов и соцсетей будут обязаны предоставлять по первому же требованию представителей российских государственных структур.

В Службе безопасности Украины предупреждают, что в условиях продолжающейся агрессии России на территории Украины, новые полномочия предоставляют ФСБ возможность получать имеющуюся в веб-среде информацию о украинских событиях и в дальнейшем использовать ее в ущерб интересам национальной безопасности.

В СБУ предупреждают всех граждан, которые обеспокоены безопасностью личной информации и рекомендуют воздержаться от использования интернет-ресурсов российской доменной зоны, в первую очередь это касается соцсетей и почтовых ящиков ***(СБУ призвала украинцев убираться из российских соцсетей // Обозреватель (http://tech.obozrevatel.com/news/50468-sbu-sovetuet-ukraintsam-ubiratsya-iz-rossijskih-sotsialnyih-setej.htm). – 2014. – 26.07).***

## Проблема захисту даних. DDOS та вірусні атаки

Група російських хакерів атакувала сайт технологічних новин CNET і викрала базу даних з іменами користувачів, зашифрованими паролями та електронними адресами понад одного мільйона користувачів, повідомляє CNET.

Атакувала сайт хакерська група з назвою W0rm. Про викрадення бази даних читачів ресурсу повідомив у Twitter її представник. Він також заявив, що W0rm отримала доступ до серверів видання через дірку в безпеці CNET.com, а саме у PHP-фреймворку Symfony (популярному програмному інструмені, що пропонує основу, з якої можна створювати цілі веб-сайти).

Як заявив представник W0rm, група не планує розшифровувати паролі чи продавати базу даних. Хакери заявляють, що їхня мета альтруїстична і вони зламали CNET для того, аби поліпшити безпеку Інтернету загалом. Вони кажуть, що, націлюючись на популярні сайти, можуть сприяти кращому розумінню недоліків безпеки.

W0rm заявляють, що наприкінці 2013 р. успішно атакували BBC, а до того їхніми жертвами стали сайти Adobe Systems та Bank of America ***(Група російських хакерів атакувала онлайн-видання CNET // MediaSapiens (http://osvita.mediasapiens.ua/material/32685). – 2014. – 15.07).***

***

Хакеры взломали страницу Facebook российской оппозиционерки В. Новодворской и оставили от ее имени оскорбительную матерную запись, пишет «Обозреватель» (http://tech.obozrevatel.com/news/01657-hakeryi-vzlomali-stranitsu-v-facebook-novodvorskoj-i-oskorbili-ukraintsev.htm).

На ее странице оскорбления были направлены в адрес ее сторонников и, в частности, украинцев.

Также в данном сообщении содержится оскорбления в сторону министра внутренних дел А. Авакова и народного депутата О. Ляшка.

Понятно, что аккаунт российской оппозиционерки был взломан, пишут комментаторы под записью ***(Хакеры взломали в Facebook страницу Новодворской и оскорбили украинцев // Обозреватель (http://tech.obozrevatel.com/news/01657-hakeryi-vzlomali-stranitsu-v-facebook-novodvorskoj-i-oskorbili-ukraintsev.htm). – 2014. – 17.07).***

***

Хакеры могут внедрить поддельные видео в веб-камеру Dropcam для удаленного наблюдения и использовать систему для совершения кибератаки, сообщили исследователи П. Вордл и К. Мур.

Для того чтобы совершить атаку, преступникам нужно было иметь физический доступ к устройствам, но эксплоиты предоставили им возможность внедрить видеокадры в камеру жертвы для ограбления домов

или офисов. Кибермошенники перехватывали видео пустого помещения, используя уязвимость Heartbleed с целью получить пароли и ключи шифрования протокола SSL.

Dropcam, которую в прошлом месяце выкупила Google за 555 млн дол., создает платформу для видеомониторинга.

П. Вордл и К. Мур исследовали аппаратное и программное обеспечение Dropcam. Эксперты выявили в ПО уязвимости, позволяющие встраивать вредоносные программы на устройства. Внедренное вредоносное ПО помогло бы злоумышленникам изымать данные из домашних или корпоративных сетей.

Проблема наличия и внедрения уязвимости в Dropcam будет обсуждаться в ходе 22-й ежегодной крупнейшей в мире конференции хакеров DEF CON в Лас-Вегасе, штат Невада, которая состоится в следующем месяце ***(В Dropcam обнаружена уязвимость // InternetUA (http://internetua.com/v-Dropcam-obnarujena-uyazvimost). – 2014. – 16.07).***

***

Как сообщили порталу SecurityLab эксперты из ИБ-компании Aorato, 95 % крупнейших компаний, входящих в рейтинг Fortune 500, подвергаются потенциальной опасности из-за уязвимости в реализации службы каталогов Active Directory. По словам исследователей, несмотря на все меры безопасности, слабое шифрование позволяет злоумышленникам без авторизации изменять пароли жертв.

Проэксплуатировав уязвимость, с помощью нового пароля атакующий может выдавать себя за жертву и получать доступ к различным сервисам и контенту, требующим введения учетных данных жертвы, например, к Remote Desktop Protocol (RDP) Logon и Outlook Web Access (OWA).

К сожалению, несмотря на все протоколы безопасности, в журналах событий не фиксируется кража личности. Злоумышленник может осуществить подобную атаку незаметно для журнала событий, делая технологии SIEM и Big Data Security Analytics совершенно бесполезными.

