СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(15.02–1.03)

2016 № 4

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(15.02–1.03)
№ 4

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

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

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2016

ЗМІСТ

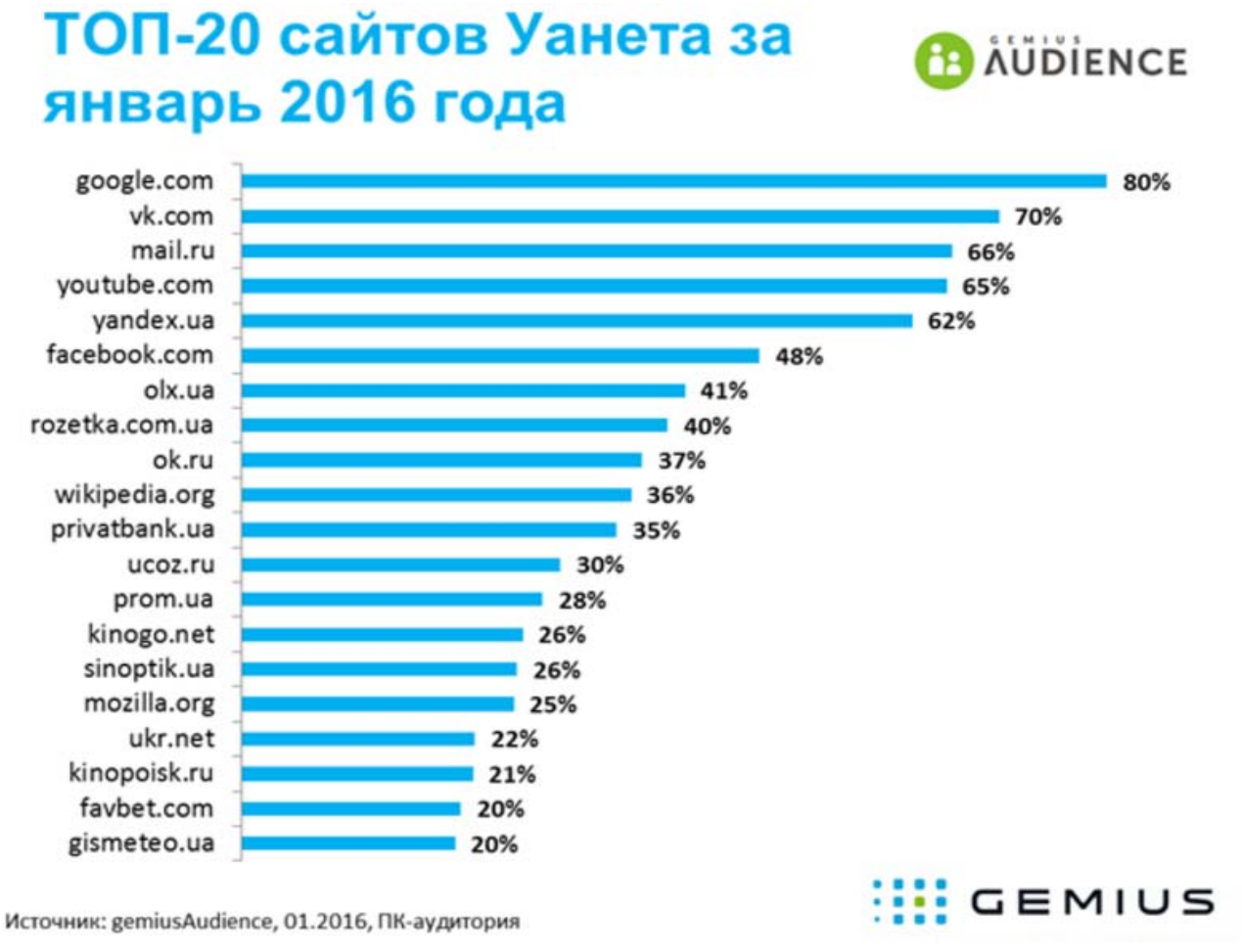
РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

18.02.2016

Топ-20 сайтов уанета за январь: впереди социальные сети и интернет-магазины

Исследовательская компания «Gemius Украина» представила результаты по аудитории уанета за январь 2016 г., а также рейтинг самых популярных сайтов среди украинских пользователей. В первую тройку традиционно вошли Google, «ВКонтакте» и Mail.ru, пишет AIN.UA.

Среди ПК-аудитории популярны сайты социальных сетей – Facebook на шестом месте и «Одноклассники» на девятом, а также ecommerce-площадки – 7 и 8 места занимают соответственно сайт объявлений OLX и интернет-магазин «Розетка». Полностью рейтинг выглядит так:



Рейтинг описывает ПК-аудиторию страны по данным gemiusAudience, международного исследования по измерению интернет-аудитории, которое Gemius проводит в более чем 30 странах региона EMEA.

***

22.02.2015

Facebook объявила о разработке социальной виртуальной реальности

В компании Facebook открылся отдел по изучению социальных взаимодействий в виртуальной реальности. Пресс-релиз с заявлением опубликован на сайте соцсети.

Как сообщается в документе, новая команда будет испытывать уже существующие технологии виртуальной реальности в области сетевого общения, пишет InternetUA.

Программисты Facebook продолжат сотрудничество с разработчиками шлема Oculus Rift. Кроме того, в Facebook озвучили ряд цифр, свидетельствующих о существенном спросе на аналогичную технологию Samsung – Gear VR. По данным компании, для платформы, появившейся в продаже в ноябре 2015 г., уже доступно 200 игр и приложений.

Владельцы Gear VR просмотрели свыше миллиона часов видео в формате виртуальной реальности. В Facebook объявили также о поддержке платформой Samsung панорамных роликов, выложенных в соцсети.

Соцсеть включила поддержку видео с круговым обзором 24 сентября 2015 г. Первым роликом в формате «360 градусов» стал трейлер «Звездных войн», выложенный в соответствующей группе. Видео позволяет наблюдать за событиями в любом направлении с места пилота транспортного средства, которое летит по пустынному ландшафту.

***

16.02.2016

YouTube приобрела стартап, помогающий музыкантам общаться с фанатами

Более 500 тыс. музыкантов со всего мира используют сервис, созданный стартапом BandPage для взаимодействия со своими поклонниками и любителями музыки. По всей видимости, в будущем возможности этого сервиса появятся на YouTube, так как совсем недавно BandPage объявила о сделке. BandPage теперь принадлежит компании YouTube, которая, в свою очередь, принадлежит компании Google, пишет InternetUA.

YouTube – это один из самых важных продуктов для Google. Он активно развивается, в том числе постепенно превращаясь и в музыкальный сервис. Сегодня многие коллективы регулярно радуют своих поклонников свежими видео на YouTube и набирают немало просмотров. Для чего им может быть полезен BandPage?

Изначально проект BandPage был создан для того, чтобы упростить работу исполнителей и позволить им проще обновлять информацию о своем творчестве на нескольких платформах, включая Spotify, Pandora, Facebook и

YouTube. Исполнители могли обновлять информацию только на странице BandPage, после чего она обновлялась везде автоматически.

Представители BandPage говорят, что их продукт помогает исполнителям увеличить количество поклонников и более эффективно продавать билеты на концерты и товары с символикой. Под крылом YouTube они смогут быстрее достичь своей цели и предложить более эффективный сервис для музыкантов.

***

16.02.2016

Facebook Messenger тепер підтримує роботу одночасно кількох акаунтів

Facebook запустила можливість одночасно працювати одразу з кількома акаунтами у Messenger для Android. Тепер користувачі зможуть перемикатися між різними обліковими записами, не виходячи з додатку, повідомляє UkrainianWatcher.

Функція в першу чергу є затребуваною з боку маркетологів, які працюють одночасно з кількома клієнтськими акаунтами, а також для компаній, які використовують Messenger для спілкування з клієнтами.

Нова функція доступна користувачам в усьому світі, для цього треба оновити Android-додаток до найновішої версії.

***

16.02.2016

Facebook и Twitter стали крупнейшими источниками для изданий в «Яндекс.Новостях»

Социальные сети Facebook и Twitter стали крупнейшими источниками информационных поводов в сервисе «Яндекс.Новости» с момента запуска функции «С чего всё началось» в декабре 2015 г. За первый месяц работы «Яндекс.Новостей» с новой маркировкой сюжета сервис отследил 3,6 тыс. первоисточников новостей. 8 % всех информационных поводов пришлось на Facebook, ещё 5 % – на Twitter, рассказали в «Яндексе», пишет МедиаБизнес со ссылкой на sostav.ua.

В целом социальные сети принесли 16 % информационных поводов, столько же – сайты различных ведомств. Традиционные российские издания стали источником 40 % новостей, зарубежные – 28 %.

Сервис «Яндекс.Новости» ввёл маркировку внутри сюжета «С чего всё началось» в декабре 2015 г. С её помощью компания отслеживает источники новостей в традиционных СМИ, на официальных сайтах различных государственных ведомств, а также в социальных сетях. Первоисточник новости в ленте обознается маркером «с чего всё началось».

***

18.02.2016
В «Одноклассники» интегрировали Instagram

Instagram запустил функцию загрузки фото и видео из приложения в социальную сеть «Одноклассники». Опция пока доступна только для iOS, но в скором времени появится и для Android. В соцсети считают, что новая функция расширит охват аудитории публикаций в Instagram, пишет InternetUA.

Ранее фотосервис позволил пользователям экспортировать снимки в Facebook, Twitter, «ВКонтакте», Flickr, Tumblr и Swarm, а также пересылать их по электронной почте.

***

17.02.2016
Instagram запускает двухфакторную авторизацию

Сервис фотошеринга Instagram начал запуск функции двухфакторной аутентификации. Нововведение призвано защитить аккаунты пользователей от взлома, сообщает МедиаБизнес со ссылкой на searchengines.ru.

Чтобы активировать эту функцию, нужно привязать номер телефона к учётной записи. После этого приложение будет отправлять смс-сообщение с пин-кодом каждый раз при входе в сервис, обеспечивая дополнительную защиту.Запуск нововведения будет производиться постепенно.

***

18.02.2016
Facebook запускает «мгновенные статьи» для всех издателей

Начиная с 12 апреля 2016 г., использовать функционал «мгновенных статей» для публикации своих материалов в социальной сети сможет любой издатель. Участие в этой программе даёт СМИ возможность создавать интерактивные статьи и размещать их напрямую в Facebook. «Мгновенные статьи» в социальной сети загружаются в разы быстрее, чем материалы на сайтах изданий, сообщает МедиаБизнес со ссылкой на searchengines.ru.

Напомним, что Facebook начала публикацию статей и видеороликов новостных изданий через новую функцию «мгновенные статьи» в мае 2015 г. Внедрение этого функционала было призвано ускорить загрузку мобильных страниц публикаций СМИ.

Партнёрами по запуску выступили девять издателей, включая The New York Times, BuzzFeed, The Atlantic, BBC News, National Geographic и NBC. Теперь их количество исчисляется сотнями.

Среди издателей существуют опасения, что использование функционала «мгновенных статей» сделает их слишком зависимыми от Facebook с точки

зрения трафика. Однако только они сами могут оценить, насколько им выгодно участие в этой программе.

***

22.02.2016

В честь Дня рідної мови Facebook пропонує вдосконалити переклад інтерфейсу соцмережі українською

Facebook пропонувала українцям долучитися до вдосконалення перекладу інтерфейсів соцмережі українською в Міжнародний день рідної мови, пише UkrainianWatcher.

І хоча день рідної мови вже закінчився, ви завжди можете зайти за посиланням facebook.com/translations, і соцмережа запропонує вам кілька опцій щодо варіантів перекладів різноманітних розділів.

***

22.02.2016

Facebook нуждается в 5G для развития технологий потокового видео и виртуальной реальности

Для продвижения наиболее современного стандарта связи 5G компания Facebook нуждается в помощи телекоммуникационных операторов. Facebook необходимо, чтобы мобильные сети передачи данных работали лучше и быстрее, передает агентство Bloomberg, пишет Politeka.

Компания М. Цукерберга обратилась к телекоммуникационным компаниям с предложением о партнерстве и обмене разработками в рамках инициативы, которая может ускорить распространение 5G. Также Facebook сделала аналогичное предложение для центров хранения данных и сетевого оборудования. Подобное сотрудничество позволит компании и ее партнерам сэкономить миллиарды долларов на развитии инфраструктуры.

В последнее время Facebook сфокусирована на создании программного обеспечения для потокового видео и виртуальной реальности. Однако подобные технологии требуют высокоскоростного соединения с очень высокой пропускной способностью.

В США два крупнейших оператора мобильной связи – Verizon Communications Inc. и AT & T Inc. – запланировали первые практические испытания 5G в этом году. Впрочем, запуск 5G в массовое использование ожидается не ранее 2020 г.

Особенностью 5G-сетей является их скорость передачи данных, которая будет в 5–10 раз выше, чем в действующих сетях 4G.

Напомним, что технология 3G запущена украинскими операторами мобильной связи лишь в прошлом году. К тому времени в большинстве развитых стран мира она уже считалась морально устаревшей.

***

22.02.2016

«Одноклассники» презентовали свое приложение для Smart TV

Одна из социальных сетей разработала собственное приложение, позволяющее просматривать видео на Smart-телевизорах, пишет МедиаБизнес со ссылкой на mediasat.info.

С помощью приложения «ОК Видео» пользователи социальной сети, имеющие Smart-телевизоры, могут смотреть любые видеоматериалы: как размещенные пользователями соцсети, так и предоставленные компаниями-производителями контента. Кроме того, это приложение обеспечивает трансляцию телевизионных каналов и online-конференций, проводимых в соцсети «Одноклассники».

Приложение позволяет управлять процессом просмотра, используя стандартный функциональный набор, включающий возможность менять качество видеоматериала, перемотку, переход к следующему видеоролику. В непрерывном режиме просмотра переход будет осуществляться автоматически. Использование приложения не предполагает оплаты и трансляции рекламы.

По информации пресс-службы «Одноклассников», каждый день пользователи сети смотрят больше 300 млн различных видеоматериалов. Использование приложения сделает для них более простым и удобным процесс поиска и просмотра видеороликов. С другой стороны, приложение поможет увеличить количество пользователей, поскольку не требует регистрации, а единственным условием является наличие Smart-телевизора.

***

23.02.2016

Несмотря на блокировку в Индии, Facebook продолжит развитие Free Basics

Facebook не намерена отказываться от дальнейшего запуска Free Basics, несмотря на блокировку сервиса в Индии. Об этом глава компании М. Цукерберг заявил на Mobile World Congress в Барселоне, пишет IGate.

«Мы разочарованы таким поворотом событий в Индии. Однако все страны – разные», – отметил руководитель.

На сегодняшний день сервис уже функционирует в 38 странах мира. Приложение даёт бесплатный доступ к ряду интернет-сайтов, включая Facebook и Wikipedia.

М. Цукерберг также сообщил, что компания по-прежнему активно инвестирует средства и в другие направления в рамках проекта Internet.org, такие как доставка Интернета с помощью дронов, спутников и лазеров. Первый спутник планируется к запуску в этом году.

Что касается Индии, здесь Facebook намерена сосредоточить своё внимание на других программах. В их числе – предоставление Интернета через

точки доступа Wi-Fi. В компании намерены установить 10 тыс. таких точек в стране и подключить их к существующим сетям.

М. Цукерберг также был возмущён обвинениями в стремлении Facebook извлечь выгоду из проекта Internet.org: «Многие люди думают, что компании заинтересованы лишь в деньгах. Но я создал Facebook, потому что хотел соединить студентов в колледже. Я никогда не думал о заработке. Однако превращение Facebook в коммерческую организацию позволило привлечь наиболее талантливых инженеров и технических специалистов в мире. У нас есть миссия, и мы должны зарабатывать».

***

24.02.2016

Facebook создала подробную карту населения Земли с помощью искусственного интеллекта

Компания Facebook начала использовать технологии искусственного интеллекта для создания карт, на которых можно в деталях увидеть, где живут люди, и как их месторасположение влияет на качество соединения с Интернетом. С помощью этих карт Facebook собирается выяснить, какие из её решений больше подходят для тех 10 % населения планеты, которые до сих пор не имеют доступа к сети, пишет InternetUA.

Проект был разработан подразделением Facebook под названием Connectivity Labs, которое, в свою очередь, является частью инициативы Internet.org, использующей дроны, спутники и лазеры для предоставления доступа к Интернету в развивающихся странах и сельских районах. С помощью вышеупомянутых карт Facebook хочет выяснить, будет ли она использовать точки доступа Wi-Fi или сотовые технологии для того, чтобы привести людей в «онлайн», а заодно заставить как можно больше людей зарегистрироваться в социальной сети.

Над созданием карт Connectivity Labs сотрудничала с научным подразделением Facebook, инфраструктурным блоком, а также с группами машинного обучения и искусственного интеллекта. Эта коалиция анализировала спутниковые снимки 20 стран мира (21,6 млн кв. км) общим объёмом в 350 Тбайт. Используя технологии машинного зрения, в том числе технологию для распознавания лиц в Facebook, команда исследователей смогла определить на снимках здания, построенные людьми. При этом компания отметила, что в проекте не использовались фотографии из социальной сети.

С помощью технологий машинного обучения и искусственного интеллекта Facebook «смогла определить контуры зданий и выделить те, в которых она была наиболее уверена, и скрыть те, которые, вероятно, не содержат созданных людьми структур». Затем с помощью данных о переписи населения команда определила, как данные могут использоваться в каждом из регионов.

Facebook пообещала открыть публичный доступ к проекту позже в этом году. Компания также собирается работать с Институтом Земли Колумбийского университета над созданием аналогичного, но более детального проекта.

***

23.02.2016

Telegram перешагнул отметку в 100 миллионов активных пользователей

Мессенджер Telegram достиг ежемесячного показателя в 100 млн активных пользователей. Об этом создатель проекта П. Дуров рассказал на конференции Mobile World Congress, пишет IGate.

По словам П. Дурова, аудитория мессенджера увеличилась в два раза за 12 месяцев. При этом рост наблюдается по всему миру, а не на одном конкретном рынке, отметил основатель Telegram.

«Мы растем исключительно благодаря тому, что наши пользователи рекомендуют Telegram своим друзьям. Каждый день 350 тыс. новых пользователей подключаются к Telegram без каких-либо усилий с нашей стороны», – отмечает П. Дуров.

В день Telegram доставляет 15 млрд сообщений. П. Дуров рассказал, что команда разработчиков состоит всего из 15 человек, поэтому они автоматизируют многие вещи и полагаются на скрипты и искусственный интеллект, а не человеческий труд.

***

25.02.2016

Google и сотовые операторы сговорились уничтожить SMS

Google договорилась почти с двумя десятками операторов о внедрении «SMS нового поколения» – новой технологии, которая позволяет обмениваться не только текстовыми сообщениями, но и любыми мультимедийными файлами. Компания выпустит бесплатный клиент для Android и предоставит разработчикам API, чтобы они могли создавать собственные приложения на базе новой технологии, пишет InternetUA.

Новый консорциум

Корпорация Google договорилась с операторами о совместном продвижении технологии нового поколения, призванной заменить SMS. Цель Google – сделать новую технологию стандартным средством для обмена сообщениями на смартфонах. Она напоминает известный мессенджер Apple iMessage, работающий в рамках экосистемы Apple, однако, разработку Google в своих мобильных операционных системах смогут использовать и другие разработчики, в частности Apple и Microsoft.

В инициативе согласились участвовать America Movil, Bharti Airtel, Deutsche Telekom, Etisalat, Globe Telecom, KPN, Millicom, MTN, Orange, Play,

Smart Communications, Sprint, Telenor Group, TeliaSonera, Telstra, TIM, Turkcell, Vimpelcom, Vodafone – 19 операторов. Анонс был сделан на сайте GSMA, что говорит о максимальной поддержке проекта отраслью.

Возможности «SMS нового поколения»

Новая технология называется Rich Communications Services (RCS). В переводе с английского – «Услуги расширенных коммуникаций». Технология позволяет обмениваться фотографиями в высоком разрешении, создавать групповые чаты, узнавать, было ли отправленное сообщение прочитано и когда абонент на другом конце набирает текст. Это лишь часть возможностей, утверждают в Google. Например, в будущем компания планирует добавить возможность звонков через RCS.

Выгода для операторов

Технология RCS поможет операторам конкурировать с поставщиками сервисов Over The Top (OTT). К таким относятся, например, WhatsApp, Viber, Telegram, Facebook Messenger, Skype и другие – все те сервисы, которые работают на базе мобильных сетей.

Ускорение перехода на новую технологию

На сегодняшний день RCS поддерживается 47 операторами в 34 странах (GSMA продвигает ее с 2008 г.). Но в Google полагают, что темпы проникновения этой технологии можно увеличить, если снять технологические барьеры.

Для этого партнеры договорились разработать универсальный профиль RCS. Google, помимо этого, разработает приложение для Android, которое позволит пользоваться RCS. Оно будет обладать открытым исходным кодом. Компания предоставит сторонним разработчикам интерфейс программирования (API), с помощью которого они смогут создавать собственные приложения, использующие преимущества технологии RCS.

Все необходимые инструменты

Универсальный профиль RCS и Android-клиент можно будет использовать на любых Android-устройствах и в сетях любых операторов в мире. Другие компании, такие как Apple и Microsoft, при желании смогут реализовать поддержку новой технологии в своих мобильных операционных системах. Все спецификации для этого будут в публичном доступе.

Для того чтобы реализовать поддержку RCS, операторы должны будут настроить оборудование. Однако они могут этого и не делать. Google предоставит облачную платформу Jibe, которая будет поддерживать универсальный профиль RCS. Операторы смогут пользоваться этой платформой без необходимости локального внедрения технологии.

***

24.02. 2016

Facebook ввів п’ять нових символів для позначення емоцій

Соціальна мережа Facebook розширює функціонал кнопки «Мені подобається», давши змогу користувачам вказувати, які саме емоції у них викликає пост, повідомляє LB.ua з посиланням на BBC.

Тепер при утриманні кнопки «Мені подобається» користувачі можуть вибрати одну з п'яти емоційних реакцій. Для оцінки публікацій і вираження почуттів користувачам мережі пропонуються символічне сердечко, а також фізіономія, яка сміється, плаче, здивована і сердита.

Нова функція кілька місяців тестувалася в Іспанії та Ірландії, а тепер доступна й іншим користувачам.

Раніше засновник Facebook М. Цукерберг також говорив, що компанія розглядає можливість появи кнопки «Мені не подобається», проте в підсумку від цих планів було вирішено відмовитися через побоювання, що негативних відгуків може виявитися непропорційно більше.

***

24.02.2016

Щомісяця понад 5 млн абонентів Київстар виходять у соціальні мережі з мобільних телефонів

Протягом 2015 р. послугою мобільного Інтернету скористалися понад 12 млн абонентів Київстару. Серед них 5 млн – користувались 3G Інтернетом – про це повідомили UkrainianWatcher в компанії.

Щомісяця понад 5 млн абонентів Київстар виходять у соціальні мережі з мобільних телефонів.

***

28.02.2016

Facebook займётся созданием глобальной mesh-сети

Социальная сеть Facebook анонсировала новый масштабный и амбициозный проект – Telecom Infra Project. Он будет реализовываться силами Facebook и ряда телекоммуникационных компаний, провайдеров, системных интеграторов и сотовых операторов. Задачей проекта является создание гибкой и масштабируемой инфраструктуры на основе беспроводных технологий для широкополосной передачи данных, например, видео или контента для виртуальной реальности, пишет InternetUA.

Этот проект позволит различным производителям выпускать совместимое оборудование, в числе которого названы точки доступа, транспортная сеть, а также компоненты ядра и системы управления сотовой сети.

По мнению Facebook, такая инициатива может обеспечить высокоскоростным беспроводным доступом те регионы, где не хватает проводных коммуникаций, а также изменит экономику развертывания сотовых сетей. По сути говоря, компания намерена активно развивать так называемые mesh-сети, которые не нуждаются в провайдерах и могут работать

децентрализованно. Facebook займётся непосредственно программной частью, а аппаратные устройства будут разрабатываться другими фирмами.

По-видимому, руководство соцсети считает, что такая технология окажется более дешёвой и быстрой в развёртывании, чем группировки низкоорбитальных спутников. Также она поможет развитию недорогой виртуальной реальности вне дома.

***

21.02.2016

В Instagram изменился способ отображения количества лайков

В социальной сети Instagram изменился способ отображения количества лайков. Раньше под публикацией отображались отметившее изображение юзеры до тех пор, пока их количество не достигало 11 – после этого указывалось лишь число.

Новость передает Utramir.net.

Теперь количество лайкнувших фото пользователей отображается числом, начиная с четырех. Любители Instagram активно обсуждают нововведение: «В мое время фотография считалась успешной, если понравилась 11 людям, а нынешним подросткам и стараться не нужно», – пишет один из пользователей, добавляя смайл.

Впрочем, большинство пользователей считают перемены удачными – теперь стало проще просматривать ленту, видеть количество отметок под не очень популярными постами, публикации выглядят аккуратнее.

***

24.02.2016

В Facebook появилась возможность отправлять видео-поздравления

Facebook начала процесс внедрения новой функции, позволяющей пользователям сайта поздравить друг другу с днем рождения путем коротких видео, пишет ProstoTECH.

Из опубликованной в сети информации следует, что решение уже работает, по крайней мере у некоторых людей, использующих операционную систему iOS. Все это, как нетрудно догадаться, должно быть стимулом к более тесным отношениям между владельцами учетных записей.

Facebook уже давно предлагает пользователям складывание пожеланий с помощью сервиса, однако все указывает на то, что компания не хочет ограничивать своих клиентов только текстовыми сообщениями, которые размещаются в ленте. Сервис ввел новую функцию, благодаря которой использующие ее люди могут все свои пожелания передать в виде 15-секундного видео. О решении мы слышали еще в прошлом году, но только сейчас оно стало доступным членам сообщества.

По словам редакции портала The Next Web, улучшения уже могут использовать некоторые владельцы устройств компании Apple. Кажется, однако, очень вероятно, что в будущем оно будет предложено всем пользователям сайта.

Новая функция находится в уведомлениях, в разделе День Рождения. Лицам, которые уже имеют к ней доступ, отображается сообщение в виде pop-up окна, которое информирует о ней. Запись можно сделать нажав на значок камеры, а перед его отправкой сервис позволяет добавить в фильм специальной рамки.

***

26.02.2016

У Facebook для Android з'явилася функція «живого» відео

Починаючи з 26 лютого, користувачі програми Facebook для Android можуть влаштовувати живі відеотрансляції на своїй сторінці. Ця функція була анонсована раніше, а з минулого року вона проходила відкрите тестування серед користувачів Facebook на iOS в США, пише Ua Format.

За словами Facebook, сервіс трансляції відео Facebook Live був запущений у 30 країнах світу, а в найближчі тижні стане доступний у всьому світі.

Функція Facebook Live дає змогу будь-якому користувачеві Facebook почати живу трансляцію відео на своїй сторінці. Для цього він повинен запустити додаток, натиснути на оновлення статусу, а потім на кнопку трансляції (чоловічок із хвилями навколо голови). Facebook почала тестувати сервіс трансляції відео влітку минулого року. Спочатку функція Live була доступна тільки знаменитостям, а в грудні доступ до неї отримали жителі США і власники деяких верифікованих акаунтів. Основним конкурентом Facebook Live стане додаток Periscope, яким володіє Twitter.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

17.02.2016

Петро Порошенко ввійшов до десятки найактивніших користувачів Instagram серед світових лідерів

Президент України П. Порошенко посів дев'яту позицію в рейтингу найактивніших користувачів Instagram, пише MediaSapiens.

Такими є результати дослідження «Світові лідери в Instagram 2016».

Лідером серед найактивніших став інформаційний департамент Брунею – 4,2 повідомлення на день. На другій та третій позиції розташувалися представники Кувейту. Міністерство закордонних справ країни розміщує трохи більше 4 дописів на день, а сам міністр – 3,8 повідомлень.

Серед світових лідерів, яких читають найбільше, переміг президент США Б. Обама з кількістю підписників понад 6 млн. На другому місці опинився російський прем'єр Д. Медведєв, який має трохи більше 2 млн підписників. До трійки лідерів також потрапила прем'єр-міністр Індії Н. Моді – у неї 1,8 млн підписників. За кількістю лайків трійка незмінна, проте Н. Моді випереджає російського прем'єра, посідаючи друге місце.

Загалом світові лідери опублікували в мережі 76 387 фото та відео, більшість з яких – зображення мітингів, конференцій, засідань та двосторонніх зустрічей із зарубіжними колегами.

Нині глави держав, урядів та міністри закордонних справ у 136 країнах (що являє собою 70 % всіх держав-членів ООН) мають офіційні акаунти в Instagram, ідеться в повідомленні.

***

16.02.2016

Мін'юст має намір надавати частину нотаріальних послуг через Skype

Протягом місяця Міністерство юстиції України представить проект щодо можливості надання частини нотаріальних послуг за допомогою системи VoIP-месенджера Skype, повідомляє МедиаБизнес із посиланням на day.kiev.ua

Про це заявив міністр юстиції України П. Петренко під час зустрічі з розробниками і представниками порталу державних послуг iGov, передає «РБК-Україна».

«Думаю, що ми дуже швидко, десь протягом місяця, презентуємо і законопроект, і модель переведення частини нотаріальних послуг у режим «Скайпу», і спрощення реально для тих людей, які зараз мають труднощі з отриманням довіреності або інших нотаріальних послуг. Ми спростимо їм життя», – запевнив глава Мін'юсту в понеділок 15 лютого.

***

16.02.2016

Управління держпраці у Полтавській області створило сторінку у соціальній мережі

Відомство відтепер доступне в мережі Facebook. Публічну сторінку полтавського управління Держпраці можна знайти за адресою: http://www.facebook.com/poltava.dsp, де будуть опубліковуватись останні офіційні новини, фото, відеозвернення та інші тематичні посилання.

Адміністратор сторінки – головний спеціаліст взаємодії зі ЗМІ, міжнародних зв'язків та питань з євроінтеграції, повідомляють Новини Полтавщини.

У соціальній мережі Facebook є також акаунт начальника управління С. Щербака. «Для нас надзвичайно вважливими є дієвий зв'язок з громадськість та засобами масової інформації. Люди мають отримувати повну, а головне, достовірну інформацію про події на виробництві області та роботу фахівців Держпраці», – зазначає керівник.

***

24.02.2016

Сайти соцмереж як джерело інформації

За результатами дослідження компанії Cision і Кентенберійського університету Церкви Христа, близько третини британських журналістів стверджують, що вони не могли би виконувати редакторську роботу без соціальних медіа. Та чи припустимо використовувати сайти соцмереж як джерела у ЗМІ? Про це в матеріалі О. Голуб для MediaSapiens.

Багатьом з нас важко уявити життя без соціальних мереж. Так, за результатами дослідження компанії Яндекс, у чотирьох найпопулярніших соціальних мережах («ВКонтакте», «Одноклассники», Facebook і Twitter) зареєстровано понад 40 млн українських акаунтів.

Соціальні мережі нині є важливим джерелом інформації не тільки для аудиторії, а й для самих традиційних ЗМІ. За результатами дослідження компанії Cision і Кентенберійського університету Церкви Христа, близько третини британських журналістів стверджують, що вони не могли би виконувати редакторську роботу без соціальних медіа. 39 % респондентів зазначили, що соціальні медіа підвищили рівень їхньої продуктивності. Дослідники провели опитування серед 3650 журналістів із 11 країн (Великобританія, Франція, Німеччина, Фінляндія, Швеція, Італія, Іспанія, Нідерланди, США, Канада й Австралія). Із загальної кількості респондентів 769 були представниками Великобританії.

Українські журналісти погоджуються, що соціальні мережі можуть бути джерелом інформації. Приміром, журналіст газети «День» І. Самокиш зазначив: «Згоден із думкою, що соцмережі можуть бути джерелом інформації. Дуже часто саме користувачі соцмереж опиняються неподалік місця події, тимчасом як журналісти дізнаються лише з Facebook чи інших соцмедіа про неї. Я довіряю соцмережам, але інформацію (якщо це потрібно для тексту) перевіряю. Її потрібно більше фільтрувати, ніж ту, яку подають медіа».

Натомість А. Крикун, прес-секретарка UMDI, у своєму блозі на «Кореспонденті» зазначає: «Оскільки життя "переноситься в Інтернет", то і багато подій транслюються одразу сюди. Тому пошук інформації в Інтернеті, у соціальних медіа є важливим інструментом для збору інформації. Багато журналістів мають сторінку у Facebook із максимально можливою кількістю

контактів (5 тис.) і, за їхніми словами, це допомагає взнавати їм про події у різних куточках України та світу».

Експерти ІМІ проаналізували 203 матеріали про конфліктно чутливі групи населення в шести загальнонаціональних інтернет-ЗМІ на предмет того, які джерела інформації журналісти використовують. З'ясувалося, що в 25 % випадків джерелом інформації були акаунти в соціальних мережах, переважно у Facebook і Twitter.

При цьому в 10 % випадків це були неверифіковані акаунти (верифікованими вважаються сторінки, автори яких надали для соцмережі фото з посвідченням особи, яке після верифікації видаляється).

Слід зазначити, що серед неверифікованих акаунтів часто трапляються акаунти досить впливових і відомих особистостей, як-от народного депутата І. Геращенко, голови Донецької військово-цивільної адміністрації П. Жебрівського, прес-секретаря Л. Кучми Д. Оліфер.

Але трапляються й випадки, коли ЗМІ використовують акаунти взагалі невідомої особи, як-от у новині «Соцсети о "культурных" боевиках "ДНР": наверное, сгорело шапито» на сайті «Обозреватель» джерелом інформації слугував акаунт у соціальній мережі такого собі П. Пряникова.

У такому разі постає питання, чи не суперечить використання соцмереж як джерела інформації професійним журналістським стандартам, де чітко вказано необхідність дотримання стандарту точності й достовірності.

Так, у редакційних настановах ВВС зазначено: «Відданість Бі-бі-сі забезпеченню достовірності є основною редакційною цінністю й фундаментом нашої репутації. Результат нашої роботи повинен мати надійні джерела, спиратися на обґрунтовані свідчення, бути ретельно перевіреним». Безумовно, від достовірності джерела залежить точність інформації, саме тому експерти відносять достовірність і точність до фундаментальних засад журналістики.

Частина експертів наголошує на небезпеці використання соціальних мереж як джерела інформації, оскільки саме так звані нові медіа є одним з найпоширеніших способів поширення неправдивої інформації та фейків.

Виконавчий директор ГО «Телекритика» Д. Дуцик наголошує: «Фактор соціальних мереж в Україні сьогодні є дуже важливим. Тому що останнім часом усе частіше класичні ЗМІ користуються соцмережами як першоджерелами, на жаль. Відповідальність лежить на журналістах, які лінуються або не мають досвіду й не перевіряють достовірність інформації. Потім ця неперевірена інформація потрапляє на телебачення й поширюється на масову аудиторію».

Беззаперечною є небезпека поширення неправдивої інформації в умовах інформаційної війни, яка є частиною гібридної війни, що її Росія веде проти України. Це впливає не лише на цивільне населення України, але й демобілізує військових, що боронять свою країну.

Про це у своєму коментарі газеті «День» розповів кандидат психологічних наук, завідувач лабораторії соціально-психологічних технологій Інституту соціальної та політичної психології НАПНУ П. Фролов: «Оскільки

ми живемо в інформаційному світі, наше бачення та реакції визначаються змістом інформації, яку ми споживаємо. З огляду на це, поширення фейкових повідомлень не може не позначитися на психічному здоров'ї суспільства. Всі ці технології давно відпрацьовано. Дослідження показують, що люди вважають найбільш важливими саме ті теми й проблеми, які активно висвітлюються й обговорюються в ЗМІ. Таким чином можна цілеспрямовано коригувати уявлення суспільства – фактично формувати нову реальність».

За інформацією сайту StopFake, неправдиві новини поширюють передусім російські ЗМІ. Українські ж ЗМІ можуть тиражувати брехню, якщо неретельно перевірять джерело інформації. Саме тому журналістам варто особливо уважно перевіряти інформацію із соціальних мереж, щоб не стати переносниками фейків.

С. Козлюк, журналіст «Українського тижня»: «Соціальні мережі – джерело, але таке, що потребує ретельнішої перевірки. Якщо це пости очевидців із місця події – фото, відео, з різних акаунтів. Якщо якісь гучні заяви медійних персон із викриванням корупціонерів, цифри – теж джерело, але паралельно треба давати запит у відповідні органи, які підтвердять / спростують».

Саме перевірка та опрацювання отриманої інформації є одним з обов'язків журналіста. Власне, тим і відрізняються традиційні ЗМІ від соціальних мереж і сайтів агрегаторів. Саме ЗМІ, яке керується у своїй роботі журналістськими стандартами, професійними й етичними, має бути фактором, що впливає на формування громадської думки.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

18.02.2016

В течении следующих пяти лет компании в два раза увеличат расходы на рекламу в соцсетях[1]

На сегодняшний день в социальные сети вкладывается 10,6 % маркетинговых бюджетов, в 2016 г. доля возрастет до 13,2 %, а в 2021-м достигнет 20,9 %. Об этом свидетельствуют результаты опроса Школы Бизнеса Фукуа, Американской Ассоциации Маркетинга и компании Deloitte. При этом большинство из опрошенных маркетологов не может доказать эффективность рекламных кампаний, проводимых в социальных сетях, пишет IGate.

Почти половина опрошенных (47,9 %) директоров по маркетингу не могут сказать, как реклама в соцсетях влияет на их бизнес. Более 40 % чувствуют положительное влияние и только 11,5 % заявляют, что могут наглядно доказать эффективность подобных инвестиций. При этом

[1] Так в оригіналі.

маркетологи тратят деньги на соцсети и собираются это делать в будущем, потому что они играют важную роль в прямой связи с потребителем.

В первую очередь, компании планируют вкладываться в создание контента (62,6 %) и аналитику (43,6 %). Средняя оценка эффективности соцсетей в связи с общей маркетинговой стратегией бренда составила 4,2 по семибалльной шкале. При этом для набольшей отдачи SMM-специалисты должны работать вместе с остальными маркетологами и взаимодействовать с отделом поддержки.

В целом, участники опроса планируют увеличить расходы на 6,9 %, рост в сегменте digital может составить 13,2 %. Зато расходы на традиционную рекламу снизятся, по оценкам рынка, на 3,2 %.

***

20.02.2016

Twitter запускает две новые функции

Сервис микроблогов Twitter запускает две новые функции для ведения бизнеса: ссылки на личные сообщения из твитов и сервис опроса клиентов Customer Feedback. Об этом «Газете.Ru» сообщили в пресс-службе компании, пишет InternetUA.

«Нередко общение пользователей и брендов в рамках клиентской поддержки начинается в твитах, а затем, когда речь идет о передаче личной информации, переносится в личные сообщения. Теперь совершить этот переход можно в один клик», – отмечают в компании.

Новая функция позволит брендам добавлять в твиты ссылки. Пользователи будут видеть кнопку «Отправить личное сообщение» прямо в переписке в Twitter.

Еще одна функция вводится для того, чтобы бренды имели возможность устраивать среди пользователей опросы. Сервис Customer Feedback позволит брендам использовать два стандартных отраслевых формата – индекс лояльности NPS (Net Promoter Score) и индекс удовлетворенности клиентов (CSAT).

***

19.02.2016

Facebook добавит рекламу в Messenger

Facebook готовится запустить рекламные объявления в сервисе Messenger, сообщает TechCrunch со ссылкой на внутренние документы компании. Предполагается, что реклама будет распространяться в виде личных сообщений от аккаунтов компаний, пишет IGate.

По данным TechCrunch, Facebook объявит о запуске рекламных объявлений во II квартале 2016 г. Издание ссылается на документы,

полученные от надёжного источника, однако отмечает, что не может их опубликовать в целях защиты собеседника.

Согласно полученным документам, рекламодатели смогут отправлять объявления тем пользователям, которые начали общение с аккаунтами компании. В частности, Facebook рекомендует компаниям предлагать как можно большему числу клиентов перевести общение в Messenger, чтобы иметь возможность отправлять им рекламу.

В документах также указано, что Facebook запустила короткий адрес fb.com/msg/, с помощью которого можно моментально открыть чат для общения с компанией. Представители соцсети подтвердили TechCrunch существование такой ссылки.

На вопрос о запуске рекламных сообщений в Facebook сообщили, что «не комментируют слухи и спекуляции». «Наша цель в Messenger – поддерживать высококачественный канал общения для 800 млн людей по всему миру, не заставляя их получать нежелательные сообщения любого рода», – отметили в компании.

Судя по всему, Facebook не собирается позволять компаниям рассылать рекламные предложения всем, кто поставил «лайк» на их страницах, отмечает TechCrunch. Однако даже это расходится со словами основателя соцсети М. Цукерберга в 2014 г. после покупки WhatsApp, который говорил, что «реклама вряд ли является лучшим способом монетизировать мессенджеры», отмечает издание.

***

25.02.2016

Число активных рекламодателей в Instagram превысило 200 тысяч

На сегодняшний день рекламу в Instagram покупает более 200 тыс. компаний, 75 % из которых находится за пределами США. Об этом сообщается в официальном блоге сервиса. «Для нас это важное достижение. Чем более разнообразной будет база наших рекламодателей, тем более релевантной мы сможем сделать нашу рекламу для пользователей», – отметил Д. Чарльз, глава по рекламе Instagram, сообщает МедиаБизнес со ссылкой на searchengines.ru.

По его словам, прошлым летом количество активных рекламодателей сервиса исчислялось лишь несколькими сотнями.

Росту рекламного бизнеса компании способствовали как нововведения в сервисе, так и сотрудничество с Facebook, владельцем Instagram: «Отношения с Facebook помогли нам увеличить базу пользователей и привлечь рекламодателей. Возможность задействовать в рекламных кампаниях обе площадки даёт брендам больший простор для творчества», – считает Д. Чарльз.

Представленная статистика также свидетельствует об успешности стратегии глобального расширения рекламного бизнеса Instagram.

***

26.02.2016
Facebook убивает Instagram, наращивая объемы рекламы

Locowise представил исследование аудитории Instagram, проанализировав в январе 2500 профилей пользователей. Сервис остается рекордсменом по росту подписчиков по сравнению с самим Facebook и Twitter, но засилье рекламы сказывается на вовлечении аудитории, сообщает МедиаБизнес со ссылкой на adindex.ru.

Наибольший рост фолловеров с августа. Рост подписчиков в Instagram в январе 2016 г. составил 0,37 %. Это на 60,87 % больше, чем в декабре 2015 г., и самый большой скачок с августа 2015 г., что звучит позитивно для стремящихся к органическому росту брендов, так как декабрьские результаты были самыми негативными за девять месяцев, с тех пор как Locowise занимается исследованиями аудитории Instagram.

При этом сервис обмена фото и видеоконтентом по-прежнему остается лидером роста подписчиков в сравнении с Facebook и Twitter. Органический рост подписчиков страниц в Facebook в январе достиг 0,16 %, а в Twitter – 0,11 %.

Средний процент вовлечения публикации в сервисе за январь составил 0,95 % всей аудитории. Это на 12,04 % меньше по сравнению с декабрем и самый низкий уровень вовлечения за все время исследований. За весь период (9 месяцев) уровень вовлечения в Instagram снизился на 66,07 %.

За это время в Instagram увеличился объем размещаемой рекламы, так как Facebook хочет поскорее вернуть инвестиции после приобретения платформы в 2012 г. Согласно данным исследовательской компании, объем показов рекламных сообщений в Instagram умножился в 13 раз за последние пять месяцев. И в планах руководства привлечь еще больше рекламодателей.

Уровень вовлечения в Instagram все еще выше, чем в Twitter (0,09 %) и Facebook (0,46 %), но может оказаться под угрозой из-за наращивания объемов рекламы. Аналитики прогнозируют, что к концу 2016 г. ежемесячная аудитория Instagram возрастет до 520 млн активных пользователей, и что платформа будет генерировать до 2 млрд дол. выручки.

К Суперкубку сервис представил для рекламодателей опцию размещения 60-секундных роликов, чтобы брендам не приходилось адаптировать созданный для прочих каналов коммуникации контент. Ш. Сандберг, COO Facebook, рассказала, что представители соцсети довольны показателями роста рекламы в Instagram. Конкретных цифр Facebook не раскрывает, но известно, что 98 из 100 крупнейших рекламодателей соцсети теперь размещают рекламу и в Instagram. Благодаря сервису в IV квартале 2015 г. количество рекламных показов компании возросло на 29 % в годовом исчислении.

Instagram ожидает роста просмотров роликов на платформе, а также числа тех, кто генерирует видеоконтент. За последние шесть месяцев время, проводимое пользователями за просмотром роликов, увеличилось на 40 %.

Однако фото и картинки остаются самым популярным форматом на сегодняшний день – 91,83 % всех публикаций, проанализированных Locowise в январе. Пост с картинкой вовлекает 0,97 % аудитории, в то время как видео – 0,68 %. В ближайшее время представители платформы обещают представить улучшения для видеоформата. Чтобы привлечь как можно больше топовых рекламодателей.

Помимо этого платформа предоставила возможность переключаться между аккаунтами. Всего в приложениях и на iOS и на Android можно сохранить до пяти учетных записей, что позволяет сделать присутствие брендов более эффективным.

***

23.02.2016

Foursquare поможет измерить влияние онлайн-рекламы на офлайн-посещения

Foursquare представил новый инструмент Attribution, который поможет ритейлерам измерить влияние интернет-рекламы на посещаемость офлайн-магазинов. Посредством нового сервиса данные Foursquare будут доступны даже тем компаниям, которые не размещают рекламу в приложениях Foursquare или Swarm, сообщает МедиаБизнес со ссылкой на searchengines.ru.

Как пояснил глава компании С. Розенблатт, они составили репрезентативную выборку из 1,3 млн пользователей (ежемесячная аудитория сервиса составляет 50 млн человек), которые активировали передачу данных о местоположении в Foursquare. Таким образом, можно найти тех людей, которые видели объявление, изучить их поведение, а затем сравнить его с поведением той группы пользователей, которые не видели рекламу. Это, в свою очередь, позволит Foursquare экстраполировать, как объявление повлияло на рост посещаемости магазина или заведения.

Партнёрами по запуску нового инструмента выступили Flipboard, Brown-Forman, TGI Fridays, Drawbridge И Adelphic.

По данным Flipboard, используя эту технологию, они смогли показать рекламодателям, что рекламная кампания привела к 12 % росту посещаемости.

По словам С. Розенблатта, компания сможет предоставлять данные на ежедневной основе. Таким образом, рекламодателям не нужно будет ждать несколько недель, чтобы получить эту информацию. Руководитель подчеркнул, что все данные пользователей будут агрегированными. Следовательно, их приватности ничего не угрожает.

***

26.02.2016

Facebook запускает Canvas – интерактивный формат мобильной рекламы

Facebook объявила о запуске Canvas – нового интерактивного формата мобильной рекламы. Продукт будет доступен рекламодателям во всём мире. В отличие от объявлений в виде карусели, Canvas – полноэкранные интерактивные объявления. Они представляют собой подобие мини-сайта, созданного для конкретных товаров, сообщает МедиаБизнес со ссылкой на searchengines.ru.

Новый формат позволяет пользователям взаимодействовать с контентом объявления: фото, видео, и GIF-анимацией. В новостной ленте объявления этого формата выглядят как обычная реклама. Однако по клику происходит мгновенная загрузка полноэкранной версии. Вернуться в новостную ленту можно, нажав на значок «X» в левом верхнем углу объявления.

За ускоренную загрузку специалисты отрасли прозвали Canvas «мгновенными статьями» для рекламодателей.

По данным Facebook, во время тестирования пользователи позитивно восприняли новый формат. В среднем, они тратили на Canvas 31 сек. и более 70 сек. на лучшие из них. В целом, 53 % пользователей просматривали более половины объявления в этом формате.

Рекламные блоки Canvas создаются в веб-интерфейсе и не требуют навыков программирования или дизайна. Работают они только на iOS и Android-устройствах. Запуск десктопной версии этого функционала в компании пока не планируют.

Новый формат будет доступен всем рекламодателям, использующим Power Editor.

Тестирование нового формата было начато в сентябре.

***

19.02.2016

Как раскрутить свой профиль в Instagram?

Ни для кого не секрет, что социальные сети могут использоваться как площадки для ведения бизнеса, поэтому очень важно знать, как работать с аудиторией и раскручивать свои профили. В частности, мы расскажем, как повысить количество подписчиков в Instagram, пишет Hyser.

Зачем это нужно

Действительно, стоит ли вообще как-то дополнительно привлекать подписчиков? Разумеется, стоит. Истина в том, что сам по себе контент, пусть даже самый качественный и интересный, вряд ли сможет существенно повлиять на рост вашей аудитории. Вы должны заявить о себе, а сделать это можно с помощью подписок, лайков и комментариев.

Всё просто: чем больше людей видят ваши предложения, тем выше уровень продаж. Вопрос только в том, как обеспечить достаточное количество подписчиков. Можно попытаться сделать это самостоятельно и потратить уйму времени или же раскрутить свой аккаунт с помощью сервиса InstaPlus.

Возможности

Главная задача InstaPlus – взаимодействие с вашей целевой аудиторией посредством лайков, уникальных комментариев и подписок. С этим он справляется великолепно: всего нескольких часов достаточно для того, чтобы существенно увеличить количество ваших подписчиков.

Постановка задач и предварительная настройка здесь настолько просты, насколько только возможно. Даже тот, кто не имеет ни малейшего представления о технологиях продвижения, легко сможет разобраться с тем, как же всё это работает. Вам нужно лишь добавить свой аккаунт (от одного в бесплатной версии до пяти в платной) и выбрать, что именно и во сколько надо сделать: поставить лайки к фотографиям, оставить комментарий с заданным вами текстом, подписаться или отписаться. Установка таймера на конкретное время совершения действий – гораздо более удобная штука, чем может показаться на первый взгляд. Ставить лайки ночью нет никакого смысла: пользователи их просто не увидят. Зато если обратиться к ним в подходящее время, результат порадует куда сильнее.

InstaPlus: выбор аккаунта

В качестве источника вы можете выбрать геометки или хэштеги в зависимости от того, ориентируетесь вы на географическое положение или на интересы пользователей. Такая точная настройка дополнительно привлекает клиентов, ведь чем точнее вы очертили границы целевой аудитории, тем больше шансов попасть в цель. Наконец, можно просто привлечь внимание тех, кто подписался на аккаунты конкурентов. Выбираете учётную запись и работаете с её подписчиками или подписками, это ведь и ваши потенциальные клиенты тоже.

InstaPlus: история заданий

Важное преимущество сервиса – InstaPlus использует облачные технологии. Для управления аккаунтами не нужно ничего дополнительно скачивать и устанавливать. Наблюдать за тем, как идёт работа, и вносить коррективы вы можете с любого устройства, имеющего доступ в Интернет. На возникающие по ходу дела вопросы в любое время суток оперативно ответят внимательные специалисты службы поддержки.

Учитывая перечисленные выше преимущества, и без того невысокая стоимость использования услуг InstaPlus становится практически сказочной. Есть варианты на 7, 30 и 60 дней – комбинируйте их в зависимости от стоящих перед вами задач.

Итоги

Если вы хотите быстро раскрутить свой аккаунт, но не готовы тратить на это много времени и постоянно контролировать процесс, InstaPlus вам понравится. С этим сервисом всё будет именно так, как нужно: быстро, качественно и без лишних движений.

Следите за тем, как увеличивается количество подписчиков вашего аккаунта, а потом решайте, будете ли и дальше использовать InstaPlus уже в расширенной версии с управлением несколькими учётными записями. Скорее всего, ответ будет положительным.

***

26.02.2016

Рекламщики уже требуют у Facebook статистику по новым «реакциям», чтобы лучше изучить вас. Но социальная сеть пока не предоставляет данных

Рекламодатели Facebook в восторге от нововведения социальной сети в виде новых «реакций» пользователей, как то «гнев», «печаль», «смех» и другие, и хотят использовать его для лучшего понимания целевой аудитории, но компания пока не предоставляет им такой услуги, пишет Politeka со ссылкой на Reuters.

Facebook не будет разделять «реакции» пользователей, чтобы определить их интересы при размещении рекламных объявлений и других сообщений в ленте новостей клиента. Все реакции будут учитываться как дополнительные «лайки», что, по мнению Facebook, значит, что пользователь хочет видеть больше похожего содержания, даже если человек отреагировал смайликом «гнев».

В Facebook сообщили, что компания решит позже, как принять во внимание новые реакции при персонализации новостных лент. Но это не достаточно скоро для рекламодателей, которые хотят подстроить свои сообщения уже сейчас.

«Я думаю, что нам нужно использовать это для таргетирования как можно скорее», – сказал руководитель отдела цифровой рекламы в нью-йорской компании Maxus Americas Д. Адамс.

Корпорации хотели бы изучить реакции, чтобы определить, являются ли хронически «печальные» или «веселые» пользователи также и более склонными покупать различные продукты.

Рекламодатели надеются, что Facebook будет предоставлять данные, показывающие новый диапазон реакций на сообщения и объявления – например, чтобы увидеть, было ли объявление смешным, чтобы они могли настроить рекламу соответственно. Facebook распространяет такую информацию о «лайках», но пока неизвестно, будет ли она выдавать информацию о «реакциях». В компании также считают, что различение «реакций» поможет им понять пользователей, которые не особенно активны в вербальном выражении отзыва о продукте.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

17.02.2016
Учені прирівняли залежність від соцмереж до наркотичної

Перегляд стрічки новин активує ті самі ділянки мозку, що і кокаїн, пише Корреспондент.net.

Постійне гортання новинної стрічки в соціальній мережі Facebook впливає на мозок у такий самий спосіб, що і кокаїн, повідомляє The Telegraph.

Учені пов'язують виникнення будь-якої залежності з порушеннями у зміні психічних процесів збудження і гальмування. Залежним людям властива надмірна чутливість до об'єктів, що стали причиною розладу їхньої психіки, і водночас у них порушуються механізми гальмування.

Дослідження, опубліковане в журналі Psychological Reports: Disability and Trauma, вивчило реакцію студентів на візуальні подразники, у тому числі ті, які пов'язані з популярною соцмережею.

Випробовувані люди, які показали високу швидкість реакції на образи у Facebook, також показали високу схильність до залежності від інтернет-ресурсу.

Зображення, які містять вказівки на соціальну мережу, викликали збудження в мигдалевидному і смугастому тільцях, вельми схоже на те, що його викликає наркотик кокаїн. При цьому учені зазначають, що під час моніторингового періоду досліджувані змогли зменшити залежність від впливу на себе.

«Це хороша новина, оскільки це означає, що поведінка може бути виправлена лікуванням. Ми припускаємо, що адиктивна поведінка в цьому випадку пов'язана з низькою мотивацією для керування поведінкою, яке частково обумовлене відносною громадською і особистісною терпимістю до зловживання технологіями порівняно, скажімо, з токсикоманією», – заявив О. Турел, професор Університету штату Каліфорнія.

Раніше повідомлялося про те, що ВООЗ має намір визнати залежність від Інтернету психічним розладом.

***

20.02.2016
Соціальна мережа Facebook буде рятувати своїх користувачів від самогубства

Розробники Facebook вирішили впровадити у свою соціальну мережу функціональність, спрямовану на запобігання суїцидів серед користувачів, повідомляє HiTech-News.ru з посиланням на Sky News.

Для цього був запущений спеціальний алгоритм, що вишукує серед користувачів соцмережі будь-які натяки на думки про самогубство.

Алгоритм сканує записи користувачів і в разі виявлення слів, які, на думку розробників, можуть свідчити про суїцидальні настрої, пропонує користувачам поговорити про це з друзями або психологами.

Сервіс запущено в рамках співпраці Facebook з некомерційною міжнародною організацією Samaritans, фахівці якої надають психологічну допомогу на добровільних засадах.

У керівництві Facebook вважають, що сам факт подібного прояву небайдужості може дійсно допомогти комусь із користувачів подолати думки про самогубство.

Маніпулятивні технології

16.02.2016
Непатріотичні «патріоти»

Бойовик із «ДНР» керує українськими пабліками в соціальних мережах

Власником та адміністратором низки антивладних, а на перший погляд, нібито патріотичних спільнот у соціальних мережах «ВКонтакте» та Facebook є росіянин С. Жук. Таку інформацію опублікували журналісти інформаційної агенції «Укрінформ» після спільного розслідування з однією з провідних ІТ-компаній України. Паблік присвячений антивладній позиції українців, де закликають до «третього Майдану» і «становлення нового етапу формування української нації без української влади та олігархів», пише Україна молода.

У соціальних мережах С. Жук називає себе С. Мазурою. Він керує пабліками «Майдан-3» і «Патріоти України» у vk.com, а також «Українська революція», «Патріоти України», «Продовження Революції гідності» у Facebook. Тобто, як зазначають журналісти «Укрінформу», всі найвідвідуваніші паблики в соціальних мережах патріотичної тематики належать саме бойовикам із «ДНР» на чолі із С. Жуком.

«Для мене це справді шок, оскільки довгий період читала ці паблики, лайкала та певним чином довіряла інформації, що там публікували», – розповідає «УМ» студентка столичного вишу М. Старовойт. «Оскільки телевізор узагалі не дивлюся, то найпростішим способом отримання інформації на сьогодні є соціальні мережі, тому і довіряла паблику “Патріоти України”, користуючись ним, відчувала, що занадто багато агресії щодо української влади, але навіть не могла подумати, що керують ним сепаратисти», – додає дівчина.

Профіль С. Мазури, яким насправді є С. Жук, у соцмережах ведеться з використанням IP-адрес, що належать до діапазону IP-адрес інтернет-провайдера PJSC Rostelecom (Росія, місто Москва). Цю інформацію вдалося отримати завдяки роботі програмістів, які швидко з'ясували, хто і де веде акаунт. Водночас, згідно з інформацією у профілі самого С. Жука, він 2014 р. воював у складі незаконних збройних формувань на Донбасі під позивним «Москва». 2015 р. він пішов на підвищення в Москву і став учасником агресії РФ вже в інформаційному просторі.

***

19.02.2016
Євросоюз шукає волонтерів для протидії російській пропаганді

Потрібні ресурси для розширення діяльності та поширення інформації про Євросоюз, пише Телекритика.

Як повідомляє Media Sapiens із посиланням на EurActive, голова програми East Stratcom Ж. Портман звернувся 18 лютого до депутатів Європарламенту з проханням про таку допомогу.

Програму було створено у вересні минулого року, але на неї не передбачено бюджету і вона має лише дев'ять людей персоналу. Близько 400 волонтерів з різних країн ЄС та Східної Європи сповіщують групу про випадки пропаганди.

Наразі програма поширює повідомлення через Twitter російською та англійською мовами та готує щомісячний випуск «Огляд дезінформації» з аналізом зразків російської пропаганди на онлайн-ресурсах.

За словами Ж. Портмана, останні опитування показали, що половина населення Франції та третина німців звинувачує у війні Київ, у Греції більше людей симпатизує Росії, а не Євросоюзу. Голова програми підкреслює, що без допомоги вони не зможуть вийти на більш широку аудиторію.

***

24.02.2016
Основатели Facebook и Twitter получили угрозы от боевиков ИГ

Боевики «Исламского государства» начали распространять через сервис Telegram видео, озаглавленное Flames Of The Supporters («Пламя сподвижников»). 25-минутный ролик содержит угрозы в адрес основателя Facebook М. Цукерберга и создателя Twitter Д. Дорси, сообщает 24 февраля InternetUA со ссылкой на Vocativ.

«Ежедневно вы объявляете о закрытии наших учетных записей. Это все, на что вы способны? Вы нам не ровня. Если вы закроете один аккаунт, мы в ответ откроем 10 и скоро сотрем ваши имена, когда удалим ваши сайты», – гласит текст в видео.

Ранее в феврале администрация Twitter объявила о блокировке 125 тыс. микроблогов за пропаганду терроризма. В Facebook утверждают, что борются со страницами, чьи авторы поддерживают действия боевиков. В ответ хакеры ИГ, именующие себя «сыновьями армии халифата», выпустили ролик, в котором продемонстрировали взлом аккаунтов социальных сервисов. Пособники террористов утверждают, что им удалось внести изменения в 10 тыс. учетных записей Facebook, 150 групп соцсети и 5 тыс. микроблогов Twitter.

***

29.02.2016

Губернатора Туку забанили у Фейсбуці на місяць за пост річної давності

Губернатора Луганської області Г. Туку забанили у Facebook на місяць за пост річної давності. Про це LB.ua розповів сам Г. Тука по телефону, пише LB.ua.

У пості, за який забанили губернатора, ішлося про перемир'я. Але Г. Тука вважає, що це був лише привід. «Поскаржилися на мене, радше за все, прихильники Опоблоку і Радикальної партії. Їм дуже не подобається, що я критикую їхній союз у міськраді Сєвєродонецька», – каже Г. Тука.

***

28.02.2016

Цукерберг пообещал разобраться с хейтерами на Facebook

Гендиректор Facebook М. Цукерберг пообещал решить проблему хейтеров в соцсети. Об этом он рассказал в ходе конференции в Берлине, пишет InternetUA.

«Это очень важный вопрос. Хейтеры – это ужасно, им не место на Facebook. В Германии мы не очень хорошо справлялись с этой проблемой. Но я обещаю – мы ее решим», – подчеркнул М. Цукерберг.

В феврале 2015 г. в невозможности справиться с хейтерами и троллями признало руководство Twitter. «Мы плохо справляемся с троллями на нашей платформе и это продолжается годами. Мы теряем ядро нашей аудитории просто потому, что не можем эффективно бороться с троллингом», – отметил Д. Костоло, в то время занимавший пост гендиректора компании.

Хейтеры – пользователи сети, открыто выражающие свою неприязнь по отношению к какой-либо личности или культурному явлению. С помощью агрессивных записей и комментариев они часто пытаются подтолкнуть собеседников к конфликту.

***

21.02.2016

В десятках групп в Facebook процветает детская порнография

Согласно расследованию, проведенному британской организацией по защите детей NSPCC, в социальной сети Facebook существуют десятки групп, возраст членов которых и размещаемый в группах контент не проходят мониторинг, и эти группы зачастую превращаются в «площадку для педофилов», сообщает NEWSru.co.il со ссылкой на Daily Mail.

Согласно правилам Facebook, аккаунт может открыть пользователь не младше 13 лет. При этом в Facebook существует множество так называемых «групп знакомств для подростков», в которых состоят не только подростки, но и дети младше 13 лет, а также взрослые люди старше 18.

Во многих из таких групп пользователи размещают свои обнаженные снимки и ссылки на порносайты.

По данным NSPCC, в Facebook существуют не только группы, для членства в которых нужно послать запрос модератору, но и совершенно открытые группы, в которые может записаться любой пользователь.

Этим, по мнению NSPCC, пользуются педофилы, записываясь в такие группы, чтобы общаться с подростками.

***

25.02.2016

Facebook считает Крым украинским, а VK показывает «две правды»

Социальные сети по-разному отображают информацию об украинских территориях для пользователей из разных стран, пишет Styler.

Facebook считает Крым и Донбас украинскими территориями – так отображается информация о городах в этих регионах, независимо от того, из какой страны заходит пользователь. А сервис «ВКонтакте» оказался двуличным: украинские пользователи «ВКонтакте» видят крымские города в списке украинских, а для российских юзеров – это Россия.

Социальные сети «Одноклассники» и «Мой мир» причислили Крым и Донбас к Российской Федерации еще в 2014 г. Тогда же российский депутат Госдумы Е. Федоров предъявлял требования включить Крым и Севастополь в состав России руководству социальных сетей Facebook и «ВКонтакте».

Руководители социальных сетей требования российского правительства восприняли по-разному. Кремлевский аппарат нашел рычаги влияния на «ВКонтакте» и отображение информации для пользователей разных стран изменилось.

Facebook же сохранила территориальную целостность Украины. При входе пользователей из Украины, России, Турции или США украинские оккупированные города отображаются именно как украинские.

После того как «Одноклассники» и «Мой мир» причислили захваченные территории к России, аудитория украинских пользователей Facebook за считанные месяцы увеличилась на 25 % – люди начали активно переходить из пророссийских социальных сетей.

В картографическом сервисе российской компании «Яндекс» государственная принадлежность Крыма и Севастополя, как и «ВКонтакте», зависит от того, из какой страны пользователь обращается к сайту.

***

25.02.2016

Facebook, Twitter і Google відмовляються блокувати проросійських терористів – волонтер

Український фахівець з веб-безпеки, засновник волонтерського руху «Українські кібервійська» Є. Докукін заявив про те, що соцмережі Facebook, Twitter, а також пошукова система Google ігнорують прохання українських IT-волонтерів блокувати профілі терористів, які перебувають під санкціями США. Про це волонтер написав у своєму Facebook, пише UAINFO.

«Два місяця Facebook, Twitter і Google відмовляються блокувати терористів, що знаходяться під санкціями США. Про це два місяці з грудня 2015 р. їм нагадую, але або жодних відповідей не отримую, або ж стандартні відмазки (коли вони «не бачать порушень», хоча я завжди вказую сайт U.S. Department of the Treasury зі списком санкцій).

Нагадаю стосовно юридичних методів боротьби з Twitter, Facebook та іншими компаніями, що блокують українських користувачів, але відмовляються блокувати тролів і терористів. В січні писав про масове блокування українських користувачів, в т.ч. тих, чиї адреси терористи публікують в списках з персональними даними українців, які я постійно закриваю на різних сайтах з 2014 р.

Стосовно блокування акаунтів та інших ресурсів терористів, то за два роки Google відповідав відмовами в 99 % випадків, Facebook і Twitter в 90 %.

Прочитайте про юридичні методи боротьби з американськими компаніями, що підтримують тероризм: http://on.fb.me/1Z4ehr0. Про що я наголошую з серпня 2014 р. Якщо б ще 1,5 роки тому активно дзвонили щодня у Facebook, Twitter і Google (саме жителі США і Канади, з якими я багато спілкувався за цей час – їм було б не важко і не дорого подзвонити в ці компанії, а тим паче подавати позов в американський суд), вимагаючи від них прибрати всі сайти, блоги і акаунти сепаратистів і терористів, а також припинити репресії проти українців, погрожуючи компаніям судовим позовом. То вони вже давно б вели себе краще».

16.02.2016

В Днепропетровске СБУ задержала администратора сепаратистских пабликов в соцсетях

Сотрудники Службы безопасности Украины задержали в Днепропетровске местного жителя, который вел активную антиукраинскую пропаганду в социальных сетях, пишет InternetUA.

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

Сообщается, что 35-летний администратор сообщества активно распространял и репостил антиукраинские материалы на различных информационно-политических пабликах.

«Злоумышленник распространял информацию, направленную на дискредитацию подразделений Вооруженных сил Украины, материалы с призывами к насильственному изменению конституционного строя Украины, гражданского неповиновения действующей власти, инструкции по предотвращению мобилизации и создания на территории Украины так называемой «Новороссии». Также сообщник террористов информировал своих кураторов о настроениях населения и социально-политическую обстановку в Днепропетровске», – сообщили в спецслужбе.

Во время проведения обыска сотрудники спецслужбы изъяли компьютерную технику с доказательствами противоправной деятельности.

В рамках уголовного производства открытого по ч. 2 ст. 110 (посягательство на территориальную целостность и неприкосновенность Украины) Уголовного кодекса Украины продолжаются следственные действия.

***

23.02.2016

В Днепропетровской области задержали администратора сепаратистских групп в соцсетях

Сотрудники Службы безопасности Украины задержали в Павлограде Днепропетровской области работника популярной радиостанции, который вел активную антиукраинскую пропаганду в социальных сетях, пишет InternetUA.

В 2015 г. радийщик через Интернет познакомился с представителями «ДНР» и на их предложение согласился распространять сепаратистские материалы и стать администратором нескольких антиукраинских групп в соцсетях.

Злоумышленник распространял материалы, которые дискредитируют украинское государство и армию, популяризировал террористические организации «ДНР / ЛНР», призвал к уклонению от мобилизации и созданию

на территории Украины т. н. «Новороссии». Администратор также информировал своих кураторов об общественно-политические настроения на предприятиях угольной отрасли Днепропетровщины.

Во время проведения обыска сотрудники спецслужбы изъяли у сообщника террористов компьютерную технику с доказательствами противоправной деятельности.

Открыто уголовное производство по ч. 2 ст. 110 Уголовного кодекса Украины.

***

25.02.2016

В Днепропетровской области СБУ задержала модератора антиукраинских групп в соцсетях

Сотрудники СБУ задержали в одном из поселков Новомосковского района Днепропетровской области местного жителя, который вел активную антиукраинскую пропаганду в социальных сетях, пишет «Главком».

Об этом сообщает пресс-служба ведомства.

«В прошлом году студент одного из вузов Днепропетровска стал администратором нескольких групп антиукраинской направленности. 21-летний молодой человек через интернет познакомился с представителями террористической организации «ДНР» и согласился распространять сепаратистские материалы на различных информационно-политических паб ликах», – сказано в сообщении.

По данным СБУ, он распространял информацию, которая дискредитировала Вооруженные силы Украины, популяризировал террористические организации «ДНР/ЛНР» и создание так называемой «Новороссии». Также сообщник террористов информировал своих кураторов о настроениях студенческой молодежи и социально-политическую обстановку в Днепропетровске.

Во время обыска сотрудники спецслужбы изъяли у подозреваемого компьютерную технику с доказательствами противоправной деятельности.

Открыто уголовное производство по ч. 2 ст. 110 (посягательство на территориальную целостность и неприкосновенность Украины) Уголовного кодекса Украины.

***

18.02.2016

На Кіровоградщині засуджено інтернет-пропагандистку сепаратизму

Знам’янський міськрайонний суд Кіровоградської області визнав винною місцеву мешканку, яка розповсюджувала в Інтернеті сепаратистські матеріали, пише InternetUA.

Співробітники Служби безпеки України в липні 2015 р. припинили діяльність адміністратора групи «новоросія Кіровоград». Жінка розміщувала в одній з російських соціальних мереж матеріали з антиукраїнською пропагандою.

Під час обшуків було вилучено розтиражовані сепаратистські агітки, зокрема «акт проголошення незалежності Кіровоградської народної республіки», «декларація про суверенітет Кіровоградської народної республіки» та «конституція Кіровоградської народної республіки».

Суд визнав зловмисницю винною у скоєнні злочинів, передбачених ч. 2 ст. 109 та ч. 1 ст. 110 Кримінального кодексу України, та призначив покарання у вигляді позбавлення волі терміном на три роки.

***

19.02.2016

В Луганской области СБУ задержала администратора антиукраинской группы в интернете

В Луганской области сотрудники Службы безопасности Украины задержали администратора онлайн-сообщества, который вел активную антиукраинскую пропаганду в социальных сетях, пишет InternetUA.

Житель Лисичанска модерировал страницу с информационным контентом на поддержку пророссийского сепаратизма. Он размещал материалы с публичными призывами к проведению акций гражданского неповиновения в поддержку «ЛНР» и «ДНР», их признание и присоединение в состав России.

Мужчина также пропагандировал идеи изменения границ территории Украины, ее конституционного строя и проведения «референдума» о независимости Харьковской области.

Модератор рассказал сотрудникам спецслужбы, что за свою деятельность получал денежное вознаграждение на карточный счет. По его словам, куратор «проекта» проживает в Москве и контролирует несколько интернет-групп, задействованных в подрывной антиукраинской пропаганде.

Открыто уголовное производство по ч. 1 ст. 110 Уголовного кодекса Украины.

Продолжается досудебное следствие, сообщает пресс-центр СБ Украины.

***

17.02.2016

У Росії значно зросла цензура в інтернеті – правозахисники

У Росії протягом 2015 р. значно зріс рівень цензури в Інтернеті, мовиться у щорічному звіті «Свобода інтернету – 2015», який підготувала міжнародна правозахисна група «Агора» й дані якого публікують російські засоби інформації, повідомляє МедиаБизнес з посиланням на radiosvoboda.org.

За цими повідомленнями, 2015 р. у Росії майже вдев'ятеро зросло число блокувань інтернет-сайтів, а кількість порушень права на свободу Інтернету зросло з двох до п'ятнадцяти тисяч.

Крім того, 2015 р. користувачі Інтернету в Росії вперше почали отримувати реальні терміни позбавлення волі за публікацію «забороненої» інформації: за це до ув'язнення були засуджені 18 людей.

Загалом автори звіту налічили 203 випадки кримінального переслідування в Росії за публікації в Інтернеті.

Крім того, правозахисники звернули увагу на зростання рівня насильства щодо блогерів та інтернет-активістів у цій країні: 2015 р. вони зафіксували 28 таких випадків.

Більш як удвічі зросло число регіонів Росії, в яких користувачі Інтернету зазнають серйозного тиску. Серед таких регіонів у звіті названі Москва, Санкт-Петербург, Татарстан, Мордовія, Ульяновська область та Чечня.

Але, зазначили правозахисники, зростає й число росіян, які мають доступ до Інтернету і здатні оминати технічні перешкоди в доступі до заблокованих сайтів, користуючись спеціальними програмами.

На думку авторів звіту, як її наводять російські засоби інформації, «найближчим майбутнім громадянам Росії, можливо, доведеться натрапити на обмеження доступу до закордонних сервісів і посиленням практики кримінального переслідування за висловлювання думок в Інтернеті.

Становище з громадянськими правами в Росії, зокрема, зі свободою слова, давно викликає стривоженість правозахисників у цій країні й за її кордоном.

***

18.02.2016

Российские правообладатели, добившись блокировки Rutracker, взялись за «ВКонтакте»

Ассоциация по защите авторских прав в Интернете (АЗАПИ) подала иск в Мосгорсуд против «ВКонтакте». Заявление подано по предусмотренной антипиратским законом процедуре, которая может привести к «вечной» блокировке сайта. Ранее АЗАПИ добилась решения о «вечной» блокировке Rutracker, пишет InternetUA.

Впервые против «ВКонтакте» подан иск в Мосгорсуд по процедуре антипиратского закона, передают «Известия». Его оформила Ассоциация по защите авторских прав в Интернете из-за нарушения прав соцсети на книгу З. Прилепина «Обитель». Более двух выигранных судебных процессов позволят правообладателям требовать полную блокировку соцсети в России.

***

20.02.2016

В России предлагают запретить социальные сети в рабочее время

Российский вице-премьер О. Голодец выдвинула предложение о запрете использования социальных сетей в рабочее время. Идею озвучила Общественная палата, в которой считают, что в России «понятие трудовой дисциплины воспринимается весьма условно», и известны ситуации, когда сотрудники организаций в рабочее время общаются в чатах и играют в игры, пишет InternetUA.

В качестве примера представитель Общественной палаты В. Слепак привел январское решение Европейского суда по правам человека в Страсбурге, принявшего постановление по делу «Барбулеску против Румынии», пишут «Известия». Согласно принятому решению признается право работодателя знать, чем занимается его сотрудник в рабочее время, осуществлять контроль за личной перепиской работников в рабочее время, а также проводить мониторинг иных личных коммуникаций с использованием технических средств, предоставленных работодателем работнику.

В Минтруда информацию о поручении рассмотреть предложение подтвердили, однако отметили, что предпосылок для запрета использования соцсетей во время рабочего дня нет.

***

17.02.2016

Прокуратура РФ присудила рік виправних робіт для жінки за репости про Україну в соцмережах

У Залізничному суді Єкатеринбурга (Росія) 17 лютого звинуваченій в екстремізмі К. Вологженіновій – продавцеві магазину і матері-одиначці, яку судять за репости в соцмережі «ВКонтакте», прокурор присудила рік виправних робіт з відрахуванням 10 відсотків заробітку в дохід держави, пише LB.ua.

Про це повідомляє місцевий сайт E1.

Настільки м’яке покарання прокурор пояснила тим, що у К. Вологженінової є маленька дитина і вона раніше не була судима.

Читаючи звинувачення, прокурор зазначила, що стаття, яку поставили К. Вологженіновій, раніше не застосовувалася, але в нових обставинах вона стала актуальною, ідеться в повідомленні.

«Звинувачення не буде давати оцінку відносинам України і Росії, оскільки кримінальне право є аполітичним, – заявила прокурор. – Однак у зображеннях, розміщених на сторінці, є інформація, спрямована на розпалення ненависті і ворожнечі до росіян, добровольців з Росії».

Нагадаємо, К. Волгоженінову звинувачують у «сприянні терористам» за лайки і репости матеріалів про Україну в соцмережах. ФСБ визначило цю діяльність екстремістською.

***

18.02.2016

Турецким пользователям интернета ограничили доступ в соцсети после теракта

В первые часы после теракта в Анкаре турецкие пользователи Интернета испытывали трудности при попытке использовать социальные сети. Об этом сообщает InternetUA со ссылкой на Hurriyet.

Издание отмечает, что многие жаловались на пропускную способность в соцсетях, будто их скорость была специально ограничена. В тексте указано, что технически такая возможность в Турции есть и что она могла быть применена в конкретно этом случае.

По данным издания, жители страны испытывали сложности при использовании таких соцсетей, как Facebook и Twitter. Тем не менее, издание не подтверждает самого факта такого ограничения, как и то, что это было сделано именно из-за теракта в столице страны.

Тем не менее, в стране нередки случаи регулирования в Интернете, такие как блокировки и задержания пользователей за публикуемую информацию, в том числе и журналистов.

***

24.02.2016

Немецкой полиции разрешили использовать «федеральный троян»

Немецкая полиция получила добро на использование «федерального трояна» – программного обеспечения, предназначенного для слежки за преступниками и подозреваемыми через их компьютеры и мобильные устройства. Распространяться Bundestrojaner будет по такому же принципу, как и другие «вредоносы», пишет HiTech-News.ru.

Кроме того, троян может оказаться предустановленным в систему в том случае, если продавец электроники сотрудничает с немецкой полицией. Bundestrojaner будет маскироваться под какое-нибудь стандартное приложение, поэтому пользователи смогут устанавливать его самостоятельно.

Троян способен собирать данные различного типа, в том числе вести логи взаимодействия с клавиатурой, совершенных звонков, сканировать файлы и директории. Использование ПО может начаться в ближайшее время.

***

25.02.2016

Ольхович А. У США почали боротьбу з ІД в Інтернеті

Влада США має намір активізувати боротьбу з терористичним угрупованням «Ісламська держава» в Інтернеті, і тому запросили сприяти

найбільшим компаніям у боротьбі з екстремістами через соцмережі, передає УНН із посиланням на CNN, пишуть Українські Національні Новини.

За їхніми даними, з цією метою в Міністерство юстиції США були запрошені керівники Apple, Twitter, Snapchat, Facebook, MTV і Buzzfeed. Відзначається, що директор національного контртерористичного центру Н. Расмуссен розповів їм про зусилля адміністрації Сполучених Штатів щодо боротьби з ІД у соцмережах.

Представники майже 50 компаній брали участь у зустрічі. У ній також взяли участь безліч урядових структур, у тому числі сам Мін'юст, а також держдепартамент і Рада національної безпеки при Білому домі.

Під час зустрічі керівників компаній розповіли про використовувану ІД-технологію поширення повідомлень, а також про плани щодо протидії терористичній пропаганді.

***

29.02.2016

У Росії в мережі стежитимуть за школярами

Спеціальна система для стеження за дітьми називається «Ангел-охоронець», пише Корреспондент.net.

У Росії створили спеціальну систему під назвою «Ангел-охоронець», яка буде інформувати батьків про зацікавленість їхніх дітей темою тероризму, передають «Известия».

Повідомляється, що в тому випадку, якщо програмне забезпечення виявить перегляд школярем інформацію про ІД, його батькам буде надходити спеціальне повідомлення на мобільний телефон.

Система «Ангел-охоронець» була розроблена фахівцями Центру досліджень легітимності і політичного протесту. Відомо, що вона буде займатися аналізом поведінки дітей у соціальних мережах, і зокрема, переглядами картинок, відео та текстів.

У разі, якщо буде виявлена зацікавленість дитини темою тероризму, вона буде сповіщати її батьків шляхом відправки SMS.

Відомо також, що безкоштовно користуватися системою зможуть не тільки батьки, але також і вчителі дитини. Наразі готується пілотний запуск «Ангела-охоронця» в Новгородській області.

***

21.02.2016

«Битва за шифрование»: Microsoft, Facebook и Twitter вслед за Google поддержали Apple в споре с ФБР

Все больше компаний и видных людей из IT-индустрии ввязываются в обостряющийся конфликт между Apple и ФБР. Вслед за Google компанию

Apple поддержали еще три крупных игрока – Microsoft, Facebook и Twitter, пишет HiTech-News.ru.

«Мы намерены и дальше активно выступать против предъявляемых компаниям требований ослабить защиту их систем», – говорится в официальном заявлении Facebook, полный текст которого приводит источник.

В Facebook уверены, что подобные требования создают пугающий прецедент и сводят на нет все усилия компаний по обеспечению безопасности собственных продуктов. Вместе с тем Facebook подчеркивает, что компания «осуждает терроризм» и «ценит тяжелейшую и важнейшую работу правоохранительных органов» по защите граждан.

Тем временем глава Twitter Д. Дорси написал на своей странице в Twitter следующее: «Мы поддерживаем Apple и Т. Кука, а также благодарим его за инициативность».

Напомним, 16 февраля суд Калифорнии обязал Apple помочь ФБР получить доступ к защищенному iPhone террориста из Сан-Бернардино С. Фарука для получения «важной информации». Говоря точнее, ФБР попросила Apple снять ограничение на количество попыток ввода пароля, чтобы подобрать пароль самостоятельно. На следующий день глава Apple Т. Кук опубликовал открытое письмо, в котором объявил о нежелании компании сотрудничать со следствием.

Microsoft выразила свою поддержку распространением письма антишпионской организации Reform Government Surveillance (RGS), членом которой является программный гигант. В нем говорится, что нельзя принуждать технологические компании создавать «черные ходы» в системах, отвечающих за безопасность пользовательской информации.

Напоследок отметим, что сторонники есть не только у компании Apple, немало поддерживает вторую сторону конфликта. Так создатель антивируса McAfee, поддерживающий правительство, пообещал за три недели взломать iPhone террориста из Сан-Бернардино.

Как бы там ни было, само дело, которое может легко дойти до Верховного суда, так как Apple не собирается отступать, пожалуй, является самой важной битвой в непрерывающемся споре по поводу технологий шифрования.

Проблема захисту даних. DDOS та вірусні атаки

15.02.2016
Instagram по ошибке позволил читать чужие сообщения

В Instagram обнаружился баг, возникший после того, как фотохостинг позволил быстро переключаться между несколькими аккаунтами. Как сообщает

Android Central на своем сайте 15 февраля, некоторые пользователи стали видеть чужие уведомления и сообщения владельцев других аккаунтов, с которыми они ведут общую учетную запись, пишет InternetUA.

В частности, если два пользователя в дополнение к собственным аккаунтам создают еще один общий, то через некоторое время один из них начинает получать оповещения для личной учетной записи, принадлежащей другому человеку.

При попытке открыть чужое уведомление приложение перенаправляет пользователя к его личному аккаунту. Однако оповещение дает возможность прочитать имена людей, с которыми связана учетная запить другого человека, а также небольшой отрывок комментария или даже личного сообщения.

В Instagram подтвердили наличие неисправности. В настоящее время компания работает над ее устранением, сообщили порталу.

***

16.02.2016
В роутерах Asus обнаружен опасный баг

Независимый исследователь Д. Лонжнекер обнаружил очень простую и очень неприятную уязвимость в маршрутизаторах компании Asus, работающих на базе прошивки ASUSWRT. «Благодаря» проблемам в интерфейсе, панель администратора доступна удаленно всем желающим, пишет InternetUA.

По оценкам исследователя, проблема затрагивает порядка 140 тыс. роутеров Asus. Большая их часть «светит» админкой в Интернете через HTTP, и еще около 15 тыс. устройств доступны через HTTPS. От бага страдают все роутеры, работающие под управлением прошивки ASUSWRT, то есть все, в названии которых присутствуют буквы RT.

Баг, судя по всему, является обычной мелкой халатностью разработчиков. Обычно, чтобы запретить удаленный доступ к панели администратора, в настройках устройства нужно найти опцию Enable Web Access from WAN, и выбрать вариант «No». Однако роутеры Asus поставляются со встроенным брандмауэром, для активации которого в настройках есть пункт Enable Firewall.

Лонжнекер обнаружил, что если встроенный файерволл отключить, выбрав «No», это по какой-то причине отменяет также и запрет Enable Web Access from WAN. То есть, если пользователь отключил брандмауэр, уже не важно, включена опция Enable Web Access from WAN или нет. Она отключается в любом случае.

Исследователь уже уведомил Asus об ошибке, и компания готовит новую версию прошивки, исправляющую баг.

***

16.02.2016
По Сети распространяется фальшивый патч для CMS Magento

Киберпреступники не оставляют попыток обнаружения неисправленных версий системы управления содержимым Magento, подверженных уязвимости известной как Magento Shoplift или SUPEE-5344. В этот раз злоумышленники распространяют фальшивый патч, якобы исправляющий вышеозначенную проблему. На деле же поддельное обновление содержит вредоносное ПО, предназначеное для хищения данных кредитных карт и другой платежной информации, пишет InternetUA.

В то время как разработчики Magento выпустили корректирующее обновление еще в феврале 2015 г., многие сайты по-прежнему работают под управлением уязвимых версий платформы (Magento CE до версии 1.9.1.1. и EE до версии 1.14.2.0.). В результате преступники получают возможность компрометации тысяч интернет-магазинов на базе Magento, отмечает исследователь ИБ-компании Sucuri Д. Синегубко.

Уязвимость SUPEE-5344 позволяет атакующим получить доступ с правами администратора на целевой системе и похитить номера кредитных карт, а также финансовую и другую конфиденциальную информацию. Помимо прочего, злоумышленники могут создавать новые фальшивые учетные записи администратора или устанавливать вредоносное ПО.

Напомним, в октябре прошлого года стало известно об атаках с использованием вредоносного ПО Guruincsite (набор эксплоитов Neutrino), осуществляемых на сайты под управлением Magento. Как удалось выяснить, все затронутые ресурсы содержали уязвимость, позволяющую удаленно выполнить код и получить доступ с правами администратора к системе.

***

16.02.2016

Хакеры захватили в заложники больничную сеть и требуют $3,6 миллиона выкупа

Компьютерная сеть в одной из больниц Лос-Анджелеса оказалась атакована хакерами. Вот уже на протяжении недели работа врачей парализована, пациентов перевели в соседние больницы, а персоналу приходится пользоваться телефонами, чтобы запросить необходимые бумажные документы, рассказывает The Verge. А хакеры тем временем требуют выкуп за освобождение сети, пишет HiTech-News.ru.

Злоумышленники обещают за 3,6 млн дол. расшифровать систему и больничные файлы. По данным западных СМИ, за последнее время это самая крупная сумма, которую затребовали хакеры. Больница не собирается идти на уступки и уже работает совместно с местным департаментом полиции и ФБР, чтобы идентифицировать преступников и освободить систему от их влияния.

В больнице отказываются рассказывать, как была инфицирована внутренняя сеть. Предполагается, что вирус проник в больничные компьютеры после того, как один из сотрудников кликнул на вредоносную ссылку или открыл вложение в письме, которое расползлось по локальной сети.

***

17.02.2016
Пользователей Facebook атаковал опасный вирус

Учетные записи в Facebook атакует новый вирус. Об этом сообщает «Русская служба новостей» со ссылкой на жалобы пользователей социальной сети, пишет InternetUA.

По словам пострадавших, вирус распространяется через систему внутренних личных сообщений Facebook. Человеку достаточно перейти по ссылке, содержащейся в сообщении, после чего его аккаунт в социальной взламывается. Позднее от имени жертвы начинают рассылать спам с такой же ссылкой.

Вредоносная ссылка рассылается как по списку друзей пользователя, так и в группы и сообщества, в которых он состоит. Пользователям, которые стали жертвами злоумышленников, рекомендуется сменить пароли на всех устройствах, через которые осуществляется выход в Facebook, а также проверить компьютеры и мобильные гаджеты на наличие вирусов.

Кроме того, в настройках Facebook нужно открыть раздел «Приложения» и удалить оттуда все незнакомые приложения.

***

17.02.2016
5 самых опасных вирусов в интернете

Разнообразие вирусных программ в Интернете не позволяет даже самым современным антивирусам полностью защитить компьютер и смартфон от кибератаки, пишет InternetUA.

В статье перечислено самое опасное вредоносное ПО, которое сейчас актуально в интернет-пространстве.

T9000

В Palo Alto Networks выявили Троян T9000 пару дней назад. Он заражает компьютеры с Windows и распространяется в формате RTF по Skype или в электронных письмах.

Для разных задач во вредоносном ПО предусмотрено несколько модулей. Первый – tyeu.dat крадет переписку и контент в Skype. Второй – vnkd.dat копирует с компьютера файлы нужных форматов. Третий – qhnj.dat открывает удаленный доступ к системе.

MazarBOT

Троян обнаружен специалистами CSIS Security Group и ориентирован на Android-устройства. Вирус передается по SMS и нацелен на кражу средств. Для этого в вирусе предусмотрена опция перехвата данных кредитных карт при расчетах с мобильного.

MazarBOT может обойти почти любую защиту интернет-банкинга. Троян запрограммирован хакерами из РФ, поэтому не крадет деньги с устройств российских пользователей.

TeslaCrypt

TeslaCrypt-вымогатель снова стал актуальным. На днях компания F-Secure обнаружила вирус в рекламе, направленной в Skype. Кроме того, инфицированная реклама появляется на ebay.it, dailymail.co.uk и игровых сайтах.

Для продвижения вируса преступники выбрали площадку AppNexus. В случае заражения при клике на рекламу, троян шифрует файлы пользователя на компьютере и требует выкуп в размере 500 дол.

Remtasu

ESET предостерегает об активности трояна Remtasu, который настроен на кражу персональных данных. Он передается в рассылке на электронную почту. Единственный способ защитить себя – не читать письма от незнакомых лиц и не смотреть прикрепленные файлы.

Adwind

У вируса испанского происхождения уникальный способ распространения в сети. Существует платформа, на которой любой мошенник может купить вредоносную программу и использовать ее для своих целей.

Этот вирус рассчитан на различные задачи. В том числе копирование и кража документов, отслеживание действий жертвы. При этом для антивирусных программ этот вирус остается незаметным.

***

16.02.2016

В продуктах Cisco обнаружены две уязвимости

Cisco опубликовала два бюллетеня безопасности, описывающих две уязвимости в продуктах компании. Речь идет об XSS-атаке в Cisco Emergency Responder и отказе в обслуживании в коммутаторах серии Cisco Industrial Ethernet 2000 Series, пишет InternetUA.

Уязвимость в Cisco Emergency Responder позволяет удаленному пользователю осуществить XSS-атаку. Код веб-фреймворка программы некорректно проверяет входные данные, позволяя злоумышленнику выполнить межсайтовый скриптинг. Уязвимость затрагивает Cisco Emergency Responder версии 11.5(0.99833.5). На момент публикации новости исправления выпущено не было.

Компания также сообщила об уязвимости в коммутаторах серии Cisco Industrial Ethernet 2000 Series. Ошибка существует из-за некорректной обработки пакетов CDP. Злоумышленник может с помощью специально сформированного пакета вызвать перезагрузку устройства.

В настоящее время способов устранения уязвимостей не существует. Возможно, исправления будут выпущены в ближайшее время.

***

17.02.2016

Тысячи устройств во всем мире могут не устоять перед новым вырусом

Эксперты обнаружили новую компьютерную уязвимость, от которой потенциально могут пострадать сотни тысяч электронных устройств, приложений и сервисов. Об этом передает Русская служба Би-би-си, пишет InternetUA.

Пока неясно, насколько серьезной является угроза. Некоторые эксперты полагают, что она может привести к катастрофе. Часть из них уверена, что с угрозой можно будет справиться.

Проблему описали в своем блоге эксперты Google. Злоумышленники могут с помощью повсеместно используемого компьютерного кода получить контроль над устройствами пользователей. Проблему обнаружили в glibc – это открытая база различных кодов, которые используются в устройствах, подключаемых к Интернету.

Этот же код лежит в основе многих языков программирования, например, PHP или Python. Это создает потенциальную угрозу для целого ряда сайтов и сервисов – хакеры могут взломать значительную часть мировых виртуальных систем или получить контроль над ними.

Инженеры Google совместно со специалистами по безопасности из Red Hat разработали программное обеспечение, способное разрешить проблему.

Проблема в том, что точно неизвестно, сколько систем и устройств используют этот код, а значит, подвержены угрозе. В зоне безопасности находятся устройства на базе Android, которые не используют эту библиотеку. Также вне зоны риска находятся операционные системы Windows и OS X.

***

18.02.2016

APT-группа Pawn Storm использует простой, но эффективный Linux-троян

Российская группировка Pawn Storm, занимающаяся кибершпионажем, инфицирует системы на базе Linux простым, но очень эффективным трояном, не требующим доступ с повышенными привилегиями. Как сообщают эксперты из ИБ-компании Palo Alto Networks, Fysbis обладает модульной архитектурой, позволяющей злоумышленникам при необходимости расширять его функционал с помощью плагинов, пишет InternetUA.

Троян может устанавливаться как с правами, так и без прав суперпользователя. Основное предназначение Fysbis – похищение данных. Даже без полного контроля над инфицированной системой вредонос способен похищать конфиденциальные документы и следить за действиями жертвы в сети. По мнению экспертов Palo Alto Networks, зачастую для достижения целей

APT-группам не нужны сверхсложные инструменты, и Fysbis – яркое тому подтверждение.

«Несмотря на устойчивую веру (и ложное чувство безопасности) в высокий уровень защищенности Linux от действий злоумышленников, вредоносное ПО для Linux все же существует и используется прогрессивными противниками», – сообщают исследователи.

Pawn Storm (также известна как Sofacy, APT28 и Sednit) – киберпреступная группировка, предположительно связанная с Россией. Основное направление деятельности – атаки на правительственные и оборонные организации по всему миру. Pawn Storm известна использованием эксплоитов для уязвимостей нулевого дня, а одним из ее главных инструментов является вредоносное ПО Sednit, предназначенное для Windows.

APT («развитая устойчивая угроза») – противник, обладающий современным уровнем специальных знаний и значительными ресурсами, позволяющими достигать целей посредством различных векторов атак.

***

18.02.2016

Злоумышленники выставили на продажу финансовые данные сотен тысяч британцев

По данным издания The Paypers, неизвестные выставили на продажу финансовую информацию о как минимум 100 тыс. жителей Великобритании. Данные о платежных картах и банковских счетах можно приобрести всего за 1,67 фунта стерлингов, пишет InternetUA.

Информация распространяется на подпольном сайте Bestvalid.cc. Ресурс функционирует как минимум с июня 2015 г., но до сих пор не привлек внимание властей либо правоохранительных органов.

Ежегодно из-за действий интернет-мошенников британской экономике наносится ущерб в размере 27 млрд фунтов стерлингов. По мнению некоторых специалистов, похищенные деньги могут использоваться, в том числе, для поддержки терроризма.

Веб-сайт продает похищенные данные вместе с дополнительной информацией, включая ответы на секретные вопросы. Сразу после получения доступа к информации злоумышленник может осуществлять покупки от имени жертвы.

По словам пресс-секретаря Национального агентства по борьбе с преступностью (National Crime Agency), ведомство регулярно обнаруживает и закрывает веб-сайты, предлагающие на продажу персональные и финансовые данные пользователей. Сотрудник агентства отказался прокомментировать ситуацию с данным сайтом.

***

18.02.2016

Сайт КременчугToday сегодня ночью подвергся хакерской атаке

Это уже не первый случай таких действий против нас со стороны злоумышленников, пишет КременчугToday.

Отметим, что атаки организовывались каждый раз, когда мы писали о незаконных действиях сильных мира сего.

То же самое произошло и в настоящее время. В последние дни мы разместили несколько статей, в которых вскрывалась деятельность партии УКРОП и владельцев Укртатнафты. В частности, о готовящихся ими в городе беспорядках.

Ночная хакерская атака направлена на то, чтобы скрыть эти статьи от читателей.

В настоящее время доступ к сайту восстановлен. Появятся и все статьи, которые так напугали кременчугских олигархов.

***

18.02.2016

Twitter обнаружила и исправила серьёзную проблему безопасности

Компания Twitter сообщила о том, что в сервисе был обнаружен баг системы восстановления пароля, из-за которого могла быть похищена информация примерно 10 тыс. пользователей, включая адреса электронной почты и телефонные номера. Баг действовал всего около 24 часов на прошлой неделе, однако сразу же после обнаружения компания его исправила. Более того, Twitter заверила, что пароли пользователей багом затронуты не были, и ни с одного аккаунта информация пока не была похищена. Также компания уведомила о проблеме всех пользователей, которые могли быть затронуты багом, пишет InternetUA.

«Мы относимся к таким инцидентам очень серьёзно, и нам очень жаль, что такое могло случиться», – написал М. Коатс, сотрудник службы безопасности Twitter. Он также добавил, что все аккаунты пользователей, которые с помощью этого бага могли получить доступ к информации других пользователей, будут заблокированы. Более того, компанией в случае необходимости будут привлекаться правовые органы для ведения расследования и наложения штрафов.

Как заявила Twitter, баг достаточно мелкий, но он может стать отличным поводом для проверки пользователями уровня защиты своих аккаунтов. В частности, в 2013 г. компания добавила в сервис систему двухфакторной аутентификации, которая при входе в Twitter запрашивает дополнительную информацию со второго устройства или из смс-сообщения. Функцию подтверждения логина можно включить в разделе безопасности в настройках сервиса.

***

18.02.2016

Новый троян для OS X способен обходить антивирусы

Исследователи компании AlienVault провели подробный анализ OS X-трояна Ocean Lotus, использовавшегося в атаках на китайские организации, пишет IGate.

Вирус обнаружили специалисты Qihoo 360 в мае 2012 г. Ocean Lotus еще с 2012 г. использовался в APT-кампаниях против правительственных организаций, исследовательских институтов и прочих компаний.

Злоумышленники распространяли троян с помощью целевого фишинга и инфицирования веб-сайтов, посещаемых жертвами. По данным исследователей Qihoo 360, в настоящее время существует примерно четыре версии Ocean Lotus, включая вариант для ОС OS X.

Специалисты AlienVault изучили два образца Ocean Lotus для OS X – раннюю версию с недостаточной функциональностью и более поздний вариант. На момент анализа последняя версия Ocean Lotus не обнаруживалась ни единым антивирусом на VirusTotal.

OS X-версия Ocean Lotus представлена в виде обновления к Adobe Flash Player. Дроппер, загружающий, дешифрующий и запускающий вредонос, выполнен в виде файла Mach-O, способного запускаться под архитектурами i386 и x86_64.

Разработчики используют шифрование XOR и технику индирекции для предотвращения обнаружения и анализа вируса. Использование специфичных для OS X команд и вызовов API позволяет судить об опытности вирусописателей.

Инфицировав систему, Ocean Lotus запускает процесс Launch Agent и пытается соединиться с C&C-сервером. Вредонос собирает базовую информацию об устройстве, включая имя компьютера, имя пользователя и уникальный идентификатор. Ocean Lotus также определяет, используются ли привилегии суперпользователя.

Вредоносное ПО способно выполнять несколько задач. Вирус может открывать наборы приложений, получать информацию о файлах, открывать список недавно открытых документов, получать данные об активных окнах, делать скриншоты, загружать файлы с интернета, запускать и прекращать работу процессов, а также удалять произвольные файлы.

***

18.02.2016

Популярные фитнес-трекеры имеют большое количество уязвимостей

С каждым годом рынок устройств «Интернета вещей» продолжает расти. Различные эксперты в сфере информационной безопасности не раз призывали

производителей сосредоточиться не только на дизайне, но и безопасности носимых гаджетов. В новом отчете исследователи общества IEEE Center for Secure Design акцентировали внимание на уязвимостях в носимых устройствах, пишет IGate.

Носимые гаджеты, в частности фитнес-трекеры, являются привлекательной мишенью для злоумышленников ввиду своей популярности и возможности хранения различных важных данных, передаваемых затем третьей стороне. По словам экспертов, значительное количество устройств подвержено разного рода уязвимостям, позволяющим осуществить SQL-инъекцию, фишинговые и CSRF-атаки, а также вызвать переполнение буфера. «Большинство атак направлены на эксплуатацию ошибок в ПО вне зависимости от используемого аппаратного обеспечения. Мы постоянно сталкиваемся с одними и теми же уязвимостями», – отмечает один из авторов отчета, главный архитектор компании NetSuite Д. Вест.

По мнению экспертов, злоумышленники могут легко перехватить данные владельцев носимых устройств или вывести гаджет из строя при помощи фальшивого обновления прошивки. Вредоносное обновление также может скомпрометировать сопряженное с фитнес-трекером устройство, например, смартфон или ноутбук.

В качестве примера можно привести фитнес-трекер FitBit Flex. Как заявила в октябре прошлого года специалист компании Fortinet А. Апврилль, злоумышленники за несколько секунд могут инфицировать систему гаджета вредоносным ПО и распространить его на любое устройство, подключаемое к FitBit Flex.

***

19.02.2016

Специалисты из «Доктор Веб» нашли троянца-»патриота»

Очередной бэкдор, обнаруженный вирусными аналитиками компании «Доктор Веб» в феврале, обладает целым рядом интересных особенностей, которые выделяют его среди аналогичных троянцев, пишет Центр Інформаційної Безпеки.

Вредоносная программа, получившая наименование BackDoor.Andromeda.1407, распространяется с помощью другого троянца-загрузчика – Trojan.Sathurbot.1, также известного под именем Hydra. Основное предназначение BackDoor.Andromeda.1407 заключается в выполнении поступающих от злоумышленников команд, в том числе скачивания и установки других вирусов.

В настоящее время вирусным аналитикам компании «Доктор Веб» известно о том, что BackDoor.Andromeda.1407 загружает и запускает на инфицированных компьютерах такие вредоносные приложения как троянец-шифровальщик Trojan.Encoder.3905, банковский троянец

Trojan.PWS.Panda.2401, троянцы Trojan.Click3.15886, BackDoor.Siggen.60436, Trojan.DownLoader19.26835 и многие другие.

Особенность бэкдора является то, что в ходе своей работы он пытается получить ряд сведений об инфицированной машине, в том числе определить разрядность ОС, ее версию, права текущего пользователя и, наконец, настроенные на атакованном компьютере раскладки клавиатуры. Если бэкдору удается обнаружить наличие в Windows русской, украинской, белорусской или казахской национальной раскладки, он завершается и автоматически удаляется из системы.

***

21.02.2016

Анализ исходного кода ОС FreeBSD выявил более тысячи серьезных ошибок

Разработчик системы статического анализа кода PVS-Studio С. Размыслов исследовал исходный код операционной системы FreeBSD на предмет потенциальных уязвимостей и некритичных ошибок. Всего эксперт обнаружил порядка тысячи серьезных предупреждений анализатора, пишет InternetUA.

С. Размыслов установил PC-BSD и написал утилиту на C++, позволяющую сохранить рабочее окружение компиляторов на момент сборки ядра. Полученную информацию специалист использовал для получения и анализа препроцессированных файлов. Подобный способ позволил исследователю провести глубокий анализ кода и найти наиболее сложные и интересные ошибки.

В ходе анализа кода было обнаружено множество опечаток, одинаковых фрагментов и прочих ошибок в исходном коде операционной системы. Исследователь сообщил о найденных неисправностях разработчикам FreeBSD. На момент написания новости создатели операционной системы приступили к устранению найденных ошибок.

***

21.02.2016

В прошивках нескольких видеорегистраторов обнаружены неизменяемые пароли

Более 80 тыс. цифровых видеорегистраторов, используемых для записи данных с камер наблюдения, поставляются с неизменяемыми или даже отсутствующими паролями. Как сообщается в отчете компании Risk-Based Security, большинство устройств видеозаписи содержат как минимум одну уязвимость, позволяющую злоумышленникам получить доступ к конфиденциальной информации, пишет InternetUA.

В качестве примера эксперты Risk-Based Security привели цифровые видеорегистраторы Zhuhai RaySharp. Устройства используют неизменяемые

логин «root» и пароль «519070». Проблема безопасности была обнаружена еще в 2015 г., но разработчик до сих пор не выпустил исправленную версию прошивки. Используя поисковик устройств Shodan, исследователи Risk-Based Security обнаружили примерно 46 тыс. уязвимых видеорегистраторов.

Для аутентификации пользователя используется функция main() в специальном CGI-сценарии. Введенные данные сверяются с логином/паролем «root/519070». Если информация совпадает, пользователю предоставляется полный доступ к веб-интерфейсу.

Уязвимость была обнаружена в сентябре 2015 г. В декабре 2015 г. производитель пообещал выпустить исправление, но до сих пор никаких шагов предпринято не было.

Аналогичная проблема была обнаружена в регистраторах Mvpower 8. Устройство не требовало какого-либо пароля для доступа к веб-интерфейсу. Уязвимость обнаружили исследователи PenTestPartners. С помощью Shodan было обнаружено примерно 40 тыс. устройств с проблемой безопасности.

***

21.02.2016

Мошенники активно эксплуатируют недооцененную уязвимость в платформе eBay

Как сообщают эксперты компании Netcraft, частично исправленная в начале февраля уязвимость в eBay активно эксплуатируется злоумышленниками для осуществления фишинговых атак и мошенничества с продажей автомобилей, пишет InternetUA.

В начале текущего месяца исследователи из Check Point раскрыли подробности о серьезной ошибке в online-платформе eBay. Уязвимость позволяет обойти фильтры eBay, отвечающие за проверку кода. Злоумышленник может открыть якобы легитимную страницу и добавить в поле описания товара вредоносный JavaScript-код.

Исследователи продемонстрировали, как мошенники могут обманным путем заставить пользователя предоставить свои учетные данные на фишинговой странице или загрузить вредоносное ПО из вредоносного магазина eBay. Поскольку фишинговые страницы связаны с легитимным доменом ebay.com, у жертвы не возникает никаких подозрений.

По словам представителей eBay, с учетом результатов исследований Check Point в платформе были реализованы фильтры безопасности, однако вредоносный контент – крайне редкое для eBay явление. Если верить компании, какая-либо вредоносная активность с эксплуатацией уязвимости обнаружена не была.

Как оказалось, принятые eBay меры не помешали злоумышленникам воспользоваться данной ошибкой. Эксперты компании Netcraft зафиксировали несколько лотов, предназначенных специально для эксплуатации уязвимости.

По словам исследователей, злоумышленники внедряют вредоносный код в скомпрометированные учетные записи.

В ходе одной из атак мошенники скопировали контент настоящей страницы eBay с описанием проданного тремя месяцами ранее трейлера и опубликовали его в скомпрометированном магазине. Заинтересовавшиеся лотом пользователи сразу же перенаправлялись на сайт, выглядевший как eBay.

На поддельном сайте трейлер, на самом деле продававшийся по цене £19295, предлагался вс его за£6,3. В данном случае злоумышленников не интересовали учетные данные пользователей. Их целью было заработать на мошеннической продаже. После нажатия на «Купить сейчас» жертве предлагалось оставить электронный адрес. Мошенники связывались с потенциальным покупателем для обсуждения условий сделки и обманным путем заставляли его перевести деньги, якобы в качестве оплаты за покупку.

***

21.02.2016

Обнаружен способ раскрытия данных на неподключенных к интернету компьютерах

Израильские исследователи безопасности обнаружили способ взлома неподключенных к Интернету компьютеров. Эксперты смогли похитить криптографические ключи, измеряя электромагнитное излучение компьютера во время расшифровки данных, пишет InternetUA.

Специалисты использовали способ осуществления атаки, известный как «атака по стороннему каналу». Исследователи получили приватный ключ компьютера с помощью GnuPG, а в дальнейшем измерили электромагнитное излучение целевого ПК. В течение нескольких секунд экспертам удалось получить секретный ключ, позволяющий расшифровать данные.

По словам исследователей, для осуществления атаки необходимо приобрести оборудование стоимостью в примерно 3 тыс. дол. Физическое вмешательство в работу компьютера – например, отсоединение крышки корпуса – не требуется.

Как сообщается в протоколе исследования, во время расшифровки измерялось электромагнитное излучение целевого ПК. Эксперты фокусировались на узком диапазоне частот. После обработки сигналов был получен «четкий след, раскрывающий информацию об операндах, используемых в эллиптической криптографии». Используя найденные данные, исследователи смогли раскрыть секретный ключ.

Для раскрытия ключа понадобилось провести 66 операций дешифровки длительностью в 0,05 секунд каждая. Общее время, необходимое для получения данных, составило 3,3 секунды. Отметим, исследователи имели в виду время вычислительных операций, а не время, необходимое для осуществления подобной атаки.

***

21.02.2016

Новый тренд в области DDoS-атак: хакеры стали использовать протокол DNSSEC

Специалисты компании Akamai зафиксировали новую тенденцию в области усиленных DDoS-атак: теперь хакеры все чаще используют для этих целей протокол DNSSEC, пишет InternetUA.

В отчете компании сказано, что в период с ноября 2015 г. и до текущего момента, было зафиксировано более 400 отраженных DNSSEC-атак. Злоумышленники преимущественно используют домены в правительственной зоне .gov, дело в том, что в США такие домены обязаны поддерживать DNSSEC по закону.

Хотя протокол DNSSEC может защитить от доменного хакинга, он одновременно является и уязвимым местом, которое удобно эксплуатировать для DDoS. Все дело в стандартном ответе DNSSEC, который, помимо обычных данных о домене, содержит также множество связанной с аутентификацией информации. Так, стандартный ответ DNS имеет объем 512 байт, тогда как ответ DNSSEC, в зависимости от конфигурации, может достигать 4096 байт в объеме.

Специалисты Akamai пишут, что атакующие не используют какие-то особенные новые техники, в целом атаки построены по давно известным схемам. Но перенаправление весьма «тяжелых» ответов DNSSEC на IP-адреса жертв – это новая тактика, позволяющая злоумышленникам усилить атаку приблизительно в восемь раз. Средняя мощность такой атаки составляет 123,5 Гбит/сек.

В основном DNSSEC-атаки направлены против игровой индустрии и финансового сектора.

***

21.02.2016

Исходный код банковского трояна для Android утек в сеть

Команда IBM X-Force предупреждает: в ближайшее время банковской малвари для Android должно стать больше. В открытый доступ попали исходные коды трояна GM Bot, на базе которого были созданы такие небезызвестные вредоносы, как SlemBunk, Bankosy и Mazar BOT, пишет InternetUA.

Эксперты разных компаний давно отмечают некоторое сходство банкеров SlemBunk, Bankosy и Mazar BOT. Оказывается, данные вредоносы действительно имеют общие корни – все они происходят от трояна GM Bot, который аналитики IBM отслеживали с 2014 г.

Сообщается, что GM Bot был создан неким русскоговорящим хакером и распространялся на андеграундных форумах, где продавался по цене примерно 500 дол. за копию. Троян также известен под названиями Acecard и Slempo.

Однако оригинальный автор малвари решил оставить разработку и заняться другими проектами (слухи утверждают, что он работает над созданием GM Bot v2.0). Но бросать GM Bot на произвол судьбы он при этом не стал, продав права на троян последней версии (v1, которая больше известна как Mazar BOT) другому хакеру.

Покупателем вредоноса оказался администратор некого подпольного форума, который стал распространять исходные коды малвари среди зарегистрированных пользователей своего ресурса в качестве награды. Исходники были опубликованы в виде защищенного паролем архива, а пользователи форума могли написать личное сообщение администратору и попросить пароль.

Разумеется, вскоре все пошло не так. Пользователи начали передавать пароль от архива друг другу в обход админа, и совсем скоро исходный код Mazar BOT был опубликован открыто уже повсюду.

Специалисты IBM полагают, что в самом скором будущем стоит ждать резкого прироста в семействе банкеров для Android. Как показывает практика, после утечки исходников какой-либо малвари в открытый доступ, аналоги начинают множиться, как грибы после дождя. Яркие тому примеры – утечки исходного кода Zeus, SpyEye или недавняя история с опенсорсной малварью Hidden Tear и EDA2.

***

20.02.2016

26 000 сайтов на базе WordPress используются для Layer 7 DDoS-атак

Эксперты компании Sucuri сообщили, что сайты под управлением WordPress вновь подвергаются массовым кибератакам. На этот раз против ресурсов на базе популярной CMS проводятся Layer 7 DDoS-атаки, которые к тому же эксплуатируют функцию pingback и генерируются ботнетом из… WordPress-сайтов, пишет InternetUA.

В отличие от обыкновенных DDoS-атак, атаки Layer 7 осуществляются на уровень приложений. То есть злоумышленники занимаются не ковровой бомбардировкой, а действуют прицельно и не задействуют при этом больших мощностей. Так, пакеты, созданные специальным образом, приводят к повышению нагрузки на CPU сервера до таких значений, что сайт жертвы эффективно выходит из строя.

Проблема с функцией pingback в WordPress и вовсе не нова. Давно известно, что ее можно использовать для осуществления DDoS-атак. Несколько лет назад разработчики CMS даже попытались исправить проблему, представив в версии 3.9 инструмент, позволяющий вести логи pingback-запросов. Теоретически, это должно помочь администраторам сайтов быстро определить

IP-адреса атакующих и добавить в их черный список. На деле этим мало кто пользуется.

Теперь эксперты компании Sucuri зафиксировали кампанию, сочетающую в себе обе вышеописанные техники. Более 26 тыс. сайтов на базе WordPress объединились в ботнет и атакуют другие ресурсы, функционирующие под управлением данной CMS. Ботнет генерирует порядка 10000–20000 HTTPS-запросов в секунду, направляя свои усилия против сервиса WordPress XML-RP. В итоге сайт жертвы задыхается под валом pingback-запросов. Сервер, на котором располагается сайт, вынужден выделять атакуемому сайту все больше ресурсов CPU и памяти, так как поддержание такого количества зашифрованных соединений – дело нелегкое.

Специалисты Sucuri пишут, что защититься от атак на XML-RPC можно не только установив патч для pingback, но и правильно настроив фильтрацию. Подробные инструкции были опубликованы в блоге компании.

***

20.02.2016

Российских хакеров обвинили в атаках на сайты сирийской оппозиции

Источники американской разведки рассказали о том, что российские хакеры атакуют сайты сирийской оппозиции и правозащитных организаций. Об этом пишет InternetUA со ссылкой на газету Financial Times.

По словам главы ближневосточного и европейского отделений организации FireEye Р. Тренера, число атак хакерской группы, которую называют APT 28, с начала года стало увеличиваться.

«APT 28 и другие российские группы действительно сосредоточили свое внимание на сборе данных о сирийских группах, в частности на тех, которые связна с областью прав человека и мониторинга российской военной активности», – заявил Р. Тернер.

Как пишет газета, атаки подразумевают под собой рассылку писем с вредоносными вложениями пресс-релизов и официальных сообщений.

***

22.02.2016

Появилась версия трояна Gozi для Windows 10

Специалисты IBM обнаружили модифицированную версию банковского трояна Gozi, нацеленную на пользователей ОС Windows 10. Вредонос поражает Microsoft Edge – браузер по умолчанию в новой оперативной системе, призванный заменить устаревший Internet Explorer, пишет InternetUA.

Вирусописатели смогли использовать устаревший метод инъекции кода для работы с браузером Microsoft Edge. Троян поражает основной процесс обозревателя MicrosoftEfgeCP.exe.

Gozi – один из старейших функционирующих банковсских троянов. Вредонос был создан в 2007 г. Злоумышленники раскрыли исходный код трояна в 2010 г. Тогда же злоумышленники начали применять вторую версию Gozi в массивной мошеннической кампании против американских банков. В 2013 г. Gozi получил возможность внедряться в сектор MBR жесткого диска, а на протяжении последнего года вирусописатели добавили в троян улучшенные возможности по веб-инъекции.

В версии для Windows 10 Gozi использует ряд хуков в kernel32.dll для внедрения кода в браузер. Троян также проникает в процесс RuntimeBroker.exe – родительский процесс Edge и внедряет код в explorer.exe. Обновленная версия Gozi способна работать и с другими браузерами, включая Internet Explorer, Chrome, Opera и Firefox.

***

22.02.2016

Взломанная версия Linux Mint была выставлена на сайте разработчиков

Скачавшие 20 февраля на официальном сайте операционную систему Linux Mint пользователи рискуют стать обладателями взломанного варианта. В блоге на сайте Linux Mint говорится, что хакеры взломали сайт и поместили там модифицированный образ Linux Mint ISO с бэкдором внутри. Использование этой версии может стать причиной утечки персональных данных. Взломанной является версия Linux Mint 17.3 Cinnamon, скачанная непосредственно с сайта, пишет InternetUA.

Бэкдоры представляют значительную угрозу конфиденциальности, позволяя хакерам или спецслужбам получать доступ к данным без ведома пользователей. В блоге указаны инструкции, по которым можно понять, какую версию системы вы скачали. Если взломанную, то её следует удалить из компьютера и с носителей.

Если эта версия была установлена, её также следует удалить. Отключившись от сети, нужно выполнить резервное копирование персональных файлов, а после удаления установить безопасную версию системы. Для безопасности можно сменить пароли на используемых сайтах и сервисах.

Также было сказано, что хакеры сумели добраться и до базы данных форума, так что при наличии учётной записи следует сменить пароль в ней и на всех других сайтах, где использовался тот же пароль. Именно по этой причине на всей сайтах и сервисах рекомендуется использовать разные пароли.

***

22.02.2016

Android стала одной из наиболее часто атакуемых платформ в 2015 году

Операционная система Android стала одной из наиболее часто атакуемых платформ в 2015 г., уступив первенство Microsoft Windows. Согласно отчету компании Hewlett Packard Enterprise, на долю Microsoft Windows пришлось 42 % от общего количества зафиксированных в 2015 г. атак, Android – 18 %, Oracle Java и Microsoft Office – 12 % и 11 % соответственно, пишет InternetUA.

Android также стала второй по количеству вредоносного ПО, разработанного для данной системы – в 2015 г. эксперты обнаружили 4,5 млн новых вредоносов. Лидером по-прежнему остается Windows, на долю этой платформы пришлось 94 % вредоносных программ.

Чаще всего в прошлом году злоумышленники использовали Android-трояны, предназначенные для установки нежелательного ПО, перехвата смс-сообщений или хищения персональной информации пользователей. К примеру, специалисты компании «Доктор Веб» обнаружили Android-троян, способный по команде злоумышленников похищать конфиденциальные данные пользователей, отправлять смс-сообщения, совершать звонки и выполнять другие опасные действия.

Согласно отчету Hewlett Packard Enterprise, ежедневно исследователи выявляют более 10 тыс. новых Android-угроз. Однако опасности подвергаются не только владельцы устройств на базе Android. В 2015 г. зафиксировали рост числа вредоносного ПО для iOS на 235 %. В общей сложности в указанный период было обнаружено порядка 70 тыс. вредоносов.

***

23.02.2016

Ажиотаж вокруг эпидемии вируса Зика используется для распространения вредоносного ПО

Специалисты Symantec предупредили о вредоносной спам-кампании, использующей ажиотаж вокруг эпидемии вируса Зика для распространения вредоносного ПО. В настоящее время кампания в основном нацелена на пользователей из Бразилии, пишет InternetUA.

В ходе кампании злоумышленники рассылают письма от имени популярного в Бразилии веб-сайта Saúde Curiosa («Занимательное здоровье»), посвященного вопросам здорового образа жизни. Для усыпления бдительности пользователей письмо содержит изображения и текст настоящей статьи издания, а также несколько ссылок якобы на загрузку инструкции по действию в чрезвычайных ситуациях, ведущих на файлообменник Dropbox.

Помимо ссылок, сообщение также включает прикрепленный документ. Как выяснили исследователи, файл в Dropbox и документ в письме содержат троянскую программу JS.Downloader. Оказавшись на системе, вредонос пытается загрузить дополнительное вредоносное ПО. По данным Symantec, переход по ссылкам уже осуществили 1610 пользователей.

Это не первый раз, когда злоумышленники спекулируют на обеспокоенности общества по поводу эпидемий, вызванных различными вирусами.

***

24.02.2016

Посетители MWC 2016 попали в «хакерскую» ловушку Avast

Компания Avast Software, знаменитая своим одноименным антивирусным программным обеспечением, провела своеобразный «хакерский» эксперимент в аэропорту Барселоны. За день до старта выставки через этот аэропорт прошли тысячи людей, прилетевших на выставку Mobile World Congress 2016. Целью Avast была демонстрация того, насколько пользователи подвергают себя риску при пользовании публичными Wi-Fi-точками, пишет InternetUA.

Конечно, по прибытии многие желают сразу же войти в Интернет, желательно бесплатный, и сообщить коллегам или родным радостную новость, посетить социальные сети и любимые сайты. И о безопасности при этом мало кто задумывается. А зря! Для эксперимента специалисты Avast развернули несколько Wi-Fi-точек доступа с SSID-идентификаторами Starbucks, Airport_Free_Wifi_AENA и MWC Free WiFi. Для SSID специально выбраны имена, не вызывающие подозрения. И на эту уловку «клюнули» практически все. Причем часто мобильные устройства настроены на автоматическое подключение к общедоступным сетям, а пользователи даже не просматривают, куда они подключились – главное, что есть Интернет. А тем временем злоумышленники могут перехватывать все передающиеся данные.

Всего за четыре часа специалисты Avast перехватили более 8 млн пакетов данных от более 2 тыс. пользователей. Для сохранения приватности пользователей все данные сразу же удалялись. Компании удалось собрать интересную статистику в ходе эксперимента:

– 50,1 % пользователей использовали устройство Apple, 43,4 % – гаджет под управлением Android, 6,5 % – устройства с Windows Phone;

– 61,7 % посетителей выставки занимались поиском в Google и проверяли свою почту Gmail;

– 14,9 % воспользовались поиском Yahoo;

– приложение Facebook было установлено на 52,3 % устройств, а Twitter оказался менее популярен – всего 2,4 %.

Как отметили эксперты, многие знают о том, что открытая Wi-Fi-сеть таит в себе опасности. Но на практике они не задумываются о том, что их устройство может самостоятельно подключиться к уязвимой сети. Кроме того, из-за желания сэкономить часто пользователи отказываются от сервисов роуминга. В таком случае Avast советует хотя бы использовать, где это возможно, VPN-соединение. Кстати, на своём стенде Avast демонстрирует посетителям, что может быть доступно хакеру при незащищённом

подключении к сетям Wi-Fi. И, очевидно, будет рекламировать свои продукты для защиты.

***

26.02.2016

Google открыл доступ к сервису защиты от DDOS-атак

IT-гигант Google официально открыл доступ к сервису защиты от DDOS-атак – проекту «Щит». Платить за пользование сервисом администраторам сайтов не надо, достаточно заполнить специальную форму и предоставить Google информацию о своем ресурсе, пишет МедиаБизнес.

Как сообщается в блоге компании, Project Shield фильтрует сетевой трафик и, используя собственные алгоритмы, пропускает только обычные запросы. Также сообщается, что при возрастании количества запросов сервис будет показывать пользователям кэшированную копию сайта, чтобы снизить нагрузку на свой сервер. Инструмент призван защитить от DDOS-атак прежде всего сайты СМИ, однако может быть использован всеми, кто «публикует то, что другие могут счесть нецелесообразным». В компании отметили, что сервис может несколько замедлить посещаемость защищенных сайтов.

***

29.02.2016

В 2015 году из-за уязвимостей были отключены более 80 тыс. компонентов Smart Grid

На сегодняшний день в области мировой электроэнергетики полным ходом идет процесс внедрения «интеллектуальных сетей» Smart Grid. Количество Smart Grid-девайсов, подключенных к Интернету без какой-либо защиты, растет лавинообразно. Согласно данным SCADASOS, в 2015 г. в связи с множественными уязвимостями от сети было отключено более 80 тыс. компонентов Smart Grid, пишет InternetUA.

SCADASOS – некоммерческая инициатива, предназначенная для повышения осведомленности о проблемах «умных» сетей. Организаторы инициативы, эксперты команды SCADA StrangeLove призывают всех желающих искать уязвимости в компонентах Smart Grid и сообщать о них производителям.

Согласно данным специалистов, в рамках программы были обнаружены множественные уязвимости по крайней мере в четырех продуктах производства RLE International GmbH, IBC Solar, Tollgrade Communications и SMA Solar Technology AG.

В частности, независимый исследователь М. Рупп обнаружил уязвимость в HMI-интерфейсе Nova-Wind Turbine от RLE International GmbH, связанную с ненадежностью идентификаторов в интерфейсе. Завладев ID, злоумышленник может выполнить любое действие на устройстве.

Еще одна уязвимость была обнаружена в системе управления солнечными батареями SMA Solar Sunny WebBox от SMA Solar Technology AG. Уязвимость возникла в связи с использованием неизменяемых паролей, установленных по умолчанию. Эксплуатация проблемы позволяет удаленному атакующему получить полный доступ к системе. Уязвимости подвержены все версии SMA Solar Sunny. Согласно бюллетеню безопасности ICS-CERT, производитель планирует снять продукт с производства и больше не намерен выпускать обновления безопасности для предыдущих версий системы.

***

28.02.2016

Обнаружен вариант трояна-шифровальщика CTB-Locker для web-сайтов

После нескольких месяцев относительного затишья вредоносное ПО CTB-Locker, также известное как Critroni, снова появилось в поле зрения ИБ-экспертов. Исследователи обнаружили новый вариант трояна и назвали его «CTB-Locker для веб-сайтов». В отличие от более ранних версий, шифрующих файлы на компьютерах жертв, данная разновидность шифрует контент интернет-ресурсов, пишет InternetUA.

Как сообщил владелец сайта BleepingComputer ИБ-эксперт Л. Абрамс, злоумышленники компрометируют серверы хостинг-провайдеров и заменяют оригинальный index.php или index.html новым index.php. Новый index.php используется для шифрования данных на сайте с помощью 256-битного алгоритма AES и отображения новой домашней страницы с требованием выкупа за расшифровку.

По подсчетам Л. Абрамса, в настоящее время «CTB-Locker для веб-сайтов» инфицировал свыше 100 ресурсов. Пик активности оригинального CTB-Locker для Windows пришелся на 2014 г., и сейчас он не столь популярен, как шифровальщики TeslaCrypt, CryptoWall и Locky. По мнению исследователя, новому варианту трояна не удастся снискать славу своего предшественника, поскольку у данных на сайтах всегда есть резервные копии, позволяющие с легкостью их восстановить без уплаты выкупа.

Как сообщил Л. Абрамс, ошибки, эксплуатируемые для заражения сайтов CTB-Locker, остаются неизвестными. Эксперт не исключает возможности инфицирования ресурсов с помощью уязвимостей в WordPress.

***

26.02.2016

Раскрыта крупнейшая кибератака в истории Google Play

Крупнейшую в истории магазина приложений Google Play кибератаку раскрыли специалисты компании ESET. Разработчики антивирусного

программного обеспечения заявляют, что от трояна-порнокликера Android/Clicker пострадали более миллиона пользователей, пишет InternetUA.

Семь месяцев и 343 модификации

Кибератаки с применением Android/Clicker начались около семи месяцев назад. По словам экспертов, в магазине приложений было обнаружено 343 модификации трояна-порнокликера, а количество скачиваний вредоносного ПО превысило 1,2 млн.

Эксперты добавляют, что систему безопасности магазина приложений Google Bouncer ежедневно обходило около десятка версий порнокликера. В среднем каждое приложение загружалось 3600 раз, рекордсмены – до 500 тыс. раз.

Как работает троян

Android/Clicker маскируется под игры и другие легитимные приложения. Чаще всего это GTA San Andreas Free, Subway Surfers 2015, Dubsmash 2, My Talking Tom v2.

После установки вредоносное программное обеспечение генерирует трафик на «сайты для взрослых». Операторы трояна за счет увеличения количества обращений получают доход. Владельцы зараженных Android-устройств в свою очередь могут получить огромный счет за мобильный Интернет.

Мы наблюдали ряд кампаний по распространению вредоносного ПО на Google Play, но ни одна из них не продолжалась так долго и не привела к такому числу заражений. Л. Стефанко, вирусный аналитик ESET

Как защититься

Чтобы не стать жертвой киберугрозы, специалисты рекомендуют установить на Android-девайс качественный антивирус и регулярно обновлять его. Перед загрузкой программ из Google Play стоит прочитать отзывы и объективно оценить рейтинг приложения – низкие оценки и негативные комментарии предупредят о том, что ПО может быть небезопасным.

***

25.02.2016

Обнаружен способ осуществления атаки на беспроводные клавиатуры и мыши

Исследователи компании Bastille Network обнаружили способ атаки на беспроводные мыши и клавиатуры, использующие для передачи данных USB-донглы. По утверждению специалистов, атакующий может перехватывать пакеты, отсылаемые на компьютер, и отправлять произвольные команды, находясь на расстоянии до 100 м от целевого ПК. К данному способу атаки уязвимы беспроводные устройства, не использующие Bluetooth для передачи данных, пишет InternetUA.

Обычно беспроводные клавиатуры и мыши, не использующие Bluetooth, передают данные на частоте 2.4 ГГц в частотном диапазоне ISM (предназначен

для работы промышленных и медицинских устройств). Поскольку единого протокола для работы подобных продуктов не существует, каждый производитель может создавать собственные реализации работы беспроводных устройств.

Исследователи проверили работу клавиатур и мышей производства Lenovo, Dell и Logitech. Как выяснилось, большинство беспроводных мышей передают данные на донгл без какого-либо шифрования. Как результат, в работе устройств отсутствует аутентификация, и злоумышленник может с помощью сторонних пакетов управлять работой мыши.

Эксперты изучили работу популярного среди производителей приемника Nordic Semiconductor nRF24L и создали программу, позволяющую в автоматическом режиме осуществлять атаки на беспроводные устройства. В результате исследователи обнаружили три наиболее распространенных вида атаки:

1. Инъекция нажатий подменной мышью или клавиатурой

Некоторые донглы не сверяют тип полученной команды с типом передающего устройства. В результате злоумышленник может с помощью стороннего устройства отправить незашифрованные пакеты на донгл жертвы.

2. Принудительное сопряжение устройств

Обычно на производстве донглы сопряжены с клавиатурой или мышью. Некоторые производители допускают добавление новых устройств к передатчику. Проэксплуатировав данную функцию, злоумышленник может принудительно спарить эмулируемую клавиатуру с донглом жертвы.

***

20.02.2016

Кибервойна: зачем государствам армии хакеров?

Государства уже давно воюют и шпионят друг за другом в Интернете. Самыми активными на этом поприще традиционно считают Россию, Китай и США. Итак, что можно поломать через Интернет?

Гонка кибервооружений с каждым годом набирает обороты: Россия готовится в 2016 г. обновить доктрину кибербезопасности (и, якобы, потратить 250 млн дол. на кибероружие), страны под эгидой ООН собираются подписать «пакт об электронном ненападении», а кибервойсками обзаводятся не только гиганты вроде Китая, но даже такие небольшие государства, как Грузия, пишет Inshe.tv.

Почему это важно? Казалось бы, убить человека через Интернет сложновато, а именно убийства – основной атрибут современных войн. Кибервойны – другие, но не менее разрушительные.

Что такое «кибервойна»?

В самом грубом смысле, кибервойна – это использование противоборствующими сторонами компьютеров и средств связи для саботажа, дестабилизации или полного разрушения критической инфраструктуры

противника. Ну, и о шпионаже, а также дезинформации противника (а также «информационной войне», но это большая отдельная тема) в рамках кибервойн забывать не следует.

Что можно поломать через Интернет?

«Поломать» можно очень многое, причем цели не обязательно должны быть подключены к сети.

Самое простое – через Интернет можно «поломать» сам Интернет в отдельно взятой стране или регионе. Мощная атака способна заблокировать сегменты телекоммуникационной сети в стране, а то и всю сеть. А это значит проблемы со связью по всей стране, паралич банковской системы (часть ее работает через Интернет) и экономики в целом.

Еще можно нападать на важные объекты, например, хакеры часто атакуют банки (как их сайты, так и внутренние сети), правительственные учреждения (например, в Украине атаковали Центризбирком) или объекты инфраструктуры – например, дамбу в США или электростанцию. