СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(3–16.11)

2014 № 21

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(3–16.11)
№ 21

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

Профессиональные социальные сети для врачей, учителей и даже солдат набирают популярность. Берут известную модель LinkedIn и закрывают ее для посторонних, чтобы пользователи могли обмениваться конфиденциальной информацией. Вертикальные социальные сети, рассчитанные на людей определенной профессии, например, Doximity, Edmodo для работников сферы образования и Spiceworks для IT-специалистов, привлекли миллионы долларов инвестиций. Венчурные инвесторы ставят на то, что эти стартапы смогут приносить прибыль за счет работы с рекрутерами и маркетологами, как это делает LinkedIn.

Многие сети смогли охватить значительную часть профессиональных сообществ, с которыми они работают. Пользователями Spiceworks стали 40 % всех IT-специалистов в мире, Doximity может похвастаться аудиторией в 40 % всех врачей в США, а в Rallypoint за первые два года зарегистрировались 10 % действующих служащих армии США.

Причина популярности

Генеральный директор Doximity Д. Тангни сказал, что количество пользователей очень возросло за четыре года, что прошли с момента создания компании, поскольку сеть позволяет врачам быстро связаться с большим количеством коллег, при этом соблюдая правила, защищающие личные данные пациентов.

Американским врачам, например, нельзя использовать для обсуждения результатов анализов или сбора мнений относительно сложного диагноза электронную почту, которая, как выразился Д. Тангни, защищена «не лучше, чем почтовая открытка». «Главный способ общения между врачами – это факс, – сказал он. – В системе здравоохранения США в год с помощью факса отправляют 15 млрд страниц».

Пользователи используют LinkedIn для построения социальных связей и поиска работы, но вертикальные социальные сети помогают многим профессионалам не только заводить новые знакомства, но и выполнять свои рабочие задачи. Spiceworks обеспечивает IT-специалистов некоторыми инструментами, которые нужны им для управления сетями, при этом предоставляя удобный способ общаться с коллегами на любые темы, от багов до бюджетов. Генеральный директор Spiceworks С. Абель сказал, что при каждом решении, которое принимает пользователь, «шесть миллионов пользователей находятся на расстоянии одного клика». Люди обзаводятся новыми связями, помогая друг другу с проблемами, а также демонстрируя свои знания.

Самореклама – это «важный элемент, люди могут демонстрировать свои навыки и опыт», – сказал он. Компания предоставляет инструменты бесплатно, а прибыль получает от рекламы IT-продуктов. Для многих

пользователей главное преимущество вертикальных сетей – знание, что они могут обсудить конфиденциальные вопросы с проверенными людьми. Это могут быть учителя, общающиеся с детьми в Edmodo, или профессиональные военные и ветераны, обсуждающие свои навыки или мнения насчет стратегии в Rallypoint.

К. Хаттер, генеральный директор Edmodo, у которой 43 млн пользователей по большей части из англоговорящих стран, сказала, что компания начала создавать ориентированное на образование пространство для классных обсуждений и обратной связи. Учителя дают своим ученикам коды для доступа к онлайн-группам. Когда ученики заходят в группы, коды уничтожаются, а учитель всегда может видеть, кто онлайн. «Наша миссия в Edmodo – связать всех тех, кто учится, с людьми и ресурсами, которые нужны для реализации их потенциала. С первого дня мы сосредоточились на том, как создать эту безопасную и защищенную среду для учителей».

Упорядоченные связи

У военных нет культуры формирования связей в реальной жизни, которую можно было бы воспроизвести онлайн, сказал генеральный директор RallyPoint Й. Вайсс. Идея создать сеть для военных пришла к нему, когда он ушел со службы, на которой доминировали иерархия и уставы, и пошел в Гарвардскую бизнес-школу.

Стартап проверяет личности действующих военных и ветеранов и нанимает модераторов, чтобы исключить обмен конфиденциальной военной информацией. «Военные даже не знают, что такое LinkedIn», – сказал Й. Вайсс. Но это не означает, добавляет он, что они не хотят получить доступ к части ее функций. Военные могут использовать RallyPoint, чтобы связаться с работающими в частном секторе ветеранами, которые лучше разбираются в навыках, нужных на гражданской работе, или конфиденциально обсуждать подготовку к миссиям за границей.

Реакция «старших братьев»

LinkedIn считает, что вертикальные профессиональные сети дополняют ее, а не конкурируют с ней за пользователей и рекрутеров. Вице-президент рекрутинговой компании Talent У. Бёрджесс сказал, что каждая сеть имеет свой контекст – точно так же, как разные офлайн-сообщества, в которых состоят люди. Б. Бойер, управляющий директор венчурной фирмы Tenaya Capital, которая инвестировала в Spiceworks, Edmodo и ResearchGate, сеть для ученых, отмечает, что сайты могут выполнять разные функции, но возможностей в этой области может быть еще много.

Примеры вертикальности

RallyPoint

RallyPoint – одна из самых молодых вертикальных социальных сетей. У нее 400 тыс. пользователей, включая 10 % действующих служащих армии США, использующих ресурс для поиска советов о военных действиях и рекламирования своих навыков в частном секторе. Недавно объем

привлеченного компанией финансирования достиг 7 млн дол. В числе инвесторов Asset Management Ventures.

Edmodo

Edmodo позволяет учителям поддерживать связь со своими учениками в виртуальных классах, а также обмениваться советами и планами уроков с коллегами. Созданная несколькими руководителями школ из пригорода Чикаго сеть привлекла 87,5 млн дол. от разных инвесторов, включая Benchmark, Union Square Ventures и Greylock Partners.

Spiceworks

У социальной сети для IT-профессионалов более 6 млн пользователей, которые заходят в нее, чтобы получить доступ к бесплатным инструментам для управлениями своими сетями и обсуждать с коллегами проблемы и предпочитаемые продукты. Созданный в Остине (Техас) стартап привлек 111 млн дол. от инвесторов, включая Goldman Sachs, венчурные компании Institutional Venture Partners и Tenaya Capital.

Doximity

Платформа, охватывающая 40 % врачей в США, получила финансирование в 81,8 млн дол. от инвесторов, включая Morgan Stanley, T Rowe Price и венчурную компанию Draper Fisher Jurvetson. Doximity позволяет подтвердившим свою личность врачам обсуждать пациентов и исследования, не нарушая правила конфиденциальности, а также заводить знакомства за пределами своей больницы и региона ***(Вертикальные социальные сети наращивают популярность // InternetUA (http://internetua.com/vertikalnie-socialnie-seti-narasxivauat-populyarnost). – 2014. – 4.11).***

***

В последнее время с завидной регулярностью начали появляться новые социальные сети, разработанные с прицелом на украинского пользователя. Впрочем, на фоне наблюдающегося с начала этого года резкого поднятия патриотического духа среди жителей Украины подобная тенденция не вызывает особого удивления. Очередным проектом из этого «репертуара» является аналог известного сервиса микроблогов Twitter – Zozu.org, сообщает itc.ua

Судя по описанию проекта, в его основе лежит идея предоставления украинцам возможности свободного самовыражения.

«Надоели эти запреты, травля со стороны соседей, людей, которые не понимают, а то и не желают понять других. Например, льют грязь на Украину, оскорбляют людей, которые здесь живут, хотя и есть, сами того не зная, виновниками всего. Я хочу свободы в выражении мыслей украинцев о власти, ситуации в государстве, обо всем, что накипело, не будучи при этом наказанным за те или иные высказывания. Слава Украине! Мы за украинский народ. И работаем благодаря ему и Украине», – говорится на сайте Zozu.org.

Внешне дизайн Zozu.org идентичен Twitter. И хотя разработчики «украинского Twitter» не призывают бойкотировать Twitter или российские соцсети, любопытно, что сайт доступен на 13 языках, среди которых есть китайский и даже греческий, но отсутствует русский.

Регистрация на сайте Zozu.org открыта, но количество зарегистрированных в пользователей пока оценить сложно. В настройках профиля есть возможность выбрать фон, установить изображение, и добавить информацию о себе. У Twitter украинский аналог позаимствовал не только общую структуру и интерфейс, но и базовые функциональные возможности.

Об основателе проекта пока данных нет, за исключением ссылки на его микроблог.

Есть еще один аспект, который стоит отметить. На Zozu.org есть специальная страница под рекламу, неизвестно только почему она находится в разделе «конфиденциальность». Видимо, за счет рекламы авторы планируют монетизировать проект. В настоящее время Zozu.org ищет программистов и верстальщиков, которые присоединяться к команде разработчиков и в дальнейшем будут отвечать за развитие проекта ***(Разработчики запустили «украинский Twitter» // Media бізнес (http://www.mediabusiness.com.ua/content/view/41281/126/lang,ru/). – 2014. – 7.11).***

***

Глава Facebook М. Цукерберг рассказал, что через 5 лет в контенте основанной им социальной сети будет превалировать видеоконтент, пишет Marketing Media Review (http://mmr.ua/news/id/mark-cukerberg-rasskazal-o-buduschem-facebook-i-objasnil-pochemu-vsegda-nosit-seruju-futbolku-42021/).

Основатель и гендиректор крупнейшей в мире социальной сети Facebook 30-летний М. Цукерберг дал возможность приблизительно представить то, как Facebook будет выглядеть в ближайшем будущем. На брифинге, прошедшем в штаб-квартире Facebook в Менло-Парк, М. Цукерберг традиционно ответил на вопросы сотрудников компании, а также – впервые – на вопросы пользователей сети Facebook. Некоторые из вопросов были личного плана.

М. Цукерберг рассказал, что команда соцсети продолжит работу над «Лентой новостей» (News Feed), стремясь превратить ее в «идеальную персонализированную новостную газеты для каждого пользователя в мире». «Лента новостей» – это центральный элемент домашней страницы аккаунта в Facebook. На ней отображаются новости от друзей. Какие именно – выбирают автоматические алгоритмы, на основе действий пользователя.

По словам М. Цукерберга, главная задача для сотрудников Facebook – сделать ленту максимально релевантной. Ежедневно каждому пользователю в среднем доступно около полутора тысяч свежих постов, но просматривает он лишь около 100 из них. Инженеры Facebook изучают эти просмотры и стараются адаптировать алгоритмы соответствующим образом.

Примечательно, что Facebook уже занимает важное место в индустрии новостей.

Цукерберг сообщил, что через пять лет основную часть контента, размещаемого в сети Facebook, будет занимать видео. Он рассказал об этом в ответ на вопрос, справляются ли дата-центры Facebook с ростом количества публикуемых фотографий. Ответив на него утвердительно, гендиректор заявил, что гораздо более важная задача – подготовить инфраструктуру к росту объемов видеоконтента.

М. Цукербергу также был задан вопрос, зачем Facebook заставила пользователей, желающих использовать социальную сеть для обмена сообщениями, скачать на свои мобильные устройства отдельное приложение Messenger. «Мы понимаем, что просили о большом одолжении, заставив всех пользователей установить Messenger», – сказал глава компании. Он пояснил, что так будет лучше, потому что на мобильных устройствах каждое приложение может качественно выполнять только одну функцию ***(Марк Цукерберг рассказал о будущем Facebook и объяснил, почему всегда носит серую футболку // Marketing Media Review (http://mmr.ua/news/id/mark-cukerberg-rasskazal-o-buduschem-facebook-i-objasnil-pochemu-vsegda-nosit-seruju-futbolku-42021/). – 2014. – 7.11).***

***

Facebook предоставила пользователям больше контроля над тем, чей контент будет появляться в их новостных лентах.

7 ноября представители социальной сети заявили, что люди смогут увидеть, у кого из их друзей или брендов, на страницы которых они подписаны, было больше всего постов за неделю, пишет AdAge.com. Также компания рассказала о том, что теперь можно будет сокращать количество постов от конкретных людей или брендов, вместо того, чтобы полностью их скрывать.

Эти изменения говорят о том, что Facebook установит больше фильтров на контент от друзей или брендов, которые пользователи «выключают»: то есть вы будете видеть в своей ленте только самые важные посты от них.

С точки зрения маркетинга, это означает, что будет проще выявлять людей, рассылающих спам и наказывать бренды за бесполезные посты. Пользователи по-прежнему смогут отписываться от брендов, просто им будет предоставлен выбор: теперь любой подписчик социальной сети сможет пойти на компромисс, указав Facebook, что хочет видеть в своей ленте меньше постов от конкретного бренда.

Воспользуются ли люди новыми фильтрами, еще предстоит увидеть. Но когда в прошлом году бренды заметили снижение своего органического охвата в Facebook, руководство социальной сети увидело, что многие брендированные посты пользователи помечали как «спам». Маркетологи тоже смогут на себе это прочувствовать – когда увидят, сколько человек хотят получать меньше контента со стороны брендов ***(Facebook поможет***

пользователям отключать надоедливые бренды // Sostav.ua (http://sostav.ua/publication/facebook-pomozhet-polzovatelyam-otklyuchat-nadoedlivye-brendy-64547.html). – 2014. – 10.11).

***

В оновленій версії Instagram для iOS і Android з'явилася можливість змінювати підписи до фотографій після їх публікації. Пункт «редагувати» з'явився у відповідному меню.

До оновлення для того, щоб виправити підпис до фотографії, доводилося видаляти її і викладати повторно. Варто відзначити, тепер користувач може змінити не тільки опис знімка, але і додати або замінити геотеги. Довгоочікувана функція отримала безліч позитивних відгуків в соцмережах.

Instagram здійснив й інші нововведення – піктограма вкладки «Цікаве» (Explore) замінили з компаса на збільшувальне скло. Змінилася і структура розділу: тепер він ділиться на дві частини – «Фото» і «Люди». Автори програми стверджують, що в оновленні значно вдосконалено роботу пошуку ***(В Instagram з'явилася можливість редагувати підписи // Intellect (http://www.intell.in.ua/publ/5-1-0-129). – 2014. – 11.11).***

***

Аудитория сервиса для мгновенного обмена сообщениями Facebook Messenger возросла до 500 млн пользователей после того, как Facebook удалила возможность обмена личными сообщениями из своих основных мобильных приложений для платформ iOS и Android. Об этом говорится в блоге Facebook.

Ранее в этом году соцсеть Facebook полностью вывела функцию мобильного чата в отдельное приложение Facebook Messenger. Таким образом, пользователи мобильных устройств, желающие обмениваться личными сообщениями, были вынуждены скачать отдельный сервис. Это решение вызвало волну критики интернет-сообщества, что отразилось в многочисленных негативных оценках приложению Messenger в магазинах Apple App Store и Google Play.

Несмотря на негативную реакцию, свыше 500 млн пользователей хотя бы раз в месяц используют Messenger, отмечают в Facebook. Гендиректор Facebook М. Цукерберг ранее пояснил решение вывести мобильный чат в Facebook тем, что концепция многочисленных функций в одном мобильном приложении больше не оправдывает себя, и пользователям будет удобнее иметь специализированный сервис для решения конкретной задачи.

Избежать «миграции» на Facebook Messenger смогли либо владельцы недорогих Android-смартфонов, версия платформы которых не поддерживает мессенджер, либо пользователи мобильного веб-сайта Facebook, либо те пользователи, которым доступно приложение-агрегатор контента Facebook Paper.

Сервис Facebook Messenger был запущен в 2011 г. и стал первым в серии сервисов, отдельных от основной мобильной версии Facebook. Кроме того, компания развивает приобретенные мобильные приложения WhatsApp и Instagram, Facebook Paper, Slingshot и Facebook Home ***(Аудитория Facebook Messenger выросла до 500 миллионов пользователей // Media бізнес (http://www.mediabusiness.com.ua/content/view/41330/118/lang,ru/). – 2014. – 11.11).***

***

Facebook хочет стать наиболее популярной социальной сетью в России и собирается взбираться на первое место пьедестала при помощи армии разработчиков приложений, сообщает itc.ua.

В интервью ресурсу Business Insider, руководитель подразделения Facebook по заключению партнерских соглашений и глава по развитию игровой платформы Facebook в регионе EMEA Д. Кодорнью отметил, что в настоящее время компания тесно сотрудничает с разработчиками и пытается убедить их перенести свои приложения на платформу Facebook.

Компания Facebook надеется, что следом за зарождающейся группой российских разработчиков на сайт подтянутся лояльно настроены по отношению к ним пользователи. Для Facebook Россия никогда не была простым рынком, который можно захватить в кратчайшие сроки, поскольку на нем присутствуют еще два очень сильных игрока: «ВКонтакте» и LiveJournal. В отличие от любой другой страны в мире, в России Facebook не является монополистом на рынке соцсетей.

Обозревателям Business Insider Д. Кодорнью в деталях рассказал о планах компании по захвату лидирующих позиций на российском рынке. Он сообщил, что игры и приложения играет ключевую роль в стратегии дальнейшего продвижения Facebook в России, и именно от них будет зависеть успех соцсет М. Цукерберга.

«В России Facebook рассматривается в качестве новой игровой платформы. На момент нашего с Марком первого визита в Россию на Facebook были представлены продукты только одной российской компании. Мы сказали им: ребята, существует место, с помощью которого вы могли бы достичь мирового рынка. В течение следующих 12 месяцев с момента нашего визита в Россию мы наблюдали цунами российских компаний, выходящих на Facebook», – рассказывает Д. Кодорнью.

По словам Д. Кодорнью, Facebook уже наблюдает новое поколение российских разработчиков, работающих с Facebook.

«Если у вас есть время и средства только на одно путешествие, посетите Восточную Европу и Израиль. Именно там в ближайшем будущем будут зарождаться многомиллиардные компании, это я вам могу сказать наверняка» – добавил Д. Кодорнью ***(Facebook рассказала о планах по захвату России // Media бізнес***

(http://www.mediabusiness.com.ua/content/view/41335/118/lang,ru/). – 2014. – 11.11).

***

Сервис микроблоггинга Twitter обновил дизайн, разместив окно публикации твитов на веб-сайте в начале хроники. Обновление призвано облегчить размещение твитов.

Twitter также изменил текст на более вовлекающий: вместо скучного и недружелюбного сообщения «Написать новый твит» пользователей встречает вопрос: «Что происходит?».

Twitter тестировал глобальный редизайн еще в феврале 2014 г. Тогда по структуре расположения основных информационных блоков страница пользователя стала похожа на популярные соцсети Facebook и Google+. Шапка вытянулась по всей ширине страницы, ее размеры изменились с 1252×626 пикселей до 1500×500. Информация о пользов ателе перенесена в левую колонку, а счетчики твитов, читаемых пользователей и подписчиков дополнились количеством опубликованных фото/видео и списков ***(Twitter перенес окно публикации твитов в начало хроники // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_perenes_okno_publikatsii_tvitov_v_nachalo_hroniki). – 2014. – 12.11).***

***

Исследовательская компания Factum Group по заказу ИнАУ составила очередной рейтинг сайтов уанета по среднедневной доле и охвату за октябрь 2014 г. Тройка лидеров все та же: Google, «ВКонтакте» и Mail.ru. Значительных изменений в рейтинге по сравнению с сентябрем не произошло. Сразу на несколько позиций поднялся сайт онлайн-объявлений OLX.UA, а российская социальная сеть «Одноклассники» сместилась с четвертого на шестое место. Кроме этого, в топ-25 рейтинга достаточно неожиданно вошел еще один российский ресурс Rambler.ru, пишет AIN.UA (http://ain.ua/2014/11/13/550029?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed %3A+ainua+ %28AIN.UA %29).