«Миллионы представителей бизнеса слепо доверяют Active Directory как основе своей IT-инфраструктуры. К сожалению, правда состоит в том, что наивное доверие не оправдывает себя, и большинство представителей Fortune 500 уязвимы к утечке персональных и корпоративных данных, – сообщил вице-президент по исследованиям Aorato Т. Бери. – До тех пор, пока компании не осознают угрозу, связанную с использованием Active Directory, и не создадут стратегию снижения рисков, мы будем и дальше наблюдать, как атакующие незаметно похищают информацию».

Эксперты из Aorato советуют представителям бизнеса:

Обнаруживать аномалии в протоколах аутентификации.

Идентифицировать атаки путем соотношения ненормального использования методов шифрования с контекстом, в котором используется личность жертвы.

Принимать меры для сокращения поверхности атаки. Здесь необходимо помнить о том, что эти меры не устраняют атаку полностью и не ликвидируют ее первопричину ***(95 % крупнейших компаний по всему миру подвержены риску из-за уязвимости в Active Directory // InternetUA (http://internetua.com/95--krupneishih-kompanii-po-vsemu-miru-podverjeni-risku-iz-za-uyazvimosti-v-Active-Directory). – 2014. – 16.07).***

***

PayPal исправила уязвимость, затрагивающую серверное приложение официального портала Ethernet, которая позволяла обходить фильтры и удаленно запускать вредоносные скрипты на системах PayPal.

«Обход фильтра позволял удаленному атакующему уклоняться от синтаксического анализа и шифровать механизмы фильтрования в веб-приложении портала PayPal, – сообщается в уведомлении компании, выпущенном еще до исправления бреши. – Устойчивая уязвимость в процессе проверки входных данных позволяет удаленным атакующим внедрять собственные вредоносные коды в приложение уязвимого сервиса».

До того как PayPal исправила брешь, злоумышленники потенциально могли осуществлять различные типы атак, в том числе похищать данные учетной записи администратора или разработчика через внутренний портал Ethernet, а также локально выполнять код на портале. Кроме того, у хакеров была возможность влиять на то, как для PayPal отображались персональные профили. Тем не менее, какие-либо признаки осуществления подобных атак обнаружены не были.

По общей системе оценки уязвимостей CVSS, данная брешь получила 8,9. Она была обнаружена аналитиком Б. Меджри из Vulnerability Laboratory. В рамках программы Bug Bounty Program исследовательская компания получила вознаграждение в размере 1 тыс. дол. ***(Эксперты обнаружили уязвимость во внутреннем портале PayPal // InternetUA (http://internetua.com/eksperti-obnarujili-uyazvimost-vo-vnutrennem-portale-PayPal). – 2014. – 16.07).***

***

Хакеры из группы «Анонимный интернационал», которые недавно поведали миру о том, как работают кремлевские тролли, опубликовали новое разоблачение. Они выложили в сеть фрагменты переписки сотрудников Министерства обороны России, сообщает AIN.UA.

Как выяснилось, российские военные, «самооборона», криминалитет и чиновники разных мастей в настоящее время решают, кому же будет принадлежать захваченное украинское имущество. На «трофеи» немало претендентов – например, Министерство обороны РФ хочет перевести в свою собственность гостиницу «Укрвоенкурорт», но никак не может это сделать, потому что она находится в собственности родственников

самоназначенного премьера Крыма С. Аксенова. Еще часть недвижимости захватила так называемая «самооборона» полуострова.

В одном из писем чиновники жалуются, что «самооборона» захватила целый городок, принадлежащий Черноморскому флоту РФ. «Губернатор Севастополя начал работу по разделу военного недвижимого имущества. Был захвачен не просто городок – а военный городок ЧФ, который числится в соглашении о разделе Черноморского флота 1997 г. Будем смотреть дальше – заберут все. Прошу содействия на уровне МО РФ», – пишет в докладной записке начальству российский интендант Д. Токарчук.

В то же время военные чиновники признаются, что официально не могут оформить на себя недвижимость, потому что до сих пор не принят федеральный закон, который официально передал бы военное имущество в Крыму российскому Министерству обороны.

Одна из причин такого активного «дерибана» – фактический запрет для российских силовиков уезжать в отпуск за границу. Сейчас Минобороны РФ хочет освоить часть побережья Крыма на строительство дач для своего генералитета.

В ближайшее время хакеры обещают выложить остальную часть переписки ***(Взломана переписка российских военных о дележке крымских «трофеев» // InternetUA (http://internetua.com/vzlomana-perepiska-rossiiskih-voennih-o-delejke-krimskih--trofeev). – 2014. – 16.07).***

***

Специалисты «Доктор Веб» обнаружили и внесли в вирусную базу новый троян Android.BankBot.21.origin. Вредоносное ПО распространяется как Adobe Flash Player и совершает кражи данных пользователей об используемой ими кредитной карте. В том числе, троян занимается перехватом и отправкой SMS-сообщений.

После того как жертва устанавливает якобы Adobe Flash Player и запускает его, троян пытается перехватить функции администратора мобильного устройства. Для этого Android.BankBot.21.origin демонстрирует соответствующий системный запрос, который пользователь не успевает отменить. Таким образом вредонос получает возможность защитить себя от удаления в будущем.

Получить платежные реквизиты используемой банковской карты жертвы Android.BankBot.21.origin может, имитируя стандартную форму привязки карты Google Play к учетной записи пользователя в случае, если приложение активно на устройстве. Далее злоумышленник получает на свой сервер всю нужную ему информацию – номер банковской карты, дату окончания ее действия, секретный код CVC, домашний адрес владельца, его номер телефона и пр.

К тому же, кроме кражи личных данных владельца карты, Android.BankBot.21.origin может выполнять иные команды, полученные от мошенника через контрольный сервер. Например, троян может перехватить

входящие SMS-сообщения или же отправить сообщения, содержащие определенный контекст, на нужный номер.

