СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(18.04–22.05)

2016 № 7

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(18.04–22.05)
№ 7

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

Відповідальний редактор
Л. Чуприна, канд. наук із соц. комунікацій

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2016

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

13.05.2016

Facebook став більш популярним в Україні, ніж Wikipedia (рейтинг сайтів)

За даними дослідження CMeter, компанії TNS, незмінною трійкою лідерів популярних сайтів серед українських інтернет-користувачів у квітні залишаються Google, «ВКонтакте», YouTube, пише Watcher.

	Сайт	Охоплення за березень 2016, (%)	Охоплення за квітень 2016, (%)
1	google.com.ua	67,6	66,8
2	vk.com	66,8	66,1
3	youtube.com	63,6	62,9
4	mail.ru	57,1	56,3
5	yandex.ua	49,5	48,8
6	olx.ua	48,5	**46,6**
7	facebook.com	43,2	43,9
8	wikipedia.org	45,8	**43,8**
9	privatbank.ua	42,0	42,1
10	odnoklassniki.ru	38,2	36,6
11	rozetka.com.ua	36,6	**34,2**
12	prom.ua	34,6	33,7
13	sinoptik.ua	27,7	**30,4**
14	ukr.net	25,9	24,8
15	blogspot.com	26,7	**23,0**
16	gismeteo.ua	20,1	22,8
17	aliexpress.com	26,2	**22,3**
18	kinogo.net	24,0	**21,3**
19	ex.ua	23,1	**20,2**
20	i.ua	20,0	20,0
21	tsn.ua	16,4	16,9
22	aukro.ua	18,9	**16,8**
23	novaposhta.ua	18,1	**16,6**
24	segodnya.ua	17,7	**16,2**
25	kinopoisk.ru	19,5	**16,2**

У першій десятці відбулися зміни: Facebook обійшов Wikipedia.org і піднявся на сьому позицію.

Дослідження CMeter об’єднує дані з трьох джерел:

1. Site-centric – лічильники, інтегровані в сайти. На момент публікації у вимірюванні враховано близько 250 сайтів.

2. Frame-centric – лічильники встановлено не на сайті, а у фреймі банерної мережі. На момент публікації у вимірюванні понад 2500 сайтів.

3. User-centric – панель, що охоплює близько 4 тис. респондентів щодня, поряд зі стандартними показниками (hits, охоплення, соціально-демографічні тощо показники по всіх сайтах, з якими контактували респонденти), також фіксує контакт панелістів з контентом.

***

25.04.2016

5,4 млн українців у Facebook: кількість користувачів в Україні почала зростати швидше, ніж у 2015 р.

З лютого по квітень 2016 р. кількість українських користувачів Facebook зросла на 400 тис., що говорить про пришвидшення темпів росту в Україні, які в річному вираженні становлять тепер 35–40 %, порівняно з 30 % у 2015 р., пише Watcher.

Станом на 25 квітня 2016 р. користувачами Facebook було 5,4 млн українців.

За методологією Facebook користувачами соцмережі є люди, які хоча б раз протягом останніх 30 днів заходили в соцмережу, будучи при цьому залогіненими. Тобто в цій статистиці не враховуються, наприклад, зареєстровані користувачі, які не заходять у соцмережу протягом останніх 30 днів, а також люди, які не зареєстровані в соцмережі, але переглядають її контент (наприклад, відео).

За останні сім років – з квітня 2009 р. – аудиторія Facebook в Україні зросла у 85 разів (з 63 тис. до 5,4 млн).

***

21.04.2016

Студент з Умані Д. Короташ створив нову соціальну мережу Mepozo

19-річний уманський студент Д. Короташ у вільний від навчання час створив принципово нову соціальну мережу Mepozo. Як інформує 04744.info, хлопець переконаний, що врахував усі недоліки популярних соціальних мереж і створив у модному форматі Landing page принципово новий, а головне, український інтернет-продукт, пише видання Провінція.

«Користувачі нової мережі будуть захищені від проникнення у їхні персональні дані, зможуть обирати у новинну стрічку найцікавіше з власних вподобань, – розповідає Д. Короташ. – Також в нашій мережі є можливість спілкуватися з “чат-ботом” – роботом, який жартома відповідатиме на репліки користувачів. Він навіть зможе стати другом для тих, кому важко спілкуватися з реальними людьми».

Для всіх користувачів мережа безкоштовна, а монетизувати свій проект засновник сподівається завдяки рекламі та спонсорам. До речі, Д. Короташ свою ідею також захищав на конкурсі бізнес-планів. Коштів, щоправда, не отримав, але запитань, каже, було багато. Наразі в команді проекту є ще троє

студентів, працюють вони над стартапом на волонтерських засадах. Кошти за надійний хостинг автор проекту вклав власні, але, каже, ідея того варта.

«Найпершими нашими користувачами можуть стати школи чи навчальні заклади. У нашій соцмережі є всі сервіси для створення локальних навчальних платформ, – ділиться власними баченням розвитку проекту Д. Короташ. – Просто клас чи група об'єднуються і мають спільний розклад занять, важливі оголошення, список домашніх завдань. Це легко, треба лише почати і зареєструватися в мережі, а далі простий інтерфейс і логіка підкажуть, що робити».

***

18.04.2016

Чем заменить Skype? Пять альтернативных мессенджеров для работы

Самый популярный мессенджер среди украинцев – Skype. Его выбирают 94 % наших соотечественников. Skype используется и для частной переписки, и для корпоративного общения. При этом многие пользователи даже не думают о переходе на другие программы. И напрасно. Ведь для рабочей переписки существуют и более подходящие решения. IGate подобрал несколько мессенджеров, которые отлично подойдут для общения с колегами.

Slack

Slack – довольно молодой проект. Мессенджер, запущенный в феврале 2014 г., быстро завоевал титул «убийцы Skype и корпоративного e-mail». Всё – благодаря уникальным возможностям интеграции. Если Skype используется как общий чат и инструмент передачи файлов, то Slack умеет синхронизироваться с другими популярными веб-инструментами. К примеру, мессенджер может уведомлять пользователей об изменениях, внесенных кем-то в общий документ Google Docs, Drobpox или GitHub. Всё это – в окне переписки. Так Slack из инструмента для общения превращается в универсальную платформу для разработки какого-либо проекта. Slack поддерживает интеграцию примерно с сотней сторонних сервисов.

Минус: увы, использовать мессенджер для повседневного общения вряд ли получится. Его практически не используют вне корпоративной среды, поэтому вряд ли в списке контактов среднестатистического пользователя обнаружится много знакомых и друзей детства.

HipChat

HipChat – еще один мессенджер, разработанный исключительно для бизнеса. Хотя этот проект не из тех, что находятся у всех на слуху, статистика HipChat указывает на высокую популярность в корпоративной среде. Так, мессенджер еще в 2014 г. перешагнул отметку в 1 млрд сообщений. Как и Slack, он позволяет пользователям определенной группы наблюдать за изменениями в синхронизированных документах сторонних веб-сервисов, приглашать в проект

«гостей» с ограниченными правами. Интересная особенность HipChat – возможность форматировать текст в окне переписки.

Минус: размер передаваемых файлов, который ограничен 50 мб. Для сравнения, в Skype вообще нет ограничения на размер файла, а в Slack оно установлено на отметке в 1 Гб.

Facebook Work Chat

Этот мессенджер ориентирован на пользователей платформы Facebook at Work, корпоративной социальной сети вроде LinkedIn. Для того чтобы пользователь мог работать с Work Chat, ему потребуется аккаунт в Facebook at Work. Мессенджер позволяет вести групповые и индивидуальные беседы, обмениваться файлами. Особенность проекта – список контактов, выполненный в формате каталога сотрудников различных компаний.

Минус: Work Chat все еще дорабатывается, потому многие возможности, свойственные корпоративным мессенджерам, будут реализованы здесь со временем.

Telegram

Если сохранение конфиденциальности информации в мессенджере – главное требование, оптимальным выбором будет Telegram. Он поддерживает интеграцию с несколькими веб-сервисами: iCloud, Dropbox и Google Drive. Большой плюс Telegram – возможность пересылать файл объемом до 1,5 Гб.

TigerText

TigerText – довольно необычный проект, также хорошо подходит для компаний, озабоченных конфиденциальностью. Это – своеобразный гибрид корпоративного Slack с молодежным Snapchat. В TigerText можно настроить функцию самоуничтожения сообщений через определенное время. Таким образом, корпоративная переписка надежно защищена от кражи.

Минус: из мессенджера невозможно копировать сообщения, даже скриншот экрана с окном программы сделать не получится.

***

18.04.2016

«ВКонтакте» создаст свой мессенджер

Летом 2016 г. планируется запустить его десктопную версию, сообщил «Ленте.ру» пресс-секретарь «ВКонтакте» Е. Красников. По его словам, версия мессенджера для персональных компьютеров уже проходит тестирование. В будущем будет создан и мессенджер для мобильных устройств, однако сроки его появления пока не сообщаются, пишет Marketing Media Review.

Е. Красников добавил, что технология шифрования End-to-end, то есть такая система, при которой зашифрованная информация передается от устройства к устройству без участия посредников, не будет использоваться в работе мессенджера из-за ее сложности. Однако при наличии запроса от пользователей в социальной сети готовы рассмотреть ее внедрение.

Е. Красников отметил, что отключать возможность обмениваться сообщениями в обычном приложении, как это было сделано в Facebook, во «ВКонтакте» не намерены. Кроме того, планируется сохранить интеграцию между соцсетью и ее мессенджером, чтобы пользователь мог свободно переключаться между ними.

***

18.04.2016

Исследование: Twitter генерирует только 1,5 % трафика для издателей

По данным нового исследования аналитической компании Parse.ly, которая промониторила данные 200 клиентских веб-сайтов за две недели в январе, Twitter генерирует только 1,5 % трафика для изданий, пишет Marketing Media Review.

В сеть компании входят такие издатели, как Upworthy, Slate, The Daily Beast и Business Insider. Как отметила компания, в среднем издатель видел восемь твитов на пост, три клика на твит и 0,7 ретвитов за каждый оригинальный твит. У топ-5 издателей с более эффективными постами в Twitter, сеть генерировала 11 % трафика.

Компания отметила, что секретом к успешной деятельности в Twitter, как и в других социальных сетях, является понимание того, что аудитория издания считает интересным и создание контента, который отвечает ее интересам. Нет также никакого ноу-хау для издателей, желающих улучшить свою результативность в Twitter. Сайты, которые достигают высокого уровня вовлечения на площадке, не обязательно самые активные, они просто создают интересный контент, привлекающий широкую аудиторию.

В Twitter существует два вида контента, по словам Parse.ly: интерактивные разговорные новости и экстренные сообщения. Типичный контент в Twitter по своей природе разговорный, когда тысячи людей вовлечены в определенную тему долгий период времени. Экстренные сообщения, с другой стороны, провоцируют резкие всплески трафика на короткий промежуток времени. К примеру, президентские выборы 2016 г. – это пример разговорной темы, генерирующей постоянные дискуссии и освещения. Твиты на тему выборов составили 6 % всех постов в марте, по оценке аналитиков Parse.ly.

Террористические атаки в Брюсселе тем временем продемонстрировали широкое распространение горячих новостей в сети. Более 92 тыс. твитов со ссылками на истории о терактах были размещены в течение 24 часов со времени трагедии. Третья часть твитов была размещена в течение первых шести часов после терактов. Несмотря на то что новости рождаются в Twitter, он остается слабым источником трафика для большинства издателей, уступая Facebook, Google и даже Yahoo.

***

19.04.2016

Приложение LinkedIn Students поможет с поиском работы

Социальная сеть для делового общения LinkedIn запускает новое приложение, которое гарантировано поможет с поиском работы. Софт под названием LinkedIn Students направлен на выпускников высших учебных заведений, пишет HiTech-News.ru.

Сообщается, что новое приложение гарантировано поможет с поиском работы. Для этого LinkedIn Students содержит множество подкатегорий, в которых потенциальные работодатели смогут размещать предложения о найме. Причем приложение найдет работу не только по профильному образованию, но и по широкому спектру предложений. То есть студенту-психологу предложат должность не только в качестве доктора, но и, например, менеджера или рядового офисного сотрудника. LinkedIn Students поможет социальной сети расширить аудиторию, а студентам – найти работу.

***

20.04.2016

Twitter тестирует новый дизайн приложения для Android

Приложение Twitter для мобильных устройств пережило множество изменений. Это относится не только к глобальным переменам в дизайне, но и к изменениям в работе самой службы. Недавно стало известно, что социальная сеть в очередной раз обновляет интерфейс приложения, добавив улучшенное навигационное меню и переместив кнопку ввода нового твита, пишет InternetUA.

В новой версии интерфейса появились отдельные вкладки, которые позволяют открыть ленту, уведомления, сообщения и «моменты». Над иконками вкладок расположена кнопка доступа к навигационной панели, через которую можно открыть профиль, подборки, списки, настройки и другие элементы управления приложением. Сюда же переместится кнопка поиска людей, которая в текущей версии дизайна находится в верхнем меню.

Кнопка ввода нового сообщения расположена внизу справа, она может исчезать, если пользователь просматривает твит, размещённый в этой области.

Новый интерфейс Twitter доступен ограниченному количеству пользователей, и неизвестно, когда социальная сеть сделает обновление доступным для всех.

***

19.04.2016

Facebook купил регистратор доменов

Facebook приобрёл компанию RegistrarSEC LLC, которая занимается регистрацией доменных имён. Об этом стало известно из еженедельного отчёта ICANN, пишет IGate.

RegistrarSEC не является обычным регистратором, предоставляющим услуги для всех. На данный момент он зарегистрировал только 11 доменов. Как Facebook планирует использовать приобретение, пока неизвестно. Есть предположения, что компания, скорее, заинтересована в интеллектуальной собственности RegistrarSEC, чем в регистрации доменов. Также не исключено, что Facebook будет предлагать услуги по регистрации доменных имён своей миллиардной аудитории.

Около двух лет назад корпорация Google создала собственный сервис по регистрации доменов domains.google. Вероятно, что Facebook последовал его примеру. И это логично, с точки зрения перспектив развития интернет-компании.

***

19.04.2016

К концу года «ВКонтакте» начнет автоматически воспроизводить видео

Социальная сеть «ВКонтакте» в скором времени начнет автоматически воспроизводить видео. В данном случае речь идет о функции уже сравнительно давно известной пользователям соцсети Facebook и позволившей заметно повысить количество просмотров опубликованных роликов, пишет HiTech-News.ru.

Реализовать эту функцию в сервисе «ВКонтакте» разработчики намерены уже к концу 2016 г., о чем сообщил операционный директор соцсети А. Рогозов в ходе конференции Mail.ru Group Mobile Day. Кроме того, он анонсировал на конец апреля автоматическое воспроизведение GIF-анимации. Функция получила вполне понятное название AutoPlay и нацелена на увеличение числа публикуемого во «ВКонтакте» контента.

А. Рогозов подчеркнул, что воспроизводится будет исключительно загруженное в «ВКонтакте» видео, не распространяясь на ролики с YouTube и прочих видео-хостингов, что должно избавить пользователей соцсети от просмотра назойливой рекламы. Операционный директор социального сервиса пообещал, что никаких ограничений в связи с содержанием и продолжительностью выдвигаться не будет.

***

21.04.2016

Facebook готов платить своим пользователям за уникальный контент

Руководство Facebook рассматривает возможность введения системы поощрения пользователей, создающих уникальный контент, информируют Экономические известия.

Это может быть эффективным решением для выхода из создавшегося «пузыря контента».

Эксперты уже давно говорят о том, что по-настоящему уникального содержимого в социальной сети практически нет, а пользователи по кругу обмениваются картинками и постами годичной давности и даже старше. Уникальный контент перемещается на сторонние сервисы, а вслед за ним уходит и наиболее активная аудитория соцсети.

Чтобы разорвать этот порочный круг, Facebook будет стимулировать тех, кто готов создавать что-то новое. Компания провела опрос, с помощью которого выяснила, какого поощрения пользователи ожидают за создание уникального контента. Большинство опрошенных ожидаемо выбрали деньги.

Когда именно будет внедрена новая система, пока не сообщается. Возможно, вся инициатива завершится на стадии опроса либо будет включена для ограниченного круга лиц, вроде самых топовых блогеров.

***

21.04.2016

Facebook Messenger внедряет функцию групповых звонков

Компания Facebook официально сообщила, что в Facebook Messenger появится функция бесплатных групповых звонков, пишет IGate.

Для совершения группового вызова пользователю достаточно нажать на иконку с изображением телефона, а затем выбрать контакты, которым он хочет позвонить. Все адресаты одновременно получат уведомление о входящем голосовом вызове и смогут ответить на него. Если кто-то из пользователей пропустит изначальный вызов, он сможет присоединиться к разговору позже, при условии, что вызов еще не завершен. Также участники разговора смогут приглашать в него новых пользователей прямо во время беседы. Одновременно в разговоре могут принимать участие 50 человек.

***

24.04.2016

Новый алгоритм Facebook скроет посты-приманки

Социальная сеть Facebook продолжает совершенствовать механизм отбора постов, чтобы пользователь мог видеть в «Хронике» релевантные и самые интересные ему записи. Напомним, что публикации в ленте появляются не в хронологическом порядке, а формируются по принципу значимости, пишет InternetUA.

Что важно – решает сама Facebook. Ранее соцсеть полагала, что чем больше пользователь взаимодействует с записями на определенную тематику

(ставит лайки, делится, комментирует), тем чаще он хочет подобные посты. В течение последнего года компания улучшала алгоритмы ранжирования новых постов в «Хронике». Например, вероятность попадания записи в новостную ленту теперь не так сильно зависит от количественных показателей, как раньше.

На этой неделе Facebook снова усложнила алгоритмы, чтобы очистить «Хронику» от провокационных заголовков и «вирусных» постов, которые собирают много лайков и комментариев, но могут быть неинтересны пользователю. Чтобы воспрепятствовать «накрутке», теперь соцсеть подсчитывает время, затраченное на прочтение публикации (но не принимает во внимание факт перехода по ссылке), а также учитывает разнообразие записей на странице.

Так, Facebook хочет лучше понять, какие посты пользователь читает дольше, чтобы потом предложить ему что-то похожее. Измененный алгоритм начнет тестироваться на «мгновенных» статьях (Instant Article), открытых на компьютерах, а также постах, читаемых с мобильных устройств.

***

26.04.2016

Facebook объявил войну Snapchat, начав разработку аналогичного проекта

Компания Facebook приступила к разработке нового проекта, который должен стать своеобразным аналогом популярного мессенджера Snapchat. Это можно расценивать как прямое объявление войны, пишет IGate.

Известно, что, как и в Snapchat, в новом приложении главным экраном станет не текстовый чат, а окно камеры. Вероятно, в это же окно будут интегрированы живые фильтры из недавно купленного компанией приложения MSQRD. Кроме того, в новинку могут быть интегрированы расширенные функции Facebook Live, заявленные на конференции F8. Благодаря этому приложение Facebook может оказаться более функциональным и конкурентоспособным, чем Snapchat.

Название проекта пока не разглашается. Известно, что разработка находится на очень ранних стадиях, а потому более подробной информации о будущем приложении компания не дает.

***

3.05.2016

В Facebook Messenger появятся самоуничтожающиеся сообщения

Разработчики Facebook Messenger планируют добавить в мессенджер функцию исчезающих сообщений. В настоящее время она уже тестируется социальной сетью. Для перехода в нужный режим пользователю будет

достаточно нажать иконку песочных часов в верхнем правом углу, пишет InternetUA.

Функция «самоуничтожения» может быть активирована для любой беседы. Включение опции запустит режим таймера для сообщения, которое автоматически исчезнет из ленты через указанный период времени. Пользователь может выбрать 1 мин, 15 мин, 1 час, 4 часа или 1 день. После подтверждения отправки данные пересылаются собеседнику. Режим будет работать только для выбранной беседы, а не для всех пользователей мессенджера, и может быть отключен в любой момент.

Условие для получения самоуничтожающихся сообщений – наличие новой версии мессенджера. Восстановить данные после удаления будет нельзя. В сети доступны скриншоты iOS-версии обновленного Facebook Messenger для iOS.

Аналогичная функция изначально была заложена в мессенджер Snapchat, где фотографии и видеоролики самоуничтожаются через несколько секунд или через 24 часа после просмотра. Недавно похожие функции были запущены и некоторыми другими приложениями, включая популярные в Азии Line и WeChat.

В конце 2015 г. популярный мессенджер Viber также запустил исчезающие сообщения. Функция доступна всем пользователям после установки дополнительного приложения Wink и представляет собой возможность отправлять самоуничтожающиеся сообщения/фото/видеоролики.

Точная дата повсеместного внедрения новой функции в Facebook Messenger пока неизвестна. Администрация социальной сети воздерживается от комментариев.

***

26.04.2016

Velever: социальная сеть для всех, кто ведет спортивный образ жизни

Кто следит за своим здоровьем, посещает фитнес-центр или спортивную секцию, увлекается здоровым питанием, знает, что сегодня это целая субкультура. Большой мир, погружаясь в который, понимаешь, почему сегодня заботу о здоровье называют «образом жизни». Тренировки, спорт, вес, сон, правильное питание – все захватывает новичка, и он ищет полезную информацию, знающих и опытных инструкторов или просто активных сторонников здорового образа жизни, пишет AIN.UA.

Создатели новой международной социальной сети для любителей здорового образа жизни, спорта, фитнеса и бодибилдинга Velever – люди, увлеченные спортом. Идея проекта родилась из потребности делиться полезной и нужной информацией и саморазвития.

«В какой-то момент я решил найти инструктора, который составит мне программы тренировок и режим питания, – рассказывает создатель Velever Р. Лихман. – Опыт у меня был, с техникой выполнения упражнений все

отлично, поэтому искал онлайн-консультации. Был очень удивлен, когда увидел, сколько персональных тренеров работает онлайн. Только в рунете их десятки тысяч. В основном все они предлагают услуги в разных соцсетях и форумах.

Я нашел тренера и стал получать программы тренировок на почту в Excel-файле. Для меня это было неудобно. Начал искать сервис, который связывал бы меня с тренером, хотелось получать из одного источника всю информацию сразу: от тренировок до питания, с уведомлениями и напоминаниями. Хороших сервисов, увы, не нашел».

Так родилась идея создать приложение, которое свяжет тренера с подопечным, позволит тренеру создавать тренировки, режим, отслеживать результаты и т. д., и своеобразную фриланс-площадку с отзывами и рейтингами лидеров и тренеров.

Р. Лихман с партнерами решили создавать сервис в формате социальной сети, чтобы пользователи получили не только функциональные возможности, но и коммуникационную площадку.

Сейчас Velever работает в режиме бета-версии. На сайте новички и профессионалы из мира фитнеса могут найти наставников и тренеров по любым дисциплинам и получить консультации или личную программу тренировок. Здесь каждый сможет приобщиться к миру бодибилдинга, откорректировать фигуру, улучшить здоровье, узнать больше о диетологии или просто снизить лишний вес. Тренеры в свою очередь могут продвигать свои программы и зарабатывать на консультациях.

На сайте созданы специальные модули для продажи тренировочных программ, ведения блогов, подписки. Профессиональный тренер может не только консультировать посетителей, но и пользоваться инструментами, которые позволят быстро создавать программы тренировок и отслеживать результаты подопечных.

Кроме того, проект является постоянно обновляемым агрегатором фитнес-центров. Зарегистрированные компании могут обеспечить себе новых клиентов, продвигать свои услуги, получать целенаправленный трафик.

