СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(31.10–14.11)

2016 № 14

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(31.10–14.11)
№ 14

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
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2016

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

31.10.2016
Yahoo собрала всех своих ботов в одном приложении

Yahoo выпустила на iOS и Android приложение Yahoo Bots, через которое можно получить доступ ко всем её ботам. Приложение использует аналогичное другим чат-платформам вроде Facebook Messenger расположение кнопок, карточек и «каруселей». Также пользователям доступна интеграция с Siri, что позволяет им отправлять сообщения ботам с помощью голоса (InternetUA).

В Yahoo Bots присутствуют новостной, погодный и финансовый боты компании, бот-питомец Monkey Pets и вышедший недавно помощник по виртуальному футболу Blitz. Все за исключением последнего боты летом стали доступны и пользователям мессенджеров Kik и Facebook Messenger.

У новой платформы – огромный потенциал для развития. Например, компания может добавить в приложение больше своих ботов, создать гибридные проекты из своих продуктов вроде Flickr и Tumblr или даже спроектировать некую комбинацию поискового движка и искусственного интеллекта вроде Google Assistant или Xiaoice от Microsoft. Компания также могла быть дать разработчикам открытый доступ к своему приложению, чтобы они могли создавать и добавлять в Yahoo Bots своих ботов. Yahoo планирует «изучить все возможности», связанные с потенциальной интеграцией сторонних продуктов, рассказал представитель компании изданию VentureBeat.

Стоит отметить, что в отличие от многих других чат-платформ вроде Facebook Messenger или Slack, Yahoo выпустила своё приложение отдельно от мессенджера Yahoo Messenger. Это означает, что в Yahoo Bots можно общаться только с ботами, но не с людьми. Тем не менее, в будущем этот недостаток может быть устранён.

«Мы начали с запуска там, где уже была создана бот-платформа и поддерживаются возможности ботов. По мере изучения и повторения мы продолжим исследовать другие возможности, включая запуск в Yahoo Messenger», – заявил представитель компании.

***

31.10.2016
Соцеть «ВКонтакте» обзавелась обложками для сообществ

Как пишут в официальном сообществе Vk.com, обложка заменит собой уже привычные стандартные аватары и за счёт своего размера даст больше пространства для экспериментов с оформлением сообщества. Название сообщества, миниатюра аватара, статус и главные кнопки находятся сразу под обложкой в том же блоке. Поддержка обложек в мобильной версии и клиентах

появится чуть позже. Эти обновления должны облегчить поиск и следать сообщества визуально приятнее (Marketing Media Review).

***

1.11.2016

Facebook изменил правила цензуры после удаления культовой фотографии

В Facebook решили пересмотреть стандарты цензуры после скандала, связанного с удалением культовой фотографии «Напалм во Вьетнаме» с голой девочкой, спасающейся от бомбардировки в Сайгоне, передает Reuters (InternetUA).

Сообщается, что компания также восстановит часть материала, который был удален ранее согласно правилам цензуры.

«После инцидента с фотографией мы провели ряд изменений в нашей этической политике и подготовили новые правила обработки спорного материала», – заявил один из представителей компании.

***

1.11.2016

Базиленко Анна

Facebook запускає фільтри-маски в стилі месенджера Snapchat

Facebook проводить капітальний ремонт у налаштуваннях камери додатку. У соцмережі вже тестують функцію, яка дає змогу накладати фільтри-маски в стилі месенджера Snapchat, фільтри, які обробляють відео в стилі відомих художників, а також «інноваційні» фільтри, які реагуватимуть на рухи тіла, пише TechCrunch (Watcher).

У Facebook обіцяють, що ділитися трансляціями з використанням масок-фільтрів можна буде не лише у стрічці новин, а й в особистих повідомленнях за допомогою скриньки короткочасних повідомлень Facebook Direct inbox.

На сьогодні функція доступна користувачам Facebook з США, Нової Зеландії та Великої Британії. Найближчим часом фільтри-маски з’являться у користувачів в інших країнах.

***

2.11.2016

Базиленко Анна

Facebook запускає власну ігрову платформу десктопних ігор

Компанія Facebook офіційно оголосила про запуск власної ігрової платформи десктопних ігор Gameroom. Нині додаток доступний для всіх

користувачів Windows 7 і новіших версій цієї операційної системи, пише TechCrunch (Watcher).

На Gameroom зібрані мобільні портовані гри, веб-ігри та ігри, створені спеціально для цієї платформи. Розмір кожної з них поки не перевищує 200 МБ, надалі їхній розмір обіцяють збільшити до 500 МБ.

Серед доступних на Gameroom уже є такі ігри, як Words With Friends, Trivia Crack, Peter Molyneux's Curiosity, Scrabble, Critical Ops.

Головний конкурент Gameroom – платформа Steam, яка має 125 млн активних користувачів. Аби наздогнати Steam, Facebook доведеться неабияк постаратися та переконати розробників долучатись до нової ігрової платформи компанії, хоча і аргумент у Facebook цілком переконливий – охоплення соцмережі. Як відомо, кількість користувачів Facebook перевищує 1,7 млрд юзерів.

Steam – сервіс компанії Valve, відомого розробника відеоігор, який надає послуги цифрової дистрибуції, багатокористувацьких ігор і спілкування гравців.

***

4.11.2016

В Facebook сидит четверть населения планеты

Количество пользователей Facebook, которые хотя бы раз в месяц посещают свой аккаунт, превысило 1,79 млрд человек. Это составляет почти четверть населения Земли, которое достигло 7,3 млрд к началу 2016 г. (Центр информационной безопасности).

При этом 1,66 млрд ежемесячных подписчиков заходят в Facebook с мобильных устройств. Компания сообщила об этом в финансовом отчете за III квартал 2016 г.

1,18 млрд человек бывает в Facebook ежедневно. По сравнению с аналогичными результатами прошлого года количество ежедневных пользователей возросло на 17 %, ежемесячных – на 16 %. Наиболее активно число подписчиков растет в Азии, где за последний год в Facebook зарегистрировалось 107 млн человек.

Финансовые результаты квартала

Выручка компании в III квартале 2016 г. достигла 7,01 млрд долл., чистая прибыль – 2,4 млрд долл. В III квартале 2015 г. чистая прибыль компании составила всего 896 млн долл. Таким образом, годовой рост равняется 170 %.

Facebook в очередной раз оставила позади ожидания Уолл-стрит, которая предсказывала ей выручку в 6,92 млрд долл. Благодаря этому компания смогла выплатить акционерам 1,09 долл. на каждую акцию, что оказалось больше предполагаемых аналитиками 0,97 долл.

6,8 млрд долл. квартальной выручки Facebook было получено от рекламы, что на 59 % больше прошлогоднего показателя. 84 % поступлений от рекламы обеспечиваются ее просмотром на мобильных устройствах. По словам

директора компании М. Цукерберга, очень эффективным для компании оказалось размещение рекламного видео.

Стоимость Facebook сейчас составляет 371 млрд долл., что на 22 % больше, чем в начале 2016 г.

Facebook и чужая аудитория

Facebook расширяет свою аудиторию в том числе за счет приобретения других брендов. В 2014 г. компания выкупила за 19 млн долл. мессенджер WhatsApp, что долгое время считалось самой крупной сделкой в IT-отрасли. Недавно Facebook и WhatsApp заключили новые соглашения об обмене данными между мобильным мессенджером и соцсетью, которые вызвали недовольство властей Евросоюза. В конце прошлого месяца власти потребовали от WhatsApp прекратить предоставлять Facebook номера телефонов подписчиков, поскольку изначально пользователи не давали на это согласие.

В 2013 г. Facebook попыталась выкупить за 3 млрд долл. популярную соцсеть Snapchat, однако получила отказ. С тех пор компания пытается привлечь аудиторию Snapchat, добавляя в Facebook аналогичные функции. В 2014 г. Facebook даже выпустила «убийцу» Snapchat – приложение Slingshot, призванное подтолкнуть пользователей смартфонов делиться фотографиями и видео из повседневной жизни.

На днях ресурс TheGuardian подсчитал, что Facebook пыталась клонировать или купить различные функции Snapchat в общей сложности 10 раз. В основном это фильтры и функции, связанные с фото- и видеоконтентом. Однако большая их часть не пользуется особой популярностью – клиенты Snapchat не спешат переходить в Facebook. В конце прошлого месяца компания попыталась выкупить азиатский аналог Snapchat, перспективную южнокорейскую соцсеть Snow, но также получила отказ.

***

7.11.2016

Facebook запускает игровую платформу

Facebook Messenger собирается запустить платформу Instant Games, с помощью которой пользователи смогут играть в игры и соревноваться друг с другом внутри приложения. Об этом сообщает sostav.ru (МедиаБизнес).

Платформу уже тестирует компания King.com, разработчик игры Candy Crush.

Технические подробности не разглашаются, но, по данным портала The Information, игры будут асинхронными, то есть пользователям не обязательно играть в них в одно и то же время. Набор инструментов, который позволит разработчикам создавать подобные игры, будет готов уже к концу месяца.

Планируется, что игры в мессенджере будут максимально простыми. Также они могут включать встроенные покупки.

***

4.11.2016

«ВКонтакте» и «Одноклассники» предупредят пользователей о ЧС

Соцсети «Одноклассники» и «ВКонтакте» будут предупреждать своих пользователей о чрезвычайных ситуациях. Соглашение о создании такой системы оповещения подписали накануне МЧС и Mail.Ru Group (Центр информационной безопасности).

Пользователи соцсетей Mail.Ru Group, находящиеся в зоне ЧС либо в зоне, где возможно возникновение ЧС, получат уведомления или сообщение об этом прямо в социальной сети. При этом данные будут обновляться в режиме реального времени. Помимо информации об обстановке в своем регионе, пользователи также смогут получить информацию о мерах обеспечения безопасности населения, приемах и способах защиты, полезных контактах (номера горячих линий, телефоны и режим работы российских посольств и консульств, скорой, полиции).

Система уведомлений уже была опробована во время терактов в Париже и Ницце, когда пользователи, находящиеся в этих городах получили сообщение о мерах безопастности. Во время попытки государственного переворота в Турции пользователи «ВКонтакте» получили сообщения с телефонами посольства и генконсульств России. Пользователей «Одноклассников» оповестила о ситуации группа OK Operatively. Также пользователи были информированы о паводках в Вологодской области, событиях в Брюсселе и землетрясении в Италии.

По словам главы МЧС В. Пучкова, система оповещений в соцсетях позволит оперативно проинформировать о ЧС огромную аудиторию, дать рекомендации о том, как надо действовать, и тем самым сохранить жизни людей.

***

8.11.2016

Google решил убить SMS, как формат обмена сообщениями

Компания Google запускает обмен сообщениями на Android-устройствах по технологии Rich Communications Services (RCS) (InternetUA).

58 операторов связи, которые охватывают сеть в 4,7 млрд абонентов по всему миру, взяли на себя обязательства поддерживать единый стандарт реализации RCS.

В компании рассказали о том, что над внедрением RCS работают весь 2016 г. Абоненты американской телекоммуникационной компании Sprint получат возможность испытать новую технологию первыми. Уже в следующем году на всех новых Android-устройствах в сети оператора Sprint будет установлен обмен сообщениями по технологии RCS в мессенджере,

разработанном компанией Google. Пользователи получат расширенные функции для обмена сообщениями, в том числе групповой чат, обмен фотографиями высокого разрешения, сообщение о статусе прочтения. Услуга будет работать на облаке Jibe RCS от Google.

RCS является частью нового стандарта Advanced Messaging, что должно улучшить функциональные возможности обмена сообщениями по умолчанию. RCS обеспечивает передачу мультимедийных сообщений до 10 МБ, позволяет создавать групповые чаты, а также совершать видеозвонки. По аналогии большинству мессенджеров, RCS указывает на то, было сообщение прочитанное или набирается текст.

***

3.11.2016

Twitter ввел функцию быстрых ответов в личных сообщениях для бизнеса

Социальная сеть Twitter ввела функции быстрых ответов и приветствий в личных сообщениях для бизнеса. Об этом говорится в блоге соцсети (InternetUA).

Новые функции упрощают общение различных компаний с пользователями. Благодаря приветствиям подписчик больше не должен отправлять первое сообщение в беседе с компанией – при начале переписки будет показано автоматическое приветственное сообщение бренда.

Быстрые ответы, в частности, позволяют пользователю выбрать типовой вопрос или ответ. В случае необходимости можно обратиться к сотруднику компании.

Новыми функциями воспользовались, к примеру, компании Evernote и PizzaHut.

***

3.11.2016

Ольга Карпенко

Сеть «ВКонтакте» представила данные по украинской аудитории: демография, интересы и активность

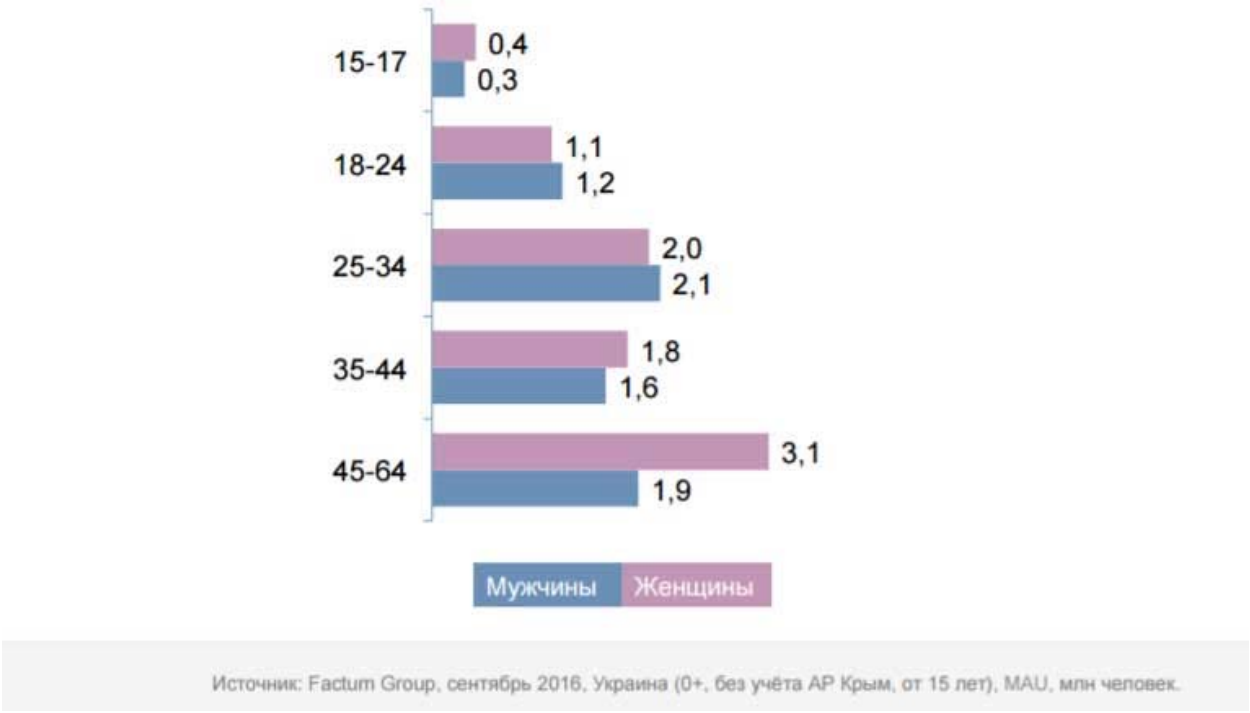
Социальная сеть «ВКонтакте» презентовала свежие данные по своей аудитории и инструментам в Украине. Это – данные медиапанели Opinion Software Media от Factum Group, а также – внутренние данные самой компании. По этим данным, «ВКонтакте» – самая популярная социальная сеть уанета по охвату, на втором и третьем месте – «Одноклассники» и Facebook (AIN.UA).