Эксперты «Доктор Веб» советуют не устанавливать на свои устройства на базе Android небезопасные или подозрительные приложения ***(Троян крадет данные о кредитных картах у владельцев Android-устройств // InternetUA (http://internetua.com/troyan-kradet-dannie-o-kreditnih-kartah-u-vladelcev-Android-ustroistv). – 2014. – 17.07).***

***

Полиция Великобритании и Национальный центр Action Fraud предупредили пользователей LinkedIn о фишинговой кампании, целью которой является заставить жертву выдать свои учетные данные для входа в профессиональную социальную сеть.

По данным правоохранителей, были зафиксированы фишинговые электронные письма, отправленные якобы от имени LinkedIn. В них идет речь о том, что учетная запись пользователя была заблокирована по причине отсутствия активности в течение длительного времени, и необходимо пройти по ссылке для подтверждения электронного адреса и восстановления доступа.

По данным аналитического сайта Hoax Slayer, который первым сообщил о мошеннической кампании, кликнув по ссылке, пользователь перенаправляется на поддельную страницу авторизации в LinkedIn. Таким образом злоумышленники получают доступ к его учетным данным.

«Преступники могут получить ваши учетные данные и использовать их для входа в вашу учетную запись в LinkedIn. После чего они могут использовать сервис для рассылки спама и осуществлять мошеннические действия от вашего имени», – говорится на сайте Hoax Slayer.

По словам экспертов, сообщения о необходимости обновить данные учетной записи являются излюбленным инструментом кибермошенников. В связи с этим они рекомендуют с осторожностью относиться к подобным письмам и не проходить по указанным в них ссылкам ***(Обнаружена новая фишинговая кампания против пользователей LinkedIn // InternetUA (http://internetua.com/obnarujena-novaya-fishingovaya-kampaniya-protiv-polzovatelei-LinkedIn). – 2014. – 19.07).***

***

Волна нападений кибермошенников с помощью трояна Pushdo скомпрометировала более 11 тыс. систем всего за 24 часа. Индийские ПК наиболее пострадали от вспышки атак, наряду с системами в Великобритании, Франции и США, говорят исследователи из Bitdefender.

Румынская компания утверждает, что 77 машин были заражены в Великобритании через ботнет в течение последних 24 часов. Более чем 11 тыс. систем были заражены во всем мире за тот же период. Другие страны, которые пострадали от трояна Pushdo, включают Вьетнам и Турцию.

Во главе списка по общему количеству заражений находятся Азия, Индия и Вьетнам. На компьютеры из этих стран приходится по 10 % от всех заражений. На долю США приходится еще 5 % от общего количества случаев инфицирования.

Троян Pushdo был использован для распространения вторичных штаммов вредоносного ПО, таких как ZeuS и SpyEye, но раньше он использовался для распространение спама. Рассылка спама осуществляется посредством Cutwail, которое часто устанавливалось на взломанные ПК.

Исследователи по безопасности четыре раза получали контроль над C&C-серверами Pushdo, однако злоумышленники продолжают заражать компьютеры пользователей этим вредоносным ПО ***(Троян Pushdo инфицировал 11 тысяч компьютеров за 24 часа // InternetUA (http://internetua.com/troyan-Pushdo-inficiroval-11-tisyacs-kompuaterov-za-24-csasa). – 2014. – 19.07).***

***

Как сообщили эксперты Symantec, банковский троян Neverquest, появившийся в ноябре прошлого года, получил несколько новых функций. Отметим, что троян относится к семейству вредоносного ПО Snifula, известному еще с 2006 г.

Neverquest способен фиксировать нажатия клавиш на клавиатуре, делать скриншоты, похищать учетные данные и цифровые сертификаты. С его помощью злоумышленники могут получить полный контроль над инфицированным устройством и осуществить атаку «человек в браузере».

После инфицирования устройства троян соединяется с C&C-сервером, откуда загружает конфигурационный файл, который содержит код, используемый для осуществления атаки «человек в браузере». Neverquest внедряет этот код в веб-страницу с целью превратить сайт в финшинговый. Попав на такой ресурс, ничего не подозревающий пользователь добровольно указывает свои конфиденциальные данные (PIN-коды, одноразовые и другие пароли, аутентификационные номера банковских транзакций и ответы на вопросы безопасности).

Конфигурационные файлы для жертв из разных стран отличаются между собой. Помимо кода в них также содержится список ссылок, определяющих типы веб-сайтов, на которых нацелен Neverquest. Троян способен сканировать URL и содержимое посещаемых жертвами сайтов с целью обнаружить связи со страницами в социальных сетях, облачными сервисами, электронной почтой и т. д.

Файл, предназначенный для жертв в Германии, содержит список из десяти финансовых институтов, предназначенный для США – из пятидесяти ***(Банковский троян Neverquest получил новые функции // InternetUA (http://internetua.com/bankovskii-troyan-Neverquest-polucsil-novie-funkcii). – 2014. – 22.07).***

***

Эксперты из Sentinel Labs обнаружили новую вредоносную программу Gyges. Вредоносное ПО, говорят они, нацелено на проведение кибершпионажа. Вредоносная программа была разработана в России для совершения атак на государственные организации.

Определенный вариант Gyges, за которым наблюдают специалисты из Sentinel Labs, содержал то, что исследователи фирмы называют «сложными для обнаружения методами борьбы». Вредоносное ПО было рассчитано на неактивного пользователя, чтобы обойти программы по безопасности для запуска вредоносной программы.