Домены	Среднедневная доля, %	Месячный охват, %
1. Google	**50 %**	**66 %**
2. vkontakte	**45 %**	**60 %**
3. mail.ru	30 %	58 %
4. yandex	26 %	50 %
5. youtube.com	**24 %**	**54 %**
6. odnoklassniki	**24 %**	**38 %**
7. ukr.net	12 %	21 %
8. facebook.com	**11 %**	**28 %**
9. megogo.net	10 %	34 %
10. wikipedia.org	9 %	38 %
11. olx.ua	9 %	31 %

12. sinoptik.ua	7 %	21 %
13. rozetka	6 %	30 %
14. ex.ua	6 %	20 %
15. i.ua	5 %	21 %
16. gismeteo.ua	5 %	16 %
17. twitter.com	**5 %**	**17 %**
18. aukro.ua	4 %	20 %
19. ask.fm	4 %	13 %
20. aliexpress.com	4 %	21 %
21. blogspot.com	4 %	25 %
22. prom.ua	4 %	23 %
23. privatbank.ua	4 %	21 %
24. pravda.com.ua	4 %	14 %
25. rambler.ru	3 %	8 %

Напомним, предыдущий рейтинг самых популярных сайтов уанета выходил в конце октября. Альтернативное исследование по самым популярным сайтам делает «Gemius Украина», последний рейтинг сайтов компания представляла летом этого года ***(Топ-25 сайтов уанета за октябрь: «Одноклассники» теряют позиции в рейтинге // AIN.UA (http://ain.ua/2014/11/13/550029?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed %3A+ainua+ %28AIN.UA %29). – 2014. – 13.11).***

***

Для цінителів алкогольних напоїв створена нова мобільна соціальна мережа – SWIG. Додаток доступний для користувачів iOS та Android.

Автори ідеї позиціонують свій проект як альтернативу Facebook і Instagram для любителів випити. База даних програми включає в себе інформацію про 70 тис. вин, пива та інших алкогольних напоїв, пише Lenta.ru з посиланням на CNET.

Користувачі SWIG можуть підписуватися на оновлення своїх друзів, барменів і сомельє, щоб стежити за тим, що вони п’ють. В додатку також діє система користувальницьких рейтингів.

«Facebook не піклується про те, щоб ви знайшли найкращу “Криваву Мері” на Манхеттені, а ми піклуємося», – говорить один з авторів ідеї.

Для запуску нового додатка було необхідно як мінімум 18 тис. дол., однак творцям вдалося зібрати від 219 потенційних користувачів понад 21 тис. дол. ***(Створена нова соцмережа для любителів випити // Racurs.ua (http://ua.racurs.ua/news/38960-stvorena-nova-socmereja-dlya-lubyteliv-vypyty). – 2014. – 13.11).***

***

Сервис для публичного обмена короткими (до 140 символов) сообщениями Twitter не исключает увеличения максимальной длины одного сообщения.

Об этом сообщил в своем микроблоге на Twitter журналист New York Times B. Гоел со ссылкой на генерального директора компании Д. Костоло.

Так, отвечая на вопрос журналиста о том, появятся ли в соцсети твиты длиной более 140 символов, он ответил: «У нас нет религиозных убеждений насчет этого» ***(Twitter допускает увеличение максимальной длины сообщений // InternetUA (http://internetua.com/Twitter-dopuskaet-uvelicsenie-maksimalnoi-dlini-soobsxenii). – 2014. – 14.11).***

***

Facebook представила новый инструмент для создания видео, способный превратить в ролик вехи взаимоотношений с друзьями по соцсети.

Новый проект Facebook «Скажи спасибо» (Say Thanks) позволит пользователям создавать персонализированные видео для своих друзей и членов семьи. Для создания ролика достаточно будет выбрать другого пользователя и тему видео с заданным звуковым сопровождением, отражающим семейные, дружеские или романтические отношения. Можно будет также добавить фотографии, которые наилучшим образом характеризуют взаимоотношения с этим человеком, и включить в ролик посты со стены – например, поздравления с днём рождения.

Для финального ролика возможно при необходимости настроить параметры конфиденциальности, скрыв его от глаз посторонних. Друг, отношениям с которым будет посвящено видео, окажется на нём отмечен.

Представители компании сообщили, что инструмент будет доступен в течение неопределённого срока ***(Facebook поможет превратить отношения с друзьями в видеоролики // InternetUA (http://internetua.com/Facebook-pomojet-prevratit-otnosheniya-s-druzyami-v-videoroliki). – 2014. – 14.11).***

***

Новый рекомендательный сервис Places от Facebook помогает пользователям находить популярные места по всему миру. Сервис построен на данных «чекинов» пользователей в социальной сети. Аналитики предполагают, что компания нацелена развивать проект до отдельного приложения, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-rekomendatelnyj-servis-places-analog-foursquare-42100/).

Поиск в Places осуществляется по названию города. Пользователь может отсортировать результаты, отобразив отдельные категории: рестораны, отели, бары, кафе, университеты и прочее. В каждой их них результаты сортируются по пользовательскому рейтингу.

Также доступны фильтры – например, можно отобразить только те рестораны, которые понравились некоторым друзьям.

Places объединены с социальным поиском Graph Search, функцией определения местоположений публичных страниц API и другими элементами соцсети.

По мнению главного редактора издания Search Engine Land Г. Стерлинга, вслед за нововведениями Facebook последует создание отдельного мобильного приложения Places – в настоящее время возможности сервиса недоступны мобильным пользователям.

По своим возможностям новый сервис Facebook похож на обновленный Foursquare. В мае 2014 г. геолокационная социальная сеть выпустила отдельное приложение – Swarm, в которое вынесена функция чекинов. Тогда же компания анонсировала полный отказ от обозначения местонахождения пользователя в основном приложении. Нововведение вызвало неоднозначную реакцию у пользователей и интернет-сообщества ***(Facebook запустил рекомендательный сервис Places – аналог Foursquare // Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-rekomendatelnyj-servis-places-analog-foursquare-42100/). – 2014. – 13.11).***

***

Новые правила игры на новостном поле устанавливает Facebook

Недавно социальная сеть предложила издательствам сотрудничать – размещать статьи и новости непосредственно в мобильном приложении Facebook и делить доходы. Учитывая, что более 1,3 млрд пользователей делают сеть крупнейшей мобильной платформой в мире, кооперация с ней может изменить будущее подачи новостей.

Многие издатели от такого предложения пришли в ужас: все это напомнило им частные торговые марки (производитель делает продукт, продает его за минимальные деньги торговой сети, а та наклеивает на него свой лейбл, ставит на полки и в большинстве случаев не упоминает реального производителя товара). Если статьи будут доступны прямо в приложении Facebook, никто не пойдет смотреть их на страницы самих журналов, и все отношения с читателями и данные об аудитории окажутся в ведении платформы.

Но Facebook уже изменил модель потребления информации. Согласно исследованию Pew Research Center, 30 % взрослых американцев узнают новости с сайта соцсети. На главные страницы изданий заходят все реже: например, трафик New York Times за последние два года упал на 50 %.

Чтобы победить Facebook и выжить, издательствам нужно собраться, выдохнуть и… лишить нас бесплатных новостей. На этом настаивает М. Линдстром, колумнист Fast Company, Time и Harvard Business Review, автор книги «Buyology: увлекательное путешествие в мозг современного потребителя» и фигурант списка 100 самых влиятельных людей мира 2009 г. по версии журнала Time.

По словам М. Линдстрома, индустрия новостей находится на грани коллапса, и, если она не хочет погибнуть, ей нужно сделать то же, что

сделали швейцарцы в начале 1980-х, когда их стали теснить японские производители кварцевых часов, – взять и перестроиться. Согласно прикидкам колумниста, пять крупнейших медиакомпаний США в случае объединения смогут контролировать 80 % рынка оригинального новостного контента. Им нужно сделать всего один шаг: не раздавать бесплатные новости. Результат? Больше никаких новостей через Google, никакой новостной ленты Facebook. Если вы хотите новости, вам придется их покупать, и это будет новая реальность.

«Конечно, поднимется оглушительный шум, начнутся попытки получать бесплатные новости обходными путями. Но вскоре потребители уяснят, что производство новостей, как и производство прочих благ, стоит денег», – пишет М. Линдстром.

Переворот не случится за одну ночь и не решит всех проблем, но этот страшный шаг может впервые за долгое время вложить штурвал непосредственно в руки производителей новостей. У часовщиков тридцать лет назад это получилось ***(Как Facebook меняет новости // InternetUA (http://internetua.com/kak-Facebook-menyaet-novosti). – 2014. – 14.11).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Вийшла друком книга «Fантомная боль #maidan», до якої увійшли пости у соціальній мережі з листопада 2013 по червень 2014 р., присвячені соціально-політичним зрушенням в України та Революції Гідності. Про це повідомляє Cultprostir.

Авторами проекту стали активні учасники Майдану А. Савицька та А. Миргородський, видання вийшло за підтримки волонтера Євромайдану Г. Лірника. Книгу присвячено людям України. Вона складається з 6 розділів: «Михайлівська площа», «Надто мирний протест», «Перші смерті», «Будь ласка, не треба більше крові», «Посттравматичний синдром», «Фантомний біль». При оформленні використано фотографії з місця подій.

Про книгу «Fантомная боль #maidan» та реакцію на неї Cultprostir розповіла А. Савицька: «Ідея створення книги з'явилась раптово. Мій друг А. Миргородський брав участь у створенні фотоальбому про події на Майдані, і вирішив розбавити фото текстами з Facebook. У цьому попросив моєї допомоги. Я почала збирати матеріал і захопилась настільки, що назбирала на книгу, але до неї увійшло далеко не все, що хотілося б. Певної миті я зрозуміла, що не хочу віддавати все це комусь іншому, бо кожна публікація, кожен пост є для мене надзвичайно дорогим. Тексти я збирала два місяці, приділяючи цьому весь свій вільний час. Можна сказати, що відтепер ми маємо матеріальне втіленні революції, яка сталася у Facebook.

Продаж книги йде дуже активно. Це надзвичайно приємно для мене як автора. Що стосується відгуків читачів, то люди у більшості випадків кажуть, що поки не можуть прочитати книгу – надто живими і болючими є спогади».

Наклад видання склав 3000 примірників. Гроші, отримані від продажу книги, підуть на придбання тренажера-вертикалізатора для Київського військового госпіталю, в якому проходять реабілітацію військовослужбовці, поранені у зоні АТО ***(Вийшла книга Facebook-постів про історію Євромайдану // Intellect (http://www.intell.in.ua/publ/2-1-0-105). – 2014. – 4.11).***

***

Дослідницька група на чолі із професором Міського університету Нью-Йорка Л. Мановичем здійснила візуалізований аналіз використання соціальної мережі Instagram під час подій Євромайдану.

Про це пише European Journalism Observatory (EJO). Науковий проект під назвою The Exceptional & The Everyday: 144 Hours in Kiev («Неймовірне та щоденне: 144 годин у Києві») охопив понад 13 тис. фотографій, що були завантажені у центрі Києва впродовж 17–22 лютого 2014 р. понад 6 тис. користувачів соціальної мережі Instagram.

Дослідники візуалізували особливості використання соціальної мережі за допомогою комп'ютерної обробки великих масивів даних. На сайті проекту можна переглянути географічні, часові та інші тренди.

Аналізовані зображення науковці відфільтрували за тегами, пов'язаними з Майданом, наприклад як #euromaidan, #євромайдан чи #майдан.

Науковці зауважують, що стосунок до подій на Майдані мали не всі зображення із тегами «майдан». Серед цих світлин були і типові для Instagram селфі.

На думку дослідників, ці зображення не є зайвими в аналізі даних, оскільки також демонструють особливість використання соцмережі під час протестів, а саме зв'язок між буденним та винятковим.

Цей зв'язок був відображений також в аналізі тегів. Вчені побачили, що зображення від 17 лютого до початку ескалації містили буденну складову. Однак 19 лютого вона повністю зникла із соцмережі і поволі поверталася 20–22 лютого.

Окремий розділ дослідницького проекту цілком присвячений «візуальній мові революції» у соцмережі. Е. Тіфентейл виявила, яким було типове зображення протестного Майдану в Instagram. Дослідниця виокремила 29 категорій контенту. Найбільш повторюваними елементами виявилися такі: натовп людей, прапор, вогонь/дим, барикади, графіті та слогани, квіти та свічки.

На думку Е. Тіфентейл, ці образи визначають міську революцію у сучасних соцмережах, подібно до зображень Французької революції 1789 р. на тогочасних картинах та ілюстраціях.

У дослідженні зазначається, що візуальна мова репрезентації протесту та революції залишається схожою, незважаючи на географію подій та часові рамки.

Переглянути усі 13 тис. фото можна переглянути на сайті проекту ***(Американські вчені опублікували аналіз використання Instagram під час Євромайдану // Телекритика (http://osvita.mediasapiens.ua/material/35980). – 2014. – 3.11).***

***

Українські користувачі соціальних мереж запустили флешмоб, присвячений спікеру Верховної Ради О. Турчинову.

3 листопада ввечері у Twitter та Facebook почали поширюватись записи з хештегом #ПасторЗалишайся – таким способом українці вирішили привернути увагу політикуму та самого О. Турчинова – для того, щоб він залишився на своїй посаді. До цього хештегу додавали пояснення, чому їм сподобався спікер за останні півроку та гумористичні картинки, що обігрують мем «кривавого пастора». Остання фраза використовувалась російською пропагандою для опису О. Турчинова як злісного диктатора ***(#ПасторЗалишайся: українці запустили флешмоб в підтримку Турчинова // UkrainianWatcher (http://watcher.com.ua/2014/11/04/pastorzalyshaysya-ukrayintsi-zapustyly-fleshmob-v-pidtrymku-turchynova/). – 2014. – 4.11).***

***

Київський метрополітен інформуватиме про зміни режиму роботи підземного транспорту через Twitter. У соцмережі був створений спеціальний акаунт Kyiv Metro Alerts, передає Еспресо.TV.

Так, відтепер у Twitter можна буде отримувати оперативну інформацію про закриття станцій та зміни руху поїздів у зв’язку з загрозою терактів ***(Про «мінування» столичних станцій метро можна дізнаватися в Twitter // Espreso.tv (http://espreso.tv/news/2014/11/06/pro_quotminuvannyaquot_stolychnykh_stanciy_metro_mozhna_diznavatysya_v_twitter). – 2014. – 6.11).***

***

«Общество спектакля»: чем отличается русский медиаконтент о войне от украинского.

Казус М. Пореченкова уже обсудили со всех сторон. Кроме, кажется, одной: если бы актер запретил работу камеры, факт стрельбы по Донецкому аэропорту остался бы эпизодом его частной биографии. Были там живые мишени или картонные, кажется, уже не очень интересует публику. Важен для нее только символизм кадра: звезда военных сериалов, герой «Ликвидации», актер, сыгравший Поддубного, выпускает автоматные очереди в сторону врагов «Русского мира».

«Общество спектакля» в военном конфликте на востоке Украины, который все-таки честнее называть русско-украинской войной, проявляет себя с самых изощренных сторон, которые не снились Г. Дебору, автору термина. На момент написания этого текста ролик с М. Пореченковым просмотрели более трех с половиной миллионов человек. Для сравнения: все видеоэпизоды со свадьбы Моторолы, все ролики с его порой бесстрашными, харизматичными и развеселыми, порой довольно гнусными пацанами, которые то в очередной раз совершают вылазку к терминалу Донецкого аэропорта, то где-то в лесополосе измываются над пленными, собирают не более 150 тыс. (минимум просмотров – от 20 тыс.).

То же количество просмотров выдает русский YouTube на украинские военные съемки той же топографии и времени, естественно, с другим идейным знаком. Украинские добровольцы, срочники и контрактники не менее харизматичны, чем их противники. С. Семенченко круче Моторолы, потому что умнее. Обе стороны на хорошем русском языке, с довольно выдающимися речевыми оборотами, периодами и гиперболами, иронией и сарказмом рассказывают противнику, чем ему стоило бы заняться вместо стрельбы, и столь же емко объясняют, что они с ним сделают, если не прислушается. Полагаю, для будущего исследователя-лингвиста эти видеодокументы – настоящая находка; у меня есть рабочая гипотеза, что такой специфический русский язык мужской драки достался им в наследство от лихих девяностых.

Я несколько разочарована количеством просмотров в сетях. Цифры говорят сами за себя, и, видимо, они соответствуют реальному интересу «диванных войск» к конфликту. Если принять это как факт, то получается, что из всех искусств для нас важнейшим по-прежнему является кино в стиле «русский блокбастер». Не донецкие репортажи «Лайфньюс» в прямом эфире (в смелости их репортерам не откажешь), не мат бойцов «Иловайского котла», не эпизоды захвата пленных или их передачи (опять говорю здесь о двух сторонах, отснятого материала достаточно). Пара автоматных очередей, пара фраз – и у общества спектакля есть повод объединиться в желании выразить свое отношение к сюжету, к эпизоду в военной эпопее, у которой пока нет названия. Полагаю, обе стороны думают, что она называется «Освобождение».

Теперь о главном отличии русского медиа- и YouTube-контента от украинского. Русская сторона в официальном пространстве вынуждена отбиваться умственными спекуляциями и хитростями монтажа. Ролики бойцов Моторолы не могут оказаться в мейнстриме русского официального эфира. А ролик знакомства Д. Яроша и С. Семенченко где-то на просторах Восточной Украины – эту встречу устроил и снял М. Найем – вполне приемлем в украинском медийном контексте. Русские же не воюют с Украиной, как сказал президент В. Путин; значит, первые каналы не могут открыто призывать идти в добровольцы за «Русский мир». А украинцы воюют за свою независимость, свободу и государственность. Это главная

мысль, с которой согласны и государство в лице вновь избранных парламентариев, и народ на улицах Киева, пару недель назад мне довелось провести там мини-опрос; даже недовольные войной как фактом (а кто из нормальных людей был бы доволен?) признают ее неизбежность.

Государство готово защищать своих граждан, армия готова их защищать, медиа готовы транслировать эту готовность; в том числе и все недостатки, которые возникают в процессе защиты. П. Порошенко снимает В. Гелетея? Нормально, давно пора. Срочники или солдатские матери вышли на демонстрацию? Отлично, мы стояли на Майдане за их права, власть должна их услышать и отреагировать. Те, кто в будние дни сидит в дорогих кафе, в выходные едут в госпитали.

На бывшем Майдане стоит огромная фотовыставка социальной рекламы, которая откровенно связывает события киевской зимы и защиту Донецкого аэропорта, битву с «Беркутом» и битву с сепаратистами. Ее главный посыл: поддержи армию, ты за это боролся, она защищает твой дом.