Пользователь спортивной социальной сети получает персональный онлайн-профайл, который, по сути, представляет собой персональный сайт с богатыми возможностями, позволяющий общаться с другими пользователями и находить друзей по интересам, публиковать заметки в блог, фото и видео, участвовать в тематических сообществах. Онлайн-профайл связывает всю активность пользователя в единую ленту, доступную его друзьям.

Создатели Velever позаботились и о возможности заработать блогерам в спортивной тематике. Для них на сайте реализован модуль платной подписки на тематические сообщества. Этот модуль также можно использовать как сбор пожертвований на развитие, например какой-то спортивной команды.

«В ближайшие дни для всех пользователей будет доступен инструмент создания программы тренировок с готовой базой упражнений. Для активных фитнес-пользователей, которым не нужны тренеры, это долгожданная новость.

Каждый сможет сам себе создавать тренировку и следить за результатами. Также будет включен модуль диетологии», – рассказывает Р. Лихман.

Следующим этапом в развитии проекта станет создание мобильного приложения и множества дополнительных модулей для самых разных функциональных возможностей сервиса. Для этой цели команда собирает средства на краудфандинговой платформе Simex.

Velever изначально был задуман как международный проект, и создатели ставят довольно амбициозные цели по выходу на западные рынки, где тоже есть потребность в такой площадке.

***

27.04.2016

«Одноклассники» запустят свой собственный мессенджер этим летом

«ОК Сообщения» будут полностью бесплатным сервисом, причем рекламы в них также не будет. Однако языковая линейка приложения будет ограничена русским, английским, узбекским и таджикским язиками, пишет IGate.

В мессенджере будут доступны индивидуальные и групповые чаты, а также функции обмена фотографиями, аудио- и видео записями, а также gif-файлами.

«ОК Сообщения» ориентированы на работу на мобильных устройствах: большинство функций работает без подключения к Интернету – пользователям доступны все переписки и медиафайлы, а сообщения, написанные офлайн, отправляются автоматически после появления доступа к сети.

Если «Одноклассникам» удастся запустить свое приложение этим летом – соцсеть основательно потеснит своего прямого конкурента «ВКонтакте», обещавшего запустить аналогичный сервис до конца года.

***

9.05.2016

Ученые создали сервис для анализа интернет-мемов

Сотрудники Университета Индианы представили сервис, который анализирует интернет-мемы. Описание и принцип сервиса доступны на сайте университета, пишет InternetUA.

Проект под названием OSoMe (The IUNI Observatory on Social Media) адресован журналистам, исследователям и широкой общественности для того, чтобы оперативно отследить масштабы какого-либо интернет-события. Так, в инструментах сервиса можно проверить, является ли пользователь Twitter ботом, отследить основные тренды и их динамику и сделать из этой информации ролик.

Кроме того, в сервисе присутствуют инструменты для анализа участников обсуждения мема и географии его распространения.

Сервис разработан на основе Apache Big Data Stack.

***

11.05.2016

Украинцы создали приложение, позволяющее пользователям быстро «списаться» с ближайшими заведениями

Украинские разработчики создали необычный мессенджер, с помощью которого пользователи смогут написать и пообщаться в формате чата с представителями ближайших заведений, не утруждая себя поиском контактов. Сервис получил название Spottle и пока доступен только для iOS-устройств, однако в скором времени авторы обещают выпустить и Android-версию. Сами разработчики называют свое творение таким себе симбиозом WhatsApp и Foursquare, пишет IGate.

Принцип работы заключается в получении координат пользователя и последующем предложении ему списка близлежащих заведений, с каждым из которых можно связаться в чате. Пока стартап делает только первые шаги, отвечать на запросы пользователей будут операторы, однако в будущем планируется, что общаться с потенциальными клиентами будет администрация заведений. Такую систему уже тестируют в Днепропетровске с владельцами кафе и ресторанов.

Пользователю сервиса также предоставляется доступ к фотографиям заведений, меню, отзывам, расписаниям фильмов в кино и прочей полезной информации.

Приложение бесплатное, зарабатывать команда планирует на продаже заведениям маркетинговых инструментов, а также статистики посещений.

***

11.05.2016

Instagram провел масштабный редизайн и стал черно-белым

Instagram изменил дизайн иконки и ленты новостей в своем приложении. Камера, которая была логотипом фотосервиса, стала более схематичной и поменяла цвет с коричневого на «радужный». Кроме того, из интерфейса пропали цветовые элементы, которые, как рассказали «Ленте.ру» в пресс-службе Instagram, отвлекали внимание пользователей от фотографий и видео, пишет InternetUA.

В новой версии фотосервиса синяя панель в верхней части экрана и черная в нижней стали прозрачными. Кроме того, Instagram решил использовать новые шрифты, адаптированные для платформ iOS и Android.

Логотип также поменяли другие приложения, которые разрабатывает Instagram: сервис для коллажей Layout, а также видеосервисы Hyperlapse и Boomerang.

По словам представителя пресс-службы фотосервиса, новый облик отражает яркость и разнообразие сегодняшних публикаций. «За последние пять лет сообщество Instagram сильно изменилось: теперь это не просто место, где пользователи делятся обработанными фото, – это глобальное сообщество людей, публикующих более 80 млн фото и видео каждый день», – пояснили в компании.

***

12.05.2016

В ленте Facebook появятся 360-градусные фото

Фото будут функционировать по принципу 360-градусных видео, необходимо лишь навести на них курсор или повернуть смартфон под другим углом. Функция будет поддерживать фото, сделанные сферической камерой, такой как Rioch Theta S, и панорамные снимки, сделанные на смартфон. Фото также можно будет просмотреть с помощью шлемов виртуальной реальности Samsung.

Facebook также планирует внести некоторые изменения в мобильное приложение для Oculus. В нем появится новый раздел «что нового», который расскажет о новинках среди игр и видео. По словам Facebook, VR видео является самым популярным контентом с использованием виртуальной реальности среди пользователей: 80 % пользователей Gear смотрят видео, пишет Marketing Media Review.

***

13.05.2016

Мобильный YouTube порадует пользователей встроенным мессенджером

Как сообщает Wired, YouTube приступил к тестированию функции мгновенного обмена сообщениями в приложениях для iOS и Android. Наверняка эта возможность придётся в сервисе очень даже к месту, другое дело, что пока её могут оценить лишь избранные счастливчики, получившие доступ к закрытому бета-тестированию, пишет InternetUA.

Суть нововведения состоит в том, что теперь внутри мобильного приложения YouTube пользователи могут отправлять друг другу видеоролики, фотографии и текстовые сообщения как в полноценном мессенджере. При этом все сообщения будут сохраняться в новом разделе Shared.

Разработчики возлагают на эту функцию большие надежды. По их мнению, она увеличит интенсивность обмена видеоконтентом внутри сервиса, а также создаст пользователям более благоприятные условия для общения. Им больше не придётся использовать сторонние мессенджеры, чтобы поделиться с друзьями ссылкой на какой-нибудь интересный видеоролик – ведь теперь сделать это можно прямо в приложении YouTube.

Как ни крути, а сохранять конкурентное преимущество сервису становится всё труднее: в спину дышат Facebook и Snapchat, которые всеми силами стремятся отвоевать часть аудитории, а не так давно к этой гонке присоединился ещё и розничный гигант Amazon. Компания запустила собственный потоковый видеосервис Amazon Video Direct, к которому уже активно привлекаются профессиональные студии и правообладатели.

***

13.05.2016

Tumblr запустил программу с экспериментальными функциями

Сервис микроблогов Tumblr запустил новую программу, которая позволяет пользователям опробовать экспериментальные функции до их стандартизации. Инициатива носит название Tumblr Labs и доступна всем пользователям без исключения – достаточно зарегистрироваться в программе через панель управления сайта. После регистрации появляется возможность выбирать отдельные функции, которые можно опробовать. При этом в любое время от экспериментальной программы можно отписаться через меню настроек, пишет InternetUA.

Подписаться на программу Tumblr Labs можно прямо сейчас. Компания предупреждает, что если стандартная версия сервиса в будущем будет обновлена, то некоторые экспериментальные возможности могут перестать работать. В настоящее время пользователям доступны четыре экспериментальные функции: графики, показывающие, насколько активно другие люди делились вашими публикациями; улучшенные возможности для выставления публикаций в очередь; доработанные функции для групповых блогов; возможность подстраивать цвет публикаций под цвет своего блога.

Все эти функции могут быть очень полезны, однако многие из них уже были доступны через сторонние дополнения. К примеру, пакет XKit даёт пользователям куда более широкие возможности настройки, чем стандартный Tumblr с его новой экспериментальной программой. Тем не менее, со временем в Tumblr Labs может появиться больше полезных возможностей – и в сторонних решениях отпадёт всякая необходимость.

***

12.05.2016

Как Facebook хочет научить искусственный интеллект программированию

Нейронные сети и системы искусственного интеллекта способны кардинально изменить работу современных технологий. В то же время их разработка требует колоссальных ресурсов, технических и кадровых, пишет InternetUA.

Даже самые маститые профессионалы смогут представить готовый продукт только после многочисленных проб и ошибок, неоднократных циклов тестирования. К тратам на оплату труда исследователя, технологическое обеспечение для создания действительно революционного AI добавляется ещё один ценный ресурс – время.

Компании, которые активнее других взялись за искусственный интеллект (лидируют в этой отрасли Google и Facebook), теперь направили усилия на автоматизацию процессов тестирования алгоритмов. С одной стороны, это сократит время разработки одного AI-продукта и ускорит его внедрение в пользовательские сервисы, с другой – освободит специалистов для интеллектуальной работы и решения важных задач.

На службе человечества

Чтобы машины поскорее «умнели» и начали «мыслить», сами же компьютеры должны принимать участие в разработке искусственного интеллекта. Так решили в Facebook и создали автоматизированного «инженера машинного обучения» – систему, которая освобождает человека от рутинной работы по тестированию разрабатываемого ПО. И хотя она пока работает неидеально, специалисты намерены всё больше привлекать искусственный интеллект к работе на уровне с человеком.

Идея создания подобной программы появилась несколько лет назад. Когда в 2012 г. компания Facebook на IPO получила оценку в 104 млрд дол., инженерам, ответственным за рекламные алгоритмы, поставили задачу по созданию более эффективных механизмов таргетирования рекламы на основе массива данных о пользователях соцсети. По словам Х. Механны, одного из членов команды, это означало необходимость создания нейронных сетей и алгоритмов машинного обучения для «глубокого» анализа поведения миллионов людей в Facebook. У самих инженеров было множество идей, как именно можно использовать AI для работы с данными, но проблема заключалась в том, что тестирование и проверка актуальности всех этих разработок требовали времени и ресурсов. Тогда в помощь самим себе инженеры создали Flow – инструмент на основе машинного обучения для работы с данными. Flow помогает разработчикам создавать, тестировать и проверять в работе алгоритмы искусственного интеллекта разных типов в масштабной базе данных Facebook.

С Flow инженеры получили возможность постоянно тестировать те или иные AI-сценарии в режиме реального времени без непосредственного участия специалистов. Результаты этих исследований, в свою очередь, способствовали запуску новых циклов тестирования других алгоритмов глубокого анализа, логических регрессий и т. д. «Чем больше идей и данных мы пробовали – тем более впечатляющим получался результат», – делится Х. Механна. Кроме того, уже разработанные кем-то алгоритмы могли использовать другие сотрудники Facebook, соединять их между собой и создавать новые последовательности действий.

Оценив удобство и полезность нового инструмента, команда приняла решение открыть доступ к Flow инженерам всей компании. Его стали применять для формирования новостной ленты пользователя Facebook, распознавания лиц друзей на опубликованных фото и создания аудиотэгов к изображениям для людей с проблемами зрения. Flow даже использовалась для создания карты мира с указанием тех регионов, в которых до сих пор существуют проблемы с доступом ко всемирной паутине.

В цифрах работа Flow выражается так: ежемесячно инструмент тестирует около 300 тыс. разных моделей машинного обучения. И если раньше Facebook могла себе позволить выпускать один готовый AI-продукт каждые два месяца, то теперь несколько новых действенных инструментов появляются каждую неделю.

AI, создающий AI

Сегодня не только Facebook работает над вспомогательными AI-программами. Схожие проекты есть в Twitter и Microsoft. Последняя, по словам аналитика Д. Сана, работает с алгоритмом «ассистирующего поиска» новых действенных AI-моделей. Но социальная сеть решила возглавить данное направление разработки – Х. Механна с командой объявили о намерении открыть доступ к технологии Flow сторонним разработчикам по всему миру.

Окрылённые успехом Flow инженеры разработали ещё один инструмент, который способен взять на себя ещё больше обязанностей человека. AutoML работает с результатами исследований Flow и самостоятельно выделяет те данные, которые пригодятся для разработки нейронных сетей и других AI-программ. Таким образом, AutoML без участия человека подготавливает и запускает тестирование следующего уровня, с более глубоким исследованием моделей искусственного интеллекта. Программа AutoML буквально использует одну версию искусственного интеллекта для создания следующих подобных продуктов.

Facebook, как упоминалось выше, уже проверяет ежемесячно около 300 тыс. разных алгоритмов, а программа AutoML может использовать результаты этих тестирований для поиска новых алгоритмов машинного обучения, которые будут совершенствовать другие AI-алгоритмы и т. д. Х. Механна сравнивает работу технологий с внедрением идей в мозг человека, показанных в популярном фильме Inception. «Одни компьютерные алгоритмы фильтруют другие, ищут самую результативную модель и даже могут предугадывать результат теста до начала испытаний работы программы».

В дополнение к имеющимся инструментам инженеры создали роботизированного инженера Asimo, который работает с системами машинного обучения. Он также самостоятельно выделяет те алгоритмы, которые наверняка принесут оптимальный результат. Специалисты констатируют, что робот пока ещё не изобрёл собственный искусственный интеллект, но вполне может прийти к этому рубежу в будущем. Компании настолько активно взялись за обучение машин, что искусственный интеллект, созданный без прямого участия человека, может появиться даже раньше, чем первые колонии на Марсе.

***

16.05.2016
В Telegram появилась возможность редактировать сообщения

В мессенджере Telegram появился ряд новых функций, среди которых возможность редактировать сообщения после их отправки. Об этом сообщается в официальном блоге компании-разработчика, пишет InternetUA.

Функция редактирования позволяет в течение двух дней после отправки сообщения изменять его. После редактирования у сообщения появится соответствующая пометка. Функция доступна как на мобильных устройствах, так и в десктопной версии.

Кроме того, в Telegram появилась возможность отмечать пользователей даже в тех групповых чатах, куда они не были приглашены. Были добавлены боты в меню вложений и реализован поиск собеседников, ранжированный по их популярности.

***

16.05.2016
Google анонсировала новый мессенджер Spaces

Google выпустила новый мессенджер Spaces, особенностью которого стал встроенный браузер, поисковик и клиент популярного видеохостинга. В приложении интегрированы основные сервисы и программные продукты компании, такие как поиск, Chrome и YouTube, пишет InternetUA.

С его помощью компания намерена помочь пользователям общаться и делиться ссылками в небольших группах. «Комиксы, ремонт, поездка в Париж или подготовка к экзаменам… Что бы вас ни интересовало, вы можете моментально создать для этого тему в Google Spaces», – пояснили в Google.

Пользователь может создать чат («темы»), посвящённый определённому вопросу, а затем пригласить в него друзей. Наличие сервисов Google позволяет пользователям передавать информацию, не переключаясь на другие приложения. «Благодаря интеграции с Google Поиском, Chrome, Google Фото и YouTube вы можете находить и открывать любой контент, а также делиться им, не переключаясь между приложениями!» – отмечают разработчики.

«Групповые чаты зачастую выходят за рамки темы, а информация теряется в бесконечных переписках, и её становится сложно найти», – отметили в Google. Компания предложила использовать Spaces в качестве инструмента для обсуждения предстоящих мероприятий и других тем.

Запуск Google Spaces состоится в ближайшее время.

***

18.05.2016
Google представила новый «умный» мессенджер Allo

В рамках ежегодной конференции Google I/O компания представила новый мессенджер Allo и приложения для совершения видеозвонков Duo, пишет InternetUA.

Главной особенностью мессенджера является его встроенный ассистент. С ним можно вести переписку прямо в приложении, вводить поисковые запросы и играть в игры. В Google отмечают, что их чат-бот гораздо умнее конкурентов, так как имеет доступ к базе данных компании. Благодаря этому бот от Google может понимать более сложные запросы, чем обычные поисковые боты. Также бот может предлагать ответы во время переписки.

Из других особенностей Allo можно отметить возможность установить размер сообщения при его отправке. Таким образом, можно выделить важное сообщение.

Все сообщения защищены шифрованием, поэтому злоумышленники не смогут их прочитать. Однако серверы Google смогут обрабатывать сообщения, но не хранить их у себя. Для тех, кто этого опасается, в мессенджере присутствует режим «Инкогнито», как в браузере Chrome. В этом режиме Google не сможет обрабатывать сообщения и, соответственно, не будут приходить рекомендации от ассистента Allo.

Остальные функции мессенджера более привычны пользователям. Так, есть стикеры, индикатор доставки и прочтения сообщений, а также большое количество настроек.

Сервис для видеозвонков Duo повторяет все функции Facetime для iOS. Оба приложения выйдут летом 2016 г.

***

19.05.2016

Facebook превратит фото пользователей в эмодзи

В Facebook планируют ввести оригинальные эмодзи, созданные на основе фотографий пользователей. Это подтверждает заявка на получение соответствующего патента, поданная в Ведомство по патентам и товарным знакам США, пишет InternetUA.

Как уточняет портал Quartz, персонифицирование смайликов будет происходить благодаря специальной программе, которая конвертирует их в фото пользователей с «нужными» эмоциями. Новшество наверняка оценят те, кто устал от стандартного набора эмодзи.

Facebook уже умеет автоматически распознавать лица на фотографиях, предлагая отметить пользователей (иногда, правда, допуская ошибки). «Оживление» эмодзи – это часть большого плана по персонализации соцсети. Напомним, недавно компания добавила к кнопке Like целый набор реакций («супер», «сочувствую», «ха-ха» и пр.), благодаря которым пользователь может более точно высказать свое отношение к опубликованному.

Кроме того, в приложении Messenger имеется масса вариантов наклеек и GIF, которыми можно дополнять сообщения.

***

20.05.2016

Facebook запустив новий сервіс з прямими трансляціями з різних точок світу

Facebook запустив у браузерній версії новий сервіс Live Map. Він являє собою інтерактивну карту світу в профілі користувача, на якій синіми точками відмічено прямі відеотрансляції, доступні в цей момент у соцмережі, пише MediaSapiens.

Адреса сервісу – facebook.com/livemap, передає Lenta.ru.

При наведенні на точку над курсором спливає вікно з відео та зазначенням кількості глядачів. Одночасно з цим Facebook показує лініями, де дивляться трансляцію. У лівій частині екрана з'явиться список найпопулярніших трансляцій.

На момент написання новини найбільше скупчення синіх точок на карті спостерігалося в Південно-Східній Азії, зокрема в Таїланді і В'єтнамі.

Facebook зробив сервіс прямих відеотрансляцій Live доступним для всіх користувачів 6 квітня. Засновник компанії М. Цукерберг зазначив, що завдяки Live користувачам буде простіше створювати відео й ділитися ними з друзями. На його думку, запуск відеосервісу для всієї аудиторії Facebook змінить уявлення людей про спілкування в соціальних мережах.

***

17.05.2016

Twitter перестанет учитывать ссылки при подсчете знаков в сообщении

Слухи о том, что Twitter намерен снять лимит на 140 знаков в сообщении, появляются с завидной регулярностью. Как правило, они так и остаются слухами. Но в сеть просочилась очень правдоподобная информация. Как стало известно агентству Bloomberg, в течение двух недель Twitter перестанет учитывать ссылки и изображения при подсчете знаков в сообщении, пишет IGate.

Ограничение в 140 знаков является своеобразной визитной карточкой Twitter. Д. Дорси, создатель соцсети, неоднократно говорил, что такой лимит вынуждает пользователей быть лаконичными и креативными. Тем не менее, в настоящее время размер ограничения подсчитывается не вполне корректно. Если пользователь хочет прикрепить к своему сообщению короткую ссылку, то она отнимает у него 23 знака. Попытка прикрепить изображение отнимает еще 24. Таким образом, на выражение своей мысли пользователю остается лишь 93 знака – в 1,5 раза меньше заявленного. В течение двух недель эта печальная

ситуация изменится. Очевидно, что после этого увеличения общего лимита знаков ждать не приходится.

***

17.05.2016

Як школярі використовують медіа: соціологічне дослідження «Соцінформ» та MyMedia

Як підлітки користуються соцмережами?

Якщо ви хочете достукатися до школярів, то вам у соцмережу «ВКонтакте» – 85 % дітей з усієї України використовують її щодня. За «ВКонтакте» слідує Instagram, а у Facebook і Twitter діти не дуже активні. Серед школярів навіть Google+ став більш популярним, ніж Facebook.

Facebook більш популярний в обласних центрах, менше – у малих містах, найбільш популярний у Західній Україні – 22 %, найменш – на Донбасі, 7 %.

Дівчата використовують Twitter більше, ніж хлопці. Чим старшими є діти, тим частіше вони його використовують. Він найбільш популярний у Південній Україні, найменш – у Західній.

Viber значно популярніший серед дівчат. Загалом, усіма соцмережами дівчата користуються частіше, ніж хлопці, крім Facebook. Viber частіше використовується в обласних центрах, і, швидше за все, його популярність ще набиратиме обертів. Нині він найменш популярний на Донбасі, найбільше – на Півдні й Півночі.

«Одноклассники» серед дітей не дуже популярні, перевагу їм віддають дівчата. Та якщо серед інших сайтів соцмереж прослідковується тенденція: чим старшими є діти, тим більше вони ними користуються, то з «Одноклассниками» усе навпаки: чим молодшими є діти, тим більше вони користуються платформою.

«Одноклассники» більш популярні в маленьких містах, ніж в обласних центрах. Західна Україна, яка більше за всіх використовує Facebook, найменше користується «Одноклассниками».

Instagram дівчата використовують частіше, ніж хлопці. Він найбільш популярний на Півночі та в Центрі. «ВКонтакте» користується абсолютна більшість дітей. Найрідше цю соцмережу використовують на Західній Україні.

***

2.05.2016

Искусственный интеллект от Twitter научился определять содержание видеотрансляций

Twitter разрабатывает технологию, которая позволит в реальном времени определять содержание видеотрансляций и давать пользователям быстрые и точные рекомендации. Прямо сейчас тысячи людей по всему миру ведут интереснейшие видеотрансляции. Благодаря технологии, которую

разрабатывают специалисты Twitter, в скором времени вы сможете без труда находить стримы по интересующей вас теме, пишет InternetUA.

Видеотрансляции становятся все более популярными, и для их ведения создано уже несколько мобильных приложений, например Periscope и Meerkat. Недавно к ним присоединился Facebook Live. Однако поиск по видеотрансляциям пока далек от совершенства – часто авторы видео не могут точно обозначить тему своих трансляций, поскольку не знают заранее, что будут снимать.

В Cortex (подразделение Twitter, которое занимается искусственным интеллектом) создали алгоритм, который способен мгновенно распознавать, что происходит в прямом эфире. Система с легкостью определит, играет ли герой трансляции на гитаре, демонстрирует новый электроинструмент или просто дурачится, развлекая зрителей.

Определение содержания видео в реальном времени – впечатляющая функция. Ранее алгоритмы с успехом опознавали объекты на фотографиях, но решить ту же задачу для онлайн-трансляций намного сложнее. Чтобы добиться стабильно хороших результатов, требуются большие вычислительные мощности. Сотрудники Cortex специально для таких целей собрали суперкомпьютер, полностью состоящий из графических процессоров (GPU).

До настоящего времени рекомендации в сервисах просмотра видео основывались на предпочтениях пользователей со сходными интересами. Это достаточно грубое решение проблемы, но и оно неприемлемо для онлайн-трансляций. Команда Cortex стремится создать новую систему рекомендаций, основанную на распознавании содержания трансляций.

Новая технология основана на так называемом глубоком обучении. Такой подход предполагает наличие мощной нейросети, которой демонстрируется множество изображений, снабженных ключевыми словами. Постепенно нейросеть учится отождествлять объекты, которые ей демонстрируются, с их языковыми обозначениями.

Б. Эдельман, профессор Гарварда, известный своими публикациями по данной теме, считает, что новая технология может быть полезной не только для системы рекомендаций, но и для фильтрации видео, защищенного авторским правом, а также для исключения нежелательного контента, например насилия и порнографии.

***

19.05.2016
Facebook тестує відеокоментарі

Найбільша соціальна мережа у світі Facebook, як завжди, на передовій прогресу і, можливо, саме тому продовжує утримувати лідируючі позиції на ринку, не даючи спуску конкурентам. Днями компанія приступила до обкатки чергової новомодної можливості: користувачам з ряду країн стала доступна можливість залишати відеокоментарі, пише Finance.UA.

Як повідомляє інформаційний портал VentureBeat, обрані користувачі, яким пощастило стати учасниками закритого бета-тестування, тепер можуть відповідати на записи в соцмережі за допомогою відеоповідомлень. Для цього в полі коментаря потрібно вибрати іконку фотокамери. До цього опція служила виключно для вставки зображень, однак тепер за її допомогою стало можливим записати на камеру відеозвернення й розміщувати їх у коментарях до постів.

Очевидно, Facebook прагне таким чином підвищити інтенсивність обміну відеоконтентом і заодно створити для своїх користувачів більш сприятливі умови для спілкування. Уже нині сумарний час переглядів відеороликів у соцмережі перевищує 100 млн год, і якщо експеримент вдасться, темпи зростання цього показника помітно зростуть.

***

10.05.2016

Twitter запускает новую вкладку «На связи»

Twitter запускает новый сервис, который поможет пользователям легко находить и подписываться на интересующие их аккаунты, пишет Sostav.ua.

Список рекомендуемых Twitter блогов будет отображаться в новой вкладке «На связи» (Connect), а выбор будет основываться на разных факторах – на аккаунтах, на которые пользователь уже подписан, на твитах, которые ему нравятся, на популярных в его регионе блогах, на актуальных событиях, происходящих в мире в этот момент, и т. д. Twitter также будет пояснять, почему рекомендует подписаться именно на эти аккаунты.

Новый сервис также по желанию пользователя может автоматически синхронизироваться с его адресной книгой, и, если кто-то из его друзей или знакомых зарегистрируется в Twitter, он получит об этом уведомление во вкладке «На связи».

Twitter планирует постоянно улучшать работу сервиса, чтобы сделать список рекомендуемых аккаунтов максимально релевантным. Новая функция уже доступна в приложениях Twitter на платформах iOS и Android для всех пользователей сервиса. Чтобы воспользоваться ей, нужно обновить приложение Twitter до последней версии. Более подробную информацию о вкладке «На связи» можно узнать в справочном центре Twitter.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

20.04.2016

Большинство украинских СМИ освещали «панамский скандал» поверхностно и эмоционально, догоняя Facebook

В VoxUkraine проанализировали динамику и структуру обсуждения Pamagates в медиа-пространстве Украины, чей Президент, один из немногих, после 3 апреля оказался в эпицентре мирового расследования, пишет Телекритика.

Были проанализированы деловые всеукраинские издания, региональные издания, интернет-СМИ и телеканалы на основе данных Mediapulse Monitoring Agency. Также проанализировали 397 статусов на Facebook в период с 3 по 5 апреля, 247 медиа-сообщений за 3 апреля и 1607 сообщений за 4 апреля.

По данным исследования, абсолютное большинство (94 %) статусов на Facebook в первые сутки после обнародования информации об офшорах имели явно выраженный негативный тон. Из 1270 наиболее популярных аккаунтов лишь 4 % имели нейтральный тон (например, предлагали дождаться официального расследования) и 2 % пытались оправдать наличие имени Президента в «панамских документах».

4 апреля, после первой реакции Президента, негативный тональный оттенок имели уже 78 % статусов, количество нейтрального контента возросло до 8 % и статусы с оправданиями действий Президента – до 14 %. Но уже на следующий день количество негативных реакций опять возросло на 4 %.

Значительная часть статусов, содержащих оправдание наличия фамилии П. Порошенко в офшорных списках, параллельно апеллировала к неэтичности расследования «Следствия.инфо». Интенсивность освещения «панамских документов» в Facebook начала активно снижаться уже 5 апреля.

Что касается традиционных СМИ, то с 3 апреля их сообщения фактически дублировали дискуссию в соцсетях: 85 % сообщений имели негативный тон, медиа прибегали к таким формулировкам, как «тайный налоговый маневр» («Медиа-вектор»), «махинации действующего Президента» («Новое время»), «двойная жизнь Президента» («Громадське»), «слепой траст существует только в его фантазиях» (24 канал), «офшорная бизнес-империя» и «офшорка Президента» (24 канал).

В первой половине дня 4 апреля (до 13:00) количество обвинительных сообщений начинает идти на спад и составляет 70 %, что также повторяет динамику дискуссии в соцсетях.

Однако уже с 4 апреля структура обсуждения темы на Facebook и в традиционных СМИ начала резко отличаться. Так, если на дискуссию Facebook реакция Президента не особенно повлияла и доля негативных сообщений

оставалась на уровне 78 %, то в СМИ доля позитивных и нейтральных сообщений резко возросла и по состоянию на 17:00 4 апреля равнялась 51 %.

Исследователи указывают, что можно было избежать подобного количества негативных сообщений в традиционных СМИ, если бы пресс-служба Президента своевременно отреагировала на обнародование фамилии П. Порошенко в «панамских документах».

Авторы приходят к выводу, что качество контента в украинском медиа-пространстве остается поверхностным, особенно когда вопрос касается сферы, для понимания которой нужны базовые экономические знания. Медиа-дискурсу также недостает профессиональности освещения такого принципа государственного управления и антикоррупционной политики, как конфликт интересов. Большинство медиа обращаются к привычной эмоциональной расцветке новостей (как негативной, так и позитивной) вместо того, чтобы предлагать аудитории объяснение базовых терминов, необходимых для понимания ситуации.

При этом соцсети выступают в качестве спускового механизма для обсуждения определенной темы в СМИ и являются традиционно более радикальными в высказываниях.

***

10.05.2016

На Львівщині в соцмережах стартував новий флешмоб до Дня Європи

Наприкінці цього місяця, 29 травня, Львівщина відзначатиме День Європи, пише Західна інформаційна корпорація.

Долучитися до святкування цієї дати запрошують і жителів та гостей регіону. Зокрема, продемонструвати свої бачення європейських цінностей пропонують користувачам соціальних мереж, взявши участь у фотоакції #LvivRegionEU. Ініціатором акції є департамент міжнародної технічної допомоги та міжнародного співробітництва облдержадміністрації. Про це повідомляє прес-служба ЛОДА.

«Щоб долучитися до акції, слід розмістити фотографії з хештегом #LvivRegionEU у своїх соціальних мережах і розповісти про те, як бути європейцем у буденному житті, – повідомила директор департаменту Т. Шепіленко. – Таким чином громадяни зможуть показати, що Європа починається з кожного з нас».

Найкращі фотографії розмістять на офіційних сторінках департаменту міжнародної технічної допомоги та міжнародного співробітництва ЛОДА.

За словами Т. Шепіленко, з нагоди святкування Львів відвідає польський дипломат, голова представництва Європейського Союзу в Україні Я. Томбінський, а жителі міста зможуть приєднатися до свята на численних розважальних заходах.

***

18.04.2016

Флешмоб від Філатова у Facebook набирає обертів

Флешмоб від очільника Дніпропетровська Б. Філатова #вільнілюдимаютьзброю набирає обертів, пише видання Дніпроград.

У соціальній мережі Facebook хештег використовують активно й розміщують фото зі зброєю. У флешмобі вже прийняли участь нардепи А. Денисенко та О. Ляшко, член політичної сили «УКРОП» та екс-кандидат на пост міського голови Павлограда Є. Терехов, адвокат О. Томчук та її чоловік – правозахисник Д. Томчук, учасник АТО О. Чистопольцев, відомий фотохудожник І. Булгарін та ін.

Серед учасників багато воїнів АТО і волонтерів. Це не тільки жителі Дніпропетровщини, а й різних куточків України.

Нагадаємо, 17 квітня Б. Філатов закликав містян брати участь у флешмобі #вільнілюдимаютьзброю. «Коли треба було захищати Батьківщину, держава не ставила в 2014 р. питання, де ми беремо зброю. Підтримайте флешмоб #вільнілюдимаютьзброю. Приєднуюсь», – зазначено в повідомленні.

***

16.05.2016

Финал «Евровидения-2016» установил новый рекорд в Twitter

Зрители финала «Евровидения-2016» написали более 7 млн твитов, посвященных конкурсу, тем самым побили прошлогодний рекорд на 1 млн постов, пишет InternetUA.

Самым обсуждаемым моментом конкурса была победа украинской исполнительницы Джамалы – в течение минуты после объявления результатов было опубликовано около 73 тыс. твитов.

Вторым самым обсуждаемым моментом финала «Евровидения-2016» стало выступление С. Лазарева, во время которого пользователи Twitter написали за 1 мин около 54 тыс. сообщений.

Также в Twitter активно обсуждали выступления Д. Тимберлейка. После его появления на сцене пользователи написали за 1 мин 32 тыс. твитов, а публикация самого Д. Тимберлейка набрала свыше 7 тыс. ретвитов.

***

16.05.2016

Ламаючи стереотипи: в ОДА Дніпропетровська зустріч з популярним блогером

Gorky Look – відомий блогер, майстер політичної сатири, письменник і «кацаповєд». Його інтернет-дописи набирають рекордну кількість переглядів, а книжку змітають з полиць як гарячі пиріжки. Послухати лекцію професора

«лукової кафедри» та поставити йому запитання зможуть мешканці Дніпропетровщини. ОДА продовжує ламати стереотипи і влаштовує зустріч з популярним політичним сатириком у власних стінах. Про це повідомив радник очільника області Ю. Голик, пише інтернет-видання Дніпропетровська ОДА.

«Тільки-но в ОДА пройшла презентація першої книги відомого письменника та блогера Павла Паштета Бєлянського, як ми вже готуємо для мешканців області новий сюрприз. Цього разу запрошуємо на зустріч з популярним сатириком Gorky Look. Комусь може здатися, що адмінбудівля і відомий блогер несумісні. Ми продовжуємо руйнувати ці стереотипи!» – зазначив радник голови ОДА.

Gorky Look, або просто «Гіркий лук», веде блог на платформі «Живого Журналу». Він легко та іронічно висміює відсталий «русский мир», розповідає про «ватну мутацію» та відстоює «антикацапську» позицію. Блог ведеться у форматі «кафедри», де «Гіркий лук» – професор, а читачі – студенти.

Лекції «лукової кафедри» читають студенти, військові, домогосподарки та бізнесмени, в Україні та за кордоном. Блог було створено в листопаді 2014 р. і вже за кілька місяців збирав рекордну кількість переглядів та коментарів. На основі дописів автор створив свою першу книгу «Ноука от Горького Лука. Сборник лекций по кацаповедению».

26 травня до Дніпропетровської облдержадміністрації запрошують усіх бажаючих познайомитися з «професором». Для цього потрібно зареєструватися: натиснути на банер заходу на сайті ОДА та заповнити анкету.

«Будуть цікава бесіда, дружня атмосфера, кава та смаколики. Обіцяємо фото з блогером та автографи. Приходьте в гості!» – запросив радник.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

8.05.2016
Маркетинг-2020: Куда исчезнет бум социальных сетей?

Сейчас технологии развиваются очень быстро и непредсказуемо. Эту ситуацию очень сложно смоделировать, но давайте послушаем мнения больших компаний, которые, как никто другой, знакомы с инновациями и потребительским рынком, пишет Hyser.

Компании Taco Bell и General Electric, которые знают о маркетинге все, поделились прогнозами о будущем брендов на следующие пять лет.

Комментарии экспертов сходятся на том, что современный маркетинг с каждым годом будет все более разнообразным.

1. Персонализация

Мобильные устройства заполонили нашу планету. Сегодня смартфон – это та вещь, которой хочет обладать каждый. Прогнозируется, что на

протяжении ближайших пяти лет между брендами и людьми установится более персонализированная связь. Поэтому успешными станут те компании, которые создадут более персонализированный контент для клиентов.

Когда пользователи с помощью социальных медиа получили возможность заявлять о своих предпочтениях, компании смогли использовать эту информацию себе на благо, а брендинг превратился в беседу.

Покупатели хотят от брендов хорошего качества и больше информации об их внутреннем функционировании. Они проверяют бренды и выбирают те, которые являются наилучшими.

Если работа компании проходит в открытом режиме, вся важная информация доходит до покупателей, а цена соответствует качеству, то такой бренд получит успех на рынке продаж.

Люди не хотят быть просто жертвами рекламы, люди хотят, чтобы их услышали и приняли во внимание их предпочтения. Вот поэтому компаниям нужно хорошенько поработать и постараться создать беседу вокруг каждого покупательского опыта.

Очень важно вызвать интерес: «Что это за продукт? Как он работает? И как о нем отзываются другие люди?». Необходимо вовлечь покупателей в эту беседу, чтобы они думали о бренде и хотели поделиться информацией с другими.

2. Популяризация видеоконтента

В мире с развитыми мобильными технологиями видео пользуется особой популярностью. Людей привлекают как маленькие видеофрагменты, так и большие видеоролики. Все это привносит новую лепту в современный маркетинг.

Есть версия, что бренды станут более гибкими, а креативные агентства будут объединяться в единое целое. Сами покупатели будут создавать брендированный контент, что поможет увеличить рекламные возможности. Для брендов будет очень важно закрепить лидирующие позиции в предпочтения своих клиентов.

3. Виртуальная реальность

В современном мире виртуальная реальность стала привычной средой. С ее помощью можно рассказывать свои истории, оказаться в любом уголке мира, общаться с друзьями, которые находятся за сотни тысяч километров.

Телевидение уже не столь популярно, поэтому маркетинг должен сконцентрироваться на поиске новых субъектов с высококачественным контентом.

Нужны издания, которые адаптируют контент, контекст и медиа к молодой аудитории. К примеру, Mic, Vice, Fusion, Circa, и Quartz уже хорошо с этим справляются.

Инновационные медиа-приложения помогут устранить помехи на пути. Свою аудиторию сначала нужно завоевать. Современный мир полон возможностей для прямых бесед – умейте их использовать.

4. Программирование

Все каналы будут «программируемыми». Технология programmatic уже достигла соцмедиа, очень скоро она охватит остальные digital-каналы. Прогнозируется, что через пять лет и радио, и телевидение тоже станут открытыми к получению маркетинговых активов через programmatic. Возможно, что маркетинг в ближайшее время будет базироваться на этой технологии.

Парадокс в том, что успешное медиа – это медиа, о котором больше не говорят и воспринимают как само собой полагаемое. «Быть онлайн» – это как выйти из дому с телефоном, все помнят и все так делают. Такое перевоплощение ожидается и в сфере социальных сервисов на протяжении ближайших пяти лет.

Вы знали, что Facebook зарабатывает на рекламе больше, чем какой-либо популярный телевизионный канал? И не думайте, что в ближайшем будущем что-то круто изменится. Instagram также имеет свой персональный маркетинг, он крутит 15-секундные видео, что похожи на рекламу.

Соцсети предлагают брендам большие возможности. Поэтому с каждым годом маркетинг будет только умножать свое разнообразие и превращаться в сложную систему. Работа маркетолога существенно усложнилась. Кроме того, через пять лет база покупателей значительно расширится.

Инновации заполоняют наш мир, и очень скоро мы уже не будем представлять нашу жизнь без этих новшеств. Компании также должны приобретать новые знания, иначе они не смогут быть достаточно конкурентоспособными на рынке.

5. Хорошие компании будут производить только хорошие продукты

Компании будут ориентироваться на покупателей, а люди будут доверять только тем брендам, которые создают хорошие продукты.

Хорошие агентства будут производить продукты, а не предоставлять услуги. Качество товара и удовлетворения покупателя будет одной из главных целей компаний. Важно, чтобы клиент оценил бренд и возвращался к нему вновь и вновь. Агентства и компании, которые поймут принципы деятельности Кремниевой долины, займут лидирующие позиции и будут впереди остальных.

Данные станут более индивидуализированными, что позволит использовать информацию для реализации целей. Продукты, что упрощают жизнь людям, будут очень популярными. Задачей маркетологов будет как можно эффективнее участвовать в этом процессе и формировать крепкие отношения между звеньями.

Люди будут ценить культуру предоставления товаров и услуг, поэтому бренды, связанные с культурой, одержат успех на рынке.

6. Большие данные станут конфиденциальными

Ценность данных в современном мире очень ощутима. С помощью мобильных телефонов мы узнаем погоду, курс валют, ситуацию о пробках на дороге в режиме реального времени.

Метаданные делают жизнь лучше и проще. Но прошлогодний скандал в системе здравоохранения в Великобритании по поводу того, что личная

информация была продана страховым фирмам, подтвердил недостаточность понимания всего процесса, ведь личная информация не имеет ценности в контексте метаданных.

Через пять лет конфиденциальность личных данных будет в безопасности, а люди станут более опытными в их использованию.

Традиционная модель маркетинговых отношений в современном мире себя изжила. Новшества очень важны, но весомой задачей становится умение пользоваться новшествами без ущерба для себя.

Исчезает такое понятие, как разработка продукта, или она будет существенно ускорена для экономии времени и денег. Теперь не маркетинг будет влиять на продукт, а совсем наоборот. И самое главное – будет четко слаженная взаимосвязь людей, отвечающих за маркетинг, и людей, занимающихся разработкой.

7. Мобильный Интернет и мобильные технологии

Мобильные технологии заполонили наш мир. Теперь люди, ранее живущие без телефона, получат доступ к ним с помощью современных девайсов.

Основной целью маркетолога будет выиграть битву за культурное влияние. Маркетинг успешных игроков будет таким же качественным, как и их продукты и услуги. Великие маркетологи сами создадут свою брендовую историю. Реклама на баннерах начнет работать в улучшенном формате. Медиа будут дополнять сайты ценностью и давать клиентам то, что они хотят, а взамен получать хорошие результаты.

Маркетинг станет более творческим, что принесет еще больше пользы и успехов компаниям, а также поспособствует развитию брендовой среды.

***

20.04.2016

YouTube: онлайн-видео приносит до 50 % выше ROI, чем ТВ-реклама

Google вновь атаковал рекламные бюджеты для ТВ, заявив, что ролики на YouTube приносят больший ROI для брендов. Интернет-гигант исследовал кампании в восьми странах, отметив, что в 77 % случаев «YouTube приносит больший возврат инвестиций, чем ТВ», пишет Marketing Media Review.

Исследование проанализировало 56 кейсов брендов из шести отраслей и отмечает, что инвестиции в YouTube должны быть увеличены от двух до шести раз. В случае 17 кейсов Google отметил, что «в более 80 % оптимизаций медиа-микса расходы на YouTube должны быть увеличены вдвое».

«Мы обнаружили, что хотя ТВ сохраняет свое влияние в эпоху диджитала, digital видео недополучает инвестиций в нескольких категориях, которые мы изучили в Великобритании, Франции и Германии», – отметил генеральный директор MarketShare, компании, проводившей анализ по заказу Google. Заявление компании вызвало сильную реакцию ТВ-отрасли. Так,

директор по исследованию в Thinkbox отметил, что «настоящая ценность ТВ-рекламы не просто возвращать инвестиции (заставляя людей покупать продукты), но она достигает лучшего возврата на инвестиции на высшем уровне инвестиций». «ТВ лучше, чем другие каналы, выстраивает бренды и приносит большую прибыль», – добавил он.

***

10.05.2016

YouTube автоматизирует покупку рекламы в вирусных роликах

Крупнейший глобальный видеохостинг запустил новый рекламный продукт под названием Google Preferred Breakout Videos, позволяющий брендам автоматически размещать спонсированные объявления в самых популярных видеороликах, сообщает cossa.ru. Продукт является расширением инструмента Preferred для покупки рекламы в видео, представленного YouTube еще в 2014 г. и позволяющего рекламодателям резервировать показы среди 5 % самых популярных каналов в сервисе.

Новый функционал, анонсированный на ежегодном мероприятии Brandcast CEO YouTube С. Войжитски, призван предоставить брендам возможность автоматизированного размещения рекламы в «вирусах», имеющих тенденцию возникать «из ниоткуда» и еще не попавших в список «раскрученных» каналов, пишет Marketing Media Review.

***

17.05.2016

Facebook показывает рекламу в зависимости от настроения пользователя

Бельгийская полиция предупредила граждан поостеречься от использования кнопки Reactions на Facebook, которую добавили на сайт в феврале, сообщает geektimes.ru. Этой кнопкой пользователи выражают своё отношение к публикации, выбирая одну из шести реакций – грусть, злость, любовь, восхищение и т. д. Полиция выяснила, что Facebook учитывает эмоции пользователя для повышения эффективности рекламы. Алгоритмы определяют, когда человек скорее всего находится в хорошем расположении духа – и тогда показывают ему рекламу.

Ограничив количество реакций шестью, Facebook упрощает работу рекламной системы, потому что обрабатывать эмоции от миллиарда пользователей в реальном времени не так просто, пишет Marketing Media Review.

Настроение клиента – ещё один параметр, по которому рекламодатели могут таргетировать рекламу. Так, тысяча показов для счастливых пользователей, очевидно, будет дороже тысячи показов для пользователей в нейтральном настроении.

Эксперты предупреждали сразу после появления этой функции, что Facebook будет использовать её для коммерческой выгоды. В то же время сам Facebook уверял, что реакции сделаны для удобства людей, чтобы они могли выражать разнообразные эмоции, а не только ставить лайки.

Кстати, вскоре после запуска Facebook подтвердил, что реакция злости на какое-то сообщение расценивается как «эмоциональное вовлечение», что может привести к увеличению количества таких сообщений в ленте.

***

17.05.2016

Instagram запустит аналитику для маркетологов

Социальная сеть тестирует детальную аналитику под названием Insights, чтобы предоставить маркетологам данные о фолловерах и постах. Информация будет включать возраст, географическое местоположение, род и активность фолловеров по часам. Топ-посты будут демонстрировать все размещённые изображения за определенный период времени (семь или 30 дней). Аналитика даст лучшее понимание того, в какое время пост получает большее вовлечение, кто взаимодействует с контентом, находят ли отклик у фолловеров старые посты, позволяя нарисовать более точную картину вовлечения, пишет Marketing Media Review.

***

17.05.2016

Facebook расширил показ видеорекламы брендов на Audience Network

Facebook запустил поддержку новых форматов видеорекламы в Audience Network. Нововведение позволит компаниям расширить охват рекламы, предназначенной для повышения узнаваемости бренда, сообщает searchengines.ru. Кроме того, они впервые получат возможность показывать видеорекламу десктопной аудитории, пишет Marketing Media Review.