Вредоносный код, используемый с целью обмануть программу по безопасности, является значительно сложнее, чем основной исполняемый файл, отметили исследователи в своем докладе. Они считают, что Gyges ранее уже был использован в качестве носителя для более изощренных атак.

По данным Sentinel Labs, код был многократно использован для осуществления атак с помощью Cryptolocker, а также мошенничества в сфере онлайн-банкинга. Вредоносная программа распространяется через скрытые загрузки, а также посредством фишинговых атак.

Вредоносная программа считывает данные с компьютера, экрана и даже клавиатуры. Но, пожалуй, самый интересный элемент Gyges – использование практически неизвестных техник осуществления иньекций ***(Россияне разработали новый вредонос Gyges // InternetUA (http://internetua.com/rossiyane-razrabotali-novii-vredonos-Gyges). – 2014. – 20.07).***

***

Поддельные приложения, которые на самом деле предназначены для кражи пользовательских данных, все чаще нацеливаются на пользователей телефонов на базе Android. К этому выводу пришли исследователи из Trend Micro в рамках своего исследования.

Компания рассмотрела топ-50 бесплатных приложений в Google Play и установила, что мошенники подделали 77 % всех приложений. Фальшивые программы часто выглядят как настоящие и имеют те же функции, но могут оказаться вредоносными.

Компания Trend Micro из Токио отметила наличие 890  482 поддельных приложений в результате исследования, проведенного в апреле текущего года. Более половины из них (394 263) были признаны вредоносными, а 59 185 – являлись агрессивным программным adware.

Наиболее распространенными являются поддельные антивирусные программы. В некоторых случаях, приложения просят пользователя утвердить права администратора, предоставляющие приложению более широкий доступ к программам и данным телефона. Именно поэтому приложение так сложно потом удалить.

Хотя многие из поддельных приложений существуют на форумах или сторонних магазинах по продаже приложений, где безопасность является либо слабее, либо вовсе отсутствует, фальшивые приложения также могут попасть в официальный магазин Google ***(Мошенники подделали 77 % ТОП-50 приложений Google Play // InternetUA (http://internetua.com/moshenniki-poddelali-77--top-50-prilojenii-Google-Play). – 2014. – 20.07).***

***

Microsoft начала принимать запросы на удаление ссылок из поисковой выдачи Bing в соответствии с правом «быть забытым». Софтверный гигант, как и Google, открыл специальную страницу, на которой можно подать заявку на удаление данных.

Таким образом Microsoft начнёт соответствовать требованию Европейского суда о том, что жители содружества государств могут обратиться к поисковым системам и потребовать удалить ссылки на информацию, если она является устаревшей или неверной. Google начала принимать соответствующие запросы несколько месяцев назад и уже удаляет данные.

Вопрос удаления ссылок на данные породил серьёзные споры в интернет-сообществе в Европе и во всем мире. На следующей неделе европейские организации, которые занимаются регулированием вопросов конфиденциальности данных, соберутся на встречу, куда также будут приглашены представители Google, Microsoft и Yahoo.

Журналистам Wall Street Journal удалось подтвердить, что Microsoft примет участие во встрече. От Google и Yahoo поступила информация о намерении сотрудничать с представителями властей Европы, однако об определенных планах касательно встречи ничего не говорилось.

На встрече будут подниматься вопросы, связанные с этической и технической сторонами исполнения решения Европейского суда. Например, не ясно, как лучше блокировать данные – для одной отдельно взятой страны, в которой проживает автор заявления, или глобально в поисковой системе. Также существуют мнения о том, что блокировку ссылок нужно осуществлять только на территории Европейского Союза, так как правительство и судебные органы других стран не требовали осуществлять блокировку ***(Google, Microsoft и Yahoo обсудят с ЕС «право быть забытым» // InternetUA (http://internetua.com/Google--Microsoft-i-Yahoo-obsudyat-s-es--pravo-bit-zabitim). – 2014. – 20.07).***

***

Согласно результатам исследования, проведенного Security Metrics, 63,86 % компаний хранят данные 16-значного кода банковских карт (PAN) в незашифрованном виде, который размещается на их лицевой стороне. 7 % хранят незашифрованными данные с магнитной ленты банковской карты.

На черном рынке стоимость незашифрованных банковских данных достигает всего 50 дол. Эксперт компании Security Metrics Д. Еллис заявил: «Незашифрованные банковские данные являются «низко висящими плодами» для злоумышленников. Это то, на что в первую очередь мошенники обращают внимание при планировании атаки на предприятие».

В рамках исследования PAN-сканер проанализировал 145,144 Гбайт данных с 2,590 компьютеров и обнаружил:

– 87 206 203 незашифрованных платежных карт;

– 63,86 % предприятий, хранящие незашифрованную информацию о PAN платежных карт;

– 7,37 % компаний хранящие незашифрованные данные с магнитной ленты банковских карт, включая PIN-код, CVV-код, срок действия карты, а также имя держателя.

Таким образом, PAN-устройство зафиксировало более 780 млн незашифрованных номеров банковских карт. Это около 2,5 карты на одного гражданина США. Специалист по оценке информационной безопасности Г. Гловер заявил, что незашифрованные данные банковских карт могут сохраняться на терминалах торговых точек, жестких дисках и др. ***(63 % предприятий не шифруют данные банковских карт // InternetUA (http://internetua.com/63--predpriyatii-ne-shifruuat-dannie-bankovskih-kart). – 2014. – 21.07).***

***

Представители компании FireEye обнаружили новый вариант трояна Havex, который сканирует OPC-серверы, используемые для контроля SCADA-систем. Обнаруженная вредоносная программа способна похищать системную информацию и хранящиеся на скомпрометированном сервере данные. Свою вредоносную деятельность вирус осуществляет посредством OPC-стандарта.