По данным компании, аудитории других популярных сетей в значительной степени с ней пересекаются:

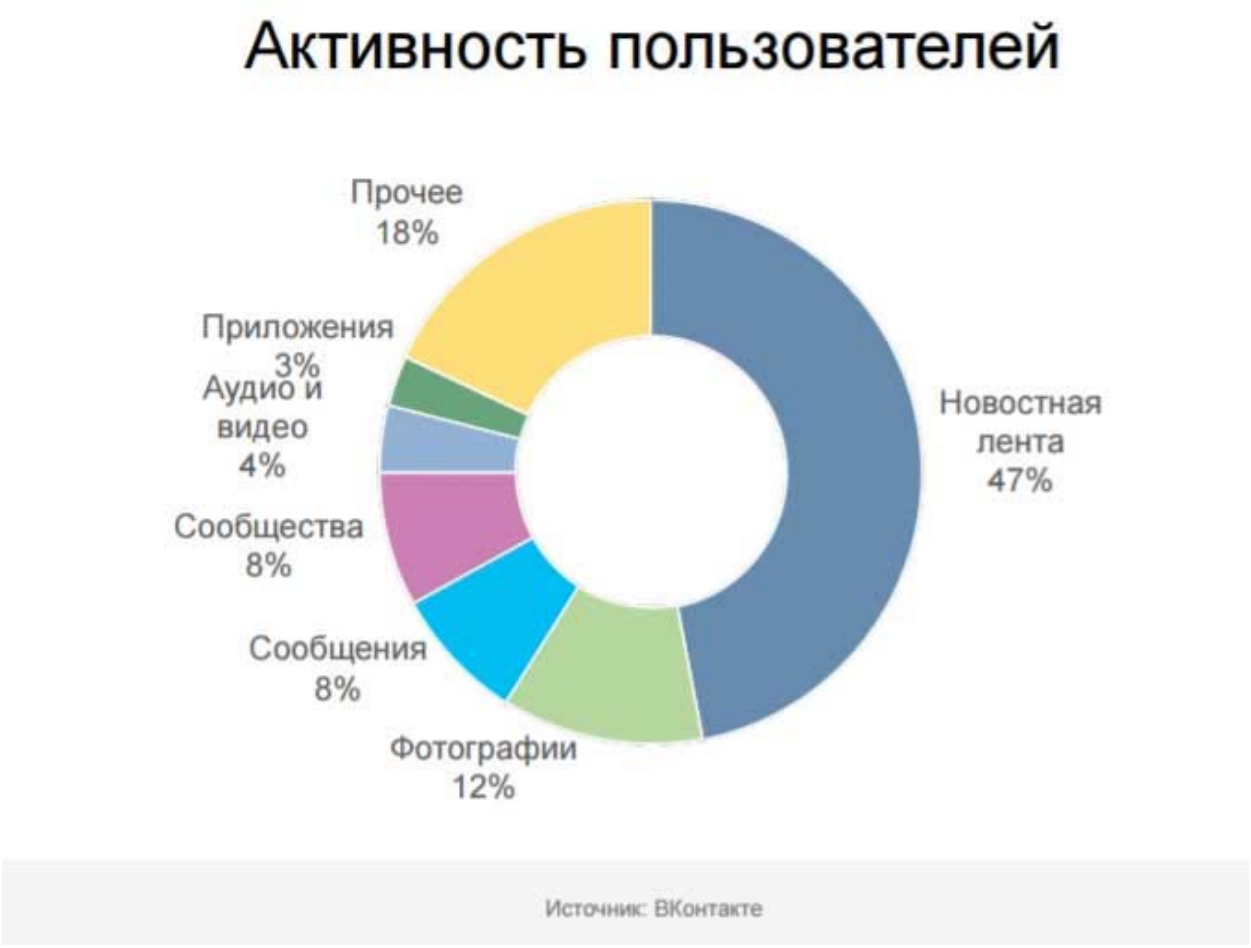
Источник: Factum Group, сентябрь 2016, Украина (0+, без учёта АР Крым, от 15 лет), MAU, % от пользователей уанета.

В демографическом разрезе аудитория сети выглядит таким образом:

Источник: Factum Group, сентябрь 2016, Украина (0+, без учёта АР Крым, от 15 лет), MAU.



Основная активность пользователей сети – чтение новостной ленты. Среди других популярных занятий – работа с фотографиями, участие в сообществах, обмен сообщениями:



По роду занятий украинская аудитория сети распределяется таким образом:

Источник: Factum Group, сентябрь 2016, Украина (0+, без учёта АР Крым, от 15 лет), MAU, млн человек.

Уровень достатка пользователей украинского сегмента «ВКонтакте» сравнили с аудиторией других сетей:

Источник: Factum Group, сентябрь 2016, Украина (0+, без учёта АР Крым, от 15 лет), MAU, млн пользователей

Около 25 % украинской аудитории заходит в сеть с настольных компьютеров, 51 % – с десктопов и мобильных, еще 24 % – только с мобильных устройств:

***

9.11.2016

YouTube представила новые инструменты для наведения порядка в комментариях

Постепенно YouTube даёт создателям контента всё больше инструментов для управления блоком комментариев. Ранее в этом году она позволила владельцам каналов назначать модераторов, а также устанавливать фильтры. Теперь же разработчики предложили ещё несколько способов навести порядок и выделить понравившиеся комментарии (InternetUA).

Отныне создатели контента смогут закреплять в верхней части блока какой-либо комментарий. Таким образом можно не только выразить свою признательность подписчику, например, но и расположить на виду важную информацию. Также лучшие комментарии можно будет отмечать сердечками, что, опять же, позволит плотнее взаимодействовать с аудиторией. Ну а чтобы слова самих владельцев каналов не затерялись в общем потоке, их имена будут выделяться цветом. У подтверждённых аккаунтов при этом рядом с именем будут отображаться значки подлинности (галочки).

Кроме того, YouTube представила бета-версию нового инструмента, позволяющего отправлять потенциально неприемлемые комментарии на рассмотрение владельцу канала, которому будет предложено их одобрить, скрыть или же, в том случае, если они нарушают правила сервиса, пожаловаться на них. Определять качество при этом будет специальный алгоритм, который, разумеется, может ошибаться, особенно на первых порах. Но разработчики обещают, что чем больше спорных комментариев будут

рассматривать пользователи, тем точнее система станет определять их качество.

***

9.11.2016
WhatsApp тестирует аналог «Историй» из Snapchat

Менее двух месяцев назад Facebook добавила в Instagram «Истории» – функцию, очень похожую на возможность под тем же названием из Snapchat, позволяющую формировать ленту контента, исчезающего через 24 часа после публикации. Теперь социальный гигант рассматривает возможность добавления аналогичной функции и в мессенджер WhatsApp (InternetUA).

Компания начала тестировать в одном из самых популярных приложений для обмена сообщениями функцию под названием «Статус», скрытую в дебрях кода последней публичной бета-версии WhatsApp для iOS и Android. Для того чтобы получить возможность опробовать новую функцию, нужно быть подписанным на программу бета-тестирования сервиса и иметь либо iPhone с установленным джейлбрейком, либо смартфон на базе Android с разблокированными root-правами.

Как и «Истории», новая функция WhatsApp должна дать людям возможность делиться с пользователями событиями из своей жизни. «Статусы» имеют 24-часовой срок действия, делиться ими можно либо сразу со всеми контактами в WhatsApp, либо с избранными людьми. Получить доступ к функции можно через новую вкладку «Статус», располагающуюся между вкладками «Чаты» и «Звонки».

Таким образом, пользователи могут отправлять своим друзьям и близким фотографии и видеоролики, которые, в том числе, можно выбирать и из библиотеки, разрисовывая их и добавляя к ним текст. Предположительно, обновления пользователей будут отображаться во вкладке «Статус» у их друзей.

Тем не менее, не факт, что функция появится в стабильной версии WhatsApp в ближайшее время. Даже бета-тестеры на Android для активации приложения вынуждены скачивать стороннюю программу, требующую root-прав.

***

12.11.2016
Facebook откажется показывать рекламу по расовому признаку

Социальная сеть Facebook готова пересмотреть правила подачи рекламы и отказаться от таргетирования по расовому или национальному признаку. Об этом пишет The New York Times (InternetUA).

Месяцем ранее появилась информация о том, что соцсеть предлагает рекламодателям подбирать аудиторию по национальному или расовому

признаку, что на языке Facebook звучало как «этническая общность». Как выяснилось, таким образом она потенциально нарушает законы о гражданских правах.

Отмечается, что такой подход к поиску аудитории наиболее актуален в рекламе жилья, трудоустройства и кредитных услуг. Facebook сообщил в блоге, что теперь будет требовать от рекламодателей не заниматься «дискриминирующей рекламой» в вышеперечисленных сферах.

***

13.11.2016

В Instagram появятся прямые трансляции

В настоящее время команда Instagram активно работает над новой функцией для своего сервиса: она хочет дать пользователям возможность вести прямые трансляции. Об этом в интервью Financial Times рассказал К. Систром (Kevin Systrom), один из основателей и генеральный директор Instagram (InternetUA).

К. Систром отметил, что, на его взгляд, стримы позволят значительно обогатить опыт взаимодействия между пользователями, помогут им поддерживать более тесный контакт: «Если бы я пытался укрепить отношения с дорогими мне людьми, прямые трансляции стали бы отличным способом быть ближе к ним». Однако он пока не стал распространяться о том, какими особенностями будет обладать эта функция Instagram, а также об ожидаемых сроках её запуска. Тем не менее, в конце октября некоторые участники программы бета-тестирования приложения заметили появление значка «Live» на некоторых иконках в разделе Stories, так что есть основания полагать, что трансляции можно будет найти именно там.

А пока же Instagram обновил тот самый раздел Stories. Теперь пользователи смогут включать в свои истории короткие видео, созданные в приложении Boomerang, упоминания других пользователей, а также прикладывать ссылки.

***

14.11.2016

Анонимная соцсеть Secret вернется спустя полтора года после закрытия

В 2014 г. анонимная социальная сеть Secret наделала много шуму и стала поводом для целого ряда обсуждений, а также спровоцировала несколько крупных скандалов. Люди публиковали самые различные посты: от бытовых оскорблений до важных утечек из технологических компаний. Однако в апреле 2015 г. основатель проекта Д. Бийтау, анонсировал закрытие проекта. Оказалось – не навсегда (InternetUA).

О перезапуске Д. Байтау объявил в своем Twitter-аккаунте, не объявив об источниках финансирования или новых способах монетизации, которые должны поддержать проект: «Вторая версия Secret близка. Это слишком важно, чтобы не существовать. Но прежде чем сервис выйдет в свет, я должен знать, что люди поддержат его».

Очевидно, возобновление работы связано с недавними президентскими выборами в США, которые резко подогрели интерес общественности к вопросам кибер-безопасности и анонимности. Позже в разговоре с TechCrunch он подтвердил это: «У людей нет пространства, где они могут быть собой. В них слишком много страха и слишком мало самосознания. Нам нужно больше самосознания, начиная с Кремниевой долины. Мы находимся в пузыре. Только когда мы лопнем пузырь и выпустим правду на свободу, тогда мы сможем помогать друг другу и работать вместе».

Тажке он уточнил, что теперь намерен работать над проектом без привлечения венчурных инвестиций и будет отдавать всю заработанную прибыль на благотворительные нужды. Главными получателями станут фонды, которые могут пострадать от недостатка финансирования при президенте Д. Трампе. Напомним, что в 2014 г. Secret в общей сложности привлек более 35 млн долл. от инвесторов.

Сейчас главной Д. Байтау заботой остается другой проект, нацеленный на предпринимательскую аудиторию – Bold. Д. Байтау не назвал точных сроков возвращения приложений Secret в маркеты.

***

14.11.2016

Facebook Messenger тестує групи за інтересами

Facebook Messenger запускає нову функцію під назвою Rooms, яка дасть змогу незнайомим між собою користувачам спілкуватися в групах за інтересами, пише Courier Mail (Watcher).

За словами продакт-менеджера Facebook Messenger Д. Моксона, Rooms створена для того, щоб «не дратувати друзів темами, які їх не цікавлять». Вступити в групу може будь-хто: для цього достатньо схвалення адміністратора.

Користувачі Facebook Messenger уже зараз можуть створювати групи, але, зазвичай, це приватні розмови між друзями. Запуск Rooms дасть змогу користувачам Facebook Messenger обговорювати специфічні теми не лише з друзями, а й з незнайомцями.

Наразі функція тестується в Канаді та Австралії і доступна на смартфонах, що працюють на платформі Android.

***

14.11.2016

Facebook успешно протестировала оборудование для интернет-дронов

Социальная сеть Facebook отрапортовала о прогрессе в реализации проекта по обеспечению интернет-доступом как можно большего количества людей за счёт беспилотных летательных аппаратов (InternetUA).

Facebook разработала дроны Aquila на солнечных батареях, не уступающие размахом крыльев Boeing 737. Для предоставления веб-доступа жителям отдалённых регионов бортовое оборудование должно обеспечивать дальность действия от 30 до 50 км. При этом пропускная способность канала связи, как ожидается, составит не менее 30 Гбит/с.

Сообщается, что во время недавно проведённых тестов был организован канал передачи данных между двумя вышками в Южной Калифорнии (США), расположенными на расстоянии около 13 км друг от друга.

Facebook тестирует систему, использующую миллиметровые волны в диапазоне от 60 до 90 ГГц. По сравнению с более низкочастотными диапазонами, радиоволны миллиметрового диапазона испытывают сильное затухание при распространении в земной атмосфере. Из-за этого подобные радиосистемы характеризуются относительной малой дальностью действия и сильной зависимостью от погодных условий.

Специалисты Facebook решают проблемы за счёт применения специализированных радиокомпонентов и сверхточного позиционирования антенн. На передающей стороне в ходе испытаний применялась 60-сантиметровая тарелка, на принимающей – 120-сантиметровая. В результате удалось достичь пропускной способности до 20 Гбит/с.

Следующий шаг – тестирование системы земля-воздух. Для этого оборудование будет установлено на борту небольшого самолёта Cessna. В 2017 г. Facebook рассчитывает показать пропускную способность на уровне 40 Гбит/с.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

7.11.2016
Д. Трампа оставили без Twitter

Советники кандидата в президенты США от Республиканской партии Д. Трампа отстранили его от собственного микроблога в Twitter. Об этом сообщает lenta.ru (МедиаБизнес).

Такое решение было принято из-за того, что миллиардер систематически использовал микроблог для очернения своих политических противников, он также предоставлял избирателям «нефильтрованный взгляд» по ряду вопросов. Издание отмечает, что микроблог Д. Трампа в Twitter насчитывает более 13 млн подписчиков.

25 октября газета The New York Times обнародовала список людей и мест, которых Д. Трамп оскорбил в Twitter. Перечень содержит 281 позицию. В своем микроблоге он затронул не только представители Республиканской и Демократической партий США, но и СМИ, компании, и даже целые страны.

Так, например, Д. Трамп назвал Китай «ужасным государством», американского лидера Б. Обаму «слабым и неэффективным», а газету The Wall Street Journal – «похожей на таблоид». Особое место в перечне людей, оскорбленных республиканцем, занимает кандидат в президенты США от Демократической партии Х. Клинтон. Ей Д. Трамп посвятил более 300 гневных сообщений.

***

13.11.2016

Д. Трамп пообещал вести себя сдержанно в соцсетях

Избранный президент США Д. Трамп пообещал вести себя умеренно в соцсетях. Об этом он сообщил в программе 60 minutes телекомпании CBS (InternetUA).

«Если я вообще буду это использовать, я буду очень сдержан», – сказал он.

Миллиардер также назвал социальные сети «прекрасной формой общения». Он добавил, что они могут помочь отвоевать свои позиции в случаях, когда СМИ распространяют неточную информацию.

Д. Трамп заключил, что большое количество подписчиков в Facebook, Twitter и Instagram помогли ему выиграть президентскую гонку.

***

2.11.2016

Сумчанам пропонують оприлюднити результати своїх тестів на ВІЛ // Мешканці міста запустили у соцмережах флешмоб #ТЕСТнаВІЛ

Обласне відділення Всеукраїнської благодійної організації «Всеукраїнська мережа людей, що живуть з ВІЛ» та «Клініка, дружня до молоді» організували в соціальних мережах флешмоб #ТЕСТнаВІЛ, приурочений до 1 грудня – Всесвітнього дня солідарності з ВІЛ-позитивними людьми, повідомляє Depo.Сумы з посиланням на департамент комунікацій сумської міськради.

Флешмоб триватиме 1 листопада до 1 грудня.

Користувачам соцмереж пропонують розповсюдити світлину з «успішно складеним» тестом із хештегом #ТЕСТнаВІЛ.

***

9.11.2016

Соцмережі «підірвав» флешмоб на підтримку української музики

У вівторок 8 листопада, коли в силу вступив закон про квоти на українську музику на радіо, в Україні запустили флешмоб у підтримку вітчизняного музичного продукту. До акції, яку започаткувала ініціативна група із нардепів, долучився навіть Президент П. Порошенко (Пресса Украины).

Зауважимо, що до введених квот українці поставились неоднозначно. Дивним чином у мережі з'явилось багато противників української музики, як такої, яка не є якісною. Звичайно, що є інша частина активних користувачів мережі насправді зраділа таким нововведенням.

«Я ніколи такого не робила, але сьогодні хочу оголосити флеш-моб. Тут у Facebook. На вашу улюблену українську пісню. Бо саме сьогодні починає діяти наш закон, і від сьогодні кожна четверта пісня в радіоефірі має бути українською. Нам казали, що їх стільки нема, що вони гіршої якості і т. д… Але цим флешмобом ми покажемо всім – українська пісня є, українська культура є, і це значить, що Україна буде. Попри всі труднощі. Бо мова і культура – це основа. Facebook дозволив відмітити лише сотню людей, яких я прошу показати всім свої улюблені українські пісні», – анонсувала акцію В. Сюмар, яка, до слова, і є головним ініціатором написання прийнятого закону.

До акції вже приєднались політики, журналісти та активісти. Одним із першим на акцію відреагував український лідер П. Порошенко.

«Маємо зробити так, щоб української пісні було якнайбільше – на радіо, на телебаченні і, звичайно, у соціальних мережах також», – написав П. Порошенко.

***

11.11.2016

«Дякую солдате!» – Українці розпочали у соцмережі акцію

Користувачі соцмережі Facebook розпочали надзвичайно проникливий, патріотичний та щирий флешмоб для підтримки українських військових, захисників мирного життя Батьківщини (ПолітІнфо).

Усі охочі приєднатися до подяки використовують хештег #дякуюсолдате.

Акцію розпочали жителі Києва, що зафільмували, якої думки звичайні перехожі про тих, хто захищає цей світ від ворожої артилерії.

«Подякувати військових захотіло так багато людей, що ми не знали, як усіх їх умістити в один ролик. Пара з Луганську, яка втекла від "руського міру", зі сльозами на очах говорила й говорила про те, наскільки важливий для них

подвиг ЗСУ. Дівчина з Маріуполя, що дякує батальйону “Азов”. Волонтер з Харкова. Україномовні, російськомовні, діти, батьки, пенсіонери, підлітки, адвокати, майстри тату, менеджери, скейтери, жінки, чоловіки», – розповів автор відео та флешмобу.

До флешмобу вже приєдналися в Міністерстві оборони та поширили відео, де прості громадяни України дякують воїнам за те, що ті «захищають наші міста від війни».

***

14.11.2016
Украинские IT-шники собирают онлайн-Майдан

После бунта обманутых вкладчиков и регулярных акций протестов других слоев населения, в Украине могут начаться акции протеста IT-специалистов. IT-шники уже запустили в соцсетях кампанию «Онлайн-протест IT и телекомпаний» с хэш-тегом #не_кошмарь_it (InternetUA).

Поводом стали постоянные наезды силовых структур на IT-компании, которые полностью парализуют их деятельность.

«Выйдя в 2013 г. одними из первых на Майдан, представители украинского IT и телеком-сообщества стремились поддержать страну в ее рвении наконец-то заявить о себе как о демократическом, прогрессивном и по-настоящему европейском обществе. Переехать на Запад каждый из нас мог давно. Но тогда Украина лишилась бы более 100 тыс. молодых, перспективных, талантливых и высокооплачиваемых специалистов. Тогда бы Украина лишилась будущего… Что мы получили взамен? Так называемые “силовики” – сотрудники СБУ, МВД, налоговой милиции, прокуратуры – кошмарят компании, которые даже в нынешних трудных условиях продолжают оставаться на плаву. Это касается не только IT и телекома, это касается всего “живого” бизнеса. Это и надуманные поводы для внеплановых проверок, и варварские методы получения вещдоков, и бесконечные вызовы специалистов на бессмысленные допросы, словно преступников. Все эти три года после Революции Достоинства мы живем в постоянном ожидании, что в любой момент в офис могут ворваться силовики и, прикрываясь поиском террористов, порнографов или шпионов, устроить маски-шоу», – говорится в обращении.

«Мы просим сделать всего несколько шагов нам навстречу: наконец наложить мораторий на изъятие техники у высокотехнологического бизнеса, прекратить надуманные проверки, принять законы о поддержке hi-tech-компаний», – призывают IT-шники.

Перепост этого обращения уже сделали сотни айтишников.

Так, А. Бондарчук на своей странице в социальной сети Facebook пишет: «IT – единственная отрасль украинской экономики, которая достойно конкурирует на глобальном мировом рынке. Не имея (но – и не нуждаясь) в каких-то глобальных олигархических политических “схемах поддержки”. IT –

повод для гордости всего украинского общества. Те, кто кошмарят IT-компании – не понимают, и не хотят понимать современных тенденций: мобильности трудовых ресурсов, прозрачности границ, конруренции идей, а не силы или капиталов, глобальной кооперации ... Они “зарабатывают” иначе, живут в другой системе координат», – написал А. Бондарчук.

А. Бондарчук напомнил, что после каждого такого «наезда» из Украины уезжают сотни опытных специалистов. «Это – потеря украинским обществом перспективы и надежд на конкурентоспособность в мировом масштабе», – отметил А. Бондарчук.

Акцию IT-специалистов поддержало одно из крупнейших волонтерских движений в Украине.

«К сожалению, в ближайшем будущем мы будем вынуждены закрыть почти все наши проекты – как информационные, так и технологические... Ведь наши компании, и компании наших партнеров сегодня подвергаются преследованиям со стороны Нацполиции, СБУ, прокуратуры. Дошло до того, что мы не можем выплатить сотрудникам зарплату не потому, что нет денег, а потому, что банковские счета блокируются со стороны правоохранителей», – пишут на официальной странице в Facebook представители «Первого Волонтерского».

Представители организации заявляют, что «IT-специалистов обвиняют в сепаратизме, распространении порно, создании онлайн-казино, уклонении от уплаты налогов», изымают серверы и другое оборудование для работы, а потом приходят и предлагают “решить” вопрос за 30 % от стоимости изъятого оборудования».

***

8.11.2016

Україна завела акаунт в Instagram

Аккаунт поки що не верифікований, але він ведеться офіційними посадовими особами (Кореспондент.net).

Офіційний акаунт країни з’явився в соцмережі Instagram. Про це повідомив офіційний Twitter-аккаунт України.

На цей момент в акаунті лише кілька постів і майже 1000 прихильників. Усі повідомлення у ньому дублюються українською та англійською.

Перший пост присвячений тому, як 11 українських військових піднімають прапор у звільненому Слов’янську. Решта постів – про красиві види з усієї країни: київські мости з висоти пташиного польоту, Білгород-Дністровську фортецю тощо.

Цікаво, що акаунт з такою назвою вже був зареєстрований раніше, й отримати до нього доступ вдалося після переговорів з Facebook.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

2.11.2016
Facebook пытался купить азиатский клон Snapchat

Социальная сеть Facebook пыталась купить азиатский клон Snapchat – мессенджер Snow. Об этом сообщает TechCrunch со ссылкой на источник. По имеющейся информации, безуспешная попытка произошла летом 2016 г. (InternetUA).

Snow – это сервис южнокорейской фирмы Naver, которая также известна по чат-приложению Line.

На сегодняшний день у Snow насчитывается около 80 млн скачиваний, каждый месяц добавляется еще примерно 10 млн, рассказал источник. Как предполагается, такой рост привлек внимание и других потенциальных покупателей, среди которых Tencent (создатель WeChat), компания Alibaba и др.

***

2.11.2016
Базиленко Анна
Instagram надає змогу купувати товари безпосередньо з фотосервісу

Instagram представив функцію shopping tags, за допомогою якої роздрібні бренди можуть позначати на своїх фотографіях товари, а користувачі – купувати їх безпосередньо з фотосервісу (Watcher).

Натиснувши на зображення з shopping tags, біля товару з'явиться його назва та ціна. Користувач зможе перейти на сторінку з описом товару після того, як натисне на таку відмітку. Далі – на сторінку товару в інтернет-магазині, де зможе оформити замовлення.

У Instagram не планують брати комісію за оформлені таким чином замовлення, пише TechCrunch. Замість цього фотосервіс пропонуватиме рекламу зображень з shopping tag в стрічках новин користувачів, які не підписані на профілі магазинів.

Згодом компанія планує додати функцію збереження фотографій, які сподобались, аби користувач зміг повернутись до покупок відібраних товарів. Очікується, що shopping tags з'являться у відео та фотокаруселях.

Наразі shopping tags доступні користувачам iOS-додатку в США. Можливість відмітити тегами свої товари отримали 20 роздрібних брендів. Планується запуск функції і в інших країнах: коли і де саме в Instagram поки не повідомляють.

***

2.11.2016

Оплачивать «коммуналку» теперь можно через Facebook Messenger

Команда разработчиков ПриватБанка создала нового специального робота для Facebook Messenger, помогающего оплачивать коммунальные услуги прямо через популярный сервис. Новый бот получил название «Мои платежи», сообщается на странице банка в Facebook (IGate).

Для того, чтобы воспользоваться услугой, необходимо один раз найти в Facebook Messenger бота и пройти несложную регистрацию. Для этого пользователю требуется ввести номер мобильного, последние четыре цифры номера карты, а также пароль от банка, который будет выслан на телефон.

На данный момент оплата коммунальных платежей через мессенджер Facebook доступна только лишь клиентам ПриватБанка по ранее созданным шаблонами в Приват24, которые можно найти в меню «Мои платежи».

***

3.11.2016
Facebook подвел финансовые итоги III квартала

Доход компании Facebook в III квартале 2016 г. увеличился на 56 % в сравнении с аналогичным периодом 2015 г. и составил немногим более 7 млрд долл. Такая информация представлена в официальной отчетности компании (IGate).

Чистая прибыль Facebook за год возросла на 16,6 % – с 896 млн долл. до 2,3 млрд долл. Представители компании отметили рост доли выручки от мобильной рекламы в общем учете доходов – сейчас она составляет 84 %.

В Facebook не стали раскрывать статистику других источников доходов. Во время презентации отчета компания предупредила, что в 2017 г. рост выручки может значительно сократиться из-за снижения темпов увеличения объемов рекламы. На фоне этого заявления акции Facebook просели более чем на 7 %.

Ежемесячная аудитория социальной сети возросла на 16 % за год и составила 1,79 млрд человек. При этом более миллиарда из них за месяц ни разу не зашли в Facebook с настольных компьютеров, использую только мобильные устройства – этот порог был преодолен в первый раз.

«Мы провели еще один хороший квартал, в котором успешно продвигали видео во всех наших сервисах и выполнили задачи, соответствующие нашему 10-летнему плану по развитию технологий», – заявил глава Facebook М. Цукерберг. Он отметил, что компания сделает ставку на развитие инструментов для «визуального общения» – в том числе, при помощи новой камеры, встроенной в приложение соцсети.

***

8.11.2016
«Одноклассники» не будут отключать рекламу за плату

Социальная сеть «Одноклассники», принадлежащая Mail.Ru Group, отказалась от функции платного отключения рекламы. Об этом сообщает sostav.ru (МедиаБизнес).

Эксперимент продлился четыре месяца, в результате тестирования выяснилось, что сервис использовали единицы пользователей. Хотя услуга больше недоступна, «Одноклассники» продолжит работать над эффективностью рекламы и запуском новых форматов.

Оценка реакции аудитории на рекламу была одной из целей эксперимента с платной подпиской. «Он вызвал довольно бурную реакцию, а мы наблюдали за отзывами экспертов и смотрели за популярностью сервиса. Тест оказался очень полезен. Мы хотели понять насколько пользователи готовы блокировать рекламу в социальном контенте и, в частности, в мобильных приложениях, где adblocks ее не выключают.

В итоге, для большинства пользователей отключение рекламы не оказалось первостепенным. Это доказало главное – реклама в «ОК» хорошо таргетирована и не мешает воспринимать контент», – рассказал первый замглавы Mail.Ru Group Д. Сергеев.

Директор по маркетингу и развитию бизнеса «Одноклассников» А. Исрапилов подтвердил, что компания внимательно относится к распространяемому контенту в соцсети. Поскольку реклама является контентом и частью продукта, цель соцсети – сделать рекламу более эффективной за счет анализа обратной связи от пользователей.

***

7.11.2016

Холдинг Look at Media отказывается от веб-версий и переходит в соцсети

Медиахолдинг Look at Media, которому принадлежат проекты The Village, Furfur и Wonderzine, в ближайшие четыре года полностью откажется от веб-версий. Об этом на форуме RIW заявил сооснователь и глава холдинга А. Аметов (МедиаБизнес).

По словам А. Аметова, веб-версия останется в качестве «витрины» холдинга, но перестанет быть основной платформой: «Это будет имиджевая витрина медиабренда, но при этом потребление будет идти на других платформах. Поэтому с точки зрения нашей медийной стратегии мы смотрим за платформами и сейчас пытаемся понять, как мы наш продукт будем нарезать для этих платформ».

Платформами он считает «Facebook, “ВКонтакте”, Apple, Androd и другие крупные экосистемы, которые внутри себя могут нести контентные и интерактивные вещи».

«Цепляться за платформу достаточно нелепо, потому что можно превратиться в издателей бумажной прессы, которые не шли в диджитал», –

заявил А. Аметов и добавил, что нужно менять и технологии подачи информации читателю на разных платформах.

***

7.11.2016
Facebook расширяет свою рекламную сеть на digital ТВ

Социальная сеть начинает тестировать продажу видеорекламы в приложениях для ТВ-приставок Apple TV и Roku, отмечает searchengines.ru. «Мы хотим протестировать, как лучше доставить видеорекламу через Audience Network пользователям подключенных к Интернету ТВ-устройств. Наша цель – обеспечить показ релевантной рекламы как пользователям Facebook, так и другим людям», – комментируют запуск в компании (Marketing Media Review).

***

7.11.2016
Музыка «ВКонтакте» стала платной

В начале ноября мобильное приложение «Музыка “ВКонтакте”», созданное партнером Mail.Ru Group – United Music Agency (UMA) – провело ребрендинг, сменив название на Boom (InternetUA).

Новая версия клиента появилась в App Store 3 ноября, а в Google Play – 31 октября. Судя по примечаниям, авторы сменили дизайн программы, название и иконку. Кроме этого, создатели отметили, что добавили новые тарифы.

В приложении пользователи могут выбирать один из четырех тарифных планов или же получить бесплатную подписку, действующую 90 дней.

***

9.11.2016
Twitter передумал закрывать Vine и хочет продать сервис

Компания Twitter передумала закрывать свой видеосервис Vine, поскольку получила массу предложений о его покупке. В настоящий момент компания занимается их рассмотрением, сообщает TechCrunch со ссылкой на источники (InternetUA).

Twitter получил сразу несколько предложений о покупке Vine, в том числе от азиатских компаний, после анонсирования скорого закрытия видеосервиса. Источники не смогли назвать весь перечень заинтересованных фирм, однако одна из них – японская Line. Также сообщается, что одна из сторон предложила за Vine около 10 млн долл.

***

10.11.2016
«ВКонтакте» запустил безналичные денежные переводы в Украину

Социальные сети Mail.Ru Group решили заполнить нишу, возникшую после того, как НБУ запретил работу российских платежных систем. Следом за социальной сетью «Одноклассники» возможность получения безналичных денежных переводов заработала и для украинских пользователей «ВКонтакте» (Finance.Ua).

Они смогут получить перевод на карты Mastercard и Maestro, выпущенные украинскими банками. Отправлять деньги из Украины пока невозможно, но в пресс-службе социальной сети сообщили, что сейчас работают над запуском переводов внутри страны.

Чтобы отправить деньги, пользователю не нужно знать номер карты получателя – тот сам решит, куда зачислить полученные средства. Сервис работает в диалогах полной и мобильной версий сайта, а также в официальных мобильных приложениях «ВКонтакте». Переводы осуществляются в рублях. Сумма одного перевода может составлять от 100 до 75 000 рублей (40–30 000 грн), в сутки можно отправлять и получать до 150 000 рублей (60 000 грн), в месяц – до 600 000 рублей (240 000 грн). При зачислении на карту со счетом в гривнах или другой валюте конвертация происходит по курсу банка, выпустившего карту получателя.

Комиссия за переводы с карт Mastercard и Maestro не взимается в рамках акции до 8 января 2017 г. За переводы с карт Visa она составляет 1 % от суммы, но не менее 40 рублей. Помимо этого, банк, выпустивший карту, может устанавливать собственные комиссии и ограничения на отправку и получение переводов с карты на карту.

Срок зачисления средств зависит от банка-эмитента получателя и составляет от нескольких секунд до нескольких дней. Пользователя может принять перевод в течение пяти суток с момента отправки. Если он этого не сделал или отклонил перевод, то деньги возвращаются на карту отправителя. Отправитель может отменить перевод, пока он не принят получателем.

«По данным международной исследовательской сети Factum Group, каждый месяц “ВКонтакте” посещают 15,8 млн украинских пользователей. Мы убеждены, что на фоне новостей об ограничении работы некоторых систем денежных переводов в Украине наш сервис будет востребован», – отметил Ю. Иванов, директор по электронной коммерции «ВКонтакте».

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

1.11.2016
Яна Смагула
Ученые обнаружили связь между Facebook и продолжительностью жизни

Американские ученые установили связь между временем, проводимым на Facebook, и здоровьем человека, а также продолжительностью жизни. Об этом сообщает издание PNAS (podrobnosti.ua).

Специалисты из Калифорнийского института в Сан-Диего проанализировали 12 млн профилей в Facebook и сравнили с записями Калифорнийского департамента здравоохранения. Владельцы профилей родились в 1945–1989 гг.

Согласно данным ученых, умеренное использование Facebook ассоциируется с самым низким уровнем смертности, а получение заявок в друзья коррелирует со снижением смертности. Отправка заявок в друзья такого эффекта не дает.

По мнению ученых, это свидетельствует о том, что человеку необязательно устанавливать социальные связи через «реальный» мир – сетевое общение тоже для этого подходит.

При этом ученые не спешат заявлять, что Facebook продлевает жизнь. На их взгляд, вероятен и обратный сценарий: у здоровых людей более активная социальная жизнь, в том числе и в Интернете.

***

7.11.2016
Мария Майорова
Почему нельзя оставлять телефон в спальне ребенка

Наличие смартфона в комнате ребенка негативно сказывается на качестве его сна, так установили ученые из Королевского колледжа Лондона, пишет novosti-n.org (podrobnosti.ua).

Также ученые утверждают, что смартфоны нельзя использовать после того, как в детской спальне гаснет свет. Ученые выяснили, когда родители просто разрешают оставить смартфон в комнате ребенка, то дети спят хуже, поскольку постоянно ожидают поступления новых сообщений.

Наблюдения показали, что дети и подростки, использующие электронные девайсы в течение 90 минут перед отходом ко сну, в два раза чаще не высыпаются и почти в три раза чаще испытывают ощущение сонливости в течение следующего дня. Доступ к электронным устройствам даже без их использования на 79 % увеличивает риск невысыпаемости ребенка, на 46% повышает опасность низкого качества сна и на 127 % увеличивает вероятность дневной сонливости.

Также дети, которые зарегистрированы в социальных сетях, это приводит к тому, что дети и подростки все время находятся в состоянии бодрствования. Исследователи подчеркивают, что большинство подростков бросаются к своим смартфонам первым делом после пробуждения, а последним, что они делают перед отходом ко сну, также является проверка новых сообщений. Из-за этого не приходится удивляться тому, что дети и подростки хронически не высыпаются, пока их мозг постоянно загружен ожиданием новой информации.

При этом другая группа исследователей пришла к выводу о том, что 72 % детей и 89 % подростков имеют, по меньшей мере, один девайс в своей спальне, и большинство пользуются ими перед отходом ко сну.

Маніпулятивні технології

8.11.2016

В Донецкой области СБУ разоблачила администратора сепаратистских групп в соцсетях

Сотрудники Службы безопасности Украины разоблачили в г. Бахмут (Артемовск, Донецкая обл.) администратора сепаратистских ресурсов «Л-ДНР» в социальных сетях (InternetUA).

Об этом сообщает пресс-служба СБУ.

«Правоохранители установили, что мужчина в 2014 г. через сеть познакомился с представителями незаконных вооруженных формирований террористов. Он согласился распространять сепаратистские материалы на различных информационно-политических пабликах (сообщества в соцсетях. – Ред.) и стал администратором группы антиукраинской направленности», – говорится в сообщении.

По данным пресс-службы, по указанию кураторов, злоумышленник распространял информацию, направленную на дискредитацию украинского государства и армии, разжигание межнациональной розни, введение русского языка как государственного. Он также пропагандировал выход юго-восточных областей из состава Украины и вхождения их на Россию.

«Во время обыска по месту жительства администратора сотрудники спецслужбы изъяли компьютерную технику с доказательствами противоправной деятельности», – добавили в ведомстве.

Открыто уголовное производство по ч. 1 ст. 256 Уголовного кодекса Украины.

Продолжается досудебное следствие.

***

8.11.2016

У Львові до трьох років засудили чоловіка, який агітував до сепаратизму в Інтернеті

Прокуратурою Львівської області підтримано державне обвинувачення стосовно мешканця міста Львова, підозрюваного у вчиненні кримінальних правопорушень проти основ національної безпеки України. Про це Львівському порталу повідомили у прес-службі прокуратури у Львівській області (Львівський портал).

Як уже раніше повідомлялось, чоловік у себе вдома через соціальну мережу «ВКонтакті», з травня 2014 р. по березень 2015 р. проводив незаконну агітаційну роботу серед користувачів Інтернету. Зокрема, розповсюджував на своїй сторінці статті (пости) із закликами до насильницької зміни або повалення конституційного ладу та захоплення державної влади, а також до змін меж території або державного кордону України на порушення порядку, встановленого Конституцією України. Його дії кваліфіковано за ч. 2 ст.109 та ч. 1 ст.110 КК України.

Відтак за результатами розгляду вказаного кримінального провадження, 4 листопада поточного року вироком Франківського районного суду м. Львова згаданого громадянина визнано винним в інкримінованих йому кримінальних правопорушеннях і призначено покарання у виді трьох років позбавлення волі з відстрочкою виконання покарання строком три роки.

***

7.11.2016

Росія має намір підірвати вибори в інших західних країнах

«Підтримана Росією серія хакерських атак, які сколихнули хід виборчої кампанії у США, може повторитись у день виборів, і скоріш за все, продовжиться у 2017 та 2018 рр. під час виборів у ключових країнах в Європі», – про це пише впливове видання Wall Street Journal, посилаючись на посадовців адміністрації Б. Обами (АРАТТА. Український національний портал).

«Втручання Росії, щоправда, може навіть бути більш вагомим в Європі, ніж у США, кажуть офіційні особи у Білому домі та експерти, тому що Москва вже довгий час залицяється до тамтешніх політиків і налагодила зв’язки з

євроскептичними політичними партіями, які посилились через наплив мігрантів та біженців», – пише автор статті А. Каллісон.

Ідеться, зокрема, про вибори у Нідерландах у березні, президентські вибори у Франції в квітні та травні, як також вибори у Німеччині восени.

Хоча широкомасштабне втручання Росії у виборчий процес – явище відносно нове для США, кажуть експерти, в Європі Росія активно веде хакерську та дезінформаційну кампанію вже протягом двох років, що має на меті послабити тих, кого Кремль вважає своїми противниками – пише автор статті.

«Навіть якщо Росії не вдасться зробити так, щоб на виборах у Європі перемогли їхні союзники, таке довготривале втручання у виборчий процес на Заході послужить досягнення кінцевої мети Кремля: а саме дезорганізує тих, кого він вважає своїми ворогами, що забезпечить йому перемогу на виборах у своїх власній країні у 2018 р.», – пише Wall Street Journal. Адже, минулі вибори у Росії західні спостерігачі назвали нечесними, цю критику В. Путін назвав прихованою спробою його повалення. Таким чином, каже один з високопосадовців Білого дому, створюючи хаос на виборах у Європі, В. Путін має на меті відволікти увагу від президентських виборів у Росії у 2018 р., а тим самим уникнути критики.

«Злам і викид електронного листування з боку Росії – це спроба очорнити американську виборчу систему, зобразити її хаотичною, вразливою до маніпулювання, втручання, шахрайства, так що довіряти їй не можна», – цитує високопосадовця Білого дому WSJ.

Росія відкидає будь-які звинувачення у втручання у вибори за межами її кордонів і каже, що немає жодного відношення до хакерських атак на сервер Демпартії цього року.

***

7.11.2016

WikiLeaks опублікував 8 тис. листів Національного комітету Демпартії США

Ресурс WikiLeaks опублікував понад 8 тис. листів представників Національного комітету Демократичної партії США (LB.ua).

Про це повідомляють у Twitter організації.

Напередодні Д. Палмьєрі, представниця передвиборного штабу кандидата в президенти США від Демократичної партії Г. Клінтон, заявила, що листи, опубліковані WikiLeaks, радше за все, підроблені.

Сайт WikiLeaks уже не раз публікував листи представників передвиборного штабу Г. Клінтон і Національного комітету демократів.

Наприклад, 23 липня ресурс опублікував майже 20 тис. листів і понад 8 тис. документів Національного комітету Демпартії США. У результаті свою посаду покинула голова комітету: з листів стало відомо, що організація,

усупереч правилам, підтримувала протягом передвиборної кампанії Г. Клінтон і перешкоджала її суперникові по партії Б. Сандерсу.

У серпні The New York Times повідомляла, що метадата (інформація про дані) вкрадених із серверів партії та опублікованих на сайті WikiLeaks документів показала, що їх «пропускали» через безліч комп'ютерів, у тому числі й з російськомовними налаштуваннями.

Нагадаємо, що засновник WikiLeaks Д. Ассанж пообіцяв, що до кінця року оприлюднить близько мільйона документів, пов'язаних із виборчою кампанією у США.

***

10.11.2016

Вміст пошти В. Суркова збігається з інформацією, вилученою СБУ під час обшуків на Закарпатті

Вміст пошти помічника президента Росії В. Суркова збігається з інформацією, яку Служба безпеки України раніше вилучала під час обшуків у сепаратистів на Закарпатті (LB.ua).

Про це повідомляє РБК-Україна.

«Зміст деяких документів (з пошти В. Суркова. – Ред.) збігається з матеріалами, які були вилучені СБУ під час обшуків, пов'язаних із сепаратистськими рухами на Закарпатті», – йдеться у відповіді СБУ на інформаційний запит видання.

«Оприлюднений план забезпечення федерального статусу Закарпаття та деяких інших документів практично збігається з документами, вилученими в одного з організаторів сепаратизму в Закарпатській області», – сказано в повідомленні.

У Службі безпеки підкреслили, що результати перевірок і експертиз будуть оприлюднені після завершення відповідно до встановленого порядку.

***

9.11.2016

Обама раскритиковал Facebook за фейковые новости

Президент США Б. Обама раскритиковал Facebook за фейковые новости, сообщает Business Insider (InternetUA).

Глава государства выступал на акции в поддержку кандидата в президенты США от Демократической партии Х. Клинтон в Мичиганском университете.

Б. Обама, в частности, заявил о «сумасшедшем построении конспирологических теорий» в таких соцсетях, как Facebook. Как отметил президент, если снова и снова повторять откровенную ложь, если эта ложь есть в Facebook и других социальных сетях и если люди могут ее видеть, то они начнут в нее верить.

«И это создает пылевое облако нонсенса», – добавил Б. Обама.

Информация о фейковых новостных материалах в Facebook появилась, когда соцсеть уволила редакторов, отвечавших за раздел Trending. В Facebook заявили, что работают над улучшением фильтрации ложных и вводящих в заблуждение новостей.

***

13.11.2016

Facebook обвинили в победе Д. Трампа

Социальная сеть оказалась в центре внимания после объявления результатов президентских выборов в США (Marketing Media Review).

И хотя М. Цукерберг опроверг заявления о том, что его компания повлияла на выборы, другие в Facebook начали более пристально изучать роль сети в медиа-ландшафте, отмечает The New York Times. М. Цукерберг разместил длинный пост в сети, обрисовав роль компании в выборах, отметив, что «99 % того, что видят пользователи, является достоверными новостями. Есть только небольшое количество фейковых новостей и лжи». Как отмечает The New York Times, несколько топ-менеджеров компании начали задавать вопросы об ответственности сети. Выборы «разбудили» компанию, которая рассматривала себя в качестве чистой доски, где каждый может выражать свои взгляды. На прошлой неделе компания признала, что ей придется еще многое сделать в борьбе с дезинформацией. М. Цукерберг отметил, что Facebook запустил инициативу, позволив пользователям отмечать фейковые новости. Он также выразил несогласие с идеей о том, что компания является медиа бизнесом, отметив, что «новости и медиа – не главные вещи, которыми люди занимаются в Facebook. Поэтому для меня странно, когда нас называют медиакомпанией». Несмотря на заявления CEO Facebook, социальные медиа превратились в главный источник новостей, согласно данным исследования PEW. Отчет отметил, что 62 % американцев получают новости из социальных медиа. Facebook предпринимает попытки уменьшить поток дезинформации, но М. Цукерберг признает, что это непростая задача: некоторую информацию можно развенчать сразу же, с другими историями все гораздо сложнее. Хотя ряд ресурсов уже борется с онлайн-ложью и фейковыми новостями, которые Facebook может использовать в своей работе: например, Snopes и PolitiFact.

Зарубіжні спецслужби і технології «соціального контролю»

7.11.2016

В Германии началось расследование против М. Цукерберга и других топ-менеджеров Facebook

Прокуратура Мюнхена начала предварительное расследование в отношении основателя и главы соцсети Facebook М. Цукерберга и других топ-менеджеров компании, сообщает Der Spiegel (Телекритика).

По информации издания, кроме М. Цукерберга, прокуратура проверит и исполнительного директора Facebook Ш. Сэндберга, представителя соцсети в Европе Р. Аллена и его коллегу Е.-М. Киршзипер, которая работает в Берлине.

Основанием для проверки послужило заявление адвоката из Вюрцбурга Чань-йо Цзюня, который обвиняет руководство Facebook в том, что оно не предпринимает необходимые меры для борьбы с распространением запрещенной и оскорбительной информации.

***

8.11.2016
Польша обвинила Facebook в цензуре

Министр цифровых технологий Польши А. Стрежинская обвинила Facebook в цензуре после того, как доступ к профилям некоторых пользователей соцсети был приостановлен из-за использования ими символа Фаланги, сообщает ТАСС (Телекритика).

По ее словам, Facebook нарушил правило не использовать превентивную цензуру, которая является конституционной нормой и ограничить которую могут только юридические акты. Свод правил соцсети содержит много неточных формулировок, которые можно интерпретировать по-разному, поэтому польский чиновник заявила о необходимости создать быстрый и эффективный способ для подачи апелляций в отношении решений Facebook, касающихся контента.

***

7.11.2016
Китай принял новый закон о кибербезопасности

Китайское правительство одобрило новый закон о кибербезопасности, вызвавший множество споров, передает Bloomberg (IGate).

Согласно этому решению, правоохранительные органы получат возможность замораживать счета иностранных организаций и граждан при подозрении их в саботаже информационной безопасности страны. Кроме того, при проведении расследования иностранцы обязаны будут предоставить контролирующим органам полный доступ к своим данным.

Законопроект также предусматривает сертификацию любого компьютерного оборудования и обязательное хранение персональных данных местных пользователей на территории Китая. По мнению аналитиков, ввод таких норм даст еще одно заметное преимущество китайским компаниям перед иностранными конкурентами на технологическом рынке Поднебесной.

«Это шаг назад для Китая. Конечно, руководство страны должно делать шаги для обеспечения безопасности цифровых систем в стране, однако такой закон не поможет добиться этой цели. Вместо этого он возводит новые барьеры для инноваций и торговли», – заявил глава Американской торговой палаты в Китае Д. Зиммерман.

Отметим, что закон вступит в силу в июне следующего года.

***

4.11.2016

Спецслужби Канади незаконно зберігали дані громадян

Канадська служба безпеки і розвідки (КСБР) незаконно зберігала персональні дані громадян протягом останніх десяти років, повідомляє телеканал CBC (Корреспондент.net).

Ідеться про дані, які збиралися електронним способом.

У постанові судді Федерального суду Канади С. Ноела, оприлюдненій 3 листопада, зазначено, що КСБР порушила свої обов'язки щодо інформування суду про таку діяльність.

Зокрема, спецслужба не мала права стільки часу зберігати персональні дані канадців, якщо вони не були безпосередньо пов'язані із загрозою національній безпеці.

Глава КСБР М. Куломб уже заявив, що його відомство підкориться рішенню Федерального суду і «вживатиме негайних заходів».

За наявними даними, з 2006 р. Канадська служба безпеки і розвідки почала використовувати спеціальну програму зі збору персональних даних, яка також відома як Аналітичний центр зі збору оперативних даних. Вона дає змогу збирати інформацію про об'єкт стеження спецслужб.

Як повідомляв Корреспондент.net, директор ФБР Дж. Комі звернувся до американського конгресу із закликом про необхідність надання спецслужбам доступу до персональних даних користувачів засобів зв'язку.

***

10.11.2016

У Росії заблокують LinkedIn

Мосміськсуд визнав законним блокування соціальної мережі LinkedIn на території Росії у зв'язку з порушенням закону про локалізацію персональних даних (LB.ua).

Про це повідомляє агентство «Интерфакс».

Раніше Таганський суд Москви ухвалив рішення заблокувати ресурс на вимогу Роскомнагляду. Соцмережа подавала апеляційну скаргу, але Мосміськсуд її не задовольнив.

У Роскомнагляді вважають, що LinkedIn порушує Закон «Про персональні дані», оскільки не перенесла серверів у Росію, а також збирає та

передає інформацію про громадян, які не є користувачами мережі, без їхньої згоди.

У LinkedIn Corporation вважають, що соцмережа не зобов'язана виконувати вимоги російського законодавства. «Користувачі фактично пребувають віртуально за межами РФ і там подають свої персональні дані», – заявила представник відповідача. За словами представників компанії, вона не порушує прав своїх користувачів, оскільки вони добровільно надають свої персональні дані, погоджуючись з умовами їхнього використання.

Роскомнагляд заблокує LinkedIn відразу після отримання судового рішення, повідомив прес-секретар Роскомнагляду В. Ампелонський. Він припустив, що це може статися наступного тижня.

Соціальна мережа LinkedIn призначена для пошуку роботи та обміну діловими контактами. У ній зареєстровано понад 400 млн осіб.

Як повідомляли в червні, Microsoft купує LinkedIn за 26,2 млрд дол. Угода буде завершена до кінця 2016 р.

***

14.11.2016
В Украине ухудшается ситуация со свободой Интернета

Украина опустилась до 38 места в ежегодном рейтинге свободы Интернета, составленном международной правозащитной организацией Freedom House, передает УНН со ссылкой на ее официальный сайт (InternetUA).

«Хотя Украина и опустилась до 38 места в рейтинге, она остается "частично свободной"», – говорится в сообщении.

Организация отмечает, что в Украине не блокируются соцсети и информационные приложения, однако есть случаи ограничения доступа к информации и арестов блогеров и активистов.

Правозащитники отметили, что рынок Интернета в Украине растет, однако он в то же время страдает от тяжелой экономической ситуации, аннексии Крыма и кризиса на Востоке, где, в частности, произошло повреждение необходимой инфраструктуры.

В организации отметили, что в отличие от традиционных медиа, доступ к онлайн-контенту на подконтрольной украинскому правительству территории не подвергся значительному влиянию оккупации Россией Крыма и ее участия в войне на Востоке, но в то же время, десятки украинских сайтов подверглись цензуре на подконтрольном боевикам Донбассе.

Freedom House утверждает, что чиновники все чаще пытались влиять на соцсети с попытками бороться с антиукраинской риторикой, сажать пользователей за сепаратистские или экстремистские высказывания.

В организации также добавили, что в целом физическое давление на комментаторов в Интернете ослабло, однако подчеркнули убийство «известного журналиста» в июле, очевидно, имея в виду П. Шеремета.

Проблема захисту даних. DDOS та вірусні атаки

1.11.2016
Ультразвук откроет хакерам доступ к миллионам устройств

Технология, работающая на основе ультразвука, может предоставить хакерам новую возможность компрометации миллионов устройств. Речь идет о распространенной технологии ультразвукового слежения за устройствами (uXDT) – «святом Граале» для маркетинговых компаний, использующих ее для отслеживания просмотренной пользователем рекламы и сбора информации о нем (InternetUA).

Технология uXDT уже сейчас вызывает опасения экспертов. В марте текущего года Федеральная торговая комиссия США разослала предупреждения 12 разработчикам мобильных приложений, встраивающих в свои программы модуль для аудиомониторинга SilverPush. По мнению комиссии, действия разработчиков компрометируют конфиденциальность данных пользователей.

По словам специалистов Университетского колледжа Лондона (University College London), отсутствие резонанса и опций, позволяющих деактивировать аудиомониторинг в приложениях на базе uXDT, представляют значительную угрозу. Подобные программы всегда активно отслеживают ультразвуковые сигналы, даже если приложение не используется. Это создает дополнительный «черный ход» для хакеров и превращает приложение в удобный инструмент. К примеру, злоумышленники могут записывать разговоры или определять набираемый на клавиатуре текст.

Риск, связанный с ультразвуковыми технологиями, вызывает серьезное беспокойство у экспертов. Прежде всего, в связи с тем, что такие решения являются главными претендентами для обеспечения связи между устройствами в сфере «Интернета вещей», отмечает издание Fortune. В настоящее время не существует стандартов защиты ультразвуковых датчиков и сигналов. Как надеются эксперты из Университетского колледжа Лондона, проведенное ими исследование стимулирует соответствующие структуры к разработке подобных стандартов.

***

31.10.2016
Число вредоносных ссылок в выдаче поисковиков возросло в шесть раз

Несмотря на все усилия Google и других IT-компаний по исключению вредоносных результатов из выдачи поисковых систем, число подобных ссылок

значительно растет. За последние три года их количество увеличилось в шесть раз. Таковы результаты исследования, проведенного независимой организацией AV-TEST.org (InternetUA).

В рамках исследования специалисты проверяли ссылки на сайты, отображающиеся в поисковой выдаче систем Google, Bing, Yandex и Faroo. Кроме того, за последние два года было проанализировано более 515 млн апдейтов Twitter на предмет наличия вредоносных ссылок.

В прошлом году AV-TEST.org проверила 80 млн сайтов и обнаружила 18 280 вредоносных интернет-страниц. В этом году специалисты выявили уже 29 632 инфицированные страницы. Анализ проводился без использования сервиса Google Safe Browsing, предназначенного для обнаружения небезопасных web-ресурсов. Для сравнения, в 2013 г. специалисты выявили только 5060 вредоносных страниц.

Для составления более точной картины эксперты посетили вредоносные страницы, используя Google Safe Browsing. Результаты оказались неутешительными – из 29 632 случаев система выдала соответствующие предупреждения только в 1337.

По мнению эксперта AV-TEST.org М. Моргенстерна (Maik Morgenstern), причина такого расхождения может заключаться в динамическом контенте, размещаемом на сайтах.

«Вполне возможно, что в момент анализа на сайте размещались вредоносные рекламные объявления, которые меняются каждый раз, когда посетитель заходит на ресурс. Веб-сайт может показывать разный контент в случайном порядке или в зависимости от местоположения пользователя. Кроме того, мне не известно, с каким интервалом Google/Bing проводят сканирование сайтов на предмет вредоносного ПО. Всегда существуют периоды, когда вредоносные программы могут находиться на сайте без ведома Google/Bing. Также не исключено, что контент, помеченный нами как вредоносный, Google/Bing не считают таковым», – пояснил М. Моргенстерн.

***

2.11.2016

Microsoft: Росіяни зламали поштові сервери США через вразливість Windows

Компанія Microsoft заявила, що пов’язане з Росією хакерське угруповання, яке раніше звинувачували у зломі поштових серверів Демократичної партії США, відповідальне за атаки на операційну систему Windows (Espreso.tv).

Про це повідомляє BBC.

За інформацією компанії, мова йде про невеликі хакерські атаки з використанням адресних фішингових листів, за якими стоїть угрупування Strontium, також відоме як Fancy Bear і APT 28.

Microsoft також повідомляє, що 8 листопада буде представлена програма, яка покликана захистити Windows від подібних атак.

Про уразливість Windows у кінці жовтня повідомив головний конкурент Microsoft, компанія Google. У повідомленні Microsoft зазначається, що такий крок з боку Google піддав ризику клієнтів компанії.

Деякі фахівці з кібербезпеки стверджують, що угруповання Strontium працює на російську військову розвідку і відповідальне за злом електронних листів Демократичної партії.

***

8.11.2016

Широкое использование «больших данных» для борьбы с преступностью ставит под угрозу гражданские свободы

Внедрение новых технологий – в частности, быстрого анализа данных и обмена данными – помогает полиции работать эффективнее и позволяет прогнозировать преступления. Некоторые эксперты утверждают, что это способствовало общему снижению преступности в последние годы (Центр информационной безопасности).

Однако широкое применение таких технологий, в частности, полицией, также поднимает вопросы гражданских свобод, пишет ресурс AllGov.

Американский союз гражданских свобод предупреждает об опасности использования полицией «больших данных», ссылаясь на отчет Департамента полиции Чикаго. Сотрудники департамента использовали компьютерный анализ для составления списка потенциальных правонарушителей и преступников – так называемого «горячего списка» (heat list), при этом несправедливо и незаконно ассоциируя с криминальным поведением невиновных людей, не совершавших никаких преступлений. Даже компании, которые специализируются на таких работах, предупреждают о рисках несоблюдения гражданских прав.

«Мы скоро будем жить в мире, где каждый мусорный бак имеет идентификатор. Даже я шокирован тем, насколько исчерпывающую информацию продают поставщики данных», – сказал К. Боуман (Courtney Bowman) из Palantir Technologies, компании в Пало-Альто, штат Калифорния, которая продает специализированные программы для анализа данных. Он читал лекции о рисках «прогностической полиции» и говорил о необходимости доказывать в суде, что прогностические модели следуют понятной логике и не усиливают стереотипов.

Компания Palantir построила свой бизнес, предлагая такие продукты, как карты социальных сетей экстремистов-организаторов взрывов и преступников, занимающихся отмыванием денег для нужд террористов; эти программы помогали прокладывать оптимальные маршруты для машин, позволяющие избежать самодельных взрывных устройств.

Аналогичные методы глубокого анализа больших массивов данных Palantir использовала в Новом Орлеане для выявления лиц, причастных к убийствам. Сотрудники правоохранительных ведомств вокруг Солт-Лейк-Сити использовали продукты Palantir и доступ к 40 000 арестных фотографий, 52 0000 историй болезни и информации о дорогах и аэропортах, чтобы составить карты предполагаемых преступных сетей.

Но есть опасения по поводу того, что технологии анализа данных, применяемые военными, могут представлять опасность для гражданских свобод – даже среди компаний, которые зарабатывают на этих технологиях.

«Это, безусловно, создает проблемы для преступников попроще, но это же создает многочисленных, так сказать, “маленьких помощников большого брата”, – сказал К. Боуман. «На сегодняшний день», – добавил он, – «проблема изобилия данных большей частью состоит в том, что большинство полицейских не очень хорошо в этом разбираются».

***

8.11.2016

Россия – наиболее атакуемая банкерами страна

Эксперты «Лаборатории Касперского» обнародовали данные по угрозам за III квартал. Данные для анализа были собраны с помощью антивирусной сети Kaspersky Security Network с компьютеров 213 стран и территорий мира. В III квартале 2016 г. «Лабораторией Касперского» было обнаружено 1 520 931 вредоносных установочных пакетов – в 2,3 раза меньше, чем в предыдущем квартале. Наиболее часто детектируемые объекты – это программы типа RiskTool, являющиеся легальными, но потенциально опасные для пользователей. Их доля за квартал увеличилась с 45,1 до 55,8 %. В то же время доля остальных программ уменьшилась (Центр информационной безопасности).

Первое место в рейтинге мобильных угроз занимает вердикт DangerousObject.Multi.Generic (78,46 %) – то есть, самые новые вредоносные программы, детектируемые при помощи облачных технологий.

Среди наиболее заметных тенденций квартала – бешеная популярность игры Pokemon GO, которой ожидаемо воспользовались злоумышленники. Зачастую они внедряли вредоносный код в оригинальную игру и распространяли ее через сторонние магазины. Известно о случае, когда киберпреступники разместили гид для игры в официальном магазине Google Play. На самом деле приложение оказалось рекламным троянцем. Еще одна вариация вредоносного приложения, замаскированная под эквалайзер, была скачана с Google Play от 100 тыс. до 500 тыс. раз.

Самым популярным мобильным троянцем в III квартале 2016 г. стал Trojan-Banker.AndroidOS.Svpeng.q, ставший популярным благодаря рекламе в Google AdSense. За квартал количество атакованных им пользователей возросло

практически в восемь раз. Абсолютное большинство его жертв (более 97 %) – из России.

За квартал «Лаборатория» обнаружила 37 150 установочных пакетов мобильных троянцев-вымогателей. В III квартале их доля заметно снизилась – в 2,4 раза, с 5,72 до 2,37 %. Эксперты объясняют это снижением активности популярного вымогателя Fusob. Он был очень активен в I и II кварталах, но теперь количество атакованных пользователей уменьшается. Тем не менее, это все еще самый популярный троянец-вымогатель. С ним столкнулись более 53 % пользователей, атакованных мобильными вымогателями. Наиболее подвержены атакам мобильных вымогателей такие страны, как Канада, США и Казахстан (0,95; 0,94 и 0,71 % атакованных пользователей, соответственно).

Больше всех страдают от мобильных зловредов Бангладеш – в нем практически 36 % пользователей хотя бы раз в течение квартала сталкивались с мобильными зловредами. В тройке лидеров также Непал (31,54 %) и Иран (31,38 %). Россия с показателем 12,1 % заняла 24-е место. Реже всего с мобильными угрозами сталкиваются Австрия (3,3 %), Хорватия (3,1 %) и Япония (1,7 %).

Доля мобильных банкеров слегка увеличилась с 1,88 до 1,98 %. Количество мобильных банкеров за квартал незначительно возросло – в 1,1 раза до 30 167 установочных пакетов. В III квартале 2016 г. в этом рейтинге первое место среди жертв мобильных банкеров заняла Россия (3,12 %), где по сравнению со II кварталом практически удвоилась доля пользователей, атакованных мобильными банковскими троянцами. В тройку «лидеров» по доле пользователей, атакованных мобильными банкерами вошли Австралия и Украина (1,42 и 0,95 %), соответственно.

Также в III квартале исследователи доложили об угасании популярного эксплойт-пака Neutrino; ранее с рынка также ушли Angler и Nuclear. Освободившуюся нишу занял RIG, также активен Magnitude. Наиболее эксплуатируемыми компонентами по-прежнему являются эксплойты для различных браузеров и их компонентов (45 %), хотя их доля уменьшилась на 3 %. За ними с большим отрывом следуют эксплойты к уязвимостям для ОС Android (19 %), потерявшие в III квартале 5 %. Замыкают тройку лидеров эксплойты для пакета Microsoft Office – их доля, наоборот, возросла за квартал с 14 до 16 %. Эксплойты Adobe Flash Player все еще популярны среди хакеров, притом доля за квартал увеличилась более чем в два раза – с 6 до 13 %.

По данным «Лаборатории», в III квартале банкерами были атакованы компьютеры 1 198 264 пользователей – на 5,8 % выше, чем в предыдущем квартале. Это связано преимущественно с сезоном отпусков, так как количество онлайн-платежей в этот период возрастает. С большим отрывом в рейтинге стран, подверженных атакам банковских троянцев, снова лидирует Россия (4,2 % атакованных пользователей), за ней следует Шри-Ланка (3,48 %) и Бразилия (2,86 %).

Наиболее активный банкер ZeuS (Zbot), атаковавший 34,58 % пользователей во всем мире, часто используется в атаках против россиян, так

как разработчики зловреда, скорее всего, также из России – они понимают менталитет жертв и устройство российских инструментов онлайн-банкинга. Также в России по-прежнему распространен банковский троянец Gozi, который находится на четвертой строчке рейтинга банкеров. На втором и третьем месте расположились соответственно QHost (9,48 %) и Fsysna (9,47 %), бесчинствующий в этом квартале в Шри-Ланке.

Опасной угрозой уже несколько кварталов подряд становятся шифровальщики. В III квартале 2016 г. специалисты «Лаборатории» обнаружили 21 новое семейство шифровальщиков и 32 091 новую модификацию. Число новых семейств шифровальщиков чуть меньше, чем аналогичный показатель II квартала (25 семейств), то число новых модификаций – в 3,5 раза больше, чем было обнаружено в предыдущем квартале. В III квартале, по данным «Лаборатории», шифровальщиками было атаковано 821 865 компьютеров. По сравнению с предыдущим кварталом, число атакованных пользователей возросло примерно в 2,6 раз.

В списке стран, страдающих от атак вымогателей-шифровальщиков, уже два квартала подряд лидирует Япония (4,83 % атакованных пользователей), за ней следуют Хорватия (3,71 %) и Корея (3,36 %).

Наиболее распространенными семействами шифровальщиков стали CTB-Locker (28,34 %), Locky (9,6 %) и CryptXXX (8,95 %). Шифровальщик TeslaCrypt, несмотря на то, что его авторы прекратили разработку зловреда и опубликовали свой мастер-ключ еще в мае, продолжает присутствовать в рейтинге (хотя его распространенность упала в этом квартале в 5,8 раз). Эксперты также отмечают рост осведомленности пользователей о программах-вымогателях, также на проблему обращают пристальное внимание представители правоохранительных органов – совместный проект ИБ-компаний и правоохранителей Европы No More Ransom уже помог тысячам пользователей расшифровать свои файлы без выкупа.

В III квартале веб-антивирус «Касперского» обнаружил 12 657 673 уникальных вредоносных объектов и 45 169 524 уникальных вредоносных ссылок. Всего в III квартале было отражено 171 802 109 атак из 190 странах мира. На 10 стран мира пришлось 83 % уведомлений о заблокированных веб-атаках. В среднем в течение квартала 20,2 % компьютеров пользователей интернета в мире хоть раз подвергались атаке вредоносного ПО.

Среди государств, чаще всего являющихся источником атаки, по-прежнему лидирует США (33,51 %), второе место заняла Германия (10,5 %), а третье – Нидерланды (9,4 %). Россия опустилась со второго места на четвертое (9 %). Наиболее атакуемыми странами стали Словения (30,02 % атакованных пользователей), Болгария (29,49 %) и Армения (29,30 %). В тройку самых безопасных для серфинга в Интернете стран вошли Хорватия (14,21 %), Великобритания (14,19 %) и Сингапур (13,78 %).

Также «Лаборатория Касперского» анализирует количество локальных угроз, детектируемых файловым антивирусом. По данным компании, в III

квартале было зафиксировано 116 469 744 вредоносных и потенциально нежелательных объектов.

Локальные угрозы наиболее распространены во Вьетнаме (52,07 % атакованных пользователей), Афганистане (52 %) и Йемене (51,32 %). В России локальные угрозы обнаружены на 25,93 % компьтерах. Безопаснее всего в том отношении такие страны, как США (8,08 %), Дания (6,53 %) и Япония (6,53 %). В среднем в мире хотя бы один раз в течение III квартала локальные угрозы класса были зафиксированы на 22,9 % компьютеров пользователей.

***

8.11.2016

Ресурс WikiLeaks подвергся масштабной DDoS-атаке

Официальный сайт организации WikiLeaks подвергся масштабной DDoS-атаке, из-за которой ресурс на некоторое время приостановил работу. Инцидент произошел сразу после публикации очередной порции документов, похищенных в результате взлома компьютерной сети Демократической партии США (Центр информационной безопасности).

В настоящее время неизвестно, кто стоит за DDoS-атакой на WikiLeaks. Специалисты организации проводят расследование инцидента. На момент публикации новости работа сайта уже была восстановлена.

***

2.11.2016

Более половины приложений онлайн-шопинга собирают персональную информацию

Более половины из 60 крупнейших Android-приложений онлайн-шопинга собирают персональную информацию пользователей с помощью трекеров (ITnews).

Таковы результаты исследования Opera, полученные во время анализа Android-приложением Opera Max возможных рисков для персональных данных пользователей при покупках онлайн. Другое исследование показывает, что персональная информация, такая как имена пользователей, email-адреса, местоположение, поисковые запросы и телефонные номера зачастую предоставляется третьим сторонам с помощью трекеров.

Среди сервисов, наиболее активно собирающих пользовательскую информацию, выделяются такие популярные приложения для онлайн-шопинга, как Amazon, BestBuy, JC Penney, Newegg и Яндекс.Маркет, которые посылают больше всего трекеров.

Исследование также показывает, что 96 % приложений для онлайн-шопинга не используют полное шифрование для связи с серверами. Это, в свою очередь, влечет за собой определенные риски для пользователей.

Персональная информация предоставляется третьим сторонам посредством трекеров в приложениях или же с помощью незашифрованных http-соединений при использовании мобильных сетей операторов. Конфиденциальная информация, такая как номера банковских счетов и другая финансовая информация, сохраняемая в личных кабинетах онлайн-ритейлеров или приложениях онлайн-шопинга, может быть перехвачена и прочитана злоумышленниками через публичные или незащищенные Wi-Fi сети.

«Большинство людей вряд ли сообщили бы детали своей кредитной карты или же их полное имя сотрудникам обычного магазина, куда они ходят за покупками. Но в случае с мобильными приложениями люди редко бывают осведомлены о том, что такая информация может быть доступна другим. Вот почему мы внедрили режим конфиденциальности в Opera Max. Мы хотим, чтобы наши пользователи знали, какие из их приложений возможно делятся информацией с третьей стороной», – отметил С. Лосев, руководитель разработки Opera Max.

Сегодня всем пользователям Opera Max становится доступным новый режим конфиденциальности. С его помощью можно в режиме реального времени видеть, какие приложения посылают высокорискованные запросы, ставя под угрозу приватность пользователей. Как только режим конфиденциальности в Opera Max активирован, он также начинает шифровать трафик всех приложений и блокирует почти все виды трекеров, чтобы максимально обезопасить пользователя.

«Когда вы узнаете, сколько трекеров и запросов посылают ваши приложения, вы, скорее всего, захотите защитить и зашифровать весь трафик ваших приложений с помощью Opera Max. Просто посмотрите на поведение того или иного приложения и примите решение», – добавил С. Лосев.

***

4.11.2016

Мошенники нашли новый способ обмануть пользователей Chrome

Кибермошенники взяли на вооружение ошибку в Chrome, обнаруженную еще в июле 2014 г., однако до сих пор неисправленную (Центр информационной безопасности).

Проблема была обнаружена в Chrome 35 и затрагивает history.pushState() – метод, представленный с HTML5 и позволяющий разработчикам добавлять URL-адреса в историю сеансов браузера. Добавление большого количества адресов (тысяч или даже миллионов) не вызовет аварийное завершение работы браузера, однако может привести к его «зависанию». Поскольку Chrome будет использовать большую часть доступной памяти устройства и ресурсов процессора, работа операционной системы существенно замедлится.

Google известно о проблеме, однако эксперты компании классифицировали уязвимость как низкого уровня опасности и отложили релиз патча на неопределенное время. Как сообщают эксперты Malwarebytes, спустя

более двух лет после обнаружения ошибки мошенники создали так называемую «команду техподдержки», использующую уязвимость в своих целях. После «зависания» браузера жертвы на экране устройства отображается фальшивое уведомление с указанием номера телефона «команды техподдержки», готовой оказать помощь в починке компьютера.

В зависимости от характеристик компьютера, жертва не всегда может запустить менеджер задач и завершить все процессы браузера. В таком случае поможет «холодная» перезагрузка системы.

***

4.11.2016

Базиленко Анна

Хакери виклали в мережу нову порцію даних з пошти помічника В. Путіна

Група хакерів «КіберХунта», FalconsFlame, Trinity та RUH8 оприлюднили черговий масив даних, отриманих, за їхніми словами, з приймальні апарату помічника президента Росії В. Суркова (Watcher).

Новий злив інформації отримав умовну назву SurkovLeaks (part 2) і в основному присвячений поштовій скриньці pochta_mg@mail.ru. У дампі міститься 336 вхідних і 87 вихідних повідомлень.

Міжнародне розвідувальне співтовариство InformNapalm провело верифікацію опублікованих даних і прийшло до висновку, що листи є справжніми, йдеться на сайті «КіберХунти». Завдяки аналізу отриманої інформації вдалося встановити і конкретного оператора імейлу – ним виявилась радник Суркова М. Виноградова. «Через вказану поштову скриньку проходили доволі цікаві і деколи навіть умовно “секретні” доноси, списки та звіти, хоча основна частина матеріалів поштового дампу є рутинною і не дуже інформативною», – додають у «КіберХунті».

Нові електронні листи у разі їхньої автентичності деталізують рівень втручання Кремля у внутрішні справи України, зокрема його роль у формуванні сепаратистських угруповань на Донбасі в 2014 р. Також у новому масиві даних містяться архіви за 2015–2016 рр.

Листи містять плани, які показують, як соратники В. Суркова розробляли сценарій щодо дестабілізації ситуації в Харківській області, досліджували українських політиків, намагаючись використати політичні розбіжності в Україні, і допомогли встановити керівництво сепаратистських груп на окремих територіях Донецької та Луганської областей.

З повним масивом даних можна ознайомитись на сайті «КіберХунти».

***

7.11.2016

Элон Маск: искусственный интеллект сможет положить Интернет, дайте только время

Интернет становится местом ожесточенной резни, и Э. Маск говорит, что продвинутый искусственный интеллект может усугубить эту резню еще больше. В Twitter Э. Маска появилось сообщение, что системы, которые поддерживают Интернет в работе, уязвимы к обычным грубым компьютерным атакам – а в этой области искусственный интеллект уже преуспел (InternetUA).

21 октября неизвестная группа хакеров отключила часть Интернета в Соединенных Штатах Америки и Европе массивной DoS-атакой. Хакеры использовали массивный ботнет – сеть связанных компьютеров, способных выполнять согласованные функции – простых устройств «Интернета вещей», чтобы перегрузить сервера Dyn Systems, которая обеспечивает DNS-обслуживание гигантскому числу сайтов, включая Spotify, Twitter, Netflix и Reddit. Считается, что атаку выполнила группа людей или один человек, которая подключила и скоординировала ботнет. Но в будущем, как говорит Э. Маск, массивные DDoS-атаки могут проводиться силами ИИ и сеять хаос в инфраструктуре, которая поддерживает нас на цифровых ногах.

29 октября Economist опубликовал статью под названием «Кто-то учится ронять Интернет», в которой изучил феномен растущего числа DDoS-атак и почему мы так плохо с ними справляемся. Э. Маск ответил на статью и добавил пугающий прогноз: однажды этим «кем-то» будет не человек, а продвинутый ИИ.

С этого момента все становится сложнее. На сегодняшний день цифровые атаки вроде тех, что используют хакеры для выведения из строя веб-сайтов, как правило, управляются людьми. Но по мере того, как ИИ становится все лучше и лучше, хакеры начнут использовать его для оптимизации атак на инфраструктуру Интернета, которая «особенно уязвима» для так называемого «алгоритма градиентного спуска». Градиентный спуск – это математический процесс, который берет сложную функцию и находит наиболее оптимальное решение. ИИ прекрасно справляется с градиентным спуском, что делает его особенно эффективным в возможном деле организации массивных DDoS-атак с использованием плохо защищенных устройств «Интернета вещей».

Но если обе стороны (хакеры и кибербезопасность) будут использовать продвинутый ИИ, Э. Маск говорит, что это может привести к разборкам ИИ против ИИ на поле битвы.

Э. Маск открыто выступает против нерегулируемого развития искусственного интеллекта. Он не против этой технологии в целом, но считает, что попытки сделать умных роботов должны быть открытыми и прозрачными, чтобы не допустить распространения гоняющихся за прибылью корпораций, которые развяжут руки ИИ. Появление разумных компьютеров неизбежно, но нужно убедиться, что они будут безопасны.

***

7.11.2016

«Левые» приложения для смартфонов крадут карточные данные украинцев

Страсть пользователей к пиратскому софту позволяет мошенникам с легкостью получать личную информацию (InternetUA).

Украинцы все чаще выходят в Интернет с мобильных, а не стационарных устройств. Соответственно, изменился и набор приложений, и способы их установки – широкий выбор бесплатного ПО в мобильных магазинах AppStore и Google Play делает ненужным скачивание пиратского программного обеспечения. При этом скачивать и устанавливать «левое» ПО стало намного опаснее.

«Пользователи начали осознавать риски “подцепить вирус”, а также бояться отвечать перед законом за свои действия. Кроме того, вендоры начали предлагать интересные модели распространения: freemium (урезанная версия программы, но с неплохим функционалом), по подписке (Adobe CC suite) и т. д.», – отметил руководитель группы технологического позиционирования Kaspersky Lab О. Горобец.

Чаще всего украинцы скачивают в сети именно медийный контент – видео, музыку. ПО пользуется намного меньшим спросом. Самые ходовые – игры, а также специфические, не имеющие хороших бесплатных аналогов программы, являющиеся де-факто индустриальным стандартом: операционные системы, офисные пакеты, пакеты креативного софта (графика, дизайн).

Хоть в Украине постепенно и начинает формироваться культура пользования Интернетом в части пользования лицензионным либо же бесплатным ПО, тем не менее, увлеченность наших соотечественников пиратским контентом закрепило за страной звание самой «пиратской» – больше 80 % программ у нас имеет нелицензионное происхождение. И за последние несколько лет эта цифра изменилась уменьшилась очень незначительно.

Как результат – Украину объявили одним из самых злостных нарушителей авторского права в мире и снова занесли в злосчастный «Список 301» стран-нарушителей интеллектуальной собственности со статусом Приоритетного иностранного государства.

И взламывают, конечно же, самые скачиваемые программы. Все это крайне негативно влияет на имидж и репутацию нашей страны и замедляет ее интеграцию в цивилизованный западный мир, считают эксперты. Помимо этого, использование нелегального ПО несет целый ряд рисков для конечных потребителей.

«В первую очередь, это угроза кражи личных данных, неавторизованные операции с банковскими карточками, взломы почтового ящика, учетных записей в соцсетях, повреждение и сбои в работе компьютера и многое другое. Все эти проблемы вызваны заражениями вредоносными вирусами и/или кибератаками. Причины кроются в устаревшем ПО, нерегулярных обновлений систем безопасности или, что чаще всего, в использовании пиратских копий

программ», – отметила директор департамента по защите интеллектуальной собственности «Майкрософт Украина» Е. Дмитриева.

Кроме всех этих проблем, никто не отменял и законодательных норм – использование пиратского софта нелегально и влечет за собой уголовную ответственность.

На уровень пиратства в нашей стране оказывают влияние два основных процесса: с одной стороны, украинцы стали покупать больше лицензионного программного обеспечения. Но с другой – экономическая ситуация в Украине сейчас нелегкая, что, увы, приводит к противоположной тенденции.

«Однако мы продолжаем замечать положительные изменения в менталитете пользователей. Во многих случаях люди, скорее, просто не купят то, что купили бы раньше. Они будут искать бесплатные аналоги, а не пытаться добыть пиратское ПО, несущее неизвестные опасности. А серьезный бизнес уже давно не рассматривает использование контрафактного ПО», – заметил нам О. Горобец.

Украинская киберполиция сейчас проводит спецоперацию «Пираты» и уже в октябре силовые органы накрыли пару онлайн-кинотеатров и столько же торрент-трекеров. Во время операции серверы компании были изъяты и организаторам теперь светят реальные сроки.

***

7.11.2016

4 факти, які потрібно знати про «темний» Інтернет

Поняття «темного» Інтернету поширилось у профільних IT-виданнях, серед спеціалістів з онлайн-безпеки увійшло до лексикону рядових користувачів. Мало хто з останніх зможе чітко пояснити, в чому полягає різниця між «світлою» і «темною» мережею. Так само не всі знають різницю між даркнетом і «глибоким» вебом – поширена точка зору, що ці поняття є тотожними. Якщо навіть поліцейські вже орієнтуються у «темному» Інтернеті, настав час і нам розібратись, що означає це поняття. Пропонуємо вам короткий огляд головних рис «темного» Інтернету (InternetUA).

Теорія

Даркнет об’єднує сайти, які дають змогу користувачу залишатись повністю анонімним. Щоби потрапити на такі платформи, потрібно встановити спеціальне програмне забезпеченння. Пошук Google не індексує «темні» сторінки, тож випадково «перейти на темний бік» практично неможливо. Анонімність об’єднує всі платформи та сервіси даркнету, а цілі користувачів можуть бути самими різними: від організації спротиву тоталітарному режиму, донесення про корупцію чи обміну криптовалютами – до торгівлі зброєю та наркотиками.

«Темний», але не «глибокий»

«Темний» Інтернет відрізняється від «глибокого». Останній містить у собі онлайн-контент, який не індексується пошуковими інструментами. Навіть вміст

поштової скриньки належить до «глибокого» вебу, адже, який би пошуковий запит я не вводила в Google, він нізащо не видасть мені посилання на лист у чийомусь gmail. Те саме стосується сайтів, які надають платний доступ до інформації – неможливо нагуглити повний текст платної статті з The New York Times. Зорієнтуватись у поняттях нескладно, але ЗМІ сприяли плутанині в термінах, коли висвітлювали справу Silk Road і судовий процес над Р. Ульбріхтом. Тож просто варто пам'ятати, що поняття відрізняються.

Як потрапити в даркнет

Вхід у «темряву» можливий через спеціальні інструменти, найбільш популярний з яких – браузер Tor. Він базується на алгоритмах Mozilla і переоснащений для анонімного користування. Через цей браузер користувач підключається до Tor-мережі і отримує доступ до даркнету. Ще одним популярним сервісом є I2P.

Захищена мережа Tor застосовує множинні перенаправлення користувача для забезпечення його анонімності. Замість того, щоб одразу під'єднати користувацький пристрій до потрібного ресурсу, Tor «блукає» кількома серверами та шифрує трафік на кожному етапі. Недарма емблемою програми обрана цибулина – на запит користувача нашаровуються нові й нові точки підключення. Кінець кінцем, трафік від вашого комп'ютера до потрібного сайту виглядає настільки заплутаним, що виключає можливість відстеження.

Наслідки користування

Теоретично, анонімна активність в Інтернеті може викликати підозру правоохоронних органів. Якщо за певних умов поліція з'ясує, що ви користувались Tor, скоріше за все, поцікавиться, що саме ви там робили. З іншого боку, прагнення анонімності в Мережі саме по собі не підтверджує, що ви порушували чинні закони в той чи інший спосіб. Інтернет і будь-яка програма – це лише інструменти, а кожен громадянин вирішує, для чого їх використовувати. Наприклад, Tor може допомогти в уникненні цензури. Навіть Facebook має спеціальну платформу для анонімного користування, через яку спілкуються громадські активісти, захисники прав людини.

***

8.11.2016

Банковский троян Svpeng атакует российских пользователей Android Chrome

Специалисты «Лаборатории Касперского» обнаружили вредоносную кампанию по распространению опасного банковского Android-трояна Svpeng. Для этой цели злоумышленники используют рекламный сервис Google AdSense (Центр информационной безопасности).

Первые случаи инфицирования были зафиксированы в августе нынешнего года. Как тогда обнаружили эксперты, при просмотре некоторых новостных сайтов, использующих AdSense для показа рекламы, на Android-устройство пользователя автоматически загружался банковский троян.

Подобное поведение вызвало интерес у исследователей, поскольку обычно при загрузке приложений браузер уведомляет пользователя о потенциально опасных программах и позволяет выбирать, сохранить файл или нет.

По данным ЛК, за два месяца жертвами вредоноса стали примерно 318 тыс. пользователей из России и СНГ. При показе вредоносной рекламы на SD-карту устройства загружался APK-файл, содержащий новую версию Svpeng - Svpeng.q.

Перехватив трафик с атакуемого устройства, эксперты выяснили, что в ответ на HTTP-запрос с C&C-сервера злоумышленников загружается скрипт JavaScript, используемый для показа вредоносного рекламного сообщения. Этот скрипт содержит обфусцированный код, включающий APK-файл под видом зашифрованного массива байт. Помимо различных проверок, код проверяет язык, который использует устройство. Злоумышленники атакуют только гаджеты, использующие интерфейс на русском языке.

Вышеописанный метод работает только в версии Google Chrome для Android. Как пояснили исследователи, при скачивании .apk с использованием ссылки на внешний ресурс, браузер выдает предупреждение о загрузке потенциально опасного объекта и предлагает пользователю решить, сохранить или нет загружаемый файл. В Google Chrome для Android при разбиении .apk на фрагменты не осуществляется проверка типа сохраняемого объекта и браузер сохраняет файл, не предупреждая пользователя.

Эксперты ЛК проинформировали Google о проблеме. Компания уже подготовила устраняющий эту уязвимость патч, который будет включен в состав следующего обновления браузера.

***

8.11.2016

В Україні розробляється система захисту від будь-яких кібератак

О. Турчинов повідомив, що нині створюється потужна система захисту поки що державних ресурсів («Главком»).

Секретар Ради національної безпеки і оборони України О. Турчинов зазначає, що інформаційна безпека та кібербезпека є безумовними пріоритетами для країни, яка перебуває в стані гібридної війни. Про це він сказав в інтерв'ю «Лівому берегу», повідомляє прес-служба РНБО.

О. Турчинов наголосив, що Росія активно використовує кібернетичні технології для агресії не лише проти України, а й проти ЄС та США.

За словами секретаря РНБО України, кібератаки спрямовані не лише на державні інформаційні ресурси, а й на об'єкти стратегічної інфраструктури. «Додайте до цього активізацію кібершпіонажу та кіберзлочинності», – сказав він.

Тому завдання нещодавно створеного Національного координаційного центру кібербезпеки, сказав О. Турчинов, полягає в об'єднанні та координації зусиль усіх відомств.

«Ми чітко розмежували сфери діяльності, уточнили спеціалізацію та сектори відповідальності. Тепер кожен знає, за що відповідає Держспецзв'язку, за що – відповідні підрозділи Служби безпеки України або Нацполіції, Міністерства оборони і розвідувальних служб», – сказав секретар РНБО.

«Перший етап пройдено, сьогодні створюється потужна система захисту поки що державних ресурсів – так звана Національна телекомунікаційна система. Проект витратний, але безальтернативний, оскільки завдання цієї системи – повністю захистити інформаційний ресурс критичної інфраструктури та держсектора від будь-яких кібератак», – сказав О. Турчинов.

У цьому контексті він зазначив, що «найпотужніша кібератака, яку було здійснено останнього тижня на систему е-декларування, не змогла її "покласти". "Ліг" лише сайт НАЗК, який не був захищений Держспецзв'язком», – додав він.

***

8.11.2016

На вибори в США можуть вплинути кібератаками – ЗМІ

Міністерство національної безпеки вважає, що система, яка використовується для виборів у США вразлива для хакерських атак (Корреспондент.net).

Міністерство національної безпеки (МНБ) США вважає, що система, яка використовується для проведення загальних виборів у країні, може бути вразлива для хакерських атак, повідомляє американська телекомпанія Fox News.

Не відкидається також можливість впливу на поширення даних про результати голосування.

У розпорядження журналістів телекомпанії надійшли висновки співробітників МНБ США.

«Ми вважаємо, що багато елементів інфраструктури для проведення виборів у США можуть бути вразливими для вторгнень у кіберпросторі», – наводить Fox News витяг з документа, який датується 20 вересня.

Зазначено, що ступінь ризику відрізняється від округу до округу, а також використовуваних у них комп'ютерних технологій.

Телекомпанія вказує, що, згідно з оцінками МНБ, хакери можуть отримати доступ до баз даних, де зберігаються відомості про зареєстрованих виборців, а також обмежити можливості громадян проголосувати. Крім того, передбачається, що шляхом кібератак можна спотворити призначену для поширення інформацію про попередні результати виборів.

***

10.11.2016

Обнаружен первый вирус, использующий мессенджер Telegram

Обнаружена первая вредоносная программа-шифровальщик, которая используя мессенджер Telegram, требует от пользователей викуп (Finance.Ua).

Вредоносный софт шифрует текстовые и графические файлы. Он является ботом Telegram. Создатели программы заранее получили от серверов мессенджера уникальный токен (служащий для авторизации пользователя, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам и надежного хранения личных данных) для идентификации бота и поместили его в тело шифровальщика.

В результате программа может использовать публичный API мессенджера и поддерживать связь со злоумышленниками. К примеру, софт отправляет сообщения в чат с заданным номером, информируя киберпреступников о факте заражения компьютера.

***

10.11.2016

На великі банки Росії здійснено DDoS-атаку

Хакери здійснили DDoS-атаку на п’ять великих банків Росії, передає УНН з посиланням на РІА «Новости» (УНН).

В атаці взяли участь бот-мережі, що складаються із так званих пристроїв «інтернету речей». Хакерським нападам піддалися лише великі банки країни.

Як повідомляє джерело, перша атака була зафіксована вранці 9 листопада, ввечері наступна складалася з кількох етапів, кожен із яких був удвічі сильніший за попередній.

Зазначається, що інформація про напади була передана до правоохоронних органів і в Державну систему виявлення, попередження і ліквідації наслідків комп’ютерних атак.

***

10.11.2016

Названы самые распространенные угрозы для компьютеров

Наиболее распространенной угрозой на компьютерах и ноутбуках названы нежелательные программы, на смартфонах и планшетах – платные мобильные подписки (UKR-TODAY.com).

Об этом сообщила компания «Яндекс», передает gazeta.ru.

Оказалось, что 12 % пользователей браузера по меньшей мере раз в месяц видят предупреждение об угрозе в Интернете. Учитывались предупреждения о главных типах угроз, в том числе об опасных страницах, нежелательных программах, страницах с платными подписками и SMS-мошенничестве.

Как отметили в компании, за компьютером пользователи ведут себя менее осторожно, чем на мобильном устройстве.

«На компьютерах предупреждения об угрозах игнорируют 29 % пользователей, в то время как на смартфонах и планшетах – лишь 6 %», – рассказали в «Яндексе».

Также выяснилось, что мужчины игнорируют предупреждения чаще, чем женщины.

Статистику собирали с помощью «Яндекс.Браузера».

***

11.11.2016

Хакеры украли 2,5 млн фунтов со счетов британского банка

Британский Tesco Bank компенсировал 9 тыс. клиентов 2,5 млн фунтов стерлингов, которые были украдены с их счетов в результате недавней хакерской атаки (Finance.Ua).

Оказалось, что количество жертв атаки на самом деле вдвое меньше, чем предполагалось ранее.

Банк принял решение компенсировать клиентам утерянные средства и возобновить полноценное функционирование через 12 часов после того, как глава финансового регулятора Великобритании (Financial Conduct Regulator) Э. Бейли заявил, что это «беспрецедентный случай для Великобритании».

В банке еще не обнародовали всех деталей атаки, но признали недочет в системе безопасности.

CEO Tesco Bank Бэнни Хиггинс заверил, что персональные данные клиентов не были взломаны и что банк продолжает сотрудничать с Национальным бюро по борьбе с преступность (National Crime Agency) с целью поимки мошенников.

***

9.11.2016

Сервис Web of Trust шпионит за пользователями

Популярный репутационный сервис Web of Trust (WOT), который формировал рейтинг сайтов, сообщал и предупреждал о вредоносном контенте, обвинили в скрытом сборе и продаже данных о пользователях (iLenta.com).

Во время расследования специалисты получили доступ к базе данных, которая содержала историю просмотров почти трех миллионов пользователей, пишет Pcmag. «Шпионом» оказалось расширение WOT. Обвинения оказались убедительными, и расширение WOT сначала были удалены из магазина расширений Firefox, а чуть позже – и с Chrome Web Store. Такие «скрытые функции» Web of Trust могут оказаться особенно неприятным для пользователей сервиса блокировки рекламы Adguard и яндекс.браузер.

Представители Adguard уже прокомментировали инцидент. Так, они использовали базы по WOT, касающиеся вредных сайтов, но при этом они использовали не стандартное дополнение WOT, а собственноручно написанный

компонент. Дальнейшая судьба Web of Trust о присутствии в Adguard сейчас решается.

Web of Trust также присутствует в «Яндекс.Браузере», как в мобильной, так и в десктопной версии. Пока представители «Яндекса» будут решать проблему, специалисты по безопасности советуют самостоятельно зайти в настройки браузера и отключить этот сервис.

***

9.11.2016

Меркель опасается российских кибератак на выборах в бундестаг

Канцлер Германии А. Меркель высказала опасения того, что власти России могут воздействовать на кампанию по выборам в бундестаг при помощи кибератак российских хакеров, передает DW (podrobnosti.ua).

Уже сегодня в Германии замечены кибератаки с российским следом, заявила А. Меркель, выступая во вторник, 8 ноября, в Берлине на пресс-конференции после встречи с премьер-министром Норвегии Э. Сульберг.

В частности, отметила канцлер, речь идет о распространении дезинформации.

«Поэтому может случиться, что это будет играть определенную роль и в предвыборной борьбе», – считает А. Меркель.

По ее словам, с подобными атаками надо разбираться каждодневно уже сегодня. В частности, правоохранительные органы Германии подозревают, что за недавними кибератаками на бундестаг и штаб-квартиру Христианско-демократического союза в Берлине стоят хакерские группы, связанные с Россией.

***

9.11.2016

Константин Семенов

В Android-смартфонах нашли опасную уязвимость

Эксперты по безопасности нашли в Android «опасную дыру». Уязвимость од страшным названием Dirty Cow не была закрыта в ноябрьском обновлении, которое вышло совсем недавно. Она позволяет обойти защиту и ограничения системы для получения root-доступа, сообщает AndroidInsider (podrobnosti.ua).

Дыру можно найти в любой версии Android с того момента, как Google начала использовать ядро Linux. Информация о ней была опубликована в октябре в надежде на то, что Google быстро закроет дыру в свежем обновлении безопасности прежде, чем ее начнут активно использовать. К сожалению, этого не случилось.

Исследователи нашли как минимум 13 приложений в Google Play, которые используют уязвимости для получения root-доступа, в том числе и

Dirty Cow. Стоит ожидать появления большего количества приложений, так как теперь уязвимость является широко известной.

Google выпустит обновление в следующем месяце. К сожалению, оно поможет только владельцам Nexus и Pixel, а также пользователям флагманских устройств от Samsung. Все остальные пользователи Android будут вынуждены мириться с существованием «грязной коровы» до момента покупки нового устройства.

***

14.11.2016

Microsoft рассказала о защите Windows 10 Anniversary Update от приложений-вымогателей

Приложения-вымогатели стали крупнейшей угрозой глобальной сети, принося своим авторам большой доход с минимальным риском. За последние 12 месяцев число таких приложений возросло более чем вдвое. Они зашифровывают файлы пользователей и требуют деньги за их расшифровку, но больший интерес представляют методы проникновения вымогателей на устройства пользователей (InternetUA).

6 из 10 самым популярных вымогателей проникают через браузеры или уязвимости их расширений, так что Microsoft затрудняет авторам использование Windows 10 и Edge. Также компания улучшает обнаружение и блокировку на своих почтовых сервисах, блокируя всё больше вредоносных вложений в письмах. В Защитник Windows добавлена технология сокращения времени обнаружения. Защита Windows Defender Advanced Threat Protection может использоваться в сочетании с Office 365 Advanced Threat Protection, помогая компаниям реагировать на атаки вымогателей.

Вместе с функциями Credential Guard, Windows Hello и другими это позволяет разработчикам называть Windows 10 Anniversary Update самой безопасной версией в истории Windows. Вот за счёт чего это было достигнуто.

Предотвращение

Усиление браузера. Adobe Flash Player является распространённым плагином, посредством которого эксплоиты скачивают вымогатели, потому в Edge Flash Player работает в изолированном контейнере. Запущенный в Edge эксплоит не может выполнять другую программу, что не позволяет вредоносному ПО незаметно скачивать и запускать дополнительный код.

Защита электронной почты. Именно по почте приложения-вымогатели распространяются чаще всего. Microsoft улучшает технологии машинного обучения для определения опасных вложенных файлов и ускоряет процесс обновления Защитника Windows.

Машинное обучение. Улучшение облачной инфраструктуры позволило за счёт машинного обучения быстрее находить и блокировать угрозы. До выхода Anniversary Update на сбор приложения для анализа, классифицирования и реагирования уходили часы, теперь минуты.

Обнаружение

Улучшенный Защитник Windows. По умолчанию этот антивирус включен и стал быстрее реагировать на угрозы за счёт более совершенной облачной защиты и распознавания вредоносной активности.

Реагирование

Защита после взлома. Здесь в дело вступает сервис Windows Defender Advanced Threat Protection (ATP). Используя данные о событиях на компьютерах с облачной аналитикой, ATP выдаёт предупреждения администраторам сетей. При попадании вымогателей на устройства консоль ATP может предоставить сведения о них, о методе проникновения, уровне урона и следующих возможных действиях.

Для защиты против вымогателей Microsoft рекомендует обновить систему до Windows 10 Anniversary Update и выбрать настройки безопасности по умолчанию, регулярно устанавливать обновления и выполнять резервное копирование.

***

14.11.2016

Facebook покупает украденные пароли ради повышения безопасности

Социальная сеть Facebook придумала новый действенный способ по борьбе с хакерами, крадущими пароли от пользовательских страниц. Служба безопасности Facebook регулярно покупает украденные пароли на черном рынке и использует их для радикального повышения уровня безопасности всей социальной сети (InternetUA).

По словам А. Стамоса (Alex Stamos), главы службы безопасности Facebook, столь необычный способ по борьбе с киберпреступниками оказался весьма результативным. Портал CNET сообщает, что выкупленные пароли в дальнейшем используются для сравнения с ныне используемыми на страницах компаний и обычных людей, и если совпадения обнаруживаются, то владелец страницы автоматически получает уведомление с информацией о недостаточной надежности выбранного им пароля.

По словам А. Стамоса, в каждой купленной у хакеров базе паролей находятся сотни тысяч аккаунтов, защищенных самыми простыми комбинациями – qwerty, 12345 и им подобными, что говорит о низком уровне знаний пользователей в вопросах защиты их личной информации. Такие люди получают уведомления о необходимости смены пароля в первую очередь, поскольку именно их данные хакерам легче всего украсть путем простого брутфорса (перебора паролей).

А. Стамос использует и ряд других не менее оригинальных методов по борьбе с хакерами, что и послужило причиной его выбора на пост главы службы безопасности, хотя он пришел в Facebook лишь в прошлом году, работая до этого в корпорации Yahoo. Однако любой метод защиты аккаунтов

от взлома не работает, если сам пользователь не стремится защитить его от кибер-преступников, что отлично видно на примере двухфакторной аутентификации, активированной у меньшинства владельцев профилей в Facebook.

А. Стамос также подчеркнул, что с недавнего времени Facebook ввела использования специальных алгоритмов машинного обучения, позволяющих автоматически определять факт взлома той или иной страницы по ряду косвенных признаков. С каждым днем определение становится все более точным, и количество спама, рассылаемого с таких страниц, снижается.

***

14.11.2016

Аккаунт Skype легко взломать. Как защититься от этого?

В последние недели многие пользователи Skype получают от своих контактов в переписке спамерские ссылки на сайты Baidu и LinkedIn. Как выяснил сайт The Verge, такие ссылки приходят даже от сотрудников Microsoft, причём те не даже догадываются, что их взломали. Что происходит и почему Microsoft позволяет такое? (InternetUA).

Судя по ветке с сайта техподдержки Microsoft, с августа 2016 г. было взломано несколько сотен аккаунтов Skype, в том числе защищённые двухфакторной аутентификацией. Такие аккаунты рассылают тысячи спам-сообщений своим контактам. Компания Microsoft признала существование проблемы, но всё ещё не знает, как её решить. По словам Microsoft, со стороны Skype не наблюдается уязвимостей, а киберпреступники каким-то образом получают действующие пары логинов и паролей.

Многие пользователи Skype полагают, что их учётные записи надёжно защищены двухфакторной аутентификацией, но на деле это не так.

Т. Уоррен с The Verge обсудил эту ситуацию с сотрудником Microsoft, чей аккаунт недавно был взломан, хотя и был защищён двухфакторной аутентификацией. По его словам, хакеры воспользовались комбинацией парой логина и пароля, не привязанной к аккаунту Microsoft. Компания просила пользователей Skype привязать свои учётные записи к аккаунту Microsoft, но даже это не защищает от взлома, потому что прежние реквизиты для входа продолжают действовать.

Очевидно, где-то произошла утечка реквизитов от учётных записей Skype, и именно поэтому компания попросила пользователей привязать к мессенджеру аккаунты Microsoft. Пока Microsoft разбирается с тем, что произошло, защитить аккаунт Skype можно следующим образом:

– Зайдите на страницу https://account.microsoft.com. Если вы залогинены в аккаунт Microsoft, выйдите из него.

– Зайдите в аккаунт Skype (используя логин и пароль от Skype, а не Microsoft).

– Объедините аккаунты Skype и Microsoft.

– Зайдите в настройки учётных записей и деактивируйте аккаунт Skype.

Теперь залогиниться в учётную запись Skype можно будет только с аккаунтом Microsoft, которая защищена гораздо надёжнее, чем аккаунт Skype. Кроме того, аккаунт Microsoft поддерживает полноценную двухфакторную аутентификацию, поэтому его гораздо сложнее взломать.

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник Терещенко Ірина

Редактор: О. Федоренко

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.