В YouTube есть украинские социальные (или пропагандистские, это вопрос терминологии) ролики военной операции на востоке Украины, в киевской терминологии – АТО. К примеру, с трогательным «равнением на маму» в момент призыва: построение на плацу, мать пришла на проводы сына, офицер командует равняться на нее, частное побеждает государственное. Или парни и девушки в военной форме, которые улетают из аэропорта Борисполь на войну: старик-офицер в гражданском отдает честь молодому бойцу, девушки бросают восхищенные взгляды. Эти ролики собирают те же цифры в YouTube, что и документальные эпизоды из зоны военных действий. Статистически сравнима со стрельбой М. Пореченкова только запись, где украинцы выстроились вдоль дороги, встречая гроб погибшего на востоке. Он называется «Смотрите, россияне, как Западная Украина встречает погибшего героя» ***(Фанайлова Е. «Общество спектакля»: чем отличается русский медиаконтент о войне от украинского // UAINFO (http://uainfo.org/blognews/430971-obschestvo-spektaklya-chem-otlichaetsya-russkiy-mediakontent-o-voyne-ot-ukrainskogo.html). – 2014. – 5.11).***

***

Українських користувачів Twitter та Facebook обурила остання доповідь ОБСЄ, в якій зазначалося, що обстріл школи № 63 у Донецьку, при якому загинули діти, вівся з українських позицій, пише ZAXID.NET (http://zaxid.net/news/showNews.do?ukrayinski_internetaktivisti_zvinuvachuyut_obsye_u_roboti_na_korist_boyovikiv&objectId=1329379).

Блогери заявили, що ОБСЄ виступає на боці Росії, а доказів обстрілу школи з української території просто немає. Навпаки, ресурс Ukraine@war проаналізував характер обстрілу школи і зробив висновок, що вогонь вівся якраз з контрольованої бойовиками Макіївки Донецької області.

Також користувачі згадали скандал місячної давності, коли в мережі з'явилися фото, що на них співробітники ОБСЄ підвозили збройних сепаратистів на своїх автомобілях.

Нагадаємо, що тоді у Спеціальній Моніторинговій Місії ОБСЄ в Україні визнали, що в Донецьку в машині місії дійсно перевозили терористів.

У зв'язку з цим користувачі Twitter почали кампанію під хештегом #mercenaryosce (ОБСЄ – найманці) ***(Ганкевич Р. Українські інтернет-активісти звинувачують ОБСЄ у роботі на користь бойовиків // ZAXID.NET (http://zaxid.net/news/showNews.do?ukrayinski_internetaktivisti_zvinuvachuyut_obsye_u_roboti_na_korist_boyovikiv&objectId=1329379). – 2014. – 8.11).***

***

Facebook започаткував кампанію зі збирання пожертв для допомогти організаціям, що борються проти поширення вірусу Ебола.

Засновник соціальної мережі М. Цукерберг оголосив про особисту пожертву у 25 млн дол. для подолання смертоносної хвороби, збудником якої є цей вірус, повідомляє CNN.

Facebook очікує пожертв трьом організаціям: Міжнародному медичному корпусу (the International Medical Corps), Міжнародній федерації товариств Червоного Хреста і Червоного Півмісяця (the International Federation of Red Cross and Red Crescent Societies), а також кампанії «Врятуймо дітей» (Save the Children).

1,3 млрд користувачів соціальної мережі бачитимуть повідомлення про це у верхній частині новинної стрічки й матимуть можливість визначати, куди саме надсилати пожертви.

Facebook, об'єднала зусилля з ЮНІСЕФ, щоб через свою мережу поширювати інформацію для населення вражених регіонів про симптоми лихоманки Ебола та її лікування.

«Під час кризи люди звертаються до Facebook, аби дізнатися, що відбувається, поділитися власним досвідом і запропонувати свою підтримку, – говориться у заяві Facebook. – Якщо не буде вирішено проблеми, пов'язаної з епідемією вірусу Ебола, може виникнути довгострокова глобальна криза у сфері охорони здоров'я».

Компанія співпрацюватиме з консорціумом неурядових організацій NetHope, надаючи послуги зв'язку медичним та гуманітарним працівникам у Гвінеї, Ліберії та Сьєрра-Леоне, особливо вражених поширенням вірусу Ебола ***(Facebook започаткував кампанію збору коштів для боротьби з вірусом Ебола // Телекритика (http://osvita.mediasapiens.ua/web/IT_companies/facebook_zapochatkuvav_kampaniyu_zboru_koshtiv_dlya_borotbi_z_virusom_ebola/). – 2014. – 7.11).***

***

Кількість користувачів, які вимагають відкриття українського представництва Facebook, наближається до 30 тис. Саме стільки людей приєдналися до ініціативи «ЗА! Українське представництво Facebook», що стартувала кілька днів тому.

Як повідомляється на сторінці події, яка запланована на 30 листопада, результатом даної ініціативи стане колективне звернення до адміністрації Facebook з вимогою відкрити представництво соцмережі в Україні. Як відомо, наразі українським сегментом Facebook займаються менеджери з Росії, що неодноразово ставало причиною конфліктів.

Російські адміністратори відзначились у неоднозначному ставленні до українських користувачів та заангажованості, особливо в період подій на Майдані та подій на сході України. У липні Facebook забанив акаунт прес-секретаря Президента України С. Цеголка.

У вересні з відкритим зверненням до М. Цукерберга виступила Нацрада з питань телебачення та радіозв'язку, також закликавши замінити адміністраторів українського сегменту. Місяцем раніше рядові користувачі також пробували звернутись до М. Цукерберга з аналогічним проханням ***(До ініціативи за українське представництво Facebook приєдналось 30000 людей // UkrainianWatcher (http://watcher.com.ua/2014/11/11/do-initsiatyvy-za-ukrayinske-predstavnytstvo-facebook-pryyednalos-30000-lyudey/). – 2014. – 11.11).***

***

Правозащитники устроили в социальных сетях акцию с требованием к Президенту Украины П. Порошенко подписать закон о переселенцах. Пользователям Facebook предлагается поместить себе на аватар картинку с надписями призывающими П. Порошенко завизировать закон № 4490а-1.

Об этом сообщается на странице сети правовых приемных Крыма в Facebook.

Надписи, нанесенные на предлагаемые аватары гласят: «Я человек – мне нужны равные права», «Я тоже гражданин. Я хочу продолжить образование!», «Я крымчанин – я гражданин Украины», «Я киевлянин, и мне неравнодушна судьба переселенцев!» и др.

Как сообщила в комментарии для «Крым.Реалии» координатор Крымского правозащитного центра «Действие» А. Дворецкая, такую акцию активисты решили проводить в связи с тем, что президент до сих пор не подписал закон № 4490а-1 «Об обеспечении прав и свобод внутренне перемещенных лиц», который был передан на подписание Порошенко еще 24 октября.

«Как нам сообщили знакомые из Администрации Президента тормозят процесс Минюст и Минсоцпполитики, требуя от Президента заветировать закон. Виртуальная акция призвана актуализировать проблему. Ведь переселенцы боролись за то, чтобы закон был проголосован и на последней

сессии Верховной Рады седьмого созыва это таки произошло под давлением общественности», – сказала правозащитница.

По словам А. Дворецкой, затягивание подписания Президентом законопроекта является незаконным, так как крайний срок принятия решения истек 6 ноября, а П. Порошенко так и не сообщил причины, почему полмиллиона людей, которые вынужденно покинули свои дома, по-прежнему ожидают изменений в законодательстве.

Закон о внутренне перемещенных лицах Верховная Рада приняла 20 октября. После этого Управление ООН по делам беженцев (УВКБ ООН) и правозащитники выразили надежду на скорейшее подписание данного документа. По данным ООН, количество перемещенных лиц в Украине составляет почти 450 тыс. человек.

По данным ГосЧС Украины, по состоянию на 9 ноября, в Украине зарегистрировано 455 тыс. 175 человек временно перемещенных лиц. Из аннексированного Крыма в другие регионы переселились 19 тыс. 221 человек, а из районов проведения АТО – 435 тыс. 954 лица ***(Порошенко призывают подписать закон о переселенцах, устроив флешмоб в соцсетях // Крым.Реалии (http://ru.krymr.com/content/article/26685643.html). – 2014. – 11.11).***

***

В украинском правительстве лишь у двух из 17 министров нет страницы в социальных сетях. Так, у некоторых министров есть даже по несколько страниц в социальных сетях – личные и публичные, пишет «Обозреватель» (http://tech.obozrevatel.com/news/35249-lish-dva-ministra-ukrainyi-ignoriruyut-sotsseti.htm).

Впрочем, у министра энергетики и угольной промышленности Украины Ю. Продана, а также у министра иностранных дел Украины П. Климкина страниц в соцсетях нет. Новости внешнеполитического ведомства публикуются на официальной странице МИДа в Facebook, а сам П. Климкин пишет посты вTwitter, передает УНН.

У министра финансов А. Шлапака даже указаны сведения о его личных отношениях – «все сложно». Впрочем, достоверность этого аккаунта можно поставить под сомнение – его активность низкая.

Как правило, министры на своих страницах отчитываются о своей деятельности и сообщают, что полезного они сделали. Хотя для этого существуют сайты и страницы ведомств в соцсетях, а также пресс-службы в каждом министерстве ***(Лишь два министра Украины игнорируют соцсети // Обозреватель (http://tech.obozrevatel.com/news/35249-lish-dva-ministra-ukrainyi-ignoriruyut-sotsseti.htm). – 2014. – 12.11).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Сотрудник сервиса для работы с социальными сетями Buffer К. Ли опубликовал заметку о том, как создать идеальный с точки зрения пользователя пост в Facebook и получить более широкий охват.

К. Ли составил схему из пяти элементов – для идеальной записи важно правильное оформление ссылки, краткое описание, время публикации, верно заданный темп обновления страницы и актуальность информации.

В качестве примера страницы с идеальными записями К. Ли приводит The Daily Muse, которой удаётся вовлечь более 50 % подписчиков при помощи каждой записи.

1. Идеальная запись содержит ссылку.

Представители Facebook говорят, что записи, к которым ссылка прикреплена в виде стандартного виджета социальной сети, собирают в два раза больше кликов, чем те записи, которые содержат текстовую ссылку и обычное изображение.

Facebook сам получает необходимую информацию из мета-тегов на странице, включая заголовок, описание материала и специальное изображение.

К. Ли отмечает, что способ создания записи с красивой ссылкой не всем очевиден, так как в поле создания новой записи нет кнопки «Вставить ссылку».

Чтобы сделать это, достаточно скопировать ссылку и вставить её в поле ввода текста, после чего подождать несколько секунд, пока парсер Facebook вытянет оттуда всю необходимую информацию. После этого можно удалить сам текст ссылки и приписать какой-нибудь цепляющий анонс.

Facebook предоставляет специальный инструмент Open Graph Debugger, который позволяет контролировать, какую именно информацию соцсеть заберёт с конкретной страницы. Для этого нужно вставить ссылку в соответствующее поле и проследить необходимые значения.

2. Длина идеальной записи не превышает 40 знаков.

К. Ли утверждает, что короткие записи привлекают больше внимания – в среднем, записи, которые состоят из 40 знаков и менее, собирают больше лайков и репостов, чем остальные. Стоит отметить, что записи такой длины публикуются на Facebook реже.

Читатель обращает внимание не столько на текст записи, сколько на заголовок и краткое описание, которое подтягивается из кода страницы.

3. Лучше публиковать записи не в прайм-тайм.

Подписчики вашей страницы следят также за десятками других страниц, и вы боретесь с ними за внимание. И у ваших записей будет гораздо больше шансов быть замеченными, если публиковать их в период затишья.

Согласно этому правилу, стоит попробовать публиковать материалы в вечерние часы и в выходные дни.

4. Идеальная запись согласуется с общей стратегией страницы.

Автор ссылается на исследование, согласно которому те немногие страницы, которые не почувствовали на себе спад органического охвата в последнее время, используют одинаковый подход: публикуют интересный и эмоциональный контент и делают это регулярно, благодаря чему получают большое количество репостов и увеличивают охват. И если наличие более-менее приверженных подписчиков и хорошего контента – совет банальный, то третья составляющая не так очевидна – последовательность.

Успешные страницы, представленные в исследовании, публикуют что-либо как минимум раз в день – пользователи, соответственно, привыкают получать дозу полезной информации регулярно.

5. Идеальная запись согласуется с новостной повесткой.

Представители Facebook говорят о том, что лента новостей, среди прочего, формируется в зависимости от тем, популярных в текущий момент – если пользователь смотрит футбольный матч и упоминает об этом, то он с большей вероятностью будет наблюдать записи об этом же матче. Актуальная тема, кроме того, гарантированно соберёт больше лайков и комментариев – а этот показатель тоже сильно влияет на шанс попадания записи в ленту ***(Анатомия идеальной записи на Facebook // InternetUA (http://internetua.com/anatomiya-idealnoi-zapisi-na-Facebook). – 2014. – 3.11).***

***

Отчет Shareaholic о трафике социальных медиа за третий квартал 2014 г. содержит данные о перенаправленном трафике каждой из 8 самых популярных социальных сетей. Данные показывают «долю посещений» сайтов в процентах от общего трафика – прямого трафика, социальных перенаправлений, органического поиска, платного поиска, и т. д. для Facebook, Pinterest, Twitter, StumbleUpon, Reddit, Google Plus, YouTube и LinkedIn.

В июне этого года Facebook доставлял почти четверть от общего числа посещений сайтов во всем Интернете. В то время как его доля трафика незначительно сократилась с тех пор, социальная сеть по-прежнему доставляет вчетверо больший трафик, чем Pinterest.

Отчет Q3 агрегирует данные из сети сайтов Shareaholic и содержит две основные части:

Раздел I: Социальные рефералы за третий квартал 2014 (июнь – сентябрь 2014 г.). Краткий обзор четырех месяцев данных, полученных от более чем 300 тыс. сайтов с общей аудиторией более 400 млн уникальных посетителей в месяц.

Раздел II: Социальные рефералы год-к-году (сентябрь 2013–2014 г.) – глубокий анализ данных за тринадцать месяцев, полученных от более чем 200 тыс. сайтов с общей аудиторией более 250 млн уникальных посетителей в месяц.

Ниже приведены четыре ключевых вывода из этого отчета:

1. Facebook лидирует, принося в 4 раза больший трафика на сайты, чем Pinterest. Facebook для бизнеса – это золотая жила данных аудитории и распространения контента. Для пользователей – это высоко персонализированное окно в интересующие их предметы / темы / новости. В итоге Facebook – это все, что нужно пользователям.

Принося 22,36 % от общего объема трафика на сайты, доля Facebook в трафике резко увеличилась в прошлом году. С сентября 2013 г. его доля увеличилась на 115,63 % (11,99 процентных пункта), с 10,37 %. В то время как сеть не испытывала значительных успехов в третьем квартале, у нее еще есть большие возможности для роста.

2. Pinterest догоняет Facebook. Pinterest приобрел огромную популярность среди американских женщин, но еще не достиг масштабов своих конкурентов. Имея 70 млн пользователей, он надежно закрепил свои позиции на втором месте списка социальных источников реферального трафика.

В сентябре Pinterest доставил 5,52 % посещений сайтов. За прошедший год его доля трафика возросла на 50,07 % (1,84 процентных пункта), придав ему заметное преимущество перед Twitter, StumbleUpon и Reddit.

3. Twitter теряет влияние. С сентября 2013 г. доля Twitter неуклонно снижалась с 1,17 % (13-месячного максимума) до 0,88 % (13-месячного минимума) в прошлом месяце. Речь идет о снижении на 0,29 процентных пункта (до 24,97 %).

4. StumbleUpon, Reddit, Google Plus, YouTube, и LinkedIn перестают быть источником трафика для большинства издателей, маркетологов и владельцев сайтов. В общем, они принесли 0,74 % от общего трафика сайтов в прошлом месяце, но эта цифра меньше, чем количество посещений одного Twitter.

За последние 13 месяцев доля StumbleUpon в трафике достигала 0,99 % в марте 2014 г., а в прошлом месяце снизилась до самого низкого уровня в 0,41 %. Год-к-году, его доля снизилась на 26,49 % (утратив 0,15 процентного пункта) с 0,56 %.

Сравнивая сентябрь 2013 и сентябрь 2014 г., можно увидеть снижение доли Reddit с 0,26 % до 0,18 %. Снизившись на 30,56 %, Reddit потерял 0,08 процентных пункта.

Google Plus еще жив. В прошлом году он увеличил свою долю трафика на 57,02 % (0,03 п. п.) до 0,07 % в прошлом месяце, по сравнению с 0,04 % за тот же период прошлого года.

YouTube оказался самым большим неудачником. Утратив 87,27 % своего веса (0,25 %), он однажды занял 5-е место выше Reddit, но теперь занимает 7-е. В сентябре 2013 г. YouTube приносил 0,29 % общего трафика на сайты. В прошлом месяце этот показатель составил всего 0,04 %.

В то время как LinkedIn стал источником для издателей, он дает сравнительно низкое число переходов из социальных сетей на сайты по всему Интернету. В сентябре 2014 г. LinkedIn предоставил 0,04 % от общего

трафика на сайты, что на 47,37 % (0,03 п. п.) меньше по сравнению с тем же периодом прошлого года.

В начале 2014 г. Агентство Shareholic установило, что более половины от всех рефералов (51 %) Facebook переходит на сторонние сайты с мобильных версий социальной сети. В ходе эксперимента была изучена статистика по 200 тыс. сайтам, численность аудитории которых превышает 250 млн уникальных пользователей в месяц ***(Shareaholic: в третьем квартале реферальный трафик из Facebook в 4 раза превысил трафик из Pinterest // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/shareaholic_v_tretem_kvartale_referalnyy_trafik_iz_facebook_v_4_raza_prevysil_trafik_iz_pinterest). – 2014. – 3.11).***

***

Компания Boft готовит к запуску сеть автоматов, которые предназначены для печати фотографий из Instagram в формате Polaroid, пишет Блог Imena.UA (http://www.imena.ua/blog/boft-instagram/).

В ближайшее время такие автоматы появятся во всех крупных городах мира. Устройство позволяет распечатать фотографии из сервиса Instagram буквально на месте.

Необходимо подойти к киоску-автомату, ввести на клавиатуре требуемое имя пользователя или хэштег, выбрать снимок и распечатать его. Следует отметить, что автомат распечатывает только парное количество снимков.

Такие кадры, по замыслу создателей автоматов, станут отличным подарком или сюрпризом, поскольку Boft позволяет распечатать фотографии любого пользователя с открытым профилем.

В случае, если профиль закрыт, автомат попросит сначала ввести пароль, который впоследствии сбрасывается.

В столице Великобритании открылся ресторан, посетители которого могут расплатиться за еду фотографией в Instagram. Picture House предлагает блюда из курятины и рыбы совершенно бесплатно, если клиент сфотографирует еду и опубликует снимок в Instagram с хэштегом #BirdsEyeInspirations.

Ресторан был открыт международным брендом Birds Eye, под которым производятся замороженные продукты. Таким образом, компания весьма оригинально рекламирует собственную продукцию ***(Представлен автомат для распечатки фотографий из Instagram // Блог Imena.UA (http://www.imena.ua/blog/boft-instagram/). – 2014. – 4.11).***

***

Зачем брендам Instagram: 14 полезных фактов для интернет-маркетологов

Согласно данным американской исследовательской маркетинг-компании L2, западные бренды используют в своей social стратегии в среднем 7,5 социально-медийных платформ, пишет Marketing Media Review (http://mmr.ua/news/id/zachem-brendam-instagram-14-poleznyh-faktov-dlja-internet-marketologov-41979/).

Первые три наиболее популярные платформы – Facebook, Twitter и YouTube – активно «догоняет» мобильный Instagram. По данным недавнего отчета L2 Intelligence Report: Social Platforms, среди 382 исследуемых крупнейших мировых брендов в 8 потребительских категориях около 90 % используют Instagram.

Другое американское агентство, специализирующееся на исследованиях в соцмедиа и разработке инструментов анализа, Simply Measured, поделилось интересной статистикой об Instagram-активности около 100 брендов из списка Interbrand за 2012–2014 г., среди которых MTV, Mercedes-Benz, H&M, Nike, Starbucks, BMW, Adidas и Disney.

1. Крупные бренды уже используют Instagram. В третьем квартале 2012 г. у 54 брендов из списка топ-100 Interbrand имело аккаунты в соцсети. В этом году их уже 86.

2. Они используют Instagram активно. 73 % из упомянутых 86 брендов публикуют минимум одно фото или видео в неделю. Статистика ежедневных постов за два года возросла втрое.

3. Аудитория растет. Количество брендов из топ-100 с аудиторией более 10 тыс. человек в этом году достигло 62. А число брендов с аудиторией более 100 тыс. человек возросло с 15 до 34.

4. Лидирует Nike. Среди 100 исследуемых брендов у 15 – более 1 млн подписчиков. Среди них лидирует Nike с аудиторией 7,3 млн.

5. Возросла вовлеченность пользователей. Лайки и комментарии каждого брендированного поста возросли за два года на 415 %. В третьем квартале 2014 г. у топ-бренда в среднем 18 822 лайков и комментариев (в 2012 их было 3 648).

6. Удачные посты долго остаются популярными. Посты топ-100 брендов из списка Interbrand набирают в среднем 216 комментариев, 50 % которых появляются в первые шесть часов. 75 % комментариев пост набирает в течение 48 часов, а еще 10 % комментариев публикуются через 13 дней.

7. Лучшие посты «выстреливают» немного позже. Самые популярные фото и видео получают комментарии позже. 50 % комментариев появляется только через 13 часов после публикации.

8. Количество знаков в тексте не так важно. В среднем описание публикации не превышает 138 знаков, но Simply Measured не выявили особого соотношения между длиной текста и вовлеченностью пользователей.

9. @упоминания пользуются большей популярностью. В среднем, посты в которых упоминаются другие бренды или пользователи популярнее

на 56 %. Но только в 36 % постов брендов используется хотя бы одно @упоминание.

10. Бренды используют не слишком много хэштегов. В 88 % изученных постов был хотя бы один хэштег; в 91 % постов их менее семи.

11. Хэштеги добавляют популярности. Посты хотя бы с одним хэштегом привлекают на 12,6 % больше внимания.

12. Местоположение имеет значение. Всего в 5 % бренд-постов в Instagram указывают местоположение, но те, кто делает это, получают на 79 % больше внимания.

13. Особенно популярны посты медиакомпаний. Только четыре медиакомпании из списка Interbrand активны на Instagram, но они делают на 62 % больше публикаций в сравнении с брендами из других категорий. В среднем каждый их пост собирает 23 906 лайков и комментариев. Это примерно на 5084 больше, чем у других компаний.

14. Самые активные бренды на Instagram – автопроизводители. Автобрендов из списка топ-100 Interbrand на Instagram на 13 больше, чем в остальных категориях.

На прошлой неделе после шести месяцев тестирования Instagram запустил новый сервис видеорекламы для брендов. Первыми рекламодателями стали такие компании, как Disney, Activision, Lancome, Banana Republic и CW.

Примерно в то же время видеосервис запустила еще одна популярная мобильная соцмедиа платформа, Snapchat.

«Наша аудитория становится все более “мобилоцентричной”, а Instagram – как раз такая платформа. Так что это – важная часть маркетинга», – рассказал в интервью Adweek представитель Activision Д. Анастас.

Он добавил, что по ожиданиям компании первоначально Instagram-видео соберет 2 млн просмотров, и благодаря лайкам и шерам, его увидят еще миллионы пользователей, которые также посмотрят более длинное видео на Facebook ***(Зачем брендам Instagram: 14 полезных фактов для интернет-маркетологов // Marketing Media Review (http://mmr.ua/news/id/zachem-brendam-instagram-14-poleznyh-faktov-dlja-internet-marketologov-41979/). – 2014. – 5.11).***

***

Команда YouScan проанализировала обсуждения украинских банков в социальных сетях. На базе упоминаний разных банков за период с 1 по 31 ктября 2014 г. аналитики определили их сильные и слабые стороны, выяснили, насколько клиенты довольны обслуживанием, а также составили рейтинг украинских финучреждений за анализируемый период. Самыми популярными банками среди пользователей соцмедиа стали ПриватБанк, Дельта Банк и Ощадбанк. Приэтом больше всего негативных упоминаний приходится на ПриватБанк, а меньше всего претензий у пользователей к Дельта Банку, пишет AIN.UA (http://ain.ua/2014/11/06/548827).

Всего YouScan включил в рейтинг 15 банков. Помимо вышеперечисленных, в первую пятерку также вошли VAB и OTPbank. Фидобанк, позиционирующий себя одним из самых технологических финучреждений в стране, занимает девятую позицию рейтинга.

Также аналитики проследили, что именно обсуждают пользователи, когда речь заходит о конкретном банке. Так клиенты ПриватБанка в соцсетях жаловались на трудности с выдачей валюты (особенно с депозитных счетов), а также на проблемы с интернет-банкингом. Чаще всего ПриватБанк обсуждали в Facebook, «ВКонтакте» и на профильных форумах.

Дельта Банк также обсуждают из-за невыдачи долларовых депозитов. В банке это мотивируют отсутствием валюты. Также шквал обсуждений вызвала новость о повышении тарифов по платежным картам. Серьезную волну негатива вызвало введение лимитов на снятие наличных и онлайн-покупки.

Ощадбанку в соцсетях задают много вопросов, однако администраторы далеко не всегда дают на них ответы. Обсуждают его преимущественно в Twitter, Facebook и «ВКонтакте». Огромную волну обсуждений в сомедиа вызвала новость о том, что украинскую армию переводят на выплаты зарплат на Ощадбанк – пользователи жалуются на неразветвленную сеть банкоматов, очереди в отделениях и другие элементы «совковости» в работе финучреждения. При этом многие отмечают изменения к лучшему – вежливый персонал и ремонт в отделениях.

Самое качественное обслуживание, по мнению пользователей соцсетей, в Ощадбанке. В Укрэксимбанке и Укргазбанке оно пока оставляет желать лучшего ***(Лучшие и худшие банки Украины по отзывам пользователей соцсетей // AIN.UA (http://ain.ua/2014/11/06/548827). – 2014. – 6.11).***

***

Начиная с 5 ноября, разработчики крупнейшей в мире социальной сети Facebook закрыли возможность использовать Like в качестве пропуска на участие в конкурсах или платы за контент.

Представители Facebook хотят убедиться, что пользователи ставят Like страницам действительно интересных для них торговых марок, а не вследствие действия «искусственных стимулов». Другие считают, что Like может быть эффективным инструментом, и что реальным мотивом Facebook в данной ситуации является развитие рекламного бизнеса для создания более широкой аудитории сети.

Владельцам страниц с кампаниями, построенными на основе Like, не придется отключать их. После внесения изменений контент будет показан любому пользователю, который посетит страницу.

Одной из причин, по которой большинство социальных экспертов не оплакивает изменения, является снижение ценности Like. Использование регистрационных данных – в частности, адреса электронной почты, – для

непосредственного взаимодействия с клиентом в конечном счете более ценно, чем Like.

Месяцем ранее Facebook сделал свою кнопку Like доступной всем разработчикам мобильных приложений для Android и iOS.

В сентябре 2013 г. окружной апелляционный суд США издал официальное постановление, согласно которому теперь нажатие пользователем кнопки Like в соцети Facebook следует расценивать как проявление человеком свободы слова. Таким образом, теперь кнопка защищена американским законом в соответствии с нормой, закрепленной в Первой поправке к Конституции США ***(Маркетологи больше не смогут использовать «like» в Facebook в качестве платы за контент и участие в конкурсах // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/marketologi_bolshe_ne_smogut_ispolzovat_like_v_facebook_v_kachestve_platy_za_kontent_i_uchastie_v_konkursah). – 2014. – 10.11).***

***

Сервис микроблогов Twitter объявил о запуске нового приложения для малого и среднего бизнеса Small Business Planner. Новинка призвана помочь предпринимателям в планировании, структурировании и управлении маркетинговыми мероприятиями в Twitter.

С помощью Small Business Planner пользователи смогут:

– Просматривать ежедневный календарь, сгруппированный вокруг 4 основных тем: рекомендуемые твиты, рекомендуемые кампании, полезные инструменты и мероприятия Twitter .

– Добавлять наиболее релевантные темы из Twitter в личный, настраиваемый календарь, который синхронизируется с календарём устройства.

– Получать напоминания, которые помогут вовремя отправить твиты, запустить компании и отследить их эффективность.

– Получить доступ к дополнительным ресурсам, таким как исследования, истории успеха, статьи в блогах и электронные книги, непосредственно внутри приложения.

– Первыми узнавать о предстоящих мероприятиях Twitter для предпринимателей.

Новое приложение запущено для предпринимателей в Северной Америке, Великобритании и Ирландии. Оно уже доступно для загрузки в App Store и Google Play.

Перед началом работы разработчики рекомендуют ознакомиться с ЧаВО внутри приложения, а также создать собственный настраиваемый календарь. Они также сообщили, что планируют часто обновлять приложение, добавляя новый контент и возможности ***(Twitter запустил приложение для предпринимателей Small Business Planner // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter***

_zapustil_prilozhenie_dlya_predprinimateley_small_business_planner). – 2014. – 11.11).

***

Пользователь сайта Geektimes обнаружил, что крупнейшая российская социальная сеть «ВКонтакте» тайно подставляет к части внутренних ссылок на китайскую торговую площадку AliExpress собственные метки. По мнению обнаружившего это явление читателя, соцсеть зарабатывает на переходах и нарушает правила реферальной программы. «Цукерберг Позвонит» (ЦП) узнал у представителей «ВКонтакте» об эксперименте, который она проводит совместно с партнёрской сетью ePN.

У AliExpress существует реферальная система, которая даёт пользователям бонусы за привлечённых клиентов. Есть и ряд партнёров, которые работают с вебмастерами. Они ставят на сайтах ссылки на торговую площадку, обеспечивая ей трафик, взамен получая 3–4 % комиссии от покупок, совершённых пользователем за 30 дней.

Читатель Geektimes обнаружил, что при переходе из «ВКонтакте» по любым ссылкам на AliExpress пользователь сначала переадресуется на сайт Alipromo.com, а уже затем на торговую площадку. По мнению читателя, ситуация попадает под описание cookie stuffing (подмена данных клиентов с целью получения дополнительных продаж), а «ВКонтакте» зарабатывает на своих посетителях.

Alipromo.com принадлежит партнёрской сети ePN, которая выплачивает вебмастерам от 2,5 % до 45 % с каждой покупки, совершённой в течение 30 дней после перехода пользователя на сайт.

Руководитель направления AliExpress ePN в группе компаний FIX И. Петров (который недавно выступал на ЦП) заявил, что речи о «стафинге» и нарушении правил не идёт: любой сайт имеет право делать любые нереферальные ссылки партнёрскими и зарабатывать на этом. Для этого в программах существует инструмент deeplink, с помощью которого владельцы площадок получают оплату за привлеченный трафик.

Пресс-секретарь «ВКонтакте» Г. Лобушкин отверг предположение о том, что социальная сеть занимается cookie stuffing, но подтвердил ЦП информацию о том, что они проводят эксперимент и добавляют свой рефер в часть ссылкок на AliExpress. По его словам, реферальные ссылки пользователей от этого не страдают. Г. Лобушкин отмечает, что пока «ВКонтакте» на переходах не зарабатывает и в настоящее время «только проводит первые тестирования» ***(«ВКонтакте» начала тайно подставлять ссылки на AliExpress в надежде заработать на партнёрке китайского магазина // IT Expert (http://itexpert.org.ua/rubrikator/item/39370-vkontakte-nachala-tajno-podstavlyat-ssylki-na-aliexpress-v-nadezhde-zarabotat-na-partnjorke-kitajskogo-magazina.html). – 2014. – 12.11).***

***

Недостаточно наблюдать лишь за своей страницей в социальной сети. Иногда полезно понимать, в чем сильные стороны других брендов. SocialBakers выпустил гид по метрикам, на которые нужно обращать внимание при мониторинге, и объяснил, почему важно вести статистику «соседа», пишет Marketing Media Review (http://mmr.ua/news/id/kak-provodit-monitoring-konkurentov-v-socialnyh-setjah-42088/).

По данным SocialBakers, социальные сети позволяют маркетологам увеличить число лояльных подписчиков бренда (65 %), узнать больше о рынке (69 %), дают больше экспозиции (89 %) и увеличивают трафик (75 %). Вместе с тем, социальные сети совсем не предоставляют информацию о конкурентах, чтобы маркетологи могли сравнивать и знать, к чему стремиться. Поэтому им остается пользоваться доступными данными. Рассмотрим на примере Facebook, что можно установить о конкуренте, не прибегая к сторонним платным инструментам.

Размер страницы

Количество подписчиков – это метрика, на которую маркетологи обращают внимание в первую очередь, особенно новички на рынке. Но количество не имеет значения, если подписчики не вовлечены в коммуникацию с брендом. Регулярный мониторинг размера страниц основных конкурентов бренда может быть очень полезен: например, информация о среднем количестве подписчиков, а также их средний ежемесячный рост, позволят быстро увидеть, на верном ли пути находится бренд, работая в социальной сети.

Уровень вовлеченности

Эта метрика вызывает больше всего дискуссий. С низким уровнем вовлеченности страница выглядит пустой, а значит, компания зря тратит средства на содержание SMM-специалиста. Отсутствие лайков и комментариев от пользователей создает впечатление, что брендом никто не интересуется, что в свою очередь снижает вероятность того, что пользователи будут подписываться на страницу.

Нужно сильно потрудиться, чтобы вычислить уровень вовлеченности страниц основных конкурентов. Поэтому стоит ограничиться одним основным конкурентом на своем рынке и анализировать его.

Количество перепостов (shareability)

Количество репостов – еще одна важная метрика, по которой можно судить о качестве и актуальности контента страницы. Показатель репостности мощнее всех других показателей, поскольку подразумевает, что пост скорее всего получил «охват в квадрате», так как пользователь поделился им со своими друзьями.

Сравнивая эту метрику с показателями конкурентов, можно утверждать о продуктивности страницы бренда, если, например, страница с меньшим количеством постов имеет больше репостов, чем конкурент по размеру больше.

Сравнив свою работу с конкурентом, можно получить представление о том, какого рода контент пользуется наибольшей популярностью на странице и есть ли различия с конкурентом. Если у последнего больше репостов, то это подсказка, что нужно менять на странице вашего бренда.

Время отклика

То, как быстро бренд реагирует на сообщения в социальной сети, говорит о том, как быстро вообще в компании обслуживают клиента (для сравнения, попробуйте написать сообщения в McDonalds и Burger King и проверить, кто быстрее ответит).

Чтобы сравнить свою метрику с метриками конкурентов, нужно лишь время от времени писать им сообщения. Если бренд сильно отстает по времени, то стоит задуматься, правильный ли человек руководит его страницей в Facebook. А если из всех конкурентов лишь ваша страница обладает высоким показателям по скорости ответа, то есть повод для гордости.

«Люди говорят об этом»

Метрика, которая по-английски звучит, как people talking about this (PTAT), исторически использовалась для измерения уровня известности страницы и взаимодействия с ней пользователей с течением времени. Этот показатель доступен в Facebook для всех пользователей, поэтому можно легко вести статистику по конкурентам.

PTAT включает в себя количество новых подписчиков за месяц, лайки, комментарии, репосты. Минус PTAT в том, что показатель нельзя разбить на части, чтобы понимать, какой компонент является самым слабым, а что является драйвером. В результате эта метрика становится все менее популярной среди маркетологов, сообщают SocialBakers в своем отчете ***(Как проводить мониторинг конкурентов в социальных сетях? // Marketing Media Review (http://mmr.ua/news/id/kak-provodit-monitoring-konkurentov-v-socialnyh-setjah-42088/). – 2014. – 13.11).***

***

Tumblr – крупный сервис микроблогов – приступил к тестированию видеорекламы. Подобная реклама будет автоматически отображаться во время просмотра информационной панели.

По словам представителей компании, видеоплеер будет демонстрировать рекламные ролики десяти брендов. Среди них будут: CW, Lexus, Universal, JCPenney и другие. Реклама будет отображаться как в десктопной версии сервиса, так и в приложениях для iOS и Android. Для мобильных приложений реклама будет загружаться только при включенном Wi-Fi.

Ролик по умолчанию будет беззвучным и закольцованным. То есть, видео будет повторяться до тех пор, пока пользователь его не закроет. Также появится возможность выбирать качество разрешения видеоролика.

В прошлом году похожие функции уже тестировал Facebook, а в этом году – Twitter. По словам экспертов, подобная реклама принесет этим сервисам дополнительные доходы ***(Тумблер начал тестирование видорекламы // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/tumbler_nachal_testirovanie_vidoreklamy). – 2014. – 14.11).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Американская журналистка А. Винтер не считает, что проникновение цифровых технологий в нашу жизнь это всегда хорошо. Смартфоны, планшеты, носимые гаджеты сделали общение очень легким и доступным, но их проникновение в нашу жизнь приводит к тому, что люди постепенно теряют навыки обычного человеческого общения. В своей статье в издании The Guardian А. Винтер рассказывает, как сенсорные гаджеты влияют на общение между людьми.

Apple не просто уменьшила iPhone и защелкнула его на вашем запястье. Т. Кук настаивал: «Вы носите часы на себе, поэтому мы изобрели новые, глубоко личные способы общения».

Глубоко личное общение, серьезно?

Apple Watch не просто завибрирует, когда вы получаете SMS, вы можете дотянуться до часов этого человека через полмира, и сделать так, чтобы они вибрировали у него на запястье.

«Мы напряженно думали над новым способом общения, – говорит К. Линч из Apple, – Мы создали кое-что, называемое цифровым касанием».

Попридержите телефон, или что там у вас, часы… Разве «цифровое прикосновение» не звучит как-то жутковато? Мы разве ничему не научились в ходе эксперимента Facebook с кнопкой Poke, который длился годами и окончился провалом? И что больше всего тревожит: разве будущее, где царят цифровые касания, где люди фактически отделены друг от друга большой дистанцией, не погубит то, что осталось от непосредственного общения в наш век Snapchat и вебинаров?

Это далеко не первый раз, когда технокомпания встраивает в свои гаджеты тактильную обратную связь: передача запрограммированной реакции через физическую задолго до умных часов Apple появлялась в различных устройствах вроде iPhone или Xbox. Но Apple Watch – это не просто очередное устройство, которое вибрирует в ответ на прикосновение.

Эти часы не только могут записывать стук вашего сердца, они освобождают нас от ограничений географии, выполняя предсказанное философом А.Боргманном, который однажды написал: «технология… аннилигирует пространство и время».

Может, все вышесказанное – немного преувеличено, но учитывая, как много времени люди проводят, уткнувшись в дисплей, мы быстро забываем, как взаимодействовать лицом к лицу.

Психолог Л. Розен, автор книги об одержимостью технологиями iDisorder, объяснял мне как-то, что когда люди общаются вживую, у них появляется доступ к мириадам знаков, которые можно интерпретировать: вербальным знакам, выражениям лица, жестикуляции – все это помогает нам общаться. Когда мы перешли на смартфоны, мы утеряли доступ к этим важным знакам (да, даже в том случае, если пользуемся FaceTime). Как и можно было догадываться, переход к текстовым сообщениям устраняет возможность читать по лицу, понимать язык тела, и вынуждает опираться только на грамматику и на, гм, смайлики.

Haptic-технологии (основанные на осязании) устраняют нашу потребность в словах, позволяя «прикоснуться» к друзьям, оставляя их недоумевать о том, что же это «прикосновение» значило. Знаков-подсказок остается все меньше и меньше, и мы все более опираемся на нарративы, созданные исключительно нами самими, на основе социальных норм и прошлого опыта. Все это приводит к тому, что все чаще общение интерпретируется абсолютно фантастическим, вымышленным образом, и это пугает.

Думаете, ожидание того, как значки на экране превратятся в текст, – это не стресс? Конечно, стресс. А переживания по поводу того, что шеф углядит что-то не то в названии вашего рабочего письма, либо же любовь всей вашей жизни не заметит в письме вашего очаровательного сарказма? Haptic-устройства заставляют нас бороться с двусмысленностью.

А что же случается, когда мы на самом деле, в реальности, касаемся человека? Бросим ли мы это делать ради «цифовых касаний» на Apple Watch просто потому, что это более эффективно? Заменит ли «цифровое касание» натуральные объятия в будущем? Звучит абсурдно, но скольким из вас приходилось сталкиваться с соблазном послать смс-ку кому-то, кто сидит в соседней комнате, вместо того, чтобы просто прийти и поговорить? Разве уже не выросло поколение детей, которые приучены к смартфонам? Соблазненные легкостью общения с помощью технологий, мы теряем общение лицом к лицу, которое учит нас сопереживать тем, кто рядом.

Наша зависимость от технологий часто приводит к тому, что в нашем жизненном опыте становится меньше человечности. Л. Розен попросил не терять надежды, отметив, что «общество всегда найдет применение технологии» до ее широкого распространения. До того, как мы полностью утратим человеческую чувствительность ***(Технологии победили: Почему***

исчезает общение между людьми // iLenta.com (http://ilenta.com/news/misc/misc_4540.html). – 2014. – 4.11).

Маніпулятивні технології

В соцсети «ВКонтакте» появилось сообщество, где пользователи могут предоставлять информацию о патриотах Украины, проживающих в «треугольнике» Северодонецк-Лисичанск-Рубежное. В группе звучат открытые призывы к моральному и физическому унижению людей. Пока неизвестно, что авторы группы будут делать с собранной информацией, ведь эти города уже давно находятся под контролем украинской власти. Об этом сообщает «Луганский Радар».

Напомним, что в ЛНР и ДНР активно практикуется поощрение доносов на «инакомыслящих». В Свердловске Луганской области с работников бюджетной сферы взяли письменное обязательство сообщать о людях, «высказывающих неуважительное мнение по отношению к ЛНР» ***(В социальной сети «ВКонтакте» собирают информацию о патриотах трех городов Луганской области // «Мой город» http://sever.lg.ua/2014-11-05-v-sotsialnoi-seti-vkontakte-sobirayut-informatsiyu-o-patriotakh-trekh-gorodov-luganskoi-o). – 2014. – 5.11).***

***

Украинцы высмеивают российскую телепропаганду и готовы бороться с ней несистемными методами

«За что вы воюете? Нам пообещали кусочек земли и два раба» – эта фраза жителя Донбасса В. Быкодорова, председателя одного из сельских советов в Донецкой области, прозвучала 2 ноября в эфире российского телевидения.

Однако о ней на протяжении нескольких дней говорят в эфирах украинского телевидения, пишет на своих страницах украинская пресса.

На пятой минуте сюжета российского Первого канала В. Быкодоров передает слова якобы услышанные от бойцов Нацгвардии: «нам пообещали кусочек земли и два раба» за, якобы «войну» на Донбассе против сепаратистов.

Автор репортажа увязывает информацию о фашистах, которые «пришли в Донбасс в 1941» и теми событиями, которые происходят сейчас в восточных областях Украины.

В Twitter и Facebook фраза о «двух рабах и кусочке земли» стала поводом для насмешек. Многочисленные авторы пишут о том, что была надежда, что после сюжета Первого канала о «распятом мальчике» в Славянске, российские тележурналисты перестанут сочинять неправду.

«Кто мальчика не распинал – за рабами не занимайте!», «Записала себя и кота в каратели – встала в очередь за рабами» – это лишь малая доля тех шуток в Интернете, которые были спровоцированы сюжетом на российском телевидении.

До этого, как подсчитали журналисты информационной программы «Телевизионная служба новостей» на украинском телеканале «Студия 1+1», было, как минимум, пять фейковых российских новостей, которые поражают своей выдумкой и неправдой.

По мнению исполнительного директора Института массовой информации О. Романюк, в случае с Россией и подобного рода информационными поделками, мы имеем дело с жесткой информационной вертикалью власти.

Ведь в нормальной стране, подобные фальшивые новости про «рабов», «распятых детей», «снятых с поезда пассажирах и отправленных в Нацгвардию» невозможны, подчеркивает эксперт. Поэтому, продолжает О. Романюк, эти сюжеты в эфире государственного российского телеканала, скорее всего, отвечают некой парадигме государственного заказа, некой установке свыше.

«Со стороны Украины этой вертикали противостоит гражданское общество. Народ это просто высмеивает. Этому идиотизму мы противостоим несистемными методами», – говорит О. Романюк Русской службе «Голоса Америки».

О. Романюк считает, что подобные действия российских журналистов еще больше диктуют украинской прессе жестче придерживаться международных стандартов работы, не скатываться до уровня тех, кто выполняет политические заказы.

«Профессиональные стандарты в украинских СМИ в 2014 г. стали намного выше, чем при президенте В. Януковиче, когда действовала цензура. Сегодня мы видим плюрализм мнений. Народ пока смеется над российскими фейками, мы искренне удивляемся и недоумеваем, неужели существует аудитория, которая способна серьезно воспринимать сюжеты “про два раба”, и кто-то в России этому искренне верит?» – отмечает О. Романюк.

В тоже время, она считает, что на государственном уровне, в украинское законодательство должны быть внесены изменения, которые позволят расширить полномочия Национального совета по вопросам телевидения и радиовещания для противодействия подобного рода «информации».

«Если внести поправки, то Национальный совет по вопросам телевидения и радиовещания мог бы системно реагировать на подобный контент, который нарушает европейскую конвенцию по трансграничному вещанию, призывает к ненависти и розни среди населения», – подчеркивает О. Романюк.

По мнению украинского медиа-эксперта С. Рачинского, информационная война, которую российские СМИ ведут против Украины, в первую очередь поражает простого россиянина.

«Это война против своего же собственного народа. Это попытка манипулировать его сознанием, пониманием того, что происходит на самом деле, это маскировка истинных целей войны против Украины, которую ведет российское государство. Поэтому то, что делает Россия – это насилие над собственным народом, это обращено к нему, это влияет на него. Пределы допустимого давно перейдены, ничего не может ограничить фантазеров, которые сочиняют небылицы», – говорит С. Рачинский Русской службе «Голоса Америки».

С. Рачинский считает, что в сложившейся ситуации для Украины «велик соблазн» действовать адекватно попыткам российской стороны искажать ситуацию.

«Соблазн очень велик, Украина может начать разворачивать собственные проекты в этом направлении. Но это не очень здоровая тенденция. Государство может предпринять попытки манипуляции сознанием своих граждан, ограничить доступ своих граждан к информации. Это опасно. Я не хочу сказать, что эта фейковая информация полезна потребителю, но крайне опасно, когда государство предпринимает попытку влиять на выбор человека – что слушать, что смотреть», – отмечает С. Рачинский.

Он считает, что агитации и пропаганде российского телевидения может быть противопоставлены усилия независимой журналистики, которую «невозможно построить по указке». Однако насколько влиятельна независимая журналистика в России, С. Рачинский не говорит.

«Все о чем мы сейчас говорим, называется “элементом информационной войны”. Существует расхожая мысль, что информационная война – это война между государствами посредством информации. Эта информационная война обостряется во время конфликта между странами. <…> Населению нужно брать инициативу в свои руки, получать информацию из Интернета, социальных сетей, от тех, кому мы доверяем», – отмечает С. Рачинский ***(Бурнос Т. «Рабы» российского телевидения // Голос Америки (http://www.golos-ameriki.ru/content/ukraine-russia-tv/2510943.html). – 2014. – 6.11).***

Зарубіжні спецслужби і технології «соціального контролю»

В Днепропетровске сотрудники СБУ задержали администратора группы «Днепропетровская народная республика» Е. Симутина

Е. Симутин вел активную деятельность в соцсетях под ником «Новоросс Днепровский». В частности, группа «Днепропетровская народная республика» насчитывает более 18 тыс. подписчиков.

Как признался в ходе допроса в СБУ администратор группы, его завербовали. «В августе 2014 г. я уехал в Крым, где установил связь с руководством “ДНР” с Д. Пушилиным», – говорит Е. Симутин.

Группу «Днепропетровская народная республика» использовали российские спецслужбы для распространения нужной им информации. В частности, в группе печатались сводки с фронта и призывы к межнациональной розни внутри Украины.

На своей странице онлайн-сепаратист делал частые репосты из группы, которую создал, предлагал друзьям поддерживать так называемое «ополчение Донбасса».

В то же время друзья Е. Симутина обратились через соцсети к СБУ с требованием освободить Е. Симутина ***(О чем писал в соцсетях сепаратист, задержанный в Днепропетровске // СЕГОДНЯ.ua (http://www.segodnya.ua/regions/dnepr/o-chem-pisal-v-socsetyah-separatist-zaderzhannyy-v-dnepropetrovske-566837.html). – 2014. – 5.11).***

***

Количество запросов к соцсети Facebook от госорганов по всему миру на раскрытие пользовательских данных возросло на четверть за первую половину 2014 г. по сравнению со вторым полугодием 2013 г. Об этом свидетельствуют данные на сайте Facebook.

По итогам января-июня 2014 г. Facebook получила почти 35 тыс. запросов от государственных структур на раскрытие регистрационных данных, IP-адресов, адресов электронной почты и другой информации о пользователях. Относительно второго полугодия 2013 г. этот показатель возрос на 24 %. Лидером по числу запросов – почти 15,5 тыс. – остаются США.

В то же время, количество запросов на ограничение доступа к тому или иному контенту в определенных странах мира увеличилось на 19 % за полгода. Причиной таких ограничений становятся местные законы, и большинство подобных запросов поступили из Индии, Пакистана и Турции.

Ранее компания Google сообщила, что число запросов к ней от госорганов возросло за первое полугодие на 15 % до 31,7 тыс., а за последние пять лет этот показатель увеличился на 150 % ***(Число запросов к Facebook от госорганов выросло на четверть // InternetUA (http://internetua.com/cislo-zaprosov-k-Facebook-ot-gosorganov-viroslo-na-csetvert). – 2014. – 5.11).***

***

Громадська палата Чечні ухвалила рішення створити спеціальну комісію з контролю за соціальними мережами в Інтернеті. Головне завдання,

що формально покладається на неї, – протидіяти екстремістській ідеології. «Кавказский узел» посилається на заяву неназваного представника Громадської палати.

«Саме тут (у соціальних мережах) останнім часом активно поширюються всілякі екстремістські ідеї та заклики, що справляють згубний вплив на користувачів мережі, переважно на молодіжну аудиторію, – стверджує він. – Щоб успішно протистояти цьому, будуть створюватися блогерські платформи. Вони не тільки відслідковуватимуть контент сайтів, а й оперативно реагуватимуть на наклепницькі заяви й випади проти нашої республіки».

Голова Громадської палати Г. Батаєв вважає, що найбільший, різнобічний вплив на життєдіяльність сучасного суспільства мають соціальні мережі. За його словами, це стосується тлумачення питань релігійного змісту, національних традицій і звичаїв, висвітлення подій, що відбуваються як у республіці, так і в Росії.

«Кавказский узел» посилається на висловлювання Г. Батаєва з газети «Чечня сегодня». «Ми маємо на меті створити певні платформи, з яких діятимуть інститути громадянського суспільства, – сказав він. – Завдання Громадської палати – координувати ці зусилля та сприяти досягненню успіху у цій сфері».

Водночас сайт наводить висловлювання керівника місцевої неурядової організації, який попросив не називати його імені. В останні місяці, заявив він, на різних сайтах були опубліковані аудіо- й відеозвернення релігійних та інших діячів, які часто відверто пропагують екстремістські думки. За його словами, під впливом подібних виступів молодь захоплюється ідеями джихадизму і радикалізму, вирушає воювати на Близький Схід або приєднується до збройних угруповань, що діють на Кавказі.

«З одного боку, ініціативу Громадської палати можна зрозуміти й підтримати. Однак з іншого – існує серйозна небезпека, що соцмережі потраплять під тотальний контроль. Це може обернутися переслідуванням інакодумців», – наголосив співрозмовник сайту.

Нагадаємо, що у жовтні цього року під приводом боротьби проти розповсюдження серед чеченської молоді радикальних ідей президент Чечні Р. Кадиров висунув ініціативу відімкнути на території республіки Інтернет.

Крім того, як нагадує «Кавказский узел», Р. Кадиров висловлювався за заборону у Росії Twitter, Skype та інших розміщених за кордоном інтернет-ресурсів. За його словами, вони «можуть безконтрольно поширюватися, створюючи загрози національній безпеці».

У серпні 2012 р. на території Чечні був закритий доступ до відеохостингу YouTube, на якому був розміщений трейлер на контроверсійний фільм «Невинність мусульман». Відновили доступ до YouTube на території Чечні лише у травні 2013 р., після того, як Р. Кадиров висловився за зняття обмежень.

Створена у травні 2009 р. Громадська палата Чеченської Республіки формально є постійно діючим незалежним суспільним органом з розвитку інститутів громадянського суспільства, громадського контролю та взаємодії громадян з органами державної влади ЧР і з органами місцевого самоуправління.

Сам соратник В. Путіна, представник партії «Единая Россия» Р. Кадиров є активним інтернет-користувачем. На його профіль у Instagram підписалося понад 500 тис. осіб ***(Чечні загрожує авторитарний контроль над соціальними мережами // Телекритика (http://osvita.mediasapiens.ua/material/36074). – 2014. – 4.11).***

***

СБУ захотела собирать данные о пользователях интернет-услуг

Госспецсвязи подготовила финальную версию комплексного законопроекта «Об основных положениях обеспечения кибербезопасности Украины», сообщает capital.ua.

Под прицелом любой сайт

Как выяснилось, кроме прочего, для обеспечения кибербезопасности должны быть внесены некоторые изменения в закон «О телекоммуникациях». Согласно сопроводительным материалам к проекту закона, Служба безопасности Украины предложила внести в профильный закон определение контент-провайдера. Это субъект хозяйствования, который предоставляет информационные и другие услуги через сети операторов и провайдеров телекоммуникаций. Глава Интернет ассоциации Украины Т. Попова говорит, что под такое определение может попасть в принципе любой сайт.

Согласно предлагаемым изменениям в закон «О телекоммуникациях», контент-провайдеры должны будут, также как и телекомщики, зарегистрироваться в профильном реестре, а при необходимости получать лицензии и разрешения (если какие-то из них предусмотрены законом).

Кроме того, контент-провайдеры и операторы связи должны будут сохранять и передавать субъектам обеспечения кибербезопасности (спецподразделениям уполномоченных госорганов) информацию для идентификации поставщиков услуг, а также маршрута, по которому была передана информация о соединении с абонентом. Госспецсвязи учла пожелания СБУ и отобразила их в законопроекте. Примечательно, что Минюст к тому же предлагал внести определения механизма блокирования доступа к интернет-ресурсам. Но Госспецсвязи не отобразила это предложение в финальной версии закона.

Т. Попова считает, что таким образом чиновники снова пытаются получить контроль над интернет-услугами в стране. С ней соглашается президент компании Mirohost\Imena.ua А. Ольшанский. «Внесудебная слежка за гражданами – это плохая идея. Если, конечно, мы не опираемся на опыт

России. Потому что в большинстве других стран такие методы не используются», – подчеркнул он.

По американскому образцу

Законопроект готовился по поручению Кабмина. Правительство должно было одобрить его на заседании 5 ноября. Но этого так и не произошло. «Премьер-министр А. Яценюк мотивировал это тем, что закон должен подавать новый Кабмин», – сообщил источник «Капитала» в Госспецсвязи. Он добавил, что правительство поручило снова доработать этот проект по американскому образцу и дало время на это до конца года.

Согласно предлагаемым изменениям в закон «О телекоммуникациях», контент-провайдеры должны будут, также как и телекомщики, зарегистрироваться в профильном реестре, а при необходимости получать лицензии и разрешения (если какие‑то из них предусмотрены законом)

Собеседник «Капитала» в Госспецсвязи подозревает, что на такое решение правительства повлияло киевское подразделение международной организации ISACA (Information Systems Audit and Control Association). «По крайней мере они с лета ходили с предложениями взять за основу американскую концепцию», – заявил он.

«Мы не предлагали отдельную концепцию, мы сделали для Госспецсвязи обзор принципов обеспечения кибербезопасности разных стран», – заявил «Капиталу» президент ISACA А. Янковский. По его словам, ассоциация также выступала за то, чтобы вся информация о пользователях услуг Интернета предоставлялась только по решению суда, поскольку есть ряд международных конвенций, которые охраняют права человека в этой сфере.

А. Ольшанский также говорит, что у него было много вопросов к документам, которые государство подготовило для борьбы с интернет-угрозами: «На мой взгляд, пока вместо борьбы к киберугрозами чиновники пытаются создать базу для злоупотреблений» ***(СБУ захотела собирать данные о пользователях интернет-услуг // Медіа бізнес (http://www.mediabusiness.com.ua/content/view/41272/126/lang,ru/). – 2014. – 6.11).***

***

Доступ к интернет-ресурсам, призывающим казахстанцев к участию в боевых действиях на территории Украины, заблокирован в Казахстане. Об этом сообщили Новостям Казахстана в Генеральной прокуратуре РК, передает Цензор.НЕТ.

В ведомстве напомнили, что в целях выявления и пресечения фактов распространения информации, направленной на вовлечение граждан Казахстана в иностранные вооруженные конфликты, генеральной прокуратурой совместно с уполномоченными органами на постоянной основе проводится соответствующая работа.

«По предписаниям Генеральной прокуратуры Комитетом связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан заблокирован доступ к видеоматериалам, содержащим признаки пропаганды/оправдания терроризма, а также интернет-ресурсам, имеющим признаки призывов к участию в боевых действиях на территории Украины», – говорится в ответе генеральной прокуратуры РК на запрос агентства.

Как сообщала ранее Генпрокуратура, наемники из Казахстана продолжают выезжать в «горячие точки» на территории Афганистана, Ирака, Сирии, Украины, несмотря на уголовную ответственность.

Согласно статье 162-1 Уголовного кодекса преступлением является неправомерное участие в вооруженных конфликтах или военных действиях на территории иностранного государства даже при отсутствии признаков наемничества. За совершение данного деяния предусмотрена ответственность в виде лишения свободы сроком до семи лет ***(В Казахстане заблокировали сайты, через которые вербовали наемников для боев на Донбассе // Цензор.НЕТ (http://censor.net.ua/news/310570/v_kazahstane_zablokirovali_sayity_cherez_kotorye_verbovali_naemnikov_dlya_boev_na_donbasse). – 2014. – 6.11).***

***

Чтобы ограничить экспорт шпионского ПО, власти Евросоюза решили поставить его в один список с технологиями двойного назначения, в том числе с ядерным оружием. Если какая-либо европейская компания решит продать такой продукт иностранному государству, ей нужно будет сперва получить разрешение. Нововведение стало ответом на претензии правозащитных организаций, которые утверждают, что шпионское ПО помогает подавлять гражданские свободы.

Европейские власти планируют приравнять легальное шпионское программное обеспечение, разрабатываемое местными компаниями для государственных заказчиков, к технологиям двойного назначения и поставить его в один список с ядерными реакторами, камерами со сверхвысоким разрешением и ракетным топливом. То есть теми продуктами и технологиями, которые «обычно служат гражданским целям, но могут быть использованы в военной сфере и для распространения оружия массового поражения», следует из текста на сайте Еврокомиссии.

Поправки в список продуктов и технологий двойного назначения были переданы Европарламенту и Евросовету. В случае их согласия, обновленный список, содержащий шпионское ПО, вступит в силу в конце декабря 2014 г.

Примером шпионского ПО, о котором идет речь, является FinFisher – решение, продажей которого занимается британская компания Gamma International. Согласно описанию на официальном сайте, Finfisher позволяет «выполнять удаленное наблюдение и инфицирование» и способен

предоставить «полный доступ к хранимым данным с возможностью получения контроля над целью».

В описании продукта упоминается, что он способен «получать доступ к зашифрованным данным и каналам» и позволяет «правительственным агентствам удаленно заражать необходимые системы».

FinFisher позволяет взламывать компьютеры под управлением операционных систем Windows, OS X и Linux, а также мобильные устройства на базе Android, iOS, Windows Phone, BlackBerry и Symbian. Решение позволяет получать доступ к аккаунтам сервисов электронной почты, таких как Gmail, Outlook и Yahoo, а также взламывать учетные записи Skype – сервиса, считающегося одним из самых надежных на рынке благодаря применяемым в нем технологиям шифрования данных.

Согласно документам, оказавшимся в распоряжении The Guardian, в 2010 г. Gamma International предложила за 287 тыс. дол. купить FinFisher правящему режиму в Египте для подавления оппозиции. В сентябре 2014 г. сайт Wikileaks опубликовал сведения о том, что FinFisher используется правительственными организациями в Австралии, Бахрейне, Бангладеше, Бельгии, Боснии и Герцеговине, Эстонии, Венгрии, Италии, Монголии, Нидерландах, Нигерии, Пакистане, Сингапуре, Словакии, Южной Африке и Вьетнаме.

С конца декабря 2014 г., в случае принятия обновленного списка, европейским разработчикам такого софта нужно будет получать лицензию на экспорт продукции за рубеж. Такое нововведение стало результатом дебатов относительно безопасности данного ПО. Правозащитные организации неоднократно поднимали вопрос о необходимости запретить продажу шпионского софта иностранным заказчикам, так как он – по их словам – служит целям государств, стремящихся подавить гражданские свободы.

В прошлом месяце был выпущен отчет OpenNet Initiative, в котором говорилось, что аналогичное шпионское ПО, разработанное компаниями в США и Канаде, используется в 9 странах на Ближнем Востоке и в Северной Африке для ограничения доступа к сайтам с политическим, социальным и религиозным материалом.

Тот факт, что правительства разных стран разрабатывают и используют подобное программное обеспечение, уже не секрет. На эту тему, к примеру, в августе 2014 г. на конференции BlackHat выступил директор по исследованиям компании F-Secure М. Хиппонен. «Не так давно идея о том, что западные демократические государства замешаны в разработке вредоносных программ, казалась дикостью. А как вам такая идея: что западные демократические государства оставляют лазейки в системах связи, чтобы следить за другими демократическими государствами? Это именно то, что происходит сейчас», – заявил он ***(Евросоюз приравняет шпионское ПО к ядерному оружию // InternetUA (http://internetua.com/evrosouaz-priravnyaet-shpionskoe-po-k-yadernomu-orujiua). – 2014. – 7.11).***

***

ФБР США при поддержке правоохранительных органов десятка стран закрыли более 400 доменов в анонимной сети Tor и арестовали 17 человек, предположительно вовлечённых в нелегальную деятельность, пишет Блог Imena.UA (http://www.imena.ua/blog/dark-web-arrests/).

В ходе масштабной операции правоохранительные органы закрыли подпольные сайты Cloud 9, Hydra, Pandora, Blue Sky, Topix, Flugsvamp, Cannabis Road и Black Market. Все эти ресурсы занимались торговлей запрещёнными веществами.

Кроме того, в рамках зачистки были закрыты некоторые сайты, специализировавшиеся на отмывании денег, включая Cash Machine, Cash Flow, Golden Nugget, Fast Cash.

По итогам операции ФБР получили в своё распоряжение монеты Bitcoin на сумму более 1 млн дол., а также 250 тыс. дол. наличными. Было конфисковано компьютерное оборудование, серверы, золотые и серебряные изделия, наркотики и оружие.

Часть конфискованной собственности будет уничтожена, а остальное продадут на аукционе, если суд признает вину обвиняемых. Личности задержанных пока не разглашаются.

Ранее стало известно, что сотрудники Агентства национальной безопасности США следят за пользователями анонимной сети Tor, используя программу XKeyscore.

Технология позволяет отслеживать практически любую активность обычных пользователей в Интернете по ключевым словам, поисковым запросам, IP-адресам и т. д. ***(Спецслужбы закрыли более 400 доменов в сети Tor // Блог Imena.UA (http://www.imena.ua/blog/dark-web-arrests/). – 2014. – 10.11).***

***

Українським міністрам можуть закрити доступ в Facebook, пише Корреспондент.net (http://ua.korrespondent.net/ukraine/politics/3442870-ministram-novoho-kabminu-mozhut-zaboronyty-korystuvatysia-Facebook)

Радник президента України М. Томенко заявив у вівторок, 11 листопада, що міністрам майбутнього складу уряду країни, можливо, буде заборонено вести записи в соціальній мережі Facebook.

«Ми хочемо заборонити Facebook міністрам. Розповідати, про що вони мріють, в робочий день не потрібно», – заявив М. Томенко, передає УНН.

Одним з найактивніших користувачів Facebook є глава Міністерства внутрішніх справ України А. Аваков ***(Міністрам нового Кабміну можуть заборонити користуватися Facebook // Корреспондент.net (http://ua.korrespondent.net/ukraine/politics/3442870-ministram-novoho-kabminu-mozhut-zaboronyty-korystuvatysia-Facebook). – 2014. – 12.11).***

***

Прокуратура Дніпропетровської області скерувала до суду обвинувальний акт відносно чотирьох громадян України за фактом розповсюдження в соцмережах газети «Новороссия». Про це повідомляє прес-служба прокуратури області.

Кримінальне провадження за фактом розповсюдження «Новороссии» було розпочато слідчим відділом управління Служби безпеки України в області. Трьом чоловікам та жінці інкримінують злочин, передбачений ч. 2 ст. 110 Кримінального кодексу України – посягання на територіальну цілісність і недоторканність України за попередньою змовою групою осіб.

Досудовим розслідуванням встановлено, що в травні 2014 р. ці громадяни України розповсюджували в мережі «ВКонтакте» видання газети «Новороссия» із сепаратистськими закликами зміни меж території України, «з метою залучити до вказаної злочинної діяльності інших мешканців Дніпропетровської області». Розповсюджувачів газети було затримано, трьох чоловіків було за рішенням суду заарештовано, жінка знаходиться під домашнім арештом.

У прокуратурі нагадують, що обвинуваченим загрожує покарання у вигляді позбавлення волі на строк від п’яти до десяти років з конфіскацією майна або без такої.

Державне обвинувачення в суді підтримує прокуратура області.

Нагадаємо, що на Харківщині розповсюджувач газети «Новороссия» отримав п’ять років умовно.

Як повідомляла «Телекритика», 22 липня в Кривому Розі (Дніпропетровська область) СБУ затримала чотирьох осіб, які займалися розповсюдженням газети «Новороссия». 28 серпня у Дніпропетровську СБУ вилучила в приміщенні однієї з компаній, яка доставляє поштові відправлення, 7 тис. примірників газети «Новороссия» ***(У Дніпропетровській області судитимуть чотирьох розповсюджувачів газети «Новороссия» у «ВКонтакте» // Телекритика (http://www.telekritika.ua/pravo/2014-11-12/100323). – 2014. – 12.11).***

***

Немецкая разведка планирует создать систему раннего предупреждения о готовящихся на государство кибератаках. Для этого она планирует шпионить за пользователями социальных сетей. При этом передача данных по протоколу шифрования HTTPS помехой стать не должно.

Разведка Германии в течение следующих 5 лет планирует потратить 300 млн евро на программу Strategic Technology Initiative (STI), предназначенную для слежки за пользователями социальных сетей «за пределами Германии». Об этом сообщили газета Suddeutsche Zeitung и ряд других германских СМИ. О каких именно соцсетях идет речь, не уточняется.

Они сослались на конфиденциальный документ, направленный Федеральной разведывательной службой Германии в Бюджетный комитет Бундестага. В заявке служба просила комитет в 2015 г. выделить ей на указанную программу 28 млн евро в дополнение к 6,2 млн, которые она уже получила.

Представитель правительства Германии подтвердил СМИ существование программы STI. По словам представителя, ее главная задача – построить систему раннего предупреждения о готовящихся в отношении Германии кибератак. Какую-либо дополнительную информацию о программе и ее бюджете он не сообщил.

Система должна работать в режиме реального времени. Она также должна быть способна осуществлять мониторинг зашифрованного интернет-трафика и расшифровывать его.

В настоящее время система находится на этапе строительства. В июне 2015 г. правительство Германии планирует протестировать прототип системы. Он сможет выполнять мониторинг открытых бесед пользователей в Twitter и различных блогах.

Помимо программы STI, Федеральная разведывательная служба Германии хочет потратить 4,5 млн евро на взлом и мониторинг зашифрованного интернет-трафика, передаваемого по протоколу HTTPS.

По данным издания Spiegel, часть своего бюджета служба планирует потратить на еще одну программу – под названием Nitidezza. Ее суть заключается в покупке на черном рынке неизвестных или неопубликованных уязвимостей, которые бы смогли облегчить работу агентов. До 2020 г. на эти цели зарезервировано 4,5 млн евро.

Эта информация о немецкой разведке заставляет вспомнить Агентство национальной безопасности (АНБ) США ***(Разведка будет шпионить за пользователями соцсетей // Украинский телекоммумникационный портал (http://portaltele.com.ua/news/internet/razvedka-budet-shpionit-za-polzovat.html). – 2014. – 13.11).***

***

Власти США собирают данные с мобильных телефонов миллионов американцев, используя специальную аппаратуру, установленную на небольших легкомоторных самолетах Cessna. Они совершают вылеты из американских аэропортов и покрывают практически всю территорию США.

Соответствующая программа службы судебных приставов реализуется с 2007 г. Фальшивые устройства связи устанавливались на самолетах Cessna, совершающих полеты, по крайней мере, из пяти крупных аэропортов США.

Оборудование действует по принципу сотовых вышек телекоммуникационных компаний, сообщает ТАСС со ссылкой на The Wall Street Journal. Цель данной программы – устанавливать местонахождение мобильных телефонов лиц, которые находятся под следствием, в том числе убийц и наркоторговцев. Подобные устройства используются американскими

военными и разведкой, в частности, в зонах военных конфликтов для поиска людей, подозреваемых в терроризме.

Технология слежения с самолетов позволяет определить местонахождение подозреваемого с точностью до трех метров. При этом в поле зрения ведомства попадают не только преступники, но и обычные американцы, против которых не выдвигалось никаких обвинений.

Власти могут также дистанционно блокировать сигнал с телефона подозреваемого и копировать данные с его аппарата, в том числе текстовые сообщения и фотографии. Упомянутая программа является очередным примером того, что власти США ведут тайную слежку за миллионами граждан.

Минюст США отказался комментировать сообщения о существовании такой программы, заявив, что ее обсуждение может предоставить преступникам или иностранным государствам важную информацию о разведывательных способностях США ***(Власти США собирают данные с телефонов миллионов американцев с помощью самолетов // InternetUA (http://internetua.com/vlasti-ssha-sobirauat-dannie-s-telefonov-millionov-amerikancev-s-pomosxua-samoletov). – 2014. – 15.11).***

Проблема захисту даних. DDOS та вірусні атаки

Facebook выпустила открытый инструмент для мониторинга операционных систем. Новая бесплатная программа Osquery от Facebook позволит администраторам создавать запросы на базе SQL по различным параметрам системы и таким образом собирать данные о запущенных процессах, загруженных модулях и открытых сетевых соединениях.

Osquery предназначена в первую очередь для крупных организаций, где инженерам нужно быстро провести диагностику систем и выявить возможные бреши в безопасности. С этой проблемой столкнулись в самой Facebook.

«Для нас стало очевидно, что исследование низкоуровнего поведения операционных систем – вовсе не уникальная для Facebook проблема», – говорят в компании.

Osquery последние несколько месяцев «обкатывалась» в рамках бета-тестирования с участием ряда компаний. Более того, чтобы окончательно устранить любые проблемы с программой, Facebook предлагает награду в 2500 дол. за каждую найденную уязвимость.

Приложение полностью открыто, исходный код можно взять на GitHub. Больше подробностей – на сайте проекта ***(Facebook выпустила открытый инструмент для мониторинга операционных систем // InternetUA (http://internetua.com/Facebook-vipustila-otkritii-instrument-dlya-monitoringa-operacionnih-sistem). – 2014. – 3.11).***

***

Как «взламывают» компьютер, полностью изолированный от сети

М. Гури из лаборатории кибернетики университета Бен-Гуриона вместе со своим научным руководителем проф. Ю. Аловичем продемонстрировали уникальную стратегию несанкционированного доступа к данным. Им удалось создать на базе обычного смартфона прослушивающее устройство, воспринимающее на расстоянии 7 метров сигналы от компьютера, не имеющего вообще никаких подключений к сети.

Компьютер предварительно был «заражен» вредоносной программой, заставляющей видеокарту компьютера испускать радиосигналы, в то время как кабель от видеокарты к дисплею служил антенной. Запущенная на смартфоне специальная программа позволяет принимать от компьютера трансляцию любых сигналов, передаваемых вредоносной программой – например, во время набора пароля.

Основным «недостатком» схемы в настоящее время является низкая скорость передачи данных, на уровне самого первого поколения модемов – пересылка файла размером в полгигабайта, к примеру, займет 11 часов. Тем не менее, для короткой текстовой информации (логин и пароль) существующей скорости вполне достаточно.

Разумеется, установить «вирус-излучатель» на должным образом защищенный компьютер – задача сама по себе сложная. Однако опасность применения этой схемы взлома против компьютеров, установленных в правительственных офисах, банках, больницах и военных базах все же нельзя сбрасывать со счетов ***(Как «взламывают» компьютер, полностью изолированный от сети // InternetUA (http://internetua.com/kak--vzlamivauat--kompuater--polnostua-izolirovannii-ot-seti). – 2014. – 5.11).***

***

На конференции по компьютерной безопасности в США ученые из университета Ньюкасла представили отчет, в котором говорится о наличии серьезных уязвимостей в новых чипах для банковских карт. Как сообщает RT, злоумышленники могут списать с чужого счета до 1 млн дол., просто находясь рядом с владельцем карты.

Новые чипы для банковских карт позволяют оплачивать покупки до 31 дол., не вставляя «пластик» в считывающие устройства или не вводя ПИН-код. Однако исследователи доказали, что микрочипы не распознают заданные лимиты при покупках в другой валюте.

Таким образом, злоумышленники могут списать с чужого счета до 999 999,99 в различных денежных единицах, всего лишь поднеся кард-ридер близко к заинтересовавшей их банковской карте.

«В настоящее время самым уязвимым местом в банковских картах является магнитная полоса, – говорит профессор А. ван Мурсел, один из

авторов исследования. – После того как мы исключим это уязвимое место, следующей целью преступников станет бесконтактная оплата. Если мы смогли найти недостатки, то и злоумышленники смогут это сделать. В этом и заключается цель нашего исследования: найти потенциально уязвимые места и устранить их до того, как карточки войдут в обиход» ***(Хакеры могут украсть до 1 миллиона долларов с новых банковских карт, просто стоя рядом // InternetUA (http://internetua.com/hakeri-mogut-ukrast-do-1-milliona-dollarov-s-novih-bankovskih-kart--prosto-stoya-ryadom). – 2014. – 5.11).***

***

Украинский разработчик антивирусного программного обеспечения под брендом «Zillya! Антивирус» получил экспертное заключение Государственной службы специальной связи и защиты информации (ГССЗЗИ) на продукт «Zillya! Антивирус для Бизнеса».

На официальном сайте компании-разработчика сказано, что антивирус получил уровень оценки Г2, что позволит компании работать со всеми категориями пользователей антивирусов в государственном секторе Украины наряду с сертифицированными продуктами компаний ESET, Norton, Kaspersky.

По словам технического директора антивирусной лаборатории О. Сыча, обеспечение информационной защиты государства с применение антивирусного ПО иностранной разработки – это путь, от которого постепенно отказываются ведущие государства мира, осознающие потенциальные угрозы, связанные с уровнем доступа данного ПО к информации на компьютере пользователя. Применение украинского антивируса в государственных органах, вне зависимости от того, будет этим продуктом «Zillya! Антивирус для Бизнеса» или нет, автоматически повысит уровень защищенности нашего государства от киберугроз за счет возможности оперативно реагировать на возникающие проблемы информационной безопасности, накопления профессионального опыта противодействия киберугрозам украинскими специалистами, а не консультантами, привлекаемыми извне.

К тому же, в текущей экономической ситуации, украинские продукты – это значительный шаг к экономии бюджетных средств.

Напомним, что 3 июля 2014 г. Верховная Рада Украины приняла постановление, в котором рекомендовала Кабинету Министров Украины обеспечить внедрение украинского антивирусного программного обеспечения в государственных органах Украины ***(Украинский антивирус готов к защите от киберугроз // Vido.com.ua (http://vido.com.ua/article/10046/ukrainskii-antivirus-ghotov-k-zashchitie-ot-kibierughroz/). – 2014. – 5.11).***

***

С завидной регулярностью в сети появляются сообщения о взломах, утечках данных, хищениях информации и других кибер-проблемах, актуальных для нашего времени. При этом подавляющее большинство пользователей каждый день используют различные мессенджеры для общения, а эти программы и сервисы зачастую подвергаются наибольшей критике из-за разного рода уязвимостей. Специалисты некоммерческой организации Electronic Frontier Foundation решили расставить все точки над «i» в данном вопросе и исследовали большинство современных мессенджеров по семи ключевым показателям.

В частности, специалисты EFF поставили перед каждым мессенджером семь простых вопросов, ответы на которые могут быть исключительно положительными или отрицательными:

– Зашифровано ли сообщение во время передачи?

– Зашифровано ли оно от провайдера, в сети которого выполняется передача?

– Можете ли вы быть уверены в личности собеседника?

– Остается ли история переписки защищена, если злоумышленник похитит актуальные ключи?

– Открыт ли код для независимой проверки?

– Задокументирована ли система безопасности?

– Был ли код проверен независимыми специалистами?

Всего семь вопросов, но они сразу же дают наглядную расстановку сил среди мессенджеров. В частности, самыми безопасными были названы приложения ChatSecure, Signal и CryptoCat, которые получили положительные отметки по каждому из семи пунктов. Однако их никак нельзя назвать массовыми, популярными среди большого числа пользователей.

А вот в массовом сегменте лидерство у Apple, чьи iMessage и FaceTime набрали по 5 баллов из 7 возможных. Что касается непосредственных конкурентов, то все они получили более низкие оценки: AIM – 1 балл, BlackBerry Messenger – 1 балл, Facebook Chat – 2 балла, Google Hangouts – 2 балла, Secret – 1 балл, Skype – 2 балла, Viber – 1 балл, WhatsApp – 2 балла. Обращает на себя внимание мессенджер от П. Дурова Telegram, который выступил на уровне решений Apple и набрал 5 баллов, хотя высокой популярностью похвастаться не может.

На фоне конкурентов среди по-настоящему массовых решений iMessage и FaceTime показали достойные результаты. И хотя сервисы Apple периодически подвергаются критике, особенно в связи с инициативой PRISM, по крайней мере, несколько базовых параметров в них можно назвать безопасными. Ближайшие конкуренты, как следует из исследования EFF, не могут похвастаться и этим ***(iMessage и FaceTime самые безопасные решения для общения // Украинский телекоммумникационный портал***

(http://portaltele.com.ua/news/software/imessage-i-facetime-samye-bezopasnye-resheniyami-dlya-o.html). – 2014. – 6.11).

***

В сети начал активно распространяться вирус, который угрожает устройствам Apple.

Данные сотен тысяч владельцев устройств Apple могут оказаться под угрозой из-за семейства вредоносного ПО WireLurker. Об этом пишет РБК со ссылкой на отчет компании Palo Alto Networks.

Преимущественно вирус угрожает китайским пользователям компьютеров и гаджетов Apple.

ПО получило свое название из-за способности распространяться с компьютеров Macintosh на мобильные устройства через USB-подключение. Источником заражения стал Maiyadi, сторонний магазин приложений для Macintosh, который является альтернативой официальному магазину приложений Mac App Store. При этом, подобно традиционному вирусу, WireLurker может заражать другие программы. По данным Palo Alto, им было заражено 467 приложений для OS X, которые были загружены в общей сложности 356 тыс. 104 раза.

После того как вирус попадает на Macintosh, он может через USB-подключение заразить мобильные устройства Apple – планшеты iPad и смартфоны iPhone. Попав на устройства, WireLurker загружает на них вредоносные приложения через технологию, обычно используемую для загрузки корпоративных приложений, минуя AppStore. При этом вредоносные приложения могут быть установлены на все гаджеты, а не только на те, которые подверглись процедуре джейлбрейка. Кроме того, вирус заражает уже установленные на смартфон приложения с помощью вредоносного кода ***(Появился опасный вирус для устройств Apple // FaceNews.ua (http://www.facenews.ua/news/2014/254240/). – 2014. – 6.11).***

***

Решения безопасности для Mac OS X по-прежнему не обеспечивают полноценную защиту от червя iWorm. Речь идет о вирусе, впервые обнаруженном в сентябре этого года и заразившем порядка нескольких тысяч компьютеров под управлением операционной системы Apple.

Интересно, что в целях обнаружения и удаления iWorm, разработчики компании выпустили соответствующее обновление для своего антивирусного движка XProtect. Однако по словам экспертов безопасности из компании Synack, это обновление позволяет выявить лишь активный установщик вирусного ПО, который запускается лишь один раз при заражении системы. Таким образом, те компьютеры, которые были заражены еще до выхода новой версии XProtect, все еще остаются инфицированными.

Напомним, что iWorm представляет собой бэкдор, способный похитить конфиденциальную информацию жертвы и устанавливаемый на систему без

эксплуатации какой-либо уязвимости. В этих целях создатели вируса обманным путем заставляют владельца компьютера самостоятельно установить iWorm. По данным аналитиков, в настоящее время во вредоносной сети насчитывается порядка 18 тыс. зараженных систем ***(Разработчики Apple не смогли обеспечить надежную защиту от iWorm // InternetUA (http://internetua.com/razrabotcsiki-Apple-ne-smogli-obespecsit-nadejnuua-zasxitu-ot-iWorm). – 2014. – 5.11).***

***

Троян Backoff, использующийся для заражения PoS-устройств, стало сложнее обнаруживать и анализировать. Об этом сообщает исследователь Fortinet Х. К. Чань в блоге компании.

Еще в августе представители Министерства внутренней безопасности и Компьютерной группы реагирования на чрезвычайные ситуации США предупреждали о существовании тяжелодетектируемого вредоносного ПО, нацеленного на PoS-устройства. Тогда специалисты ведомств обнаружили ряд уязвимостей, которые эксплуатировались киберпреступниками для получения доступа к платежным терминалам. Несмотря на предупреждения, этот вид вредоносного ПО до сих пор широко используется для взлома PoS-девайсов.

Исследователям Fortinet удалось заполучить новый вариант Backoff, который выдает себя за медиапроигрыватель (mplayerc.exe). Ранее вирус маскировался под Java-компонент, прописывающий себя в разделы автозагрузки системного реестра. Модифицированная версия вредоноса получила название Backoff ROM.

В отличие от предыдущих версий, для саморазмножения вирус использует функцию WinExec вместо CopyFileA. Для усложнения процесса анализа названия функций переводятся в хешированные значения, которые расшифровываются отдельной функцией. Вдобавок к этому, Backoff ROM содержит «черный список» из 29 процессов, которые игнорируются вредоносом.

Похищенные данные платежных карт хранятся в зашифрованном файле locale.dat. Перед соединением с C&C-сервером вирус проверяет наличие файла, после чего расшифровывает его и пересылает через POST-запрос по порту 443. Трафик между сервером и вредоносом шифруется.

Интересно, что новая версия Backoff не может перехватывать нажатия клавиш. Тем не менее, исследователи полагают, что такое изменение носит временный характер, и функционал кейлоггера вернется во вредонос уже в ближайшем времени ***(PoS-троян Backoff стало труднее обнаружить и проанализировать // InternetUA (http://internetua.com/PoS-troyan-Backoff-stalo-trudnee-obnarujit-i-proanalizirovat). – 2014. – 6.11).***

***

Согласно данным отчета исследователя безопасности компании Trustwave SpiderLabs О. Хафифа, новый вектор веб-атаки Reflected File Download (отраженная загрузка файла) позволяет отправлять на ПК жертвы исполняемые файлы посредством перехода пользователя по вредоносной ссылке на домены легитимных провайдеров. После загрузки файла злоумышленник получает полный контроль над атакуемой машиной. Такой метод действий значительно облегчает фишинг, поскольку пользователь даже не подозревает об угрозе.

Злоумышленники могут использовать отраженную загрузку файла для похищения персональных данных пользователей, получить полный контроль над браузером Google Chrome, включая зашифрованные соединения, а также эксплуатировать уязвимости в установленном программном обеспечении.

Спецификации URI предусматривают передачу параметров в URI через использование точки с запятой («;») в универсальном идентификаторе ресурса. Данную функцию поддерживают многие веб-сервисы. Проще говоря, если веб-сайт принимает параметры из адресной строки, ему можно передавать произвольный контент. Тем не менее, не все браузеры работают корректно с параметрами после точки с запятой и если там поместить содержимое файла, браузер воспримет параметры как файл и сохранит его на ПК пользователя.

Несмотря на то, что данная атака не предусматривает несанкционированное выполнение кода, некоторая опасность все же существует. Поскольку пользователь уверен, что загружает файлы с легитимного сервера, его легко можно подтолкнуть к запуску программы. Тем более, что ОС Windows 7 запускает выполнение без предупреждения файлов .bat или .cmd если в их названиях присутствуют слова «setup», «install» и «update» ***(Уязвимость с «отраженной» загрузкой файла позволяет получить контроль над ПК пользователя // InternetUA (http://internetua.com/uyazvimost-s--otrajennoi--zagruzkoi-faila-pozvolyaet-polucsit-kontrol-nad-pk-polzovatelya). – 2014. – 7.11).***

***

Хакеры придумали новый способ похищения пользовательских данных в Интернете – теперь они воруют информацию, используя черновики популярных почтовых сервисов Yahoo Mail и Gmail.

Теперь программистам в этих компаниях предстоит срочно устранить обнаруженные уязвимые места.

К настоящему времени удалось установить, что киберпреступники выполняют взлом сразу в несколько этапов: сначала хакеры устанавливают обновленный интерпретатор скриптового языка Python и затем с его помощью выполняют произвольный код. А на завершающем этапе интернет-воры внедряют в хостингах почтовых сервисов управляющий код ***(Хакеры воруют пользовательские данные в Интернете // Світ24.net***

(http://svit24.net/technology/117033-khakery-voruyut-pol-zovatel-skie-dannye-v-internete. – 2014. – 9.11).

***

6 листопада українські Кібервійська заблокували 14 сатів терористів. Загалом, «лежало» 46 сайтів проросійських організацій, терористів та сепаратистів. Про це повідомив на своїй сторінці у Facebook куратор кібервійськ Є. Докукін.

Зокрема, заблоковано сайти: без-вести.рф, ungu.org, pravdatoday.info, bne.su, lvs-global.ru, slemtt.myjino.ru, odessa-antimaydan.com, новорус.рф, novorossia.co, nol.su, dnrepublic.info, ukrnovosti.info, donetsk-gov.su та k61.dn.ua.

За словами експерта, тривалий час «лежав» сайт molotpravdu.com.

У кібервійськах зазначили, що в липні було закрито 7 сайтів, 15 сайтів у серпні, 5 сайтів у вересні, rusblok.com і ще 3 сайти у жовтні.

Операція зі знищення сайтів терористів називається «Відплата» і вона триває.

«Сьогодні лежали 46 сайтів терористів. DDoS атаки – це артилерія Українських Кібер Військ. Яка працює і в день, і в ночі» – зазначили хакери ***(За останню добу кібервійська заблокували 14 сайтів терористів // «Вголос» (http://vgolos.com.ua/news/za_ostannyu_dobu_kiberviyska_zablokuvaly_14_saytiv_terorystiv_162742.html. – 2014. – 7.11).***

***

Украинский хакер Е. Докукин заблокировал новый счет боевиков в Яндекс.Деньги. Хакер уточнил, что в системе Яндекс.Деньги кошелек уже заблокировали, причем еще в октябре. А в WebMoney счета отказались блокировать.

За месяц не получилось их убедить. «Таким образом, я своими действиями остановил финансирование терроризма в системе Яндекс.Деньги. Украинские кибервойска нанесли очередной удар по сепаратистам и террористам», – отметил хакер.

Напомним, что ранее киевский программист, который называет себя «белым хакером» заблокировал сайт скандального О. Царева. Хакер рассказал, что блокировка ресурса заняла немало времени, так как руководство украинской компании Hosting.ua add долго отказывалось закрывать его, ссылаясь на законодательство.

До этого на сайте экс-регионала О. Царева, который активно поддерживает членов «ДНР» и «ЛНР», регулярно публиковались новости с антиукраинской пропагандой ***(Украинский хакер заблокировал счета «ДНР» и «ЛНР» // Голая Пристань (http://golapristan.com/ukrnews/34672-ukrainskiy-haker-zablokiroval-scheta-dnr-i-lnr.html). – 2014. – 8.11).***

***

Эксперты ИБ-компании «Доктор Веб» сообщили о новом трояне, заражающем Android-устройства. Примечательно, что вредоносное ПО, получившее название Android.Becu.1.origin, встроено прямиком в образ операционной системы. Троян способен без ведома пользователей загружать, устанавливать и удалять приложения, а также блокировать SMS-сообщения с определенных номеров.

По данным «Доктор Веб», троян инфицирует мобильные устройства среднего класса, например, UBTEL U8, H9001, World Phone 4, X3s, M900, Star N8000, ALPS H9500 и т. д. Вредонос активизируется при каждом включении зараженного смартфона, а также при получении SMS-сообщения. Одним из наиболее распространенных путей попадания трояна на устройства эксперты называют модифицированные злоумышленниками прошивки, которые пользователь загружает из сети и устанавливает самостоятельно.

Стоит отметить, что полностью удалить вредонос довольно сложно, поскольку он встроен непосредственно в операционную систему. В связи с этим эксперты советуют «заморозить» его в меню управления приложениями (найти Android.Becu.1.origin в списке установленных программ и нажать «Отключить») и удалить установленные вредоносом вспомогательные компоненты. Пользователи с правами администратора также могут удалить его основные компоненты вручную или установить неинфицированный образ ОС. Тем не менее нужно помнить, что оба процесса могут вызвать потерю информации и работоспособности устройства ***(Обнаружен новый троян, встроенный в образ платформы Android // InternetUA (http://internetua.com/obnarujen-novii-troyan--vstroennii-v-obraz-platformi-Android). – 2014. – 9.11).***

***

Как следует из сообщения исследователей безопасности компании Trend Micro, им удалось выявить новую технику проведения вредоносных кампаний, которая упрощает злоумышленникам реализацию фишинговых атак. Конечной целью нападения при этом по-прежнему остается хищение финансовой информации и конфиденциальных данных держателей банковских карт.

Новая методика, получившая название Operation Huyao, не только сокращает время и количество усилий, необходимых инициаторам фишинговой кампании, но и делает вредоносные действия более незаметными для жертв.

Так, в ходе стандартных нападений такого типа хакеры вынуждены создавать реалистичную копию легитимного веб-сайта, пользователей которого они намерены скомпрометировать. Однако исследователь Н. Хаяси обнаружил, что в настоящее время злоумышленники используют специальные «прокси программы».

«Прокси ретранслирует трафик между веб-сайтом и жертвой, а также управляет отображаемым контентом независимо от используемого устройства. Пока пользователь лишь просматривает ресурс, он видит его оригинальное содержание», – поясняет Н. Хаяси.

Лишь при попытке осуществить покупку упомянутая «прокси программа» перенаправляет жертву на поддельную страницу, где и происходит хищение конфиденциальных данных ***(Хакеры разработали упрощенный метод проведения фишинговых атак // InternetUA (http://internetua.com/hakeri-razrabotali-uprosxennii-metod-provedeniya-fishingovih-atak). – 2014. – 9.11).***

***

Kaspersky Lab объявила о раскрытии новой кампании кибершпионажа Darkhotel. Целью злоумышленников в первую очередь стали остановившиеся в отелях премиум-класса бизнесмены и высокопоставленные лица.

Кроме целевых атак применялись также методы массового заражения пользователей файлообменных сетей, из-за чего в настоящее время по всему миру скомпрометированы тысячи компьютеров. Среди жертв кампании – генеральные директора, вице-президенты, а также топ-менеджеры по продажам и маркетингу предприятий различных сфер деятельности. Киберпреступники действовали незаметно в течение как минимум 7 лет.

Владеющие корейским языком злоумышленники распространяли вредоносное ПО для слежки тремя способами: через файлообменные и P2P-сети, целевые атаки по электронной почте, а также с помощью общественных Wi-Fi-сетей в некоторых отелях Азии. Последний из перечисленных способов нацелен на высокопоставленных лиц, которые ведут бизнес и привлекают инвестиции в странах Азии, поэтому заслуживает особого внимания.

Механика такого рода атаки была тщательно продумана: после того, как жертва заселялась в отель и подключалась ко взломанной Wi-Fi-сети, указывая свою фамилию с номером комнаты, ей автоматически предлагалось скачать обновление для популярного ПО – GoogleToolbar, Adobe Flash или Windows Messenger. В действительности запуск инсталлятора приводил к установке бэкдора, который помогал киберпреступникам оценить степень своего интереса к жертве и необходимость доставки более сложных инструментов. Среди них – кейлоггер, троянец Karba, собирающий информацию о системе и установленных защитных продуктах, а также модуль, ворующий сохраненные пароли в Firefox, Chrome и Internet Explorer вкупе с данными доступа к ряду сервисов включая Twitter, Facebook и Google.

Другой вектор атаки этой же группировки предполагает рассылку целевых писем по электронной почте с вредоносными модулями. Рассылки нацелены на предприятия оборонной промышленности, а также государственный сектор и общественные организации. Последние несколько

лет вложением к этим письмам служил эксплойт для уязвимостей в ПО Adobe, либо же они содержали ссылки на веб-ресурсы, эксплуатирующие неизвестные ранее уязвимости браузера Internet Explorer.

Другие способы заражения менее изощрены и таргетированы: к примеру, злоумышленники распространяют троянца через японские файлообменные ресурсы в составе архивов под видом дешифровщиков для видео-файлов, которые набирают десятки тысяч скачиваний.

«Данная атака не просто таргентирована – это точно просчитанная операция. Однако наряду с такой хирургической точностью мы наблюдаем классические почтовые рассылки и вовсе нецелевое распространение троянца через файлообменные сети – скорее всего, злоумышленники решали сразу несколько задач в рамках одной кампании, – комментирует В. Камлюк, ведущий антивирусный эксперт Kaspersky Lab. – Помимо использования надежного защитного ПО мы рекомендуем с осторожностью относиться к обновлениям ПО во время путешествий – лучше позаботиться об этом до начала поездки. Использование технологий VPN или хотя бы HTTPS-протокола при выходе в Интернет в путешествии также является необходимой мерой по защите от подобных атак».

Все вредоносные компоненты, применяемые злоумышленниками в кампании кибершпионажа Darkhotel, выявляются и нейтрализуются защитными продуктами Kaspersky Lab ***(Kaspersky Lab раскрывает кампанию кибершпионажа Darkhotel // ITnews (http://itnews.com.ua/news/74883-kaspersky-lab-raskryvaet-kampaniyu-kibershpionazha-darkhotel). – 2014. – 10.11).***

***

Израильские инженеры из университета Бен-Гурион разработали технологию AirHopper, которая позволяет взломать любой компьютер при помощи FM-приёмника в мобильном телефоне, пишет Блог Imena.UA (http://www.imena.ua/blog/computer-air-gap-near-mobile-phone/).

Для осуществления взлома достаточно просто заразить компьютер определённым вредоносным кодом. При этом, ни телефон, ни компьютер не требуется подключать к любой современной беспроводной связи.

В паре с указанным кодом программа AirHopper получает данные от излучения монитора компьютера, а также, от нажатия клавиш на клавиатуре. Данные собирает приёмник, работающий в FM-диапазоне. Другие подробности нового метода пока что не опубликованы.

Как сообщается, AirHopper имеет эффективную дальность работы до 7 м и, так как он получает радиосигналы FM, не имеет никаких проблем с преградами в виде стен.

Ранее специалист по информационной безопасности доказал, что хакеры могут довольно легко получить доступ ко всей электронике самолёта по Wi-Fi посредством обычных компьютеров, которые установлены на каждом месте для развлечений в полёте ***(Израильские инженеры взломали***

компьютер при помощи FM-приёмника // Блог Imena.UA (http://www.imena.ua/blog/computer-air-gap-near-mobile-phone/). – 2014. – 10.11).

***

День парламентских выборов в Украине сопровождался множеством попыток хакерского взлома и DDoS-атаками на сайт ЦИК.

Однако в отличие от внеочередных выборов Президента, киберпреступникам не удалось достичь хоть каких-нибудь заметных успехов, говорится в анализе группы «Кибероборона».

Специалисты группы выделяют несколько инцидентов.

Так, утром в субботу, за день до выборов, в российских СМИ появилась новость о якобы блокировке сайта ЦИК. Как оказалось, киберпреступники то ли по ошибке, то ли умышленно взломали совершенно другой веб-ресурс – vyborkom.org, который уже давно не использовался для освещения процесса выборов. Впоследствии сайт был отключен самим владельцем.

Кроме того, в день выборов некоторые СМИ написали о взломе базы данных окружной комиссии № 217. Как выяснили специалисты киберкоманды CERT-UA и Госспецсвязи, утром 26 октября под учетной записью председателя окружной комиссии (всего системой предусмотрено 4 учетных записи: администратора, председателя и двух операторов) в систему зашел неизвестный пользователь, который подключил к консольному компьютеру USB-накопитель с вредоносным ПО. Однако штатный антивирус обнаружил и удалил вредоносный файл, который был классифицирован как «сетевой червь».

В любом случае, информация о взломе не соответствовала действительности, поскольку понятия «база данных окружной комиссии» не существует, подчеркивают в CERT-UA. Дело в том, что в состав электронной автоматизированной системы «Выборы» входит единая база данных, которая размещена исключительно на серверном оборудовании ЦИК. Тем не менее, в целях профилактики ИТ-служба ЦИК изменила пароли доступа к данным для пользователей ОИК № 217.

Отдельно стоит выделить DDoS-атаку на сайт ЦИК. С утра 25 октября интернет-провайдеры зафиксировали подозрительную сетевую активность, направленную на сайт cvk.gov.ua. Позже эта активность была классифицирована как DDoS-атака. Эксперты команды CERT-UA проанализировали журналы сетевых операций провайдеров и пришли к выводу, что в DDoS-атаках использовались следующие технологии: UDP flood, DNS amplification и TCP SYN flood. Однако суммарная мощность атак была относительно невелика. Пиковое значение атаки на одно из зеркал сайта составило лишь около 600 Мбит/с, что не могло сильно повлиять на работоспособность веб-ресурса. Для защиты от атак в ЦИК были приняты меры по развертыванию средств сетевой защиты.

В CERT-UA проанализировали географическое распределение источников атак. Анализ показал, что больше всего атак выполнялось из РФ, Германии, США, Польши и Украины ***(Специалисты проанализировали кибератаки во время виборов // Polittech.org (http://polittech.org/2014/11/10/specialisty-proanalizirovali-kiberataki-vo-vremya-vyborov/). – 2014. – 10.11).***

***

Аналитики компании Shape Security, занимающейся безопасностью данных, установили, что хакеры часто используют черновики писем почтовых сервисов Gmail и Yahoo! чтобы контролировать пользовательские устройства, пишет Блог Imena.UA (http://www.imena.ua/blog/hackers-using-gmail-drafts/).

Что характерно, такой метод слежки весьма сложно определить. Атака проходит в 2 этапа: сначала хакеры инфицируют машину через простую вредоносную программу, которая устанавливает Python на пользовательское устройство.

Далее, используя почту, хакеры применяют черновики электронных писем для запуска командных и управляющих запросов на заражённых системах, позволяя «сливать» данные с инфицированных устройств.

Данный вид уязвимости опасен тем, что хакеры используют черновики писем. Это, в свою очередь, приводит к тому, что ни одно электронное сообщение не передаётся через шлюз безопасности ***(Хакеры шпионят за пользователями, используя черновики писем // Блог Imena.UA (http://www.imena.ua/blog/hackers-using-gmail-drafts/). – 2014. – 11.11).***

***

Прошло более четырех лет с момента обнаружения одной из сложнейших и опаснейших вредоносных программ – червя Stuxnet – но в этой истории по-прежнему много загадок.

До сих пор неизвестно, кто стоял за разработкой программы, и какую именно цель преследовала вся операция. Однако есть следы, указывающие, откуда была совершена атака. Эксперты Kaspersky Lab делятся информацией о первых пяти жертвах, через которые Stuxnet попал в мировую сеть.

С самого начала специалисты были уверены в том, что вся операция носила таргетированный характер. Код вредоносной программы был явно написан профессионалами, кроме того, были найдены следы применения чрезвычайно дорогих эксплойтов нулевого дня. Однако до сих пор было неизвестно, какие компании приняли первый удар, и как в итоге вредоносная программа попала в блоки управления газовыми центрифугами, предназначенными для получения обогащенного урана на критически важных объектах.

В ходе нового исследования удалось установить, что первые пять компаний, подвергшихся атаке, работали в сфере разработки промышленных

систем или поставки соответствующих комплектующих. Пятая по счету жертва наиболее интересна – помимо продуктов для индустриальной автоматизации она также производит центрифуги для обогащения урана – именно на них, как предполагается, был нацелен Stuxnet.

Очевидно, злоумышленники рассчитывали, что компании будут обмениваться данными со своими клиентами – например, заводами по производству обогащенного урана – тем самым прокладывая путь вредоносным программам к их конечной цели. Как показала история, план сработал.

«Анализ сферы деятельности организаций, которые первыми стоят в списке жертв, позволяет нам понять, как была спланирована вся операция Stuxnet. Это яркий пример косвенной атаки через цепочки поставщиков, в рамках которой вредоносные программы попадают от предполагаемых бизнес-партнеров жертвы в ее инфраструктуру. Давно известно, что Stuxnet – одна из самых сложных и продуманных кибератак из тех, о которых мы знаем. Выбор первых целей позволяет наглядно понять, насколько тщательно была проведена подготовка к ней», – поясняет А. Гостев, главный антивирусный эксперт Kaspersky Lab.

Еще одной интересной находкой исследования является опровержение одной из теорий о способе первоначального заражения, использованном злоумышленниками. Поначалу, расследующие инциденты специалисты предположили, что червь попал к жертвам через USB-накопители, подключенные к компьютеру. Однако по меньшей мере в случае первых жертв это не соответствует действительности – анализ следов самой ранней атаки показал, что первый экземпляр Stuxnet был скомпилирован за считанные часы до заражения. За такой короткий промежуток времени крайне маловероятно успеть собрать вредоносную программу, записать ее на USB-носитель и обеспечить доставку на компьютер жертвы. Скорее всего, злоумышленниками был использован иной способ заражения ***(Kaspersky Lab публикует подробности атаки на ядерный проект Ирана // ITnews (http://itnews.com.ua/news/74898-kaspersky-lab-publikuet-podrobnosti-ataki-na-yadernyj-proekt-irana). – 2014. – 11.11).***

***

Исследователи ИБ-компании ESET проанализировали вредоносный инструмент, который одна из подозреваемых в связи с Российским правительством группировок, известная как Sednit, APT 28 и Sofasy, использовала для хищения ценной информации из физически изолированных сетей.

Специалисты изучили вредоносную программу под названием Win 32/USBStealer, которая использовалась злоумышленниками по крайней мере с 2005 года в кампаниях, нацеленных на правительственные организации стран Восточной Европы. В настоящее время существует несколько модификаций этой программы.

Согласно анализу ESET, в начале, замаскированный под легитимное российское приложение USB Disk Security файл-носитель (дроппер), в котором содержится USBStealer, инфицирует подключенный к интернету ПК правительственной организации. Затем дроппер проводит мониторинг на наличие съемных дисков и в случае обнаружения таковых копирует вредоносную программу на диск. Его файл автозапуска модифицирован таким образом, что выполнение USBStealer происходит при вставке диска в другой ПК. На этом этапе вредонос маркирует USB-накопитель как использованный на машине, подключенной к Интернету.

При подключении к компьютеру с изолированной сетью, инфицированный накопитель внедряет в него вредоносную программу. Имя машины регистрируется на съемном диске, что позволяет преступникам определить устройства, к которым они могут получить доступ.

Когда USB-накопитель опять подключается к компьютеру с интернет-соединением, оператор вредоносной программы внедряет серию команд, предназначенных для извлечения данных. Исполнение этих команд начинается после подключения накопителя к ПК в закрытой сети.

Данная атака возможна только в том случае, если на компьютере жерты активирована функция автозапуска. По словам специалистов, в 2009 г. в новом обновлении Windows эта функция была деактивирована, однако подобный метод действий может принести результаты, если учесть, что большинство изолированных компьютерных систем являются устаревшими из-за отсутствия интернет-подключения ***(Хакеры используют вредоносное ПО для хищения данных из закрытых сетей // InternetUA (http://internetua.com/hakeri-ispolzuuat-vredonosnoe-po-dlya-hisxeniya-dannih-iz-zakritih-setei). – 2014. – 13.11).***

***

Китайские хакеры взломали системы Национального управления океанических и атмосферных исследований США (NOAA), в том числе систему Национальной метеорологической службы, пишет The Washington Post со ссылкой на источники. Утверждается, что атака произошла еще в конце сентября, но узнали о случившемся только 20 октября. По словам источников, после выявления проблемы представители NOAA не стали сообщать о ней в компетентные органы.

В агентстве отказались обсуждать предполагаемый источник хакерской атаки и то, отразилась ли она на секретных данных. В октябре NOAA публично заявляло, что проводит «внеплановый ремонт» своей сети, однако о его причинах тогда не говорилось.

12 ноября пресс-секретарь агентства С. Смаллен признал, что хакерская атака действительно произошла, и подчеркнул, что реагирование на инцидент началось «немедленно». Как отметил С. Смаллен, все системы вновь работают, и прогнозы погоды продолжают передаваться общественности ***(Китайские хакеры взломали системы метеослужбы***

США // InternetUA (http://internetua.com/kitaiskie-hakeri-vzlomali-sistemi-meteoslujbi-ssha). – 2014. – 13.11).

***

Разработчик антивирусных решений FireEye обнаружил в iOS уязвимость безопасности, которая позволяет злоумышленникам подменять настоящие приложения вредоносными. Об этом говорится в отчете компании.

Согласно сообщению специалистов, уязвимость была обнаружена 26 июля. Вредоносная программа, которая получила название Masque Attacks, может заражать iOS через беспроводное подключение или подключение USB. У злоумышленников есть возможность заменять оригинальные приложения, установленные на iPhone и iPad, на вредоносные, например онлайн-банкинг или почтовые клиенты. В результате, атакующие могут получить доступ к персональным банковским данным человека.

В сообщении говорится, что под удар попадают пользователи iOS 7.1.1, 7.1.2, 8.0, 8.1 и 8.1.1 beta, вне зависимости от того, сделан джейлбрейк на устройстве или нет. Приложение подменяет только приложения из App Store, штатные программы не уязвимы перед этой угрозой. В процессе установки «вредонос» предлагает пользователю загрузить игру, например New Flappy Bird, после чего подменяет собой стороннее приложение, рассказали в FireEye.

Специалисты говорят, что оповестили Apple о «дыре» безопасности еще в июле этого года. Несмотря на это, компания не решила проблему. Вирус WireLurker, получивший распространие на минувшей неделе, основан на уязвимости Masque Attacks. Последняя, по заявлению FireEye, является еще более опасной, так как позволяет злоумышленникам подменять приложения без подключения к USB-порту компьютера ***(Уязвимость в iOS позволяет хакерам заменять настоящие приложения на вредоносные // InternetUA (http://internetua.com/uyazvimost-v-iOS-pozvolyaet-hakeram-zamenyat-nastoyasxie-prilojeniya-na-vredonosnie). – 2014. – 11.11).***

***

Уязвимость Heartbleed, обнаруженная в апреле этого года, до сих пор эксплуатируется для компрометации веб-сайтов. Несмотря на многочисленные исправления, призванные защитить владельцев ресурсов и их пользователей, хакеры до сих пор эксплуатируют эту брешь для похищения паролей. Об этом сообщают исследователи Университета штата Мэриленд.

Эксперты изучили 1 млн американских сайтов, чтобы выяснить, применили ли системные администраторы корректные меры по предотвращению дальнейших атак. По данным исследователей, 93 % веб-мастеров установили исправление, устраняющее уязвимость Heartbleed, но

лишь 13 % из них выполнили остальные действия, необходимые для защиты сервера.

Для полного устранения Heartbleed требуется установить исправления для OpenSSL, отозвать текущие сертификаты безопасности и выпустить их новые версии. Если эти меры не будут приняты, хакеры все равно смогут скомпрометировать веб-сайт, используя приватный ключ ресурса.

Исследователи также обнаружили достаточно забавный факт. Они составили график, показывающий частоту отозвания сертификатов безопасности уязвимых сайтов в зависимости от дня недели. Оказалось, что наименьшее число отозваний приходилось на выходные дни.

Эксперты представят результат своей работы на конференции 2014 Internet Measurement Conference, которая пройдет на этой неделе в Ванкувере ***(Злоумышленники до сих пор эксплуатируют Heartbleed для компрометации сайтов // InternetUA (http://internetua.com/zloumishlenniki-do-sih-por-ekspluatiruuat-Heartbleed-dlya-komprometacii-saitov). – 2014. – 11.11).***

***

Исследователи из G Data обнаружили новый троян, позволяющий хакеру получить удаленный доступ к зараженному устройству. Вирус предположительно разработан авторами Snake. Проанализировав новый вредонос, получивший название ComRAT, эксперты пришли к выводу, что он является наследником известного вируса Agent.BTZ, с помощью которого в 2008 г. были взломаны компьютеры Минобороны США. Несмотря на то, что многочисленные аспекты кампании по кибершпионажу Snake были раскрыты экспертами во всем мире, существование ComRAT свидетельствует о том, что операция до сих пор находится в активной стадии.

Эксперты обнаружили два варианта ComRAT: 3.25 и 3.26. В версии 3.25 используется такой же ключ кодировки и имя лог-файла установки, как и в Agent.BTZ и Snake. В версии 3.26 разработчики попытались скрыть связь между ComRAT и Agent.BTZ, а также увеличили сложность анализа угрозы.

Вдобавок к использованию одинакового ключа кодировки и одинаковым именам лог-файлов установки, существуют и другие связи между Snake, ComRAT и Agent.BTZ. Вредоносы используют одинаковые C&C-сервера, а фрагменты кода ComRAT напрямую скопированы из Snake и Agent.BTZ. Именно это и позволило экспертам идентифицировать новый троян как модификацию Snake.

Наиболее значительное отличие между ComRAT и Agent.BTZ заключается в их дизайне. Специалисты G Data говорят, что ComRAT гораздо более опасен, чем Agent.BTZ. По их словам, вредонос загружается в каждый процесс на инфицированной машине, но его пэйлоад исполняется исключительно в рамках процесса explorer.exe. C&C-трафик встраивается в браузерный трафик, что значительно осложняет обнаружение вируса. Об этом говорит эксперт G Data П. Расканьер.

По данным G Data, версия 3.25 была скомпилирована в феврале 2014 г. Более новая версия (3.26) выглядит так, будто ее создали в январе 2013 г., но исследователи уверены, что дата была сфабрикована ***(Обнаружен троян, разработанный авторами Snake и Agent.BTZ // InternetUA (http://internetua.com/obnarujen-troyan--razrabotannii-avtorami-Snake-i-Agent-BTZ). – 2014. – 15.11).***

***

Исследование, проведенное специалистами Incapsula, показывает, что DDoS-атаки наносят значительный финансовый ущерб всем организациям, против которых они совершались. Эксперты пришли к такому выводу, опросив системных администраторов, сотрудников службы безопасности, сетевых архитекторов, работников веб-сайтов и разработчиков 270 американских организаций, в которых работает от 250 человек.

По данным Incapsula, 45 % респондентов сказали, что на сайты организаций, в которых они работали, совершались DDoS-атаки. Исследование показало, что ущерб, наносимый организациям вследствие DDoS-атак, в среднем равен 40 тыс. Дол. в час. Тем не менее, были случаи, когда за один час компании теряли более 100 тыс. дол. прибыли. С учетом того, что 49 % всех атак длились от 6 до 24 часов, средний ущерб от одной DDoS-атаки равен 500 тыс. дол., хотя некоторые компании говорили о миллионах долларов потерь.

Организации, ставшие жертвами DDoS-атак, в дальнейшем сталкивались с потерей доверия со стороны клиентов (43 %), кражей данных о клиентах (33 %) и потере интеллектуальной собственности (19 %). Большая часть пострадавших от DDoS-атак меняла серверное ПО и оборудование. В половине случаев после атаки на серверах компаний обнаруживалось установленное вредоносное ПО ***(Ущерб от DDoS-атак достигает $40 тысяч в час // InternetUA (http://internetua.com/usxerb-ot-DDoS-atak-dostigaet--40-tisyacs-v-csas). – 2014. – 16.11).***

***

Компания Trend Micro Incorporated представила ежегодный отчет с прогнозами по информационной безопасности на 2015 г., сообщается в пресс-релизе компании.

Эксперты компании выделили 7 главных направлений в области киберугроз.

– Все больше киберпреступников будут использовать подпольные сети, закрытые форумы и биржи для обмена и продажи программного обеспечения криминального профиля.

– Большую роль в заражении устройств будут играть мобильные уязвимости; получат распространение новые вирусы, направленные на Android.

– Наиболее распространенным видом киберпреступности станут целенаправленные атаки.

– Новые методы мобильных платежей приведут к появлению новых угроз.

– Более активно будут использоваться уязвимостей в приложениях с открытым кодом.

– Будут происходить массовые атаки на центры обработки пользовательских данных.

– Появятся новые, еще более опасные угрозы для онлайн-банкинга и других финансовых сервисов ***(Эксперты прогнозируют киберугрозы в 2015 году // InternetUA (http://internetua.com/eksperti-prognoziruuat-kiberugrozi-v-2015-godu). – 2014. – 16.11).***