«На протяжении года злоумышленники используют Havex в атаках на компании, задействованные в энергетической отрасли. Однако окончательное количество пострадавших от вируса ICS-систем неизвестно», – говорится в блоге компании FireEye.

Для того чтобы понять принцип работы вируса исследователи решили провести тестирование компонента Havex, который сканирует OPC. С этой целью эксперты создали типичную среду OPC-сервера. Отметим, что ICS- или SCADA-системы включают в себя OPC-клиент, который напрямую взаимодействует с OPC-сервером. Последний, в свою очередь, работает в тандеме с PLC для того, чтобы контролировать работу оборудования SCADA.

Когда вирус Havex попадает в сеть, его загрузчик использует процесс runDll и затем начинает сканировать OPC-серверы, задействованные в SCADA-системе.

Для того чтобы определить потенциальный OPC-сервер, вирус использует WNet-функции, к примеру, WNetOpenEnum и WNetEnumResources.

«Сканер Havex составляет список серверов, доступных по всему миру через Windows networking. Впоследствии, составленный список проверяется на наличие COM-интерфейса», – отмечают в FireEye.

Сканируя OPC-серверы, Havex способен похищать любые данные о подключенных к ним устройствах и отправлять инфорамцию на C&C-сервер, подконтрольный злоумышленникам.

По словам специалистов FireEye, обнаруженный вариант Havex – первая вредоносная программа, способная сканировать OPC-серверы ***(FireEye обнаружила новый вариант Havex, сканирующий OPC-серверы // InternetUA (http://internetua.com/FireEye-obnarujila-novii-variant-Havex--skaniruuasxii-OPC-serveri). – 2014. – 21.07).***

***

Новый компьютерный вирус, созданный для кражи реквизитов на вход и финансовых данных с сервисов онлайн-банкинга, активно рекламируется и продается на черном рынке.

Вредоносный код Kronos способен похищать данные через интернет-сессии в браузерах Internet Explorer, Mozilla Firefox и Google Chrome, пишет CyberSecurity.

В компании Trusteer, обнаружившей троян, говорят, что вредонос может использовать техники перехвата данных из веб-форм и HTML-контента.

Согласно рекламному объявлению на одном из подпольных хакерских форумов, новинка совместима с контент-инъекционными скриптами, также известными как веб-инъекты. Изначально данная техника появилась в нашумевшем вредоносе Zeus, который уже не находится в разработке.

В описании вируса сказано, что вдобавок к возможностям по краже данных, троянец имеет компоненты для работы с 32- или 64-битными компонентами, вдобавок к этому код имеет средства для защиты от антивирусных средств и блокировки конкурирующего вредоносного ПО.

Разработчики Kronos также говорят, что код способен обходить так называемые «песочницы», используемые в современных операционных системах как среды изолированного исполнения кодов.

На черном рынке вредонос продается за 7000 дол., причем в эту сумму входят подписки на дальнейшие обновления и баг-фиксы. Также создатели говорят, что по техническим возможностям вредонос не уступает таким кодам, как Zeus, Carberp и SpyEye. В Trusteer говорят, что им пока не удалось получить исходники вредоноса ***(Новый вирус Kronos для кражи денег во время онлайн-банкинга продается на черном рынке за $7000 // InternetUA (http://internetua.com/novii-virus-Kronos-dlya-kraji-deneg-vo-vremya-onlain-bankinga-prodaetsya-na-csernom-rinke-za--7000). – 2014. – 22.07).***

***

Вирус-червь, использующий уязвимости Windows XP, вошел в тройку наиболее опасных вредоносных программ II квартала 2014 г. по версии Trend Micro. За этот период 40 % электронных сообщений, распространивших вирус, были отправлены с инфицированных червем Downad ПК.

Эксперты Trend Micro назвали червь Downad одной из самых опасных программ, с которыми специалисты столкнулись во II квартале 2014 г. Вредоносное ПО под названием Downad (его также называют Conficker) может инфицировать сеть целиком, получив доступ через URL-адрес, электронное сообщение или съемный накопитель. XP считается особенно подверженной этой угрозе, поскольку вирус использует уязвимость в Windows Server Service (MS08-067) для запуска произвольного кода.

У Downad также есть собственный алгоритм генерации доменного имени (DGA), позволяющий червю создавать произвольные URL, и впоследствии подключаться к ним для скачивания файлов в систему. Согласно Trend Micro, найдено около 175 IP адресов, связанных с Downad, сгенерированных случайным образом с помощью алгоритма DGA и использующих разнообразные порты. «Проанализировав сложившуюся ситуацию, мы обнаружили, что во втором квартале 2014 г. более 40 % электронных сообщений, каким-либо образом связанных с вредоносным ПО, было отправлено инфицированными Downad ПК», – говорит специалист по анти-спам исследованиям в Trend Micro М. Мэнли.

«Сегодня некоторое количество компьютеров по-прежнему заражено и используется для рассылки спам-сообщений, передающих “червя” дальше по цепочке. И поскольку Microsoft прекратила поддержку XP в этом году, мы ожидаем, что количество зараженных систем будет расти», – рассуждает М. Мэнли.

Кампании по рассылки спама, рассылающие вредоносное ПО семейств Fareit, Mytob, и Lovgate во вложениях, отправляются зараженными Downad компьютерами. Fareit – семейство вредоносного ПО, похищающее информацию, в то время как Mytob относится к старому семейству червей, рассылающих собственные копии по почте. «За последние несколько недель мы сообщили о нескольких волнах спама, использующих ссылки Dropbox для хранения вредоносного ПО, такого, как UPATRE, – комментирует М. Мэнли. – Мы также нашли спам-сообщение, замаскированное под голосовое, содержащее вариант трояна Cryptolocker. Самым последним, что мы наблюдали, была спам-компания, использующая Cubby, сервис для хранения файлов. На этот раз рассылка содержала ПО для взлома банковских систем, определяемое как TSPY_BANKER.WSTA».

Согласно результатам исследования Trend Micro, хакеры могут использовать платформы для хранения данных для маскировки своей деятельности: именно так ПО проникает в систему и сеть. «Спам с вредоносными вложениями продолжает множиться, как и спам, включающий ссылки на вредоносные сайты, – утверждают эксперты Trend Micro. –

Похоже, эксплуатация сервисов хранения файлов для распространения вирусов стала сейчас любимым способом злоумышленников пройти через спам-фильтры» ***(Вирус поражает ПК через лазейку в Windows XP // InternetUA (http://internetua.com/virus-porajaet-pk-cserez-lazeiku-v-Windows-XP). – 2014. – 22.07).***

***

В сети появилась новая программа-вымогатель под названием Critroni. Она продается последний месяц на подпольном форуме и в настоящее время попала в набор эксплоитов Angler. Программа-вымогатель имеет ряд необычных свойств. Специалисты утверждают, что Critroni является первой программой-вымогателем, которая использует сеть Tor в качестве командного C&C-сервера.

Critroni можно приобрести за 3 тыс. дол. Эксперты по информационной безопасности сообщают, что в настоящее время при помощи Critroni осуществляется большое количество атак. Некоторые злоумышленники используют для достижения преступных целей набор эксплоитов Angler, чтобы внедрить спам-бот в компьютеры потенциальных жертв.

Внедренный спам-бот устанавливает еще несколько вредоносных программ, включая Critroni. Попадая на компьютер пользователя, Critroni шифрует различные данные, в том числе фотографии и документы. После этого на экране пользователя выводится диалоговое окно, сообщающее об инфицировании персонального компьютера.

Для разблокировки устройства пользователю предлагается оплатить в электронной валюте Bitcoins покупку кода. На оплату жертвам отводится 72 часа. Для тех пользователей, которые не имеют возможности оплаты кода в Bitcoins, злоумышленники разместили детальную инструкцию, каким образом можно приобрести Bitcoins в разных странах мира.

Особенностью Critroni (или CTB-Locker) является то, что программа использует сеть Tor в качестве C&C сервера. Исследователи и ранее фиксировали подобные свойства, однако, не в программах-вымогателях ***(Новая программа-вымогатель Critroni использует сеть Tor // InternetUA (http://internetua.com/novaya-programma-vimogatel-Critroni-ispolzuet-set-Tor). – 2014. – 22.07).***

***

Найбільші інтернет-компанії світу, серед яких Google, Facebook, Yahoo та інші, закликали користувачів змінити всі свої паролі через виявлену уразливість в системі програмної захисту OpenSSL.

Згідно з повідомленням, унаслідок виявленої помилки в програмі SSL-шифрування інтернет-користувачі можуть втратити персональні дані та паролі різних веб-сервісів. Визначити сайти, на яких використовується пакет шифрування OpenSSL, можна за допомогою картинки замка, яка з’являється в адресному рядку браузера.

За даними видання, деякі компанії вже оновили свої ресурси таким чином, щоб вразливість не могла нашкодити користувачам. При цьому фахівці з Google відзначають, що навіть після встановлення оновленої версії OpenSSL деякі акаунти можуть все одно залишатися уразливими для атаки.

Крім того, уперше дана уразливість з'явилася близько двох років тому. На думку IT-експертів, за цей час нею могли скористатися багато хакерів. Утім, фахівці також припускають, що далеко не всі хакери могли знати про цю уразливість до офіційного оголошення про дефект ***(Facebook закликає користувачів змінити паролі // Інформаційний портал «Стик» (http://styknews.info/novyny/sotsium/2014/07/23/facebook-zaklykaie-korystuvachiv-zminyty-paroli). – 2014. – 23.07).***

***

Хакери зламали Facebook-сторінку The Wall Street Journal і опублікували там кілька неправдивих повідомлень, пише mashable.com.

Хакери, які зламали сторінку видання в соцмережі, написали, що авіадиспетчер втратив зв'язок з пілотом американського «борта номер один» у небі над Росією.

Також з'явилося неправдиве повідомлення про те, що віце-президент США Д. Байден виступить зі зверненням до нації через 15 хв.

Пізніше газета повідомила, що її сторінка була пошкоджена. Технічну проблему співробітники WSJ вирішили, а фейкові дописи видалили. Хакери контролювали акаунт видання приблизно 20 хв ***(Хакери опублікували фейкові новини про Обаму і Байдена на зламаній Facebook-сторінці WSJ // MediaSapiens (http://osvita.mediasapiens.ua/material/32873). – 2014. – 21.07).***

***

Как сообщают израильские СМИ со ссылкой на Общую службу безопасности Израиля (ШАБАК), за последние несколько дней участились попытки с помощью DDoS-атак обрушить интернет-связь в стране. Предполагается, что это связано с обострением вооруженного конфликта в Газе.

Атаки осуществляются хакерами по всему миру из различных арабских стран. Как сообщил эксперт из Университета Тель-Авива И. Бен-Исраэль, в их осуществлении также принимают участие специалисты, работающие на ХАМАС.

Сотрудники ИБ-отдела ШАБАК совместно с Министерством связи, компаниями, предоставляющими интернет-услуги, и частными лицами активно работают над отражением атак. Представители израильской спецслужбы просят пользователей, столкнувшихся с невозможностью доступа к тем или иным интернет-ресурсам, немедленно сообщать об этом провайдерам.

По данным ШАБАК, с продолжением военной операции «Нерушимая скала» попытки киберпреступников обрушить интернет-связь в Израиле

будут продолжаться ***(Спецслужба Израиля: Хакеры пытаются вывести из строя интернет-связь в стране // InternetUA (http://internetua.com/specslujba-izrailya--hakeri-pitauatsya-vivesti-iz-stroya-internet-svyaz-v-strane). – 2014. – 23.07).***

***

Эксперты Sucuri сообщили о новой вредоносной инфекции, жертвами которой в последнее время стало большое количество сайтов, использующих WordPress. Ее главной особенностью является тот факт, что при внедрении вредоносной нагрузки сайт продолжает работать в обычном режиме.

В настоящее время эксперты пока еще исследуют вредонос, однако уже известны некоторые его особенности:

1. Поражает только сайты, построенные на популярной платформе WordPress.

2. Жертвами инфекции становятся сайты, использующие устаревшие (уязвимые) плагины или слабые пароли администраторов.

3. ПО является очень сложным, а его цель – внедрение спама на зараженные сайты.

Кроме того, вредонос разрушает легитимные файлы сайта. Он поражает не только файлы ядра WordPress, но также темы и плагины. В результате этого вместо нормального контента сайта отображаются различные ошибки PHP. О возможном взломе сайта свидетельствует отображение следующей ошибки:

Parse error: syntax error, unexpected ‘)’ in /home/user/public_html/site/wp-config.php on line 91

Единственным решением этой проблемы в настоящее время является удаление вредоносного ПО и восстановление резервных копий пораженных файлов ***(Новая вредоносная инфекция поражает сайты, использующие WordPress // InternetUA (http://internetua.com/novaya-vredonosnaya-infekciya-porajaet-saiti--ispolzuuasxie-WordPress). – 2014. – 24.07).***

***

Хакеры, деятельность которых нацелена на пользователей Facebook, стали еще более агрессивными. Обычно мошеннические схемы предполагают заполнение пользователем поддельных опросов или обмен видео и фотографиями. Очень редко злоумышленники задействуют набор эксплоитов.

Недавно эксперты Symantec зафиксировали атаку под названием «Мама зарабатывает $ 8,000/месяц» в Facebook, в которой использовался набор эксплоитов Nuclear Exploit Kit.

Если пользователи верят таким объявлениям о работе и нажимают на ссылку, то их перенаправляют на страницу в Facebook. В свою очередь, эта страница перенаправляет пользователей через серию ссылок на сторонний веб-сайт, содержащий набор эксплоитов Nuclear Exploit Kit. Это может

позволить злоумышленнику скомпрометировать компьютер жертвы без необходимости его заражения.

Если пользователь нажимает кнопку Like или делиться ссылкой с другими, мошенник зарабатывает деньги. В случае компрометации системы жертвы, злоумышленник может использовать ее для выполнения различных команд.

Хакер получает возможность убедить жертву поделиться следующими ссылками или же они могут быть разосланы автоматически.

Tin[REMOVED]ew7.com

Daily[REMOVED]alerts.com

Ранее набор эксплоитов Nuclear Exploit Kit использовал уязвимости, позволяющие удаленному пользователю выполнить удаленный код на системе Oracle Java SE ( CVE-2011-3544 ) и в Adobe Reader и Acrobat ( CVE-2010-0188 ). Текущая версия набора эксплоитов использует уязвимости в Microsoft Internet Explorer (CVE-2013-25-51) и в Oracle Java SE (CVE-2012-1723).

После успешного использования уязвимости, набор эксплоитов Nuclear Exploit Kit распространяет троян Trojan.Ascesso.A, известный рассылкой спама и загрузкой файлов из удаленного местоположения.

Регионы, наиболее пострадавшие от кибератаки с использованием трояна, – Северная Америка и Европа ***(Набор эксплоитов Nuclear Exploit Kit распространяется через Facebook // InternetUA (http://internetua.com/nabor-eksploitov-Nuclear-Exploit-Kit-rasprostranyaetsya-cserez-Facebook). – 2014. – 24.07).***

***

Злоумышленники усовершенствовали программу-вымогатель Simplocker, работающую на Android-устройствах. Вредоносное ПО нацелено на англоязычных пользователей Интернета.

Усовершенствованная англоязычная версия программы-вымогателя Simplocker требует 300 дол. за возможность разблокировки устройства. Последняя версия способна шифровать более расширенный спектр файлов. Усовершенствованный Simplocker более трудно удалить из устройства по сравнению с предыдущими версиями вредоносного ПО.

Напомним, что предыдущие версии программы-вымогателя уведомляли жертв о необходимости платной разблокировки устройства на русском языке. Стоит отметить, что злоумышленники требовали осуществить оплату в украинской валюте – гривнях.

Как и раньше, в усовершенствованном вредоносном ПО пользователи обвиняются в просмотре и распространении детской порнографии и других развращений. Предыдущие версии вредоносного ПО вымогали оплату суммой в 260 грн (21 дол.). Simplocker требует теперь такую же сумму в 300 дол., как и CryptoLocker, заражающий Windows-устройства. Злоумышленники требуют перечислять средства за разблокировку

устройства через MoneyPak, заменивший MoneXy, использовавшийся мошенниками ранее.

Согласно информации представителей компании по разработке антивирусного ПО ESET, усовершенствованный Simplocker не является широко распространенной программой в англоязычных странах. Эксперты подчеркнули, что с технической точки зрения механизм шифрования файлов остался неизменным. Однако, вредоносное ПО способно теперь шифровать файлы с расширением ZIP, 7z и RAR. Такая способность трояна может затронуть систему хранения резервных копий файлов на Android-устройствах ***(Злоумышленники усовершенствовали программу-вымогатель Simplocker // InternetUA (http://internetua.com/zloumishlenniki-usovershenstvovali-programmu-vimogatel-Simplocker). – 2014. – 24.07).***

***

Bromium Labs проанализировала известные общественности уязвимости и эксплоиты, обнаруженные за первые шесть месяцев текущего года. В рамках исследования было установлено, что количество уязвимостей в браузере Internet Explorer выросло более чем на 100 % по сравнению с 2013 г., превысив количество уязвимостей в Java и Flash.

Специалисты Bromium Labs установили, что хакеры все чаще нацелены на Internet Explorer. О тенденции роста уязвимостей в браузере свидетельствует также выпуск компанией обновлений для ПО.

Количество уязвимостей нулевого дня в Java снизилось в 2013 г. За первые шесть месяцев текущего года не было обнаружено ни одного эксплоита для уязвимостей в Java. При осуществлении атак нулевого дня на Internet Explorer и Flash использовалась Action Script Sprays – техника, позволяющая пропускать случайное размещение схем адресных пространств.

ИБ-специалист в Bromium Р. Кашяп сообщил, что одной из задач специалистов по информационной безопасности является обеспечение защиты пользователей сети, которые являются наиболее подвержены атакам со стороны злоумышленников ***(Количество уязвимостей в Internet Explorer увеличилось на 100 % // InternetUA (http://internetua.com/kolicsestvo-uyazvimostei-v-Internet-Explorer-uvelicsilos-na-100). – 2014. – 25.07).***

***

Несколько исследовательских компаний опубликовали аналитические отчёты о состоянии дел с DDoS-атаками в Интернете. Такие отчёты вышли от Prolexic/Akamai по результатам II квартала 2014 г., и от Incapsula.

По сравнению с прошлым годом, DDoS-атаки стали короче, но сильнее. Prolexic сообщает, что средняя мощность атаки увеличилась на 72 %, а пиковая – на 241 %. В то же время средняя продолжительность атак заметно упала и в настоящее время составляет 17 часов. Но этого достаточно, чтобы нанести серьёзный ущерб любому бизнесу.

Кстати, во II квартале DDoS-активность снизилась, по сравнению с I кварталом 2014 г.: средняя мощность упала с 9,7 до 7,76 Гбит/с. Очевидно, что это всего лишь временные флуктуации. Может быть, они связаны с летними отпусками и каникулами.

Аналитики говорят, что в самых больших атаках используются ботнеты не из домашних компьютеров, а из серверов. Злоумышленники внедряют вредоносный код в инфраструктуру PaaS- и SaaS-провайдеров, где виртуальные машины работают на программном обеспечении с известными уязвимостями: старые версии Linux, Apache, MySQL, PHP, Microsoft Windows. Подобные атаки на инфраструктуру – на сегодняшний день самая главная тенденция в этой области.

В свою очередь, Incapsula знакомит читателей с двуличным гуглоботом. С одной стороны, это нормальные краулеры Google, которые заходят на сайт, в среднем, 187 раз в день и скачивают, в среднем по четыре страницы. Частота захода ботов напрямую зависит от популярности сайта.

А с другой стороны – неизвестные, которые выдают себя за гуглоботов. Такие заходят примерно восемь раз в день но при этом выполняют вредоносные задачи: сканирование на уязвимости, спам, скрапинг страниц. В 23,5 % случаев они используются для Layer 7 DDoS-атак.

Так что на рынке DDoS'а кипит интересная жизнь ***(Последняя статистика по DDoS-атакам: ботнеты и гуглоботы // InternetUA (http://internetua.com/poslednyaya-statistika-po-DDoS-atakam--botneti-i-gugloboti). – 2014. – 27.07).***

***

Эксперты из «Лаборатории Касперского» сообщили об обнаружении нового семейства вредоносного ПО, использующегося для вымогательства. Троян Onion (авторское название – CTB-Locker) является одним из самых сложных шифровальщиков и обладает характеристиками, позволяющими назвать его оригинальной разработкой.

При создании вредоноса его авторы использовали как уже известные техники (требование выкупа в Bitcoin), так и совершенно новые, нетипичные для подобного ПО. Особенностью Onion является то, что C&C-сервер скрыт в сети Tor, что намного усложняет обнаружение злоумышленников.

Расшифровка файлов, зашифрованных вредоносом, невозможна даже при перехвате трафика между ним и сервером из-за необычной криптографической схемы. Кроме того, он сжимает файлы перед тем, как их зашифровать, что также нетипично для программ-вымогателей.

Схема работы трояна типична для ПО, использующегося в вымогательских целях. Попав на систему, он копирует себя в <CommonAppdata> (CSIDL_COMMON_APPDATA) и добавляет запуск этого файла в «Планировщик задач» (Task Scheduler). Осуществляет поиск на всех несъемных, съемных и сетевых дисках файлов по списку расширений, а

затем шифрует их. После этого пользователь получает уведомление с требованием выкупа и списком зашифрованных файлов.

Примечательно, что Onion устанавливает на рабочий стол жертвы изображение AllFilesAreLocked.bmp ***(Обнаружено абсолютно новое семейство программ-вымогателей // InternetUA (http://internetua.com/obnarujeno-absoluatno-novoe-semeistvo-programm-vimogatelei). – 2014. – 27.07).***