В ближайшие недели для показа в Audience Network будет доступна видеореклама в двух форматах:

– ***in-stream*** – объявления, которые транслируются перед (pre-roll), во время (mid-roll) или после видеоролика (post-roll) на сайте или в приложении как на мобильных, так и на десктоп-устройствах;

– ***in-article*** – реклама этого формата будет показываться между параграфами текста и будет автоматически воспроизводиться, когда станет видна, как минимум, половина пикселей изображения.

В первую очередь эти видеообъявления появятся в мгновенных статьях. «Рекламодатели смогут расширить свои кампании за пределы Facebook и привлечь большую аудиторию, обеспечить более широкий масштаб и охват», – комментирует нововведение Б. Вогель, менеджер по продукту Facebook

Audience Network. Чтобы запустить показ видеорекламы в Audience Network, нужно будет поставить соответствующую галочку при выборе мест размещения.

Новая опция будет доступна всем рекламодателям. Первым рекламодателем, использующим новые форматы видеорекламы, стал Jack in the Box. Поддержу видеорекламы на свои сайты и в приложения добавили такие издатели, как Sports Media Group, Daily Mail и Mashable.

По данным Facebook, пользователи социальной сети ежедневно просматривают 100 млн часов видео, а длительность просмотра видео в Instagram за последние полгода возросла более чем на 40 %.

Facebook запустил рекламную сеть Audience Network два года назад. Она представляет собой сеть сторонних приложений и сайтов, которые рекламодатели могут использовать для увеличения охвата рекламы в Facebook и Instagram.

***

30.04.2016

Музыка «ВКонтакте» стала платной

Популярная российская социальная сеть «ВКонтакте» представила первое музыкальное приложение с легальным контентом. В будущем прослушивание музыки через него будет платным, пишет ProstoTECH.

Первое приложение с легальной музыкой «Музыка “ВКонтакте”» работает для мобильных устройств на операционной системе iOS от Apple. Сервис появился в магазине приложений AppStore. Создатель приложения – ООО «Объединенное медиа-агентство» (United Music Agency, UMA), которое занимается легализацией музыки для интернет-холдинга Mail.Ru Group, сообщает газета «Ведомости».

В сервис можно войти через аккаунт «ВКонтакте». В будущем прослушивание музыки будет платным, но пока в условиях приложения нет информации о стоимости подписки. «Музыка “ВКонтакте”» предлагает тариф «Базовый», который позволяет слушать музыку бесплатно в течение 90 дней, а также загружать композиции общей продолжительностью 60 мин, чтобы прослушивать музыку без доступа к Интернету. По истечении срока подписки данная функция станет недоступной.

По мнению экспертов, стоимость сервиса будет «средней по рынку».

Отметим, что на данный момент «ВКонтакте» подписала соглашения о сотрудничестве практически со всеми крупными мировыми и российскими правообладателями.

***

4.05.2016

В приложении Instagram появится новый вид рекламы

Приложение Instagram расширяет свой сервис для рекламодателей. Теперь на фотохостинге можно размещать не только фотообъявления, но и видеорекламу, пишет OneProg.ru.

Популярное приложение Instagram пользуется большим спросом не только среди пользователей, но и рекламодателей. Чтобы расширить возможности для рекламодателей, руководство приложения решило пересмотреть и увеличить возможности своего рекламного формата «карусель». В Instagram добавится видеореклама, длительностью не более 1 мин.

Формат рекламы «карусель» в Instagram запущен не так давно, впервые он появился в приложении в марте 2015 г. Примечателен он тем, что рекламодатели могли поместить в одно объявление несколько фотографий товаров.

После обновления формат «карусель» будет модернизирован и появится возможность добавлять в него короткие видеоролики. Правила следующие: в «карусели» может быть пять или менее видео, длительностью до 1 мин.

В настоящее время этот формат тестируется. Первыми воспользоваться его услугами смогут лишь несколько топ-партнеров Instagram. Но сразу после теста он станет доступен всем желающим.

***

6.05.2016

Сеть Instagram тестирует обновленный интерфейс бизнес-аккаунтов

Популярная сеть Instagram приступила к тестированию обновленного интерфейса, предназначенного для бизнес-аккаунтов. В новой версии появился расширенный набор инструментов, позволяющий компании напрямую взаимодействовать со своими клиентами, пишет HiTech-News.ru.

После обновления интерфейса в учетную запись какой-либо фирмы добавляется специальная кнопка Contact. Благодаря последней клиент может написать непосредственно компании, а также узнать ее адрес на карте. Расположена новая функция в верхней части профиля, вблизи другой кнопки «Подписаться».

Уточняется, что после нажатия на Contact у пользователя соцсети появляется дополнительная панель, позволяющая через электронную почту связаться с нужной компанией. Кроме того, открывается также местоположение фирмы на карте. Одновременно с этим написать компании в личные сообщения по-прежнему нельзя. Когда именно функция станет доступна для всех, не уточняется.

***

11.05.2016

Facebook обновил рекламные инструменты на своей платформе и в Instagram

Теперь рекламодатели смогут находить на этих площадках тех клиентов, которые заинтересованы именно в их продуктах и услугах. Нововведения помогут им стимулировать спрос и увеличить объём мобильных продаж, пишет Sostav.ua.

Изменения коснулись следующих рекламных инструментов:

1. Динамическая реклама. Динамические объявления (Dynamic Ads ранее известные как Dynamic Product Ads) теперь доступны и в Instagram. Этот функционал также был расширен на туристические компании – появились дополнительные опции указания места и времени путешествия.

2. Индивидуально настроенные аудитории (Custom Audiences). Изменения позволят рекламодателям настраивать таргетинг таким образом, чтобы определять наиболее активных посетителей сайта компании, исходя из частоты посещений пользователя и времени, проведённом на сайте.

Запуск данных обновлений в компании связывают с меняющимися привычками людей в поиске новых продуктов и услуг. В частности:

– они всё больше времени проводят с мобильными устройствами и всё чаще используют приложения или мобильные версии сайтов вместо поиска в браузере;

– именно мобильные устройства помогают постоянно растущему числу пользователей находить, выбирать и покупать новые продукты.

В Facebook также поделились следующей статистикой:

– 1 из 5 мин, проведенных пользователями со своими мобильными устройствами, тратится на использование Facebook или Instagram (Comscore);

– 98 из топ-100 рекламодателей в Facebook в конце 2015 г. также размещали рекламу в Instagram;

– в Facebook была размещена информация о более чем 2,5 млрд товаров;

– 440 млн людей за последние три месяца видели динамическую рекламу товаров на Facebook.

Своим опытом в использовании обновлённых инструментов Facebook поделился Р. Горка из компании Allegro – крупного интернет-аукциона, основанного в Польше: «Allegro использовал инструмент Facebook для создания индивидуально настроенных аудиторий, и это привело к крайне положительным результатам: число посетителей сайта и прибыль стали расти с каждым месяцем. С помощью Facebook мы получили возможность определять, какие пользователи так и не приобрели продукты, отложенные в корзину, а также тех людей, которые заходили на наши страницы и искали нужные им товары. За время использования тестовой версии инструмента Facebook наш показатель ROI возрос почти в 5,5 раз. Инструмент для создания индивидуально настроенных аудиторий помог нам привлечь больше покупателей, которые проводят на нашем сайте больше времени, изучают большее число товаров и чаще совершают покупки».

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

6.05.2016
По сообщениям в Twitter можно определить уровень счастья

Сотрудники Университета Айовы разработали специальный алгоритм, который по сообщениям в Twitter определяет уровень счастья и степень удовлетворенности человека своей жизнью. Исследователи проанализировали 3 млрд твитов. Ученые отобрали сообщения со словами «я», «меня» и «мой», рассказывает The TeCake.

Исследование показало: твиты счастливых людей не менялись в течение долгого времени. Они не зависели от таких событий, как голод, землетрясения, крупные спортивные мероприятия или выборы. Между тем, согласно данным предыдущих исследований, внешние события сильно влияют на настроение людей. Также специалисты установили, что несчастные люди часто использовали личные местоимения, союзы и ненормативную лексику в своих сообщениях, сообщает Настроение по материалам сайта Meddaily.

Участники, недовольные своей жизнью, на 10 % чаще пользовались такими словами, как «следует», «будет», «ожидать», «надеяться» и «нуждаться», отражающими их надежды на будущее. Счастливые люди, довольные жизнью, в основном использовали в твитах больше 140 символов. В их сообщениях чаще встречались позитивно окрашенные слова и поднимались позитивные темы. Например, они писали о здоровье, сексуальности, деньгах и религии.

***

11.05.2016
Половина подростков из США зависят от смартфонов

К такому неутешительному выводу пришёл колумнист CNN, основываясь на данных Common Sense Media, пишет InternetUA.

Любопытно, что в своей зависимости уверены 50 % детей в возрасте 12–18 лет, а количество уверенных родителей достигает 59 %.

Х. Хаос изучает явление «цифрового детокса». По мнению исследователя, предпочтение поиграть дома, а не встретиться с друзьями – первый тревожный звоночек. Однако в Америке пока не рассматривают зависимость от смартфонов как болезнь, но в Китае уже лечат в специальных учреждениях.

По данным Common Sense Media, 80 % детей проверяют раз в 60 мин, 72 % желают общаться с виртуальными друзьями через SMS и социальные

сети. Семьдесят семь процентов родителей уверены, что гаджеты отвлекают чад во время разговоров. Такая невнимательность часто приводит к семейным ссорам. Это подтверждают 32 % детей и 36 % взрослых.

***

24.04.2016
Появился способ бороться с зависимостью от Facebook

Новый плагин для браузера Chrome под названием Focusbook призван бороться с зависимостью от Facebook. Об этом сообщает The Next Web, пишет InternetUA.

После установки плагина в браузер Focusbook начнет контролировать, сколько времени пользователь тратит на Facebook. После слишком длительной сессии плагин закроет страницу с соцсетью полупрозрачным окном и спросит, зачем вам нужен Facebook в данный момент, или потребует вернуться к работе. Если пользователь действительно занят чем-то важным, плагин даст еще немного времени. В противном случае вкладка с социальной сетью будет закрыта. В отличие от прочих контролирующих плагинов Focusbook предлагает пользователю порефлексировать, нужен ли ему Facebook прямо сейчас или он просто поглощает время.

***

12.05.2016
Как Facebook контролирует нашу жизнь

Детище М. Цукерберга стремится стать единственной соцсетью, которой вы будете пользоваться, пишет InternetUA.

«Сейчас пользователи проводят в Facebook в среднем 50 мин в день. Как и большинство знакомых, я захожу туда, чтобы следить за новостями друзей и хвастаться своей жизнью. Это в какой-то мере забавно, но я точно не трачу на это час в день. А теперь Facebook планирует отбирать у нас еще больше времени», – пишет журналист Observer С. Содха в колонке для The Guardian.

«В целом я провожу в соцсетях намного больше времени, например, в том же Twitter. Среднестатистический британец тратит на это 80 мин в день и заводит аккаунты в среднем в четырех соцсетях», – добавляет автор.

Она рассказывает, что люди проглядывают новостную ленту соцсетей в общественном транспорте, во время просмотра телевидения, когда ждут в очереди в банке, и это в некотором роде снижает их продуктивность.

Но, с другой стороны, позитивные стороны соцсетей для С. Содхи перевешивают негативные: она успевает читать новости в пути и получает информацию, которая не поместилась бы в формат обычной ежедневной газеты.

«Полагаю, как и большинство людей, я подстраиваю соцсети под свою жизнь, а не наоборот. Поскольку можно одновременно сидеть в соцсетях и

заниматься чем-то еще – путешествовать, смотреть, ждать – естественно, что время их использования может увеличиться. Но всему наступает предел, поскольку есть вещи, требующие от нас полного внимания: чтение книг детям, обеды с друзьями, рабочие встречи, – предупреждает журналист. – Так что желание Facebook захватить больше нашего времени можно рассматривать как стремление оттянуть на себя время, которое мы проводим в других соцсетях. Facebook хочет получить и те 30 мин, которые мы проводим в Twitter, LinkedIn или Pinterest. Так же, как Microsoft пыталась стать единственным "правильным" программным обеспечением, а Apple – единственным выбором для тех, кто покупает телефон или планшет, Facebook хочет стать единственной соцсетью, которой вы будете пользоваться».

Она отмечает, что у Facebook есть все шансы на успех: 85 % взрослых, использующих Интернет (исключая Китай), имеют аккаунты на одном из сервисов Facebook (Instagram, Messenger и WhatsApp).

Facebook прошел путь от скромного университетского сайта для общения до сайта, где признаются в любви и тайно следят за теми, с кем не общались годами.

«Стремление Facebook быть "приложением для всего" вызывает беспокойство. Мы платим за Facebook, просматривая рекламу. Именно поэтому компания заинтересована в том, чтобы мы проводили в этой соцсети больше времени: больше времени – больше рекламы. Стратегия роста Facebook рассчитана на постоянное создание контента под пользователя, чтобы мы все чаще применяли сеть для всех своих нужд», – объясняет журналист.

Это, по ее мнению, главный недостаток плана Facebook: чем больше рекламы будет производиться, тем больше будет падать ее качество, и в результате соцсеть рискует утопить сама себя.

***

11.05.2016

Чем больше комментариев пишет пользователь, тем меньше в них смысла – исследование

Ученые из Университета Южной Калифорнии провели исследование, результаты которого показали, что чем больше комментариев оставляет пользователь, тем более бессмысленными они становятся, пишет Телекритика со ссылкой на Apparat.

Исследователи просмотрели более 55 млн комментариев на социальном новостом сайте Reddit, на котором зарегистрированные пользователи могут размещать ссылки на любую понравившуюся информацию в Интернете, и обнаружили закономерность: пользователи, потратившие на комментирование больше часа, отправляли короткие, малоинформативные комментарии, получавшие в итоге мало голосов и ответов.

По словам одного из соавторов исследования Э. Феррара, длительное комментирование негативно влияет на слог пользователя и содержание его

комментариев. Он уточнил, что во время исследования изучалась лишь длина и грамматическая изящность комментариев, тогда как природа их агрессивности во внимание не бралась. Этот вопрос будет изучен на следующих этапах исследования.

Пока ученые исследовали только Reddit, однако в будущем планируют рассмотреть и другие платформы, в том числе Twitter и Facebook, чтобы выявить эту закономерность и там.

***

14.05.2016

Как вычислить лгуна в соцсети

Группа научных работников утверждает, что электронные письма могут многое рассказать о представителях слабого и сильного пола, которые пользуются Интернетом, пишет InternetUA со ссылкой на «Вестник здоровья».

Отмечается, что благодаря проведению экспериментов врачи зафиксировали уникальную закономерность. Психологи уверены, что мужчины и женщины, хранящие тайну, часто меняют язык сообщений, а также свое поведение при общении с товарищами и друзьями. Такую информацию медики рассказали после проведения комплексных наблюдений.

Научные работники полагают, что их открытие поможет в разработке специальной системы, автоматически фиксирующей ложь. К примеру, в социальных сетях могут появляться сообщения с текстом: «Внимание! Данный пользователь предоставляет Вам ложные сведения».

По словам сотрудников из Мэрилендского университета, в новых исследованиях приняли участие более 1 тыс. респондентов, которые хранили тайну в течение семи лет своей жизни. Для дальнейшей реализации испытаний психологи пригласили только 61 человека.

***

2.05.2016

Ретвиты назвали тормозом прогресса

Ретвиты (распространение чужих записей в Twitter) признали тормозом прогресса. Ученые Корнелльского и Пекинского университетов доказали, что они создают «когнитивную перезагрузку», сообщает Naked Science, пишет InternetUA.

Ретвитить или нет?

Человеческий мозг, в соответствии с традиционным сценарием, после прочтения должен осмыслять информацию. Однако ретвиты запустили совершенно другой алгоритм, который вызывает «когнитивную» перезагрузку. Теперь пользователи стали, в первую очередь, думать, делать ретвит или нет. Это снизило эффективность работы мировой системы и замедлило прогресс.

Суть эксперимента

Добровольцев, набранных из числа студентов Пекинского университета, разделили на две группы. Первой показывали сообщения из социальной сети Weibo (китайский аналог Twitter) и давали на выбор две возможности: ретвит или переход к следующему сообщению. У второй группы не было возможности сделать ретвит.

После этого студентов попросили пересказать содержимое сообщений. Участники из первой группы ошибались вдвое чаще, чем из второй.

Ученые подчеркивают, что хуже запоминались те сообщения, которыми студенты делились.

Во втором эксперименте студентов, до этого общавшихся в социальных сетях, попросили прочесть статью из журнала New Scientist. «Когнитивная утечка» проявилась и здесь: студенты, поделившиеся материалом, поняли его хуже остальных.

В чем дело

Профессор кафедры развития человека из Корнелльского университета Ц. Вон рассказал, что люди всё реже публикуют оригинальные мысли или идеи – им проще поделиться чужим материалом одним нажатием кнопки. Однако пользователи не понимают, что регулярные ретвиты имеют и обратную сторону, которая осложняет взаимодействие между людьми. По словам ученого, ретвит и другие способы распространения контента приводят к дополнительной нагрузке на мозг. Кнопки привлекают пользователей, и если упростить их, часть нагрузки с мозга получится снять.

Маніпулятивні технології

10.05.2016

Большой скандал в Facebook: журналисты обвинили крупнейшую соцсеть в цензуре

Журналисты американского издания Gizmodo опубликовали две статьи с комментариями бывших сотрудников Facebook, вызвавшие большой резонанс в СМИ. По словам анонимных редакторов, которые ранее работали над разделом Trending Topics в Facebook, выбор новостей модерируется вручную и даже подвергается цензуре, пишет Телекритика.

Бывшие редакторы Trending Topics рассказали, что многие материалы о Республиканской партии США сознательно не включались в список популярных тем, даже когда их активно обсуждали пользователи Facebook. Кроме того, бывшие сотрудники раскрыли механизм работы Trending Topics.

Что произошло

В первой публикации, появившейся еще в марте, собеседники Gizmodo сообщили, что работали в специальном подразделении Facebook, которое занималось формированием ленты Trending Topics – специального блока

социальный сети, куда попадают самые обсуждаемые и популярные темы в определенном регионе. Это один из наиболее мощных новостных источников в мире, который единовременно читает около 167 млн человек только в США.

Во второй публикации Gizmodo раскрыли еще более поразительные данные. Согласно информации сразу от нескольких бывших сотрудников, многие статьи и темы, касающиеся Республиканской партии США, сознательно убирались из трендов.

В чем суть цензуры

Facebook позиционирует Trending Topics как совершенно непредвзятый источник новостей, но сразу несколько бывших сотрудников компании признались, что он таковым не является.

В своей работе редакторы следуют определенным правилам, но выбор тем все равно остается за ними. По утверждению экс-редакторов Trending Topics, их, например, просили не использовать название Twitter, заменяя его словами «в социальных сетях», а любые новости о Facebook проходили жесткую проверку у начальства, прежде чем попасть в тренды.

Бывшие редакторы раскрыли методику так называемой новостной инъекции – иногда темы, которые казались руководству Facebook важными, но еще не получали достаточной популярности, вводились в Trending Topics искусственным путем. Такими темами, например, были расстрел редакции Charlie Hebdo и обсуждение войны в Сирии.

«Подавление» статей о республиканцах вряд ли было связано непосредственно с установкой начальства. Один из собеседников, сторонник республиканцев, признался, что так произошло просто потому, что многие из редакторов были сторонниками демократов и скептично относились к статьям о партии оппонентов.

Как это работает

В 2014 г. Facebook специально для работы над разделом нанял значительное количество журналистов. Среди них были как вчерашние выпускники, так и бывшие сотрудники ведущих мировых СМИ. Большая часть из них – не старше 30 лет. Их работа заключалась в том, чтобы проверять «трендовость» той или иной темы, переписывать ее заголовок, писать подводку в виде двух-трех предложений и подбирать релевантное видео. Норма в день составляла около 20 материалов.

Бывшие редакторы признаются, что данная работа имела мало общего с журналистикой и скорее напоминала дейстия роботов. Более того, редакторов оставляли в статусе внештатных сотрудников, а после увольнения просили нигде не указывать свой опыт работы в Facebook. В результате из начального состава департамента не осталось практически никого.

К чему это привело

После публикации расследования Республиканская партия США выступила с обвинениями в адрес Facebook. Ситуацию накаляет также близость президентских выборов в США, в которых социальные сети могут сыграть определяющую роль.

Вслед за обвинениями Т. Стоки (вице-президент Facebook и глава подразделения Trending Topics) выслал в издания BuzzFeed и TechCrunch официальную позицию компании (журналу Gizmodo соцсеть не отвечала в течение двух месяцев). «Популярные темы формируются при помощи алгоритма, а потом просматриваются и утверждаются участниками моей команды, чтобы убедиться, что это действительно трендовые новости, а не просто похожие или ошибочные», – заявил Т. Стоки, отвергнув все обвинения.

Он также сообщил, что исследовал конкретные кейсы, описанные в публикациях Gizmodo, в частности с искусственным форсированием тренда BlackLiveMatters, и убедился, что никакого форсирования не было. Помимо этого, Т. Стоки сообщил, что никакого предвзятого отношения к статьям о Республиканской партии тоже не было, а люди, нарушающие рабочую дисциплину, мгновенно увольняются.

Большинство крупных мировых СМИ уже опубликовали новости по мотивам скандала. Примечательно, что эта тема мгновенно попала в Trending Topics.

***

15.05.2016

М. Цукерберг проведет внутреннее расследование в Facebook

Создатель всемирно популярной соцсети Facebook М. Цукерберг проводит расследование после появления информации о том, что все новости в ленте подвергаются цензуре, пишет InternetUA.

М. Цукерберг рассказал, что начинает проводить расследование на своей собственной странице в соцсети. Основатель Facebook сообщает, что выступает за то, чтобы каждый человек мог свободно высказать свое личное мнение в Интернете. Весь мир станет лучше, если люди с разными убеждениями и взглядами получат возможность общаться друг с другом без каких-либо проблем. Именно это и делает социальные сети самым лучшим средством. Решение провести внутреннее расследование появилось после сообщения, что новостная редакция сдерживает посты консервативного характера.

***

27.04.2016

Жителя Запорожья накажут за антиукраинскую пропаганду в Интернете

Житель Запорожья, который занимался антиукраинской пропагандой в соцсетях, разоблачен сотрудниками СБУ. Об этом сообщает пресс-служба управления ведомства в Запорожской области, пишет InternetUA.

Запорожец, деятельность которого пресекли сотрудники спецслужбы, в апреле познакомился с помощью Интернета с «представителем “ДНР”».

Последний за денежное вознаграждение предложил ему размещать в социальных сетях антиукраинские материалы.

В дальнейшем, выполняя задание кураторов «ДНР», житель Запорожья использовал несколько групп одной из российских социальных сетей. Там он размещал специально подготовленные публикации с призывами к насильственному изменению конституционного строя Украины, гражданского неповиновения действующей власти и другие тенденциозные материалы, целью которых было увеличение социальной напряженности в обществе и дестабилизация общественно-политической обстановки в регионе.

В ходе обыска по месту проживания любителя «русского мира» была изъята компьютерная техника с доказательствами антиукраинской деятельности.

Решается вопрос о возбуждении уголовного производства по ст. 109 (действия, направленные на насильственное изменение конституционного строя), ст. 110 (посягательство на территориальную целостность Украины) Уголовного кодекса Украины.

***

21.05.2016

Политолог из Гарварда уличил власти Китая в миллионах фейков в соцсетях

Власти Китая ежегодно публикуют в социальных сетях около 488 млн фейковых постов, чтобы отвлечь внимание граждан от плохих новостей и политических дебатов. Об этом сообщает Bloomberg со ссылкой на исследование политолога из Гарвардского университета Г. Кинга, пишет InternetUA.

Г. Кинг выяснил, что практически все подобные фейки создаются работниками правительственных учреждений. Ранее считалось, что пропагандой в китайских социальных сетях занимаются обычные люди, которые получают за каждый такой пост по 50 центов.

Политолог также обнаружил, что пропагандисты занимались несколько иной деятельностью, чем предполагалось ранее. Они не высмеивали власти других стран и не вступали в политические дебаты, а публиковали посты, в которых отмечали положительные моменты жизни в стране и писали о великом революционном прошлом Коммунистической партии Китая.

Исследователь уверен, что такие публикации создаются для отвлечения внимания граждан от важных общественных и политических проблем. По его данным, на 178 постов в китайских социальных сетях приходится один подобный проправительственный фейк.

12 мая в Китае заработал онлайн-сервис, с помощью которого пользователи Интернета смогут сообщать властям о распространяемой в социальных сетях и блогах недостоверной информации, в том числе о слухах и сплетнях.

22.04.2016
Facebook, Snapchat и Twitter ограничат свободу детей в соцсетях

К 2018 г. Facebook, Snapchat, Instagram и Twitter разработают специальные алгоритмы, которые будут запрещать детям заводить аккаунты в социальных сетях без согласия их родителей. Механизм обработки их согласия или отказов еще в разработке. Об этом пишет The Financial Times, сообщает МедиаБизнес.

В 2018 г. в Евросоюзе вступят в силу новые правила пользования социальными сетями: дети младше 16 лет не смогут создавать личные аккаунты без согласия родителей. В связи с этим, необходимо разработать ограничивающие алгоритмы.

Издание приводит данные, что в Великобритании сегодня около 20 % детей младше 11 лет имеют аккаунты в Facebook, хотя согласно внутренним правилам соцсети, пользователями могут быть те, чей возраст превышает 13 лет. И около 80 % британских подростоков от 12 до 17 лет имеют аккаунты в Facebook.

Во Франции аккаунты в Facebook разрешают только лицам старше 16 лет.

***

20.04.2016
ФБР держит в секрете уязвимость нулевого дня в Firefox

Исследователь из Международного института информатики в Беркли (ICSI) Н. Уивер полагает, что ФБР больше года знает об уязвимости нулевого дня в Firefox, успешно пользуется этим и отказывается раскрывать сведения о дыре разработчикам браузера, пишет InternetUA.

В марте 2013 г. ФБР удалось захватить сервер форума любителей детской порнографии под названием Playpen, который действовал в анонимной сети TOR. Это позволило выследить более тысячи его завсегдатаев. В результате 137 граждан США привлекли к ответственности, а данные об иностранных пользователях Playpen передали правоохранительным органам в других странах.

Один из американских пользователей форума, на которого указало ФБР, отрицает свою вину. Он требует, чтобы технические средства, которые использовались для идентификации пользователей форума, проанализировали независимые эксперты.

Во время последовавшей за этим судебной тяжбы стало известно, что на страницах Playpen был размещён эксплойт, собиравший информацию о

посетителях. ФБР яростно защищает своё право сохранить в секрете принцип его действия.

Для доступа к сайтам в сети TOR служит специальный браузер, основанный на Firefox. Скорее всего, уязвимость, при помощи которой ФБР следила за педофилами с Playpen, найдена именно в нём. Н. Уивер полагает, что если это действительно так, то та же уязвимость почти наверняка присутствует и в обычном Firefox.

По мнению исследователя, ФБР поступает безответственно. Если не исправить эту уязвимость, она рано или поздно попадёт не в те руки – последствия могут оказаться катастрофическими. «Эксплойт в Firefox, попавший не в те руки, может запросто привести к заражению миллионов компьютеров троянами-вымогателями или позволить неприятелю проникнуть в правительственные сети при помощи прицельного фишинга», – предупреждает он.

***

26.04.2016

В Иране сетевую цензуру обходят через спутниковое ТВ

В наше время не одна и не две страны мира могут «похвастаться» государственным сетевым фильтром, который ограничивает доступ граждан к ресурсам Интернета. Иран, наряду с Китаем, является одним из лидеров в данной области и блокирует доступ практически ко всем социальным сетям, YouTube, почтовым сервисам, множеству торговых площадок и сайтов новостей. Но иранские пользователи используют для обхода блокировок не только привычный VPN, который в стране работает плохо и тоже отсекается властями. Команда активистов The Net Freedom Pioneers создала систему Toosheh, которая позволяет буквально скачивать Интернет через тарелки спутникового ТВ, пишет InternetUA.

Власти Ирана очень щепетильны в вопросах сетевой безопасности, всё началось еще в 2010 г. после знаменитого инцидента со SCADA-червем Stuxnet. По сути, в Иране под запретом даже VPN и трафик HTTPS, такие соединения блокируются, что делает практически невозможным даже просмотр видеороликов, не говоря о скачивании больших файлов.

Toosheh предлагает интересную альтернативу. Достаточно подключить к приставке спутникового ТВ флешку, соединиться с каналом Toosheh, включить запись и оставить работать. Сам канал не показывает ничего, кроме текстовых инструкций по настройке системы, но менее чем за час на флешку закачается гигабайт данных из внешнего запрещенного Интернета, который в цикле раздается активистами The Net Freedom Pioneers.

Toosheh поставляет данные в формате .ts-файлов, то есть, на первый взгляд, это обычное видео MPEG. Однако если флешку с данными подключить к компьютеру и расшифровать их с помощью официального приложения, пользователь получит свежий подбор контента, в который входят ролики с

YouTube, выступления TED talks, информация с заблокированных сайтов новостей и др. Авторы Toosheh собирают каждый свежий информационный пакет вручную и заявляют, что в сборники входят образовательные и развлекательные материалы, а также контент, посвященный правам человека. К примеру, здесь можно найти не только новости и интересные видео, но и инструкции по скачиванию и установке Tor, Psiphon и Lantern.

К сожалению, Toosheh не позволяет запрашивать конкретные файлы и скачивать контент по требованию. Пользователям придется довериться вкусу и выбору разработчиков из The Net Freedom Pioneers.

Тестирование Toosheh стартовало еще в октябре 2015 г., и на сегодняшний день официальное приложение для десктопов скачали более 56 тыс. раз. Власти Ирана, конечно, не оставили данную инициативу без внимания. Так, сайт Toosheh давно заблокирован на территории страны. Впрочем, для обхода запрета пользователям достаточно воспользоваться Tor или каким-либо другим прокси-инструментом. Спутниковый канал Toosheh, тем не менее, не заблокирован до сих пор. Авторы инициативы полагают, что власти просто не имеют технической возможности его заглушить, а спутниковое телевидение в Иране распространено очень широко. По официальным данным Национального совета сопротивления Ирана, спутниковые тарелки есть у 70 % жителей страны.

***

25.04.2016

Бельгія закликала відкрити поліції доступ до даних соцмереж

При плануванні терактів злочинці використовують для переговорів соціальні мережі на зразок Viber, WhatsApp, Twitter, Skype і Facebook. Тому правоохоронні органи ЄС повинні мати можливість легко отримувати доступ до даних користувачів у соцмережах, якщо це потрібно для розслідування. Про це заявив міністр юстиції Бельгії К. Геєнс, повідомляє ВВС, пише LB.ua.

За його словами, раніше телекомунікаційні оператори активно співпрацювали з правоохоронними органами, а ось компанії, що керують соціальними мережами, не настільки зговірливі.

ЄС, на думку міністра, потрібно якомога швидше налагодити роботу із соцмережами. Однак це не означає, що потрібно масово стежити за всіма. Пріоритет слід віддавати розвідці та вибору окремих цілей.

***

26.04.2016

У Росії блогера звинуватили в екстремізмі за статтю про Сирію

Слідчі Головного слідчого управління Слідчого комітету Росії офіційно висунули звинувачення в екстремізмі блогеру А. Носику, повідомляє радіо «Свобода», пише LB.ua.

«Експертиза, проведена в рамках розслідування кримінальної справи, підтвердила винність особи в інкримінованому йому злочині», – ідеться на сайті Слідчого комітету РФ.

Раніше стало відомо про результати лінгвістичної експертизи однієї з публікацій блогера в «Живому Журналі», згідно з якими в ній міститься «розпалювання ворожнечі до національно-територіальної групи сирійців».

Кримінальну справу стосовно А. Носика порушили в листопаді минулого року, після того як він опублікував у ЖЖ пост під назвою «Стерти Сирію з лиця землі». У суперечливому пості блогер висловив думку, що Сирія завжди була й залишається «реальним військовим супротивником», і порівнював Сирію з нацистською Німеччиною.

За статтею про екстремізм А. Носику загрожує позбавлення волі до двох років.

Сам блогер свою провину заперечує, заявляючи, що своїм текстом він надав «усебічну підтримку» Повітряно-космічним силам Росії під час їхньої операції в Сирії.

***

17.05.2016
Twitter продает данные Путину и отказывает ЦРУ

Компания Twitter решила, что американские спецслужбы больше не смогут покупать услуги у фирмы Dataminr, которой Twitter предоставляет полный доступ к потоку сообщений своих пользователей, пишет Wall Street Journal. При этом Dataminr спокойно продолжает продавать данные телекомпании RT, которую финансируют российские власти во главе с В. Путиным, – то есть Twitter отдает предпочтение России перед США, подчеркивает автор, пишет 24news.com.ua.

Враждебное отношение Кремниевой долины к американским спецслужбам и правоохранительным органам достигло новых высот, когда компания Twitter отказала Центральному разведывательному управлению в предоставлении данных на основе твитов – но продолжает обслуживать организацию, подконтрольную В. Путину.

Как выяснила Wall Street Journal, компания Twitter решила, что американские спецслужбы больше не смогут покупать услуги у фирмы Dataminr, которая поддерживает уникальные отношения с Twitter. Dataminr – единственная компания, которой Twitter предоставляет полный доступ к потоку из сотен миллионов твитов ежедневно и разрешает продавать полученную информацию клиентам. Dataminr применяет алгоритмы «больших данных» для выявления необычных событий в режиме реального времени. Те клиенты, которые могут иметь выгоду от мгновенного получения такой информации, скажем, хедж-фонды и новостные организации, платят большие деньги за оповещения.

Последние два года Dataminr предоставляла свои услуги ЦРУ в рамках экспериментальной программы. Затем ЦРУ и Dataminr заключили контракт о дальнейшем предоставлении услуг. Однако, как заявляют источники, председатель совета директоров Twitter Д. Дорси в последний момент наложил вето на этот контракт, так как не захотел продолжать оказывать помощь разведывательным службам. Непонятно, какая судьба ожидает другое соглашение, которое Dataminr ранее заключила с Министерством внутренней безопасности. Согласно проводимой Twitter новой политике, Dataminr должна отказаться на своем веб-сайте от претензий на то, чтобы она «обслуживала клиентов из государственного сектора, в первую очередь предоставляя информацию тогда, когда в опасности оказываются жизни людей».

Среди клиентов, получающих оповещения от Dataminr, – широковещательная компания RT, созданная и финансируемая российским правительством. В. Путин заявлял, что его правительство создало RT в попытке сломить «англосаксонскую монополию на информационные потоки». RT сообщила, что является клиентом Dataminr, в своей новости об отказе Twitter Центральному разведывательному управлению. Агенты российской Федеральной службы безопасности, ранее называвшейся КГБ, через RT имеют неограниченный доступ к оповещениям, в которых Twitter отказала ЦРУ.

На прошлой неделе один бывший американский руководитель по борьбе с терроризмом объяснил значение тех оповещений, в которых Twitter отказала ЦРУ. По его словам, Dataminr информировала спецслужбы, пока не появились новости об атаках исламистов в Сан-Бернардино, Париже и Брюсселе. «Эти оперативные предупреждения в режиме реального времени особенно полезны в том случае, когда совершается сразу несколько нападений. В таких случаях даже незначительное предостережение может радикально изменить ситуацию, – сказал этот руководитель. – Dataminr в этих случаях предупредила нас о произошедшем за 15–30 мин до появления новостей, а это значит, что мы смогли эффективнее отреагировать на эти нападения».

ЦРУ владеет пятью процентами Dataminr через свое подразделение венчурного капитала In-Q-Tel (Twitter также владеет пятью процентами.) Это одна из нескольких инвестиций, вложенных управлением в стартапы, отслеживающие информацию из таких открытых источников, как твиты. Представитель ЦРУ в ответ на утрату данных из Twitter заявил, что информация из твитов «крайне важна для выявления случаев готовящихся терактов» с участием «Исламского государства» и «Аль-Каиды».

Второй человек в ЦРУ, Д. Коэн, выступая в сентябре с речью в Корнелльском университете, рассказал, что «твиты и прочие сообщения в социальных сетях, рекламирующие их деятельность, зачастую дают такую информацию, которая в своей совокупности обладает реальной разведывательной ценностью».

Отстаивая свое решение, компания Twitter заявила, что не разрешает использовать свои данные «в разведывательных целях». Но Dataminr не ведет никакой разведки, поскольку в тех твитах, которые перерабатывает компания в

поисках данных, нет ничего секретного. В любом случае, Dataminr использует публичную информацию из Twitter, чтобы выявить те или иные события, а не собирать информацию о тех или иных людях.

Аргументы компании вызвали удивление даже среди тех, кто обычно считает, что конфиденциальность информации – важнее безопасности. «Если Dataminr просто сортирует публичные данные, а затем отказывается передавать полученное разведывательному сообществу, то в такой информации мало смысла, – объяснил журнал Wired. – Но если, с другой стороны, Dataminr дает такую информацию, на получение которой должен быть допуск, то предоставление такой информации никем не регулируемому хедж-фонду кажется проблематичным».

В отличие от Twitter, компания Apple по крайней мере заявила о защите личной тайны пользователей, когда отказалась помочь ФБР в получении доступа к iPhone, которым пользовался один из террористов в Сан-Бернардино. Но вопреки мрачным предостережениям главы Apple Т. Кука о создании «черного хода», когда ФБР воспользовалось программным обеспечением третьей стороны для взлома указанного iPhone, ни о каких нарушениях конфиденциальности не сообщалось.

Похоже, Кремниевая долина думает, что потребители и клиенты хотят от нее начала войны с американским разведывательным сообществом и правоохранительными органами. Может, компании информационных технологий и правы, заявляя, что конфиденциальность частной информации важна, но сейчас Twitter и Apple сознательно создают препятствия американской безопасности даже тогда, когда ничья конфиденциальность не находится под угрозой.

***

6.05.2016

В России пользователя «ВКонтакте» осудили за репост материала «Крым – это Украина»

В российской Твери за репосты в социальной сети «ВКонтакте» об аннексированном РФ Крыме пользователь А. Бубеев приговорен к двум годам и трем месяцам колонии-поселения, сообщает радио «Свобода», пишет Телекритика.

Адвокат осужденного С. Сидоркина рассказала, что А. Бубеев обвинялся в публичных призывах к осуществлению экстремистской деятельности и призывах к деятельности, направленной на нарушение территориальной целостности России. А поводом для уголовного преследования послужили репост материала «Крым – это Украина» публициста Б. Стомахина и картинка на эту же тему, которую пользователь разместил на своей странице.

По мнению самого А. Бубеева, его преследуют за убеждения.

Отметим, это уже не первый срок, который мужчина будет отбывать в колонии. Так, в августе прошлого года он уже был осужден за репосты

аналогичных материалов и картинок и приговорен за возбуждение ненависти или вражды к 10 месяцам лишения свободы с отбыванием наказания в колонии-поселении.

***

12.05.2016

Тернополян позбавили спілкування в російській соцмережі

Популярну тернопільську інтернет-спільноту заблокувала російська соцмережа, пише Газета «Місто».

Найчисельнішу на теренах Тернопільщини групу «Від Тарнополя до Тернополя» заблокувала соціальна мережа «ВКонтакті». Група налічувала 172 тис. користувачів.

***

16.05.2016

Треть страниц российской соцсети «ВКонтакте» рассказывают о способах самоубийства – Роспотребнадзор

Согласно расследованию российского надзорного ведомства Роспотребнадзор, около трети из запрещенных законодательством России описаний способов самоубийства в русскоязычном секторе Интернета приходится на соцсеть «ВКонтакте». Об этом сообщает Би-би-си, пишет ОстроВ.

«С 1 ноября 2012 г. Роспотребнадзором в рамках Единой системы электронного взаимодействия проведена экспертиза более 9555 ссылок на страницы сайтов [русскоязычного сектора] в информационно-коммуникационной сети Интернет, из них 9357 страниц содержали информацию о способах совершения самоубийства и призывы к совершению самоубийства», – отмечается в сообщении ведомства.

«При этом на паблики и страницы “ВКонтакте” приходится 3050 ссылок и страниц, признанных содержащими запрещенную информацию», – говорится в сообщении.

При этом, как отмечают в Роспотребнадзоре, в социальных сетях и на видеохостингах по-прежнему часто можно найти описания способов совершения самоубийства, сопровождающиеся фото- и видеоматериалами.

***

18.05.2016

Вьетнам заблокировал Facebook из-за массовых протестов

Во Вьетнаме пропал доступ к ряду социальных медиа, включая Facebook. Впрочем, причина проблемы довольно очевидна, ведь неприятное явление совпало с массовыми протестами в городах страны, пишет IGate.

Протесты во Вьетнаме начались еще в апреле. Они связаны с массовой гибелью рыбы в водах центральных провинций страны. Протестующие связывают катастрофу с деятельностью построенного недавно тайваньского металлургического комплекса Formosa Plastics. Гибель рыбы началась практически сразу после того, как сталелитейный завод стал сбрасывать отходы в местные водоемы.

Протестующие требуют от правительства принять меры и закрыть предприятие, но их требования игнорируются. Более того, правительство принимает меры для того, чтобы не допустить проведения протестов и митингов. Последнее время ситуация накалилась до предела. В крупных городах, таких как Хошимин и Ханой, протесты перешли в столкновения с полицией. В одном лишь Хошимине были арестованы более 300 человек. В стычках многие протестующие получили ранения.

Доступ к Facebook пропал практически сразу. Правительство никак не комментирует это, но многие полагают, что социальная сеть была заблокирована, чтобы не дать протестующим возможности координировать свои действия.

***

19.05.2016

В Днепродзержинске суд вынес приговор мужчине, проводившему антиукраинскую пропаганду в соцсетях

Баглейский районный суд Днепродзержинска вынес приговор местному жителю, который вел активную антиукраинскую пропаганду в социальных сетях. Уголовное производство проводилось следователями Управления СБ Украины в Днепропетровской области, пишет InternetUA.

Об этом ИА «МОСТ-ДНЕПР» сообщили в пресс-службе УСБУ в Днепропетровской области.

Сообщается, что в течение марта – июня 2014 г. 31-летний мужчина через социальные сети в Интернете распространял дискредитирующие материалы об украинской власти, призывы к антиконституционному перевороту, дестабилизации ситуации в стране и изменения границ территорий и государственной границы Украины.

Суд признал администратора виновным по ч. 2 ст. 109 (действия, направленные на насильственное изменение или свержение конституционного строя или на захват государственной власти) и ч. 1 ст. 110 (посягательство на территориальную целостность и неприкосновенность Украины) Уголовного кодекса Украины.

Он приговорен к лишению свободы сроком на три года условно.

***

29.04.2016

Facebook почав активніше співпрацювати з українською владою щодо розкриття інформації про користувачів

Facebook оприлюднив свій звіт щодо фактів розкриття інформації про користувачів соцмережі на вимогу урядів різних країн. Такий звіт компанія оприлюднює двічі на рік, пише UkrainianWatcher.

Загалом звіт містить запити не лише щодо Facebook, а й Facebook Messenger, WhatsApp та Instagram, які також належать корпорації.

Згідно з документом, за другу половину 2015 р. представники української влади дев'ять разів звертались до Facebook щодо отримання інформації про певних користувачів. При цьому задоволено було чотири запити.

У першій половині 2015 р. запитів було сім, але з них задоволено було лише один. А в другій половині 2014 р. був лише один запит, який не був задоволений.

***

22.05.2016
СБУ вычислила в соцсетях пособника российских террористов

Сотрудники СБУ в социальной сети «ВКонтакте» установили гражданина, который инициативно контактировал с боевиком так называемой террористической организации ДНР, пишет InternetUA.

Как сообщает пресс-группа УСБУ в Херсонской области, во время общения в сети Интернет террорист предложил жителю г. Херсона за деньги совершить поджог военной техники одной из частей в областном центре с применением коктейлей «Молотова». Условием расчета за «проделанную работу» должно быть сообщение в средствах массовой информации о совершенном террористическом акте.

Мужчина отказался от преступной предложения, поскольку понимал, что последствия могут быть трагическими и привести к человеческим жертвам.

От имени Службы безопасности Украины херсонцу объявлено официальное предостережение. В случае повторного совершения таких действий, его привлекут к уголовной ответственности по ст. 258 Уголовного кодекса Украины (террористический акт), а если эту инкриминируют статью, то злоумышленнику грозит наказание от 5 до 10 лет лишения свободы.

***

20.05.2016
Казахстан на время остался без соцсетей и мессенджеров

В Казахстане перестали работать социальные сети Facebook, «ВКонтакте», Twitter, Instagram и мессенджеры Viber и WhatsApp. Об этом сообщает радио «Аззатык» (отделение радио «Свобода» в Казахстане), пишет InternetUA.

Все коммуникационные сервисы были недоступны примерно около часа. Некоторым пользователям удалось получить к ним доступ с помощью VPN.

Жители Казахстана связывают массовое отключение мессенджеров и соцсетей с проведением 21 мая митинга против земельных поправок. По данным портала, с 17 мая за призывы к несанкционированным митингам по стране арестовали более 20 человек.

В настоящее время, судя по сообщениям пользователей Twitter из Казахстана, доступ к сервисам восстановлен.

***

29.04.2016

Спецслужбы смогут взломать любой компьютер на планете

Американские спецслужбы могут взломать любой компьютер – конечно, на основании ордера, выданного судьей. Соответствующие поправки к законодательству одобрил Верховный суд США, сообщает Hightech.fm со ссылкой на агентство Reuters, пишет ProstoTECH.

Ранее мировые судьи могли выдавать ордеры на взлом компьютеров и другие действия в пределах юрисдикции своего суда – это, как правило, один или несколько округов. Однако кибер-преступность меняется, в связи с чем внесение изменений в законодательство необходимо.

Вопрос поднимался ещё в 2013 г., но одобрение Верховного суда авторы поправок получили только сейчас. Теперь документы переданы в конгресс. Если до 1 декабря орган не откажется от принятия поправок, они автоматически вступят в законную силу.

Судья сможет выдать ордер на взлом компьютера, если подозреваемый скрывает свою личность. В частности, он может пользоваться Tor, анонимайзером или другими подобными инструментами. Действие поправок распространяется не только на США, но и на другие страны мира.

Правозащитные организации и гражданские активисты выступают против принятия поправок. К ним уже присоединилась корпорация Google и ряд других компаний.

Противники инициативы утверждают, что поправки позволят американским спецслужбам следить за любым человеком. Если поправки одобрит конгресс, то сотрудники ФБР, АНБ и других органов смогут взломать любой компьютер, даже если на это не будет достаточных оснований.

Проблема захисту даних. DDOS та вірусні атаки

18.04.2016

Новый алгоритм разоблачает анонимов по данным геолокации из двух источников

Группа исследователей из Колумбийского университета и Google обнаружила, что двух независимых наборов данных геолокации достаточно для того, чтобы точно идентифицировать человека. Их алгоритм с лёгкостью определяет посты в разных соцсетях, принадлежащие одним и тем же авторам, и верно сопоставляет данные о платежах по банковской карте с историей звонков у сотового оператора, пишет InternetUA.

Исследователи пытались найти метод, который позволит сопоставить два независимых набора данных, где каждой записи соответствуют географические координаты, и выделить записи, связанные с одним и тем же человеком. Примером таких наборов данных могут служить посты в соцсетях, данные о платежах по банковской карте и данные о телефонных звонках, собираемые сотовым оператором.

Алгоритм, который они разработали, действует в два этапа. Сначала он сравнивает все записи в разных наборах данных попарно и вычисляет для каждой пары рейтинг, описывающий вероятность того, что они принадлежат одному пользователю. Затем он строит полный двудольный граф, в котором каждая запись представляет собой вершину, а соединяющие их дуги имеют вес, равный вычисленному на первом этапе рейтингу. В двудольном подграфе, где все дуги имеют максимальный вес, соединённые между собой вершины принадлежат одному пользователю.

Чтобы испытать точность алгоритма, исследователи проверили его на трёх парах наборов данных. Во время первых двух тестов алгоритм сопоставлял посты в Twitter и Foursquare и в Twittter и Instagram. Он должен был определить, какие аккаунты в разных соцсетях принадлежат одним и тем же людям, используя лишь геолокационные метки на постах, и успешно справился с этой задачей.

Во время третьего теста алгоритм сопоставлял набор данных мобильного оператора, в котором для каждого звонка указано время и координаты ближайшей соты, с набором данных платёжной системы, где каждому платежу соответствует время и координаты терминала. Он связал абонентов сотового оператора с клиентами банка и продемонстрировал при этом более высокую точность, чем другие методы.

«В действительности это показывает, что простой анонимизации данных недостаточно, – говорит специалист по защите данных из MIT Media Lab Ив-Александр де Монжуа. – Нам следует перейти к модели защиты персональных данных посредством безопасности. Вместо анонимизации данных перед публикацией нам нужен технический контроль над тем, кто получает к ним доступ, как они используются и для чего именно».

***

19.04.2016

Для слежки за человеком хакерам нужен лишь его номер телефона

Очередная уязвимость, найденная в современных смартфонах, позволяет следить за их владельцами без использования дорогостоящего оборудования. Все, что нужно хакерам или представителям правоохранительных организаций за слежки за определенной личностью – это его номер мобильного телефона, пишет InternetUA.

Шокирующее открытие сделал немецкий специалист в сфере информационной безопасности К. Нол, основатель компании Security Research Labs, передает портал CNET. Об этом г-н Нол сообщил в эфире популярной в США телепередаче «60 минут», а как доказательство его правоты процесс слежки был продемонстрирован в реальном времени.

«Жертвой» К. Нола стал калифорнийский политик – конгрессмен Т. Лью, к смартфону которого на глазах у зрителей было совершено «несанкционированное» подключение. Сам конгрессмен был заранее поставлен в известность об этом и любезно согласился принять участие в демонстрации возможностей, которые предоставили хакерам разработчики программного обеспечения для мобильных устройств и сотовых сетей.

Во время слежки за американским политиком К. Нол в два счета выяснил его текущее местоположение, смог получить список звонков с его телефона и даже тексты сообщений, отправленных и полученных им в различных сервисах. Название программы, которой пользовался немецкий специалист по информационной безопасности, не раскрывается, но ему действительно понадобился лишь номер конгрессмена, чтобы установить за ним наблюдение в реальном времени.

Т. Лью владеет одним из современных Apple iPhone, однако, по словам К. Нола, модель и марка телефона никак не влияют на возможность слежки за пользователем. Также это не зависит от наличия или отсутствия PIN-кода на SIM-карте или самом смартфоне и от набора установленных приложений.

***

18.04.2016

За год киберпреступники похитили полмиллиарда учетных записей

Без сомнения, век информационных технологий делает нашу жизнь гораздо проще и прогрессивнее, но в то же время мы начинаем сталкиваться с новыми опасностями, пишет InternetUA.

Основной угрозой для нас становится киберпреступность, из-за которой в руках злоумышленников могут оказаться ваши персональные и личные данные.

Компания Symantec провела исследование относительно киберпреступности в области учетных записей. Как выяснилось, буквально за один год преступники смогли украсть порядка полумиллиарда учетных записей пользователей сети Интернет.

В 2015 г. учетных записей, которые преступным путем были обнародованы и попали во всемирную паутину, на 23 % больше, чем годом

ранее. Более того, как заявляют эксперты компании Symantec, реальные цифры могут быть гораздо выше ввиду того, что некоторые компании, опасаясь за свой имидж, скрывают, сколько данных попали в сеть из-за кибермошенничества.

***

20.04.2016

Viber усилит шифрование данных

Мессенджер Viber усилит систему безопасности данных с помощью введения end-to-end шифрования для всех устройств, включая компьютеры PC и Mac, а также смартфоны и планшеты на платформах Android и iOS, пишет InternetUA.

В сообщении компании сказано, что новая система шифрования станет доступной для всех пользователей версии Viber v6.0 и выше в течение нескольких недель.

Пользователю будет доступна информация об уровне безопасности переписки – в правом углу экрана будет отображаться специальный символ серого, зеленого или красного цвета соответственно.

Также Viber объявил о запуске «скрытых чатов», которые не будут отображаться в списке чатов до тех пор, пока пользователь не пройдет идентификацию, которая может заключаться в введении PIN-кода или отпечатке пальца.

***

19.04.2016

Уязвимость в JBoss поставила под угрозу 3,3 млн серверов: их атакует шифровальщик

Специалисты компании Cisco заметили, что злоумышленники используют уязвимость в старых версиях JBoss для атак на серверы компаний. Через эксплуатацию этого бага, распространяется шифровальщик Samsam, впервые замеченный еще в марте 2016 г., пишет InternetUA.

О самом вымогателе Samsam мы писали совсем недавно: эксперты Cisco провели настоящее расследование и заключили, что Samsam и подобные ему угрозы – это новый этап эволюции вымогательского ПО. Тогда в отчете экспертов сообщалось, что шифровальщик распространяется через непропатченные версии JBoss. Оказалось, что масштаб этой проблемы куда больше, чем аналитики Cisco предполагали.

Эксперты Cisco рассказали, что в поисках уязвимых версий они провели дополнительное расследование и выявили более 3,2 млн серверов, работающих с устаревшими версиями JBoss. Потенциально любой из этих серверов уже мог быть заражен бэкдором.

Более детальная проверка показала, что из трёх миллионов серверов скомпрометированы 2100 машин, работающие на 1600 разных IP. Фактически злоумышленники уже провели на эти серверы первую стадию атаки – бэкдор внедрен, осталось лишь загрузить пейлоуды шифровальщика. Исследователи пишут, что пострадавшая аппаратура принадлежит школам, правительственным учреждениям, авиационным компаниям и т. д.

Более того, исследователи выявили, что операторы SamSam – не единственные, кто использует уязвимости в JBoss. На исследованных серверах нашли бэкдоры mela, shellinvoker, jbossinvoker, zecmd, cmd, genesis, sh3ll, а также Inovkermngrt и jbot. Судя по всему, это дело рук разных хакерских группировок.

Наиболее очевидным признаком заражения является появление в системе файлов: jbossass.jsp, jbossass_jsp.class, shellinvoker.jsp, shellinvoker_jsp.class, mela.jsp, mela_jsp.class, zecmd.jsp, zecmd_jsp.class, cmd.jsp, cmd_jsp.class, wstats.jsp, wstats_jsp.class, idssvc.jsp, idssvc_jsp.class, iesvc.jsp или iesvc_jsp.class.

Также специалисты заметили, что на большинстве скомпрометированных серверов используется ПО Destiny, созданное для организации работы библиотек. Оказалось, что компания Fellot, стоящая за разработкой Destiny, сумела создать отличную систему обновлений и исправляет на серверах своих клиентов, в том числе, ошибки в JBoss, а также отслеживает появление подозрительных файлов. Разработчики Fellot охотно согласились помочь экспертам Cisco, уже устранили все проблемы в своем ПО и теперь помогают своим клиентам избавиться от заражения.

***

21.04.2016

Во «ВКонтакте» доступны сканы паспортов, интимные фото и пароли

В социальной сети «ВКонтакте» по-прежнему можно без труда найти копии чужих паспортов, списки паролей и сугубо личные фотографии интимного характера. «Газета.Ru» выяснила, каким образом пользователи продолжают сознательно выкладывать личные данные в сеть и как избежать утечки ценной информации в общественный доступ, пишет InternetUA.

На этот раз «масштабная утечка» документов из «ВКонтакте», как ее успели окрестить некоторые издания, никак не связана с уязвимостью соцсети. В общем доступе оказываются документы, которые когда-то были опубликованы в публичном доступе – к примеру, в открытых сообществах.

Но это никак не мешает пользователям публиковать самые важные документы: номера банковских карт, сканы паспортов и водительских удостоверений.

Кроме того, во вкладке «Документы» можно найти самые разные доклады, рефераты, дипломные работы и даже диссертации.

Ряд СМИ, ссылаясь на программиста из Петербурга, поспешили назвать происходящее «дырой» во «ВКонтакте» и обнаружили поиск по документам через личные сообщения.

В действительности же пользователи соцсети добровольно размещают подобные важные материалы в открытом доступе.

Особенно удивляет наличие в поисковой раздаче документов с названием «пароли». В большинстве своем они принадлежат злостным любителям массового спама, которые создают поддельные аккаунты и охотно делятся ими со своими коллегами по цеху.

Но среди множества фейков можно найти и файлы, содержащие список из связки «логин-пароль» для электронной почты и аккаунтов в социальных сетях. Ради каких целей такие ценные данные размещаются в свободном доступе, неизвестно.

«Газета.Ru» попробовала несколько вариантов размещения документов. В результате те данные, которые были посланы в личном сообщении или размещены в закрытой группе, не выводятся в общий поиск.

Но в поисковую раздачу гарантированно попадают те документы, которые публикуются в открытых сообществах.

Как показали результаты поиска по «Документам», в раздаче действительно встречаются копии документов и документы с претензией на приватность. При этом легко найти не только конкретный документ, но и его автора – в ссылке на материалы содержатся восемь цифр, указывающих на ID пользователя.

Так, оказалось, что копию паспорта со всеми данными молодого человека, проживающего в поселке Куженер в Марий Эл, выложила девушка, проживающая в этом же поселке.

Как объяснил «Газете.Ru» пресс-секретарь соцсети Е. Красников, в случае использования сервиса «Документы» все материалы по умолчанию отмечены как личные и не попадают в поисковую выдачу.

Помимо «личного» документа пользователи могут использовать варианты «Учебный документ», «Книга» и «Другой документ». В этом случае поиск учитывает эти данные и они становятся доступными для публичного использования.

«Начинающие писатели, например, могут сделать свои книги доступными всем, чтобы познакомить со своим творчеством сотни миллионов пользователей “ВКонтакте”», – отметил Е. Красников.

***

21.04.2016

Хакеры научились воровать пароли от Apple ID с помощью SMS

Пользователи устройств Apple массово получают сообщения о якобы блокировке Apple ID. Об этом сообщает Independent, пишет InternetUA.

В сообщении, которое маскируется под техподдержку Apple, предлагается перейти по ссылке. После перехода на сайт, который выглядит как официальная страница компании, пользователям предлагают ввести свой логин и пароль.

После этого всплывает сообщение о том, что аккаунт якобы заблокирован «в целях безопасности». Для разблокировки хакеры требуют ввода персональной информации и номера банковской карты.

Сообщения не имеют ничего общего с техподдержкой Apple и являются результатом хакерской атаки, подчеркивает издание.

***

20.04.2016

Устаревшая версия Git в OS X подвергает пользователей Mac риску кибератак

Даже новейшие версии операционной системы OS X уязвимы к кибератакам, утверждает независимая исследовательница Р. Кролл. Проблема заключается в том, что в составе ОС по умолчанию распространяется устаревшая версия Git 2.6.4, содержащая две уязвимости CVE-2016-2324 и CVE-2016-2315, позволяющие атакующему с доступом к Git-репозиторию выполнить произвольный код на целевой системе, пишет InternetUA.

Уязвимости существуют из-за ошибки целочисленного переполнения в функции path_name(). С помощью специально сформированной команды git push или git pull злоумышленник может скомпрометировать систему. По словам Р. Кролл, преступнику достаточно скрыть код в репозитории и заманить туда жертву. В конце марта текущего года была выпущена исправленная версия Git 2.7.4, однако Apple до сих пор не обновила пакет Command Line Tools, в составе которого распространяется Git.

Согласно словам эксперта, пользователь не сможет самостоятельно обновить или как-то ограничить Git в связи с наличием интегрированной защиты System Integrity Protection (SIP), исключающей возможность модернизации папок и файлов пользователем в определенных защищенных директориях, например, /usr и /bin.

Как выяснилось при ближайшем изучении, путь /usr/bin/git является ссылкой, ведущей к файлу /Applications/Xcode.app/Contents/Developer/usr/bin, через который можно «отключить» уязвимый Git.

Apple пока не сообщала о том, когда планирует выпустить патч для распространяемой компанией версии Git.

***

22.04.2016

В мире насчитывается около 400 млн уязвимых Android-устройств

В выпущенном Google годовом отчете о безопасности Android за 2015 г. упоминается о 71 % устройств, работающих на базе Android 4.4.4 или более поздней версии. По данным Google, в прошлом году насчитывалось порядка 1,4 млрд активных Android-устройств в мире. Значит более 400 млн смартфонов и планшетов не защищены от атаки злоумышленников. Это иллюстрирует проблему, с которой сталкивается Google и пользователи Android. Компания должна разработать обновление, передать его производителю, потом в сервисный центр и, наконец, установить на устройство пользователя «по воздуху», пишет InternetUA.

По словам главного инженера Android Security А. Людвига, сейчас Google ежедневно сканирует 6 млрд приложений и 400 млн устройств. Количество установок потенциально вредоносных приложений сокращается. В 2015 г. такие приложения были установлены через Google Play на 0,15 % устройств из 70 млн. Около 0,5 % мобильных устройств были поражены вредоносными приложениями не только через Google Play, но и через другие источники.

Verity Apps Service отметил увеличение вредоносной активности в 2015 г., не связанное с Google Play. Были остановлены несколько скоординированных попыток установки вредоносных приложений на устройства пользователей из источников, не связанных с Google Play.

***

21.04.2016

Новая технология отличает злоумышленников с краденными паролями от честных пользователей

Компания DB Networks разработала технологию, которая способна отличить честных пользователей от злоумышленников с краденными паролями и враждебно настроенных инсайдеров. Это позволяет быстрее реагировать на проникновение в сеть, пишет InternetUA.

Обычная система управления базами данных проверяет лишь наличие должных прав у обращающегося к ней пользователя или приложения. Её не волнует, каким образом были получены эти права, и для чего именно они используются. Технология DB Networks восполняет этот пробел.

Она следит за двумя аспектами каждого обращения к базе данных. Первый аспект называется указателем базы данных. Он состоит из четырёх атрибутов: сервера, базы данных, её схемы и таблицы, к которым обратился пользователь.

Другой аспект – это так называемый контекст обращения. Он объединяет IP-адрес клиента, порт прослушивания сервера базы данных (listener port), название пользователя или приложения, отправившего запрос, и сервис СУБД, к которому он обратился.

В DB Networks обнаружили, что определённым указателям почти всегда соответствуют одни и те же контексты. Комбинации указателей и контекстов поразительно стабильны, а их число не так уже велико. Появление необычной

пары указателя и контекст – серьёзный повод для беспокойства. В большинстве случаев оно свидетельствует о том, что запрос отправлен злоумышленником или враждебным инсайдером.

Технология реализована в двух продуктах DB Networks: DBN-6300 и Layer 7 Database Sensor. DBN-6300 представляет собой специальное устройство, которое устанавливается между серверами базы данных и серверами приложений. Layer 7 Database Sensor – это софтовый аналог DBN-6300.

После установки продукты DB Networks в течение нескольких дней анализируют трафик между серверами баз данных и серверами приложений и запоминают возможные комбинации указателей и контекстов. Затем они переключаются в режим поиска аномалий и бьют тревогу, когда замечают странные пары указателей и контекстов.

***

21.04.2016

Новый вымогатель способен похищать биткойны и личные данные пользователей

Исследователи компании Proofpoint обнаружили новый вид вымогательского ПО с довольно интересным функционалом. Помимо шифрования файлов на инфицированном компьютере, CryptXXX способен похищать биткойны, пароли и другую важную информацию. За восстановление доступа к данным операторы вредоноса требуют выкуп в размере 1,2 биткойна (приблизительно 515 дол.), пишет InternetUA.

Для распространения CryptXXX злоумышленники используют набор эксплоитов Angler, в частности вредоносное ПО Bedep, способное загружать других троянов на зараженные системы и инициировать мошеннические клики.

Помимо шифрования контента, CryptXXX собирает данные об установленных на компьютере приложениях для мгновенного обмена сообщениями, почтовых клиентах, FTP-менеджерах и браузерах. Вредонос также может похищать биткойны и учетные данные жертвы. По словам экспертов Proofpoint, некоторые признаки указывают на то, что авторство CryptXXX принадлежит создателям эксплоит-кита Angler, вредоносного ПО Bedep и Reveton.

CryptXXX – не единственный новый вымогатель, обнаруженный за последнее время. К примеру, исследователи компании CheckPoint сообщили о появлении новой версии трояна Kovter, способной шифровать файлы на целевом устройстве. По словам экспертов, троян обфусцирует только первую часть файлов. Вредонос быстро зашифровывает большинство интересных ему документов. Поскольку ключ шифрования хранится локально на устройстве, доступ к файлам легко восстановить.

Исследователь компании Emsisoft Ф. Восар обнаружил новое вымогательское ПО AutoLocky, имитирующее известный вредонос Locky. Программа написана на языке AutoIt и не настолько сложна, как оригинальный

Locky. В частности, AutoLocky не использует C&C-инфраструктуру для осуществления обмена ключами в памяти до шифрования файлов. В настоящее время метод распространения вредоноса неизвестен.

Оказавшись на системе, AutoLocky изучает хранящиеся на дисках данные, а затем шифрует их, используя алгоритм AES-128. Вредонос добавляет расширение .locky к файлам на системе, однако в отличие от настоящего Locky не меняет их имена. Ф. Восар уже разработал инструмент, позволяющий восстановить зашифрованный AutoLocky контент.

***

22.04.2016

У Литві тривають кібератаки на держвідомства

Хакерські атаки проти литовських державних відомств тривають кілька тижнів відтоді, як було атаковано сайт парламенту, пише Європейська правда.

Про це заявив директор департаменту безпеки мереж та захисту інформації Служби регулювання зв'язку Литви Р. Райніс, повідомляє видання Delfi.

За його словами, ця безперервна атака є однією з найбільших у литовській історії.

«По суті, це безперервний процес, з минулого тижня почалося, і сьогодні атаки подібні за своїм типом, але змінюються їхні вектори та способи, що створює перешкоди і певні проблеми», – сказав Р. Райніс. Оскільки на сервер Комітету з розвитку інформаційного суспільства була здійснена хакерська атака, постраждали системи інформаційних технологій більше десяти литовських держустанов.

За словами Р. Райніса, за останні кілька тижнів був атакований «більш широкий спектр» інформаційних систем.

З хакерськими атаками зіткнулися парламент, Міністерство сільського господарства, Мінфін, Міноборони, МВС, Міністерство культури, Міністерство охорони здоров'я, а також Державна податкова інспекція, Центр інформації про сільському господарстві та бізнесі, Фонд утримання дітей, Центральне проектне агентство.

Подібні атаки відчули на собі інформаційні системи парламенту, адміністрації президента, МЗС, Міністерства юстиції. У зв'язку з інцидентом канцелярія парламенту і МЗС звернулися в поліцію, ведеться розслідування.

Хакери останнім часом також атакували деякі ЗМІ, компанії комунальних послуг.

За словами Р. Райніса, усі відомства зіткнулися з DDoS-атаками. Під час таких атак надходить безліч запитів з різних точок, внаслідок чого вносяться перебої в роботу інтернет-сайтів через занадто велику кількість відвідувачів. За попередніми даними, хакерські атаки здійснювалися з-за кордону.

***

22.04.2016

Боты «ВКонтакте» самостоятельно выявляют и удаляют пиратские книги

На просторах «ВКонтакте» функционируют специальные боты, которые в автоматическом режиме выявляют, а после удаляют пиратские копии книг. К такому выводу после анализа социальной сети пришли аналитики новостного портала Roem.ru, пишет HiTech-News.ru.

Еще в 2015 г. «ВКонтакте» уведомил о запуске специальной системы, которая не позволяет скачивать файлы с сайта, удаленные по требованию правообладателя. Эта технология позволяет загрузить недопустимый файл на просторы «ВКонтакте», но дальнейшее распространение пиратской копии делается невозможным. Для проверки корректности работы «ВКонтакте» был создан специальный аккаунт без друзей, а после и сообщество, куда загрузили книгу «Обитель» от З. Прилепина, распространение которой запрещено. Через неделю, даже несмотря на то, что книгу никто не пытался скачать, файл удалили.

Одновременно с этим второе произведение авторства Б. Акунина до сих пор находится в сообществе. Журналисты сделали вывод, что для удаления пиратского контента «ВКонтакте» прибегает к помощи ботов. Последние удаляют только запрещенные для публикации файлы, поскольку книгу «Обитель» в других сообществах найти также не удалось.

***

25.04.2016

Составлен рейтинг самых защищенных от прослушки мессенджеров

Компания Falcongaze, специализирующаяся на разработке программного обеспечения для предотвращения утечек данных, составила рейтинг мобильных мессенджеров, исходя из их степени надежности в плане защищенности переписки, пишет InternetUA.

После отбора семи наиболее популярных мессенджеров, сделанного по результатам опроса Falcongaze, аналитики оценили безопасность приложений по ряду факторов: является ли протокол мессенджера открытым или закрытым (то есть доступен ли он для изучения), есть ли шифрование и, если есть, то какое (какие участки маршрута передачи сообщения шифруются).

Из этих факторов первым по важности было наличие сквозного шифрования, далее – при отсутствии сквозного шифрования – наличие сервер-абонентского шифрования, затем – доступен ли протокол мессенджера для изучения. Кроме того, была учтена имеющаяся информация об уязвимостях, были ли они устранены разработчиками.

В итоге каждому мессенджеру была присвоена оценка от 1 до 7 баллов. По количеству баллов было назначено соответствующее место. По результатам

исследования, первое место занял Telegram, второе – WhatsApp, третье – Viber, четвертое – Skype, пятое – Google Hangouts, шестое – Facebook Messenger и, наконец, последнее, седьмое – ICQ.

1. Telegram

Первое место в рейтинге надежности занял Telegram П. Дурова, основателя «ВКонтакте», обогнав WhatsApp. Такой результат получится даже несмотря на то, что в WhatsApp недавно было введено сквозное шифрование всех данных, тогда как в Telegram эта функция опциональна (пользователю предлагается самостоятельно активировать защищенный чат, если он этого желает).

2. WhatsApp

WhatsApp по очкам оказался на втором месте. Как пояснили в Falcongaze, дополнительные баллы были присвоены Telegram за открытый исходный код, а также дополнительные функции, которых нет у конкурента. К этим функциям относятся: удаление всех сообщений после прочтения с устройств отправителя и получателя, отсутствие синхронизации секретных чатов с другими устройствами и технически реализованная невозможность сделать скриншот секретного чата.

3. Viber

Viber удостоился третьего место благодаря многочисленным нововведениям, о которых разработчик мессенджера сообщил на днях. Во-первых, сквозного шифрования, во-вторых, функции автоматического удаления сообщения с устройства получателя (как в Telegram), и, в-третьих, скрытых чатов, которых не видно на экране. Все эти нововведения компания пообещала запустить в ближайшие несколько недель.

4. Skype

Skype занял среднюю позицию по ряду причин. «Протокол этого мессенджера закрыт, поэтому сложно оценить заложенные разработчиками меры безопасности, а используемое шифрование не обеспечивает должной защиты. После того как в 2011 г. Skype был куплен компанией Microsoft, тот факт, что спецслужбы имеют доступ к переписке пользователей, особо не утаивается. То и дело появляется информация о новых уязвимостях, которые, к примеру, позволяют контролировать звонки в Skype при помощи шпионских программ», – пояснили в Falcongaze.

5. Google Hangouts

Достаточно простой в использовании Google Hangouts шифрует всю информацию, включая видеоконференции. Однако данные шифруются только на участке между устройством и серверов компании-разработчика и на участке между сервером и собеседником. То есть, когда они попадают на сервер, гарантии безопасности нет.

6. Facebook Messenger

«Facebook Messenger не обеспечивает сквозного шифрования. Кроме того, ранее этот мессенджер был замечен в центре скандала, поскольку при установке запрашивал разрешение использовать микрофон девайса

пользователя для записи аудио, в любое время и без получения подтверждения пользователя. Если пользователь по невнимательности давал это разрешение, мессенджер имел возможность не только записывать аудио, но и снимать фото и видео в любое время, а также получать доступ к файлам», – рассказали эксперты.

7. ICQ

На последнем месте рейтинга расположился мессенджер ICQ, развитием которого занимается компания Mail.ru Group. Несмотря на недавнее открытие его исходного года, эксперты сходятся во мнении, что безопасным с точки зрения конфиденциальности переписки этот мессенджер не назовешь. «Протокол не отличается надежностью, а о шифровании данных и говорить не приходится», – вынесли вердикт исследователи.

***

23.04.2016

Проросійські хакери зламали сайт Львівської ОДА

Зловмисники зламали сайт Львівської обласної державної адміністрації й розмістили на ньому інформацію антиукраїнського змісту, пише InternetUA.

У суботу, 23 квітня, близько 15:00 на сайті Львівської ОДА з'явились чорні зображення з написом «Спрут был здесь». Крім того, зловмисники замінили частину публікацій на сайті повідомленням про «київську хунту» та іншими звичними висловами сепаратистів.

***

25.04.2016

От хакеров не скрыться – даже Facebook не может гарантировать безопасность

После ситуации со взломом того самого iPhone 5c террориста из Сан-Бернардино, тема безопасности личных пользовательских данных стала особенно актуальной, поэтому соответствующий вопрос то и дело поднимается мировыми СМИ. Сегодня в центре их внимания оказался Facebook, который не может гарантировать конфиденциальность передаваемой через него информации, пишет InternetUA.

Как оказалось, достаточно продолжительное время во внутренних серверах Facebook злоумышленниками был установлен специальный хардварный чип, которые давал им доступ к любой информации работников компании. О личной переписке и других пользовательских данных достоверной информации нет, однако и они могли оказаться под пристальным взглядом хакеров.

Нет сомнений, неизвестное стороннее устройство к оборудованию Facebook подключил кто-то из работников компании – ни у кого другого доступа к нему просто не было. В этом случае самые разнообразные методы

защиты социальной сети оказались бессильны. Конечно, количество аналогичных ситуаций в недрах этой и другой IT-компаний могут исчисляться десятками и даже сотнями. Жаль, в руки СМИ попадает информация далеко не о всех таких случаях.

***

26.04.2016
Вредоносное ПО продается в Интернете

Хакерские программы – перспективный продукт в сфере услуг. Мошенники разрабатывают собственные вредоносные программы и за деньги предоставляют к ним доступ через Интернет. Создатели вирусов используют облака для продажи специфического продукта, пишет InternetUA.

Компания Trustwave, которая работает в сфере информационной безопасности, провела исследование рынка и составила отчет под названием «Trustwave: глобальная безопасность 2016». В нем указано, что в Dark Web кибер-преступники успешно продают вредоносные программы, которые сами написали.

Подобно продажам официального программного обеспечения, этот вид услуг превращается в бизнес. Теперь мошенники, которые не располагают ресурсами для создания собственного ПО, могут легко приобрести его в Интернете и использовать в своих целях. Заказчик может купить, или взять в аренду необходимый ему код. При этом во всем, что связано с репутацией, хакеры ведут себя ответственно: гарантируют качество продукта, возврат средств, и даже систему скидок.

***

26.04.2016
Мошенники начали вымогать деньги у пользователей WhatsApp

О новом виде мошенничества через WhatsApp рассказала компания ESET. Злоумышленники рассылают спам с предложением активировать функцию видеозвонков, пишет InternetUA.

Сначала приходит сообщение с прикрепленной ссылкой. Нажав на нее, пользователь переходит на сайт с инструкцией по активации функции видеозвонков. На странице есть кнопка «Активировать видеозвонки сейчас», после нажатия на нее пользователю предлагается переслать спам-сообщение десяти контактам или пяти группам в мессенджере для «проверки активности».

Уже после осуществления рассылки предлагается обновить ПО, а вместо «новой версии WhatsApp» пользователь автоматически становится обладателем подписки на дорогостоящие SMS-сервисы, после чего с его счета снимаются деньга за входящие сообщения.

Функция видеозвонков в мессенджере была анонсирована в конце 2015 г., но пока не активна. Новая схема ориентирована на пользователей, говорящих

на испанском языке, позже она может быть нацелена и на более широкую аудиторию, включая российских пользователей.

***

25.04.2016

Хакеры переключили внимание с финансового сектора на организации здравоохранения

Как показывает исследование компании IBM, кибер-преступники стали переключаться с банков на медицинские учреждения. Согласно отчету «2016 Cyber Security Intelligence Index», в прошлом году организации здравоохранения вышли на первое место по количеству кибер-атак, пишет InternetUA.

В отчете представлены данные об угрозах безопасности, собранные в период с 1 января по 31 декабря 2015 г. с 8 тыс. устройств клиентов IBM в 100 странах мира. Пять из восьми крупнейших атак с 2010 г. произошли в первой половине 2015 г. В общей сложности в прошлом году было похищено свыше 100 млн записей пользователей системы здравоохранения.

Записи клиентов медицинских учреждений остаются актуальными и достоверными в течение многих лет и поэтому высоко ценятся среди хакеров. Данные кредитных карт, номера социального страхования, электронные адреса, информация о состоянии здоровья и сведения о профессии могут использоваться злоумышленниками в мошеннических целях и для кражи личности.

Как сообщают эксперты IBM, в списке компаний, чаще всего подвергавшихся кибер-атакам в 2015 г., организации сферы здравоохранения находятся на первом месте. Далее следуют производственные предприятия, банки, правительственные учреждения и транспортные предприятия. Финансовые организации, ранее занимавшие первое место среди излюбленных жертв хакеров, в 2015 г. оказались на третьей позиции благодаря переключению внимания злоумышленников на сектор здравоохранения и промышленность. Снижению количества кибер-атак также способствовало улучшение защиты систем банков.

По данным IBM 60 % кибер-атак в прошлом году были осуществлены инсайдерами с доступом к системам организаций.

***

27.04.2016

Ежемесячно один миллион человек подключается к Facebook через Tor

Социальная сеть Facebook достигла отметки в один миллион пользователей, ежемесячно заходящих на сайт с помощью системы прокси-

серверов Tor. За последние десять месяцев этот показатель возрос почти на 100 %, пишет InternetUA.

Согласно компании, ещё в июне 2015 г. к Facebook с помощью Tor подключалось 525 тыс. человек. В апреле 2016 г. впервые была достигнута отметка в миллион пользователей за один месяц. Вероятно, всё это – благодаря тому, что недавно появилась возможность входить в Facebook через Tor на Android-устройствах посредством прокси-приложения Orbot.

«Люди, выбирающие коммуникацию через Tor, делают это по ряду причин, связанных с приватностью, защищённостью и безопасностью», – сказал А. Маффетт, специалист по программному обеспечению в подразделении по безопасности социальной сети. «Как мы писали раньше, для нас важно предоставлять людям методы, позволяющие безопасно использовать наши сервисы – в частности, если им не хватает надёжных методов делать это».

Tor – акроним The Onion Router («луковый роутер»). Это программное обеспечение, позволяющее с помощью системы прокси-серверов устанавливать анонимное сетевое соединение. Обычно Tor используют либо активисты, либо жители стран со строгими правилами использования Интернета. Однако ПО может использовать любой человек, который хочет сохранить полную анонимность в сети. К технологии обратилось множество крупных компаний, включая и Facebook.

***

27.04.2016

В безопасности Windows найдена серьезная брешь

Согласно последним данным американских экспертов, в работе операционной системе Windows найдена новая брешь, позволяющая хакерам проникать в систему и запустить любое приложение без разрешения администратора, пишет InternetUA.

Об этом стало известно из сообщения, опубликованного изданием The Next Web. По данным специалистов, многие пользователи ОС Windows, установившие на своем компьютере функцию Applocker, убеждены, что система находится в безопасности, однако это не так. Недавно эксперты нашли в работе бизнес-версий Windows (Windows 7 и выше) уязвимость, из-за которой хакеры могут обойти расширяющую функцию операционных систем Windows Applocker путем команды regsvr32.

Компьютерные мошенники могут при помощи этой команды зайти в систему Windows и запустить любое приложение, находящееся в компьютере. Специалисты утверждают, что система владельца подвергается запуску вредоносного программного обеспечения, даже если в системе установлена функция Applocker. При этом, система не требует предоставлять информации об администраторе или изменять системный реестр.

Разработчики Microsoft пока не выпустили патч, чтобы исправить эту ситуацию. Однако эксперты рекомендуют: чтобы избежать взлома системы,

пользователь может отключить Regsvr32.exe и Regsvr64.exe с помощью брандмауэра Windows.

***

26.04.2016
DDoS-атаки становятся мощнее и изобретательнее

Компания Imperva опубликовала отчет за I квартал 2016 г., посвященный DDoS-угрозам. Как сообщают исследователи, кибер-преступники экспериментируют с инструментами и методами атак. Наблюдались изменения атак на уровне приложений и сетей, а также увеличилась активность DDoS-ботнетов. Касательно атак на уровне приложений, преступники стали больше использовать имитирующих работу браузера DDoS-ботов, способных обходить стандартные системы безопасности (36,6 %). Кроме того, злоумышленники используют новые пути осуществления атак на уровне приложений, таких как HTTP/S POST-флуд мощностью в 8,7 Гбит/с, пишет InternetUA.

В отчете также отмечается увеличение частоты атак за I квартал 2016 г., поскольку 50 % атакованных сайтов не единожды становились жертвами преступников. Более того, 31,8 % веб-сайтов были атакованы от двух до пяти раз.

Из 5267 атак на уровне приложений за рассматриваемый период времени 87,8 % длились более получаса. Самая продолжительная атака длилась (и сейчас продолжается) 36 дней. Наибольшая атака достигла 100 100 запросов за секунду. Исследователи также обнаружили, что 18,9 % DDoS-ботов могли обойти cookie-файлы, а 17,7 % из них обходили и cookie-файлы, и JavaScript.

Среди DDoS-атак сетевого уровня количество многовекторных атак возросло на 33,9 %. Мощность самой масштабной атаки достигла максимума в более чем 200 Гбит/с, а пропускная способность – 120 млн пакетов в секунду. Согласно отчету, количество атак сетевого уровня составило 3791 за первые три месяца этого года. Самая продолжительная из них длилась 48,5 часов. Специалисты компании столкнулись с множественными атаками мощностью более 100 Гбит/с, при этом атаки с пропускной способностью более 50 млн пакетов в секунду возникали каждые четыре дня, а атаки с пропускной способностью более 80 млн пакетов в секунду были зафиксированы в среднем каждые восемь дней.

Согласно докладу Imperva, за I квартал увеличилась активность ботнетов в Южной Корее, ставших источником 29,5 % атак. Большая часть атак исходила от ботнетов Nitol (52,9 %) и PCRat (38,2 %). Из них 38,6 % атак были направлены против японских веб-сайтов, а 30,3 % атаковали американские сайты.

Исследователи также наблюдали рост использования ботов Generic!BT. Разновидности этого вредоноса используются в DDoS-атаках с 7756 уникальных IP-адресов, расположенных в 52 странах. Большинство адресов находится в России (52,6 %) и Украине (26,6 %).

***

30.04.2016

Пользователей Google Chrome и Facebook атакует новый троян

«Доктор Веб» предупреждает о том, что злоумышленники распространяют вредоносный плагин для браузера Google Chrome, способный рассылать спам в социальной сети Facebook, пишет InternetUA.

Дополнение, по сути, представляет собой троянскую программу, получившую имя BPlug.1074. Если пользователь Chrome, у которого установлен этот плагин, войдёт в Facebook, зловред определяет его идентификатор (UID) и вносит изменения в оформление сайта социальной сети в окне браузера. В частности, удаляется меню «Быстрые настройки конфиденциальности», а также все остальные выпадающие меню, которые могут демонстрироваться в интерфейсе социальной сети.

После этого троян получает перечень друзей жертвы. Далее формируется новая страница сообщества, название которой генерируется автоматически. С использованием ID сообщества, фотографии жертвы, установленной как аватар, и адреса веб-страницы, извлекаемого из конфигурационного файла, зловред формирует пост формата «поделиться ссылкой» и с определённым временным интервалом размещает его в своей ленте. Поскольку троян при создании поста «упоминает» в нём всех друзей текущего пользователя из полученного ранее списка, это сообщение также появляется в их ленте событий.

При переходе по ссылке, указанной в таком сообщении, пользователь попадает на веб-страницу с заголовком Hello please watch my video, копирующую внешний вид Facebook. Если жертва использует браузер Chrome, то при попытке просмотреть видеоролик появляется диалоговое окно с предложением загрузить и установить плагин для браузера. Этот плагин на деле является копией трояна. На сегодняшний день известно о тысячах пострадавших от зловреда BPlug.1074. Кстати, аналогичным образом троян может распространять и другие плагины для браузера Google Chrome.

***

5.05.2016

Хакеры взломали около 300 млн аккаунтов социальный сетей

Взломщики занялись продажей паролей от соцсетей и популярных поисковых систем, пишет Телеграф.

Журналистам удалось выяснить сенсационную информацию. Как оказалось, в Интернете продаются пароли от страниц социальных сетей и электронной почты частных лиц. Доступ к личным данным стал возможен благодаря работе хакеров, которые взломали 272 млн аккаунтов и паролей к таким популярным поисковым системах, как Google и Yahoo.

Кроме того, вся полученная информация продается в Интернете в открытом доступе. Злоумышленники установили на украденную базу данных

(1,17 млрд учетных записей) цену в сумме 0,7 дол. Также удалось установить, что больше всего от действий хакеров пострадал популярный почтовый сервис Mail.Ru, в котором было взломано 57 млн аккаунтов.

В компании уже заявили, что большинство из взломанных аккаунтов являются поддельными, а пароли к ним не принадлежат действующим аккаунтам.

Специалисты в области компьютерных технологий предполагают, что подобные взломы и хакерские атаки будут продолжаться в дальнейшем, поскольку большинство пользователей Интернета игнорируют призывы к более частой смене паролей к учетным записям.

***

2.05.2016

75 % DDoS-атак достигают цели за несколько минут

Согласно оценкам специалистов, проведенных в рамках исследования Data Breach Investigations Report, большая часть хакерских атак ломают защиту всего за несколько минут. Ученые уверены, что из общего числа DDoS-атак взлом осуществляется в 75 % случаев, пишет InternetUA.

Об этом стало известно из сообщения, опубликованного компанией Verizon. Сообщается, что в рамках исследования Data Breach Investigations Report специалисты изучили 100 тыс. инцидентов, связанных с нарушением кибербезопасности. Среди них эксперты выявили 2260 подтвержденных фактов утечек данных за прошлый год.

По словам специалистов из компании Verizon, которая уже девятый год проводит аналогичное исследование, на сегодняшний день борцы с хакерскими атаками по-прежнему остаются позади киберпреступников, которые научились обходить защиту той или иной системы. Эксперты утверждают, что в 75 % случаев хакеры во время DDoS-атак достигают своей цели за считанные минуты, а 99 % – киберпреступники всего за пару недель могут взломать систему.

***

6.05.2016

«Анонимный интернационал» опубликовал содержимое электронной почты гендиректора «ВКонтакте»

Спустя всего несколько дней после публикации содержимого электронных почтовых ящиков известного российского телеведущего Д. Киселева, хакерская группировка «Анонимный интернационал» (также известна как «Шалтай-Болтай») представила общественности конфиденциальные данные генерального директора соцсети «ВКонтакте» Б. Добродеева, пишет InternetUA.

По словам хакеров, «полузаброшенный почтовый ящик» содержал множество рекламных рассылок и спама, однако среди мусора им удалось обнаружить «любопытную финансовую документацию», относящуюся к соцсети «ВКонтакте». В частности, «Анонимный интернационал» обнаружил переписку с обсуждением бюджета компании на 2014 г. (год ухода П. Дурова с поста гендиректора), увольнения П. Дурова и утверждении кандидатуры Б. Добродеева на посту генерального директора «ВКонтакте».

В одном из вложений хакеры обнаружили результат обсуждения бюджета компании с комментариями и вопросами акционеров. Согласно документам, более всего акционеров волновали неоправданно большие на их взгляд комиссии для рекламных агентств. Кроме того, они были обеспокоены связями некоторых сотрудников «ВКонтакте» с компаниями-подрядчиками (VKT Rus LLC, Peering LLC и GlobalNet LLC).

***

10.05.2016
В сети появился дешевый троян-вымогатель

В киберпространстве едва ли не каждую неделю возникают новые разновидности вымогательского ПО. На сей раз внимание исследователей безопасности привлек троян-вымогатель AlphaLocker. Самым «привлекательным» во вредоносе оказалась его цена, пишет InternetUA.

AlphaLocker – вредонос, распространяемый по бизнес-модели RaaS (ransomware-as-a-service). Вымогатель можно приобрести непосредственно у разработчика всего за 65 дол. в биткойнах. Оплатив стоимость вредоноса, покупатель получает его копию, программу расшифровки бинарного кода и собственную административную панель. Столь низкая стоимость вымогателя может серьезно увеличить количество его жертв.

Вредонос AlphaLocker шифрует информацию на всех логических дисках компьютера жертвы при помощи алгоритма AES. Вымогатель продолжает шифрование файлов, даже если компьютер выключен. После того, как вредоносное ПО зашифрует информацию на компьютере, жертва получает текстовый файл с требованием выкупа. Сумма оплаты составляет 0,35 биткойнов (около 158 дол.). Разработчики вымогателя периодически обновляют его код, что позволяет AlphaLocker избегать обнаружения антивирусами.

AlphaLocker основан на открытом исходном коде EDA2. Проект EDA2 был разработан турецким исследователем Ютку Сеном (Utku Sen). Позднее он выложил исходный код EDA2 в Сеть с образовательной целью. На основе открытого исходного кода ранее был разработан вымогатель Magic.

По предположению специалистов из компании Cylance, вредонос AlphaLocker происходит из России, поскольку его рекламировали на российских форумах. Содержащиеся в некоторых файлах вредоносного ПО данные также говорят в пользу этого утверждения.

***

9.05.2016

Украинские хакеры атакуют сайты сепаратистов

Украинские хакеры альянса групп #FalconsFlame и #Trinity взломали более девяти сайтов с антиукраинской пропагандой, в том числе четыре ресурса ДНР, пишет InternetUA.

Об этом сообщили блогеры Klide Shelton в «Вільний Журнал» и Р. Бурко в Facebook.

«Эта локальная, но важная победа в киберпространстве дает чувство братского локтя, чувство духовного единения и победы. Они показали «как свет с легкостью побеждает тьму». Более девяти сайтов (9+, 9 мая) получили инъекцию сыворотки правды.

«Украинцы очень добрый и волевой народ, даже взлом враждебных ресурсов российских террористов они провели эстетично и красиво. Вставили видеоролики о настоящей истории и трагедии WW2 и об огромном вкладе украинского народа в борьбу над захватчиками. Победили тогда, победим и сейчас», – написал Р. Бурко.

Напомним, ранее украинские хакеры из альянсов Falcons Flame и Trinity взломали один из популярных в ДНР сайтов «Анна-Ньюз» и разместили на нём видеообращение к «противникам и союзникам».

***

9.05.2016

Новый троян крадёт документы жертвы

«Доктор Веб» предупреждает о появлении новой вредоносной программы – бекдора Apper, атакующего компьютеры под управлением операционных систем Microsoft Windows, пишет InternetUA.

Зловред распространяется с помощью дроппера, который представляет собой документ Microsoft Excel, содержащий специальный макрос. Этот макрос собирает по байтам и запускает самораспаковывающийся архив с исполняемым файлом. Последний имеет действительную цифровую подпись компании Symantec. В архив также входит динамическая библиотека, в которой сосредоточена основная функциональность бэкдора.

Троян регистрирует в автозагрузке исполняемый файл, который после своего запуска загружает в память атакуемого компьютера вредоносную библиотеку. Затем исходный файл удаляется.

Вредоносная программа предназначена для хищения документов и шпионажа. После успешного запуска зловред действует как кейлоггер – фиксирует нажатия клавиш и записывает их в специальный зашифрованный файл. Ещё одна функция Apper – мониторинг файловой системы. Если на диске компьютера имеется конфигурационный файл, содержащий пути к папкам,

состояние которых троян должен отслеживать, он будет фиксировать все изменения в этих папках и передавать информацию на управляющий сервер.

Перед установкой связи с командным сервером бэкдор собирает данные о заражённом компьютере: его имя, версию операционной системы, сведения о процессоре, оперативной памяти и дисках, после чего отсылает полученные сведения злоумышленникам. Затем троян добывает более подробную информацию о дисковых накопителях, которая также передается на управляющий сервер вместе с файлом журнала кейлоггера.

Зловред может по команде отправить злоумышленникам сведения о содержимом заданной папки или указанный киберпреступниками файл, удалить или переименовать какой-либо файловый объект, создать на заражённом компьютере новую папку, а также сделать снимок экрана и отправить его на принадлежащий вирусописателям сервер.

***

6.05.2016

Facebook собирает и хранит биометрические данные пользователей

Группа пользователей социальной сети Facebook из штата Иллинойс (США) подала на компанию в суд из-за «меток» на фотографиях, сообщает Reuters, пишет Телекритика.

По их мнению, функция распознавания лиц Facebook, которая предполагает установку «меток» на фотографиях, незаконно собирала и сохраняла биометрические данные пользователей. И этим компания нарушила закон штата о конфиденциальности биометрической информации (BIPA).

Первый раунд в суде Facebook проиграл 5 мая.

***

10.05.2016

Эксперты показали, как взломать Telegram и WhatsApp

Эксперты Positive Technologies доказали, что Telegram и WhatsApp можно взломать без поддержки оператора связи, который бы передал SMS с паролями. Это позволяет утверждать, что взлом Telegram-аккаунтов оппозиционеров мог произойти без привлечения оператора МТС, сообщает SecurityLab, пишет InternetUA.

Всё просто

Для демонстрации технологии взлома эксперты создали тестовые аккаунты в Telegram и обменялись несколькими сообщениями. Затем через сеть SS7 (она же ОКС-7, набор сигнальных телефонных протоколов, используемых для настройки большинства телефонных станций) специалисты провели атаку на один из тестовых номеров.

В результате они узнали IMSI (международный идентификатор мобильного абонента, ассоциированный с каждым пользователем мобильной

связи стандарта GSM, UMTS или CDMA) и перерегистрировали абонента на свой терминал, чтобы получить профиль жертвы. После этого номер телефона оказался под полным контролем экспертов.

Прочитать невозможно только секретные чаты – они не подгружаются с сервера

В дальнейшем специалисты подключились с другого устройства к Telegram под аккаунтом жертвы (использовался только номер телефона) и получили SMS с кодом доступа к аккаунту мессенджера. С этого момента они могли читать всю переписку, которую Telegram подгрузил с сервера, и вести общение от имени жертвы.

WhatsApp также взломали

Аналогичным образом эксперты получили доступ к аккаунту WhatsApp. Однако этот мессенджер не хранит переписку на сервере, поэтому прочитать её со смартфона жертвы оказалось невозможно.

Вести переписку в WhatsApp от имени жертвы можно, и она даже не будет знать об этом. Впрочем, бэкап переписки лежал в Google Drive, поэтому после взлома аккаунта Google и эти данные могут оказаться в руках злоумышленников.

Из-за слабой защищенности сетей SS7 одноразовые коды по SMS не являются безопасными

Атаку на сеть можно выполнить из любой точки мира. В результате взлом аккаунтов доступен не только спецслужбам, но и многим другим пользователям Интернета.

***

11.05.2016

Новый банковский троян для Android-устройств использует тактику социальной инженерии

По словам исследователей из Avast, новый банковский троян для Android-устройств использует тактику социальной инженерии, обманывая жертву и оставаясь незамеченным на зараженном мобильном устройстве. Название приложения на иконке может быть разным, включая AVITO-MMS, KupiVip и MMS Центр. Однако после первого запуска программы значок становится скрытым, что делает троян более неуловимым, пишет InternetUA.

Троян совершает обычную проверку эмулятора. Если проверка не показывает работу приложения в эмуляторе, запускается фоновый таймер. Таймер безостановочно открывает диалоговые окна активации административного доступа к устройству, пока не будут получены права администратора. После нажатия на кнопку «Отмена» сразу появляется новое окно. Процесс продолжается до момента получения административного доступа. Процедура повторяется уже с диалоговыми окнами диспетчера SMS, который требуется сделать по умолчанию.

Вредонос отправляет информацию об устройстве и перехваченные SMS на C&C-сервер и получает от преступников дальнейшие команды. Отправляемая на сервер информация включает серийный номер мобильного устройства, код государства, название мобильного оператора, версию Android-устройства, номер телефона, серийный номер SIM-карты, текущий номер версии трояна и уникальный идентификационный номер зараженного устройства. Помимо получения данных о контактах, SMS, звонках и установленных приложениях, вредонос получает GPS координаты устройства. Также троян отправляет на сервер данные о наличии административных прав и переведении диспетчера SMS в статус «по умолчанию». Права администратора также дают возможность трояну удаленно заблокировать зараженное устройство.

Для получения данных кредитных карт жертвы троян открывает на устройстве поддельное окно Google Play. Однако при внимательном рассмотрении окна видно, что слово Play пишется с маленькой буквы. Помимо этого, вредонос поддерживает команды для загрузки APK, позволяет блокировать экран и перенаправлять вызовы. Антивирусными решениями компании Avast троян идентифицируется как Android: Banker-IR. В случае заражения пользователю придется сбросить настройки устройства до заводских.

***

10.05.2016

Microsoft: самый популярный эксплоит 2015 г. использует уязвимость 2010 г.

Команда безопасности компании Microsoft сообщает, что в 2015 г. самый популярный эксплоит задействовал уязвимость CVE-2010-2568, появившуюся в 2010 г. и применявшуюся в вирусе Stuxnet. CVE-2010-2568 представляет собой уязвимость системы безопасности в версиях Windows 7, Vista, XP, Server 2008 и Server 2003. Она позволяет при помощи файлов LNK или PIF выполнять код на компьютерах пользователей, получая контроль над ними, пишет InternetUA.

Закрывающее уязвимость обновление было выпущено в том же 2010 г., однако установили его далеко не все пользователи. Именно это и позволило часто задействовать уязвимость, о чём Microsoft рассказала в докладе Security Intelligence Report (SIR). Хакеры активно используют слабости старых операционных систем, которым не хватает механизмов безопасности, появившихся в Windows 8, 8.1 и 10, и которые пользователи зачастую обновляют не слишком оперативно.

В этом же докладе говорится, что в прошлом году хакеры отдавали предпочтение комплектам эксплоитов (exploit kits) перед другими методами распространения вредоносного кода, что позволяет автоматизировать процесс инфицирования. Самым популярным семейством вредоносного ПО стало Win32/Gamarue, один из крупнейших и старых ботнетов. Также растёт число

потенциально нежелательных приложений и фишинговых атак против финансовых организаций.

В ответ на это с 74,3 до 77,1 % возросло число пользователей с работающими в реальном времени приложениями безопасности.

***

11.05.2016

В Google Play Store обнаружен опасный троян

Новое семейство вредоносного ПО было найдено на платформе Android. Оно получило название Viking Horde и позволяет при помощи приложений магазина Google Play Store выполнять атаки типа кликфрод, СМС-фрод, рассылку спама и проводить DDoS-атаки, пишет InternetUA.

Обнаружили новую угрозу в компании Check Point. Код Viking Horde был найден в пяти приложениях – Viking Jump, Parrot Copter, WiFi Plus, Memory Booster и Simple 2048. Google уже удалила их из магазина, но специалисты Check Point уверены, что использовавшиеся в них методы обхода механизма защиты магазина могут быть использованы снова при загрузке новых приложений.

Check Point видит особую опасность Viking Horde в умении атаковать устройства с рутом и без. В первом случае компонент обновления позволяет постоянно расширять вредоносную функциональность. Со своего командного сервера атакующие рассылают на инфицированные устройства (боты) инструкции. Связь осуществляется через анонимный прокси-сервер, разный для каждого устройства.

Главным занятием Viking Horde является распространение рекламы и имитация перехода по ней пользователей. Анонимные прокси помогают не попасть в чёрные списки рекламных сетей. Большинство скачавших Viking Horde пользователей находятся в России (44 % случаев), Испании, Ливане, Мексике и США.

***

14.05.2016

Автор трояна Lost Door рекламирует себя через Facebook и YouTube с 2007 г.

Специалисты компании Trend Micro рассказали об интересном случае, который им довелось наблюдать. Хакер, известный как OussamiO, еще в 2007 г. создал RAT (Remote Access Trojan) Lost Door. Как ни странно, девять лет спустя OussamiO продолжает совершенствовать и продавать свой «продукт», при этом не ограничивая себя рекламой в даркнете. Автор малвари открыто продвигает трояна через Facebook, YouTube и Blogspot, и не похоже, чтобы это кого-то волновало, пишет InternetUA.

Основной рекламной площадкой трояна в Интернете все эти годы выступает блог OussamiO на Blogspot (lost-door.blogspot.com), в котором создатель вредоноса регулярно публикует новости об обновлениях Lost Door, грядущих патчах и даже различные туториалы по использованию малвари. Многие из его уроков представлены в формате видеороликов, которые хакер не стесняясь выкладывает на YouTube. Кроме того, OussamiO уже несколько лет ведет собственную страницу в Facebook. Удивительно но факт: за это время никто даже не попытался забанить OussamiO ни на одном из сайтов.

Не брезгует OussamiO и более стандартными методами продвижения малвари, то есть активно рекламируется на различных площадках в даркнете, ориентированных на бразильскую, российскую и китайскую аудиторию. Хотя создатель RAT не оглашает цены на Lost Door публично, известно, что в зависимости от конфигурации троян стоит от 10 до 50 дол.

Однако интерес представляют не только способы продвижения трояна, но и сам Lost Door. Исследователи Trend Micro пишут, что многие антивирусные решения по сей день не обнаруживают этого вредоноса, так как он скрывает трафик и использует ряд других техник, чтобы не привлекать внимания.

Lost Door поставляется с билдером, то любой покупатель трояна может создать на его базе собственную, вполне уникальную и работоспособную малварь. Lost Door – это настоящий мультитул. Будучи установлен на компьютере жертвы, троян предоставляет своему оператору доступ к файлам, возможность загрузки контента с устройства, возможность установки любого дополнительного ПО на скомпрометированный ПК, предоставляет доступ к веб-камере, может перехватывать нажатия клавиш. Фактически Lost Door полностью контролирует зараженную ОС.

OussamiO утверждает, что проверял работоспособность Lost Door на всех основных версиях Windows, начиная от XP и заканчивая Windows 10.

«Lost Door использует в роутерах функцию Port Forward, похожую тактику применял вредонос DarkComet. Применяя эту функцию не по назначению, удаленный атакующий может получить доступ к серверной стороне приватной сети, и не важно, работает она у кого-то дома или в офисе», – пишут исследователи Trend Micro. – «Также это означает, что любой вредоносный трафик или коммуникации могут быть замаскированы под обычный внутренний трафик, что также помогает атакующим скрыть адрес управляющего сервера, так как серверная сторона не сообщается с ним напрямую. Вместо этого, все что нужно атакующим: знать IP-адрес роутера и иметь доступ к открытым портам (после настройки Port Forward)».

***

18.05.2016

Использующий кликфрод вредонос заразил около 1 млн компьютеров по всему миру

За последние несколько лет сотни тысяч компьютеров оказались инфицированы вредоносом, подменяющим результаты поиска в браузере. Ботнет перехватывает поисковые запросы в Google, Bing и Yahoo! с компьютеров пользователей и заменяет легитимные результаты поиска на поддельные из созданной преступниками поисковой системы. Как сообщают исследователи из компании Bitdefender, злоумышленники совершают подмену с помощью вредоносной программы Redirector.Paco. С сентября 2014 г. вредонос инфицировал более 900 тыс. компьютеров по всему миру, преимущественно в Индии, Малайзии, Греции, США, Италии, Пакистане, Бразилии и Алжире, пишет InternetUA.

Вредонос включен в модифицированный пакет установки таких хорошо известных программ, как WinRAR, Connectify, YouTube Downloader, Stardock Start8 и KMSPico. После установки на компьютер жертвы, вредонос изменяет интернет-настройки и использует прокси-сервер, указанный злоумышленниками в файле PAC (Proxy auto-config). Redirector.Paco устанавливает на инфицированном компьютере корневой сертификат, сгенерированный вредоносом. Затем вредоносное ПО генерирует поддельные сертификаты для Google, Yahoo! и Bing, которые принимает браузер жертвы. Redirector.Paco устанавливает уникальный корневой сертификат на каждый зараженный компьютер. Вредоносное ПО позволяет осуществить атаку «человек посередине». Прокси-сервер подключается к легитимной поисковой системе, заменяет результаты поиска на поддельные из созданной преступниками поисковой системы, повторно шифрует страницу с помощью сертификата SSL для соответствующего доменного имени и после отображает ее в браузере пользователя.

Существует две разновидности вредоноса. Первая версия использует удаленный сервер для размещения PAC-файла и прокси. Процесс подмены результатов поиска занимает некоторое время. Пользователь может наблюдать сообщения на панели состояния браузера наподобие «ожидание прокси туннеля» («waiting for proxy tunnel») или «загрузка скрипта прокси» («downloading proxy script»).

У второй разновидности PAC-файл и прокси хранятся на локальном компьютере. Эта версия создана с помощью платформы .Net, и влияние вредоноса на скорость работы браузера не так заметно. Функциональность перехвата HTTPS обеспечивается библиотекой .Net, называемой FiddlerCore.

***

19.05.2016

Хакер выставил на продажу 117 млн аккаунтов LikedIn

Хакер под псевдонимом «Мир» при помощи нелегального сайта The Real Deal выставил на продажу 117 млн логинов и паролей пользователей LikedIn, сообщает The Next Web. Подобное уже происходило в 2012 г., тогда кибер-

преступник из России выложил в сеть данные 6 млн пользователей (InternetUA).

Сейчас 117 млн почтовых адресов и паролей продаются за 5 биткоинов, что эквивалентно 2275 дол. Злоумышленник заявляет, что данные были получены благодаря той же утечке 2012 г. По словам хакера, 90 % этих аккаунтов уже взломаны.

Издание отмечает, что, несмотря на то, что на LinkedIn не хранятся данные банковского счета пользователей, в социальной сети все равно содержится большое количество конфиденциальной информации и предлагает пользователям немедленно сменить свой пароль, особенно, если он используется одновременно на нескольких ресурсах.

***

18.05.2016

Хакеры взломали оккупантов Крыма и объявили о депортации россиян

Falcons Flame и Trinity взломал один из сайтов оккупантов Крыма и от имени ставленника Кремля С. Аксенова опубликовал обращение в связи с 72-й годовщиной депортации крымских татар, пишет InternetUA.

«Дорогие крымчане, предлагаю сегодня отдать дань уважения тем нелегким дням 1944 г. и приложить максимум усилий для недопущения этих трагических событий вновь. Нынешняя международная обстановка такова, что в 2017 г. депортации из Крыма могут подвергнуться и россияне», – говорится в сообщении, опубликованном хакерами.

В конце текста от имени С. Аксенова говорится, что он очень рад победе Джамалы на Евровидении и рассчитывает на успешное проведение конкурса в 2017 г. «в Украине, а именно – в Крыму». Обращение завершается хэштегом #OpMay18, характерным для альянса Falcons Flame и Trinity.

***

19.05.2016

«Невидимое» вредоносное ПО Furtim похищает пароли и обходит обнаружение

Исследователи безопасности предупредили о новом вредоносном ПО, похищающем учетные данные. Вредонос получил название Furtim, что в переводе с латыни означает «украдкой», поскольку его очень сложно детектировать. Первым о новом ПО сообщил российский разработчик FireF0X, однако его более подробный анализ представил исследователь компании enSilo Й. Готтесман, пишет InternetUA.

Furtim состоит из драйвера, загрузчика и трех полезных нагрузок. Первая из них представляет собой энергосберегающий конфигурационный инструмент, позволяющий держать компьютер жертвы все время включенным и

подключенным к C&C-серверу вредоноса. Вторая является популярной программой для похищения паролей Pony Stealer. Третий файл пока еще не был проанализирован экспертами.

Вредонос блокирует доступ почти к 250 связанным с безопасностью сайтов, заменяя файл hosts в Windows. Furtim также обходит сервисы фильтрации DNS, сканируя и заменяя фильтруемые серверы имен публичными. Установившись на систему жертвы, программа обходит любую политику перезагрузки, тем самым обеспечивая запуск полезной нагрузки. Furtim деактивирует уведомления Windows и всплывающие окна, а также блокирует жертве доступ к командной строке и диспетчеру задач, лишая ее возможности прервать вредоносный процесс.

C&C-сервер отправляет полезную нагрузку определенному компьютеру только один раз, чтобы исследователи безопасности не могли получить с сервера образцы Furtim. Предназначение вредоноса пока не известно, однако наличие Pony Stealer свидетельствует о том, что оно может применяться во время целевых атак. По словам Готтесмана, C&C-сервер размещен в российском домене, связанном с несколькими украинскими IP-адресами.

***

19.05.2016

Опасности глобальной сети отпугивают от неё пользователей

Достаточно почитать новости за один день, чтобы понять, что Интернет является крайне небезопасным местом. В нём перед пользователями встают угрозы утечки персональной информации при взломе баз данных почтовых сервисов, онлайн-магазинов и сайтов знакомств, слежки со стороны правительств и хакеров, вирусы, трояны, приложения-вымогатели, ботнеты и прочие неприятности, пишет InternetUA.

Недавно в США Национальная администрация по телекоммуникациям и информации провела опрос, в котором американцы высказали опасения в связи с проблемами сетевой конфиденциальности и безопасности. 41 тыс. домохозяйств в результате этих опасений стали меньше пользоваться Интернетом.

45 % респондентов перестали проводить финансовые операции, покупать товары и услуги, писать в социальных сетях и высказывать в Интернете мнения по политическим и другим противоречивым вопросам. 19 % домохозяйств (примерно 19 млн) только за последний год сталкивались с разными видами вредоносной сетевой активности, что только усугубило их страхи.

63 % пользователей опасаются хищения персональных данных, 45 % бояться мошенничества с кредитными картами и банковскими счетами, 23 % – сбора данных в сети, столько же опасаются потери персональных данных, 18 % не хотят стать жертвой сбора данных правительством, 13 % видят в Интернете угрозу личной безопасности. Все эти страхи становятся причиной замедления темпов роста цифровой экономики.

***

22.05.2016
В Facebook обнаружили новый вид мошенничества

В Facebook обнаружили новый вид мошенничества – злоумышленники создают профиль, идентичный аккаунту друзей пользователя, и отправляют заявку на дружбу от их имени. Об этом сообщает Fox News, пишет InternetUA.

Эксперты в области безопасности отмечают, что таким образом мошенники в том числе пытаются завладеть информацией, которая содержится в профилях с ограниченным доступом. К примеру, это могут быть даты рождения и реальные имена и фамилии.

Кроме того, злоумышленники, выдавая себя за друзей, могут «попросить денег взаймы» – такие ситуации происходят довольно часто.

Авторы статьи отмечают, чтобы обезопасить всю личную информацию, будь то данные владельца профиля или посты, которые не предназначены для публичного просмотра, необходимо не добавлять в друзья посторонних людей и тщательно проверять, действительно ли имеющийся уже в друзьях профиль создал еще одну страницу.

***

13.05.2016
Кибербезопасность: человеческий фактор

Большинство успешных хакерских атак за последнее время – результат целевого фишинга. Механизм этого «нового слова» в сетевом мошенничестве и причины его успешности изучает команда профессора Нью-Йоркского университета А. Вишваната. Они утверждают, что самая уязвимая часть любой компьютерной системы – это ее пользователь, пишет InternetUA.

Обыкновенный, сейчас уже уходящий в историю фишинг, как правило, принимал форму легендарных «нигерийских писем». Мошенники старались обманом заставить пользователей предоставить им личную финансовую информацию. Целевой фишинг во многом похож на своего рода предтечу, но намного опаснее. Он убеждают жертв нажать на ссылку или вложение, которое содержит вирус, предоставляющий взломщикам доступ к компьютеру пользователя или даже ко всей корпоративной сети. Вирус распространяется не только в имэйлах, но и через сообщения в социальных сетях, рекламные и новостные баннеры, записывает себя на флешки.

Проблема в том, что мы мало что можем сделать против этих атак. Отчасти потому, что целевой фишинг опирается на социальную инженерию. Эти атаки очень адаптивны и потенциальной жертве иногда очень сложно обнаружить обман. Все существующие технические средства защиты: антивирусы, фаерволы, мониторинг сети – созданы для защиты компьютера и сети от нападений извне. Если злоумышленники проникают в систему при

помощи целевого фишинга, они занимают позицию «законных пользователей», и программное обеспечение против них бессильно.

Таким образом, только мы, пользователи, можем защитить свой компьютер и локальную сеть от злоумышленников. Но мы же – самое слабое звено в кибербезопасности.

Цель – человек

Чтобы бороться с целевым фишингом, надо понимать, почему люди попадаются на уловки мошенников. Исследователи обратились к психологии поведения и изучили действия пользователей, чтобы вычислить, какими особенностями пользуются мошенники. Собранная статистика показала, что у сетевой «небезопасности» есть две основные поведенческие причины.

Во-первых, человек – существо энергосберегающее по своей природе. Человеческий разум создает десятки «автопилотов», чтобы получать максимальное количество пользы при минимальном участии мозга в деятельности. Например, вы же не читаете надпись на упаковке, покупая любимые чипсы? Ваш мозг и так знает, что Lays с беконом – это вон те в красной пачке. Психологические «ярлыки» приклеиваются к логотипам, названиям брендов или даже просто фразам типа «Отправлено с устройства Android». Все это мошенники часто включают в свои сообщения. Люди видят логотип своего банка – и их автопилот предполагает, что емэйл именно от него. В результате они не замечают опечаток, странных фраз и вопросов, даже зачастую не проверяют адрес, с которого пришло письмо.

Усугубляет эту проблему подсознательное убеждение большинства людей, что Интернет безопасен. Ощущая, что они находятся в безопасной зоне, они не прилагают никаких усилий к исследованию небольших странностей, указывающих на большую проблему.

И это ощущение ложной безопасности характерно не только для Интернета в общем. Из-за того, что в заголовках новостей чаще мелькает информация о компьютерных вирусах, многие люди убеждены, что операционные системы смартфонов вирусам в принципе не подвержены. Другие верят, что файлы PDF безопаснее, чем документы Word – как будто к тому файлу, который нельзя редактировать, не может быть привязан вирус. Третьи присваивают статус «домашней сети» бесплатному вайфаю от своего мобильного оператора в кафе, предполагая, что сеть, носящая название «Киевстар», каким-то образом безопаснее других.

Такого рода недоразумения ведут к тому, что некоторые файлы пользователи открывают не глядя и вовсе не задумываются о возможных опасностях, пользуясь определенными устройствами или находясь в любимой сети. Все это заметно повышает риск инфицирования.

Привычка – враг безопасности

Второй фактор заключается в том, что люди привыкли к сетевым технологиям. В наше время большинство использует мейлы, соцсети и сообщения так часто, что это становится привычнее разговора. Если спросить человека, который каждый день ездит на работу одним и тем же маршрутом,

сколько раз он сегодня остановился на светофоре, он вряд ли сумеет ответить. Точно так же привыкший к виртуальности человек не запоминает, какие письма он открывал, на какие ссылки или вложения кликал. Сколько раз вы проверяли новые сообщения на прогулке? За обедом? Во время разговора? Хуже, за рулем? Невнимательность на дороге может привести к ДТП. Невнимательность в сети – к тому, что вы перейдете по зараженной ссылке, даже не заметив этого.

Некоторые организации пытаются бороться с технологическим разгильдяйством, моделируя фишинговые атаки и штрафуя тех сотрудников, которые попадаются. Но и это не очень эффективный метод, ведь от штрафа поведение человека не меняется, а значит, проблема остается там же.

А что делать-то?

Единственный способ бороться с такими проблемами – понять их суть и изменить поведение. Правила безопасности просты и известны, осталось начать их применять. В первую очередь, стоит присмотреться к своим действиям и понять, какие опасные действия вы совершаете. Кликаете по ссылкам, не глядя? Считаете, что «вирусов для Андроида не существует»? Просматриваете почту за обедом, одним глазом смотря «Игру Престолов»?

Если вы занимаетесь вопросами безопасности – «тренировочные» атаки, на самом деле, достаточно полезный способ. Но его следует применять правильно. Не просто делить сотрудников на тех, кто почувствовал подвох, и тех, кто попался. Обязательно нужно донести до вторых суть их ошибок и то, как не совершать их в будущем. Еще можно узнать, как именно определили опасность те, кто прошел проверку. Возможно, из этого вам удастся почерпнуть полезные идеи.

Соціальні мережі

як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»

Упорядник **Касаткіна** Тетяна

Редактори: Т. Дубас, О. Федоренко, Ю. Шлапак

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, просп. 40-річчя Жовтня, 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
www.nbuv.gov.ua/siaz.html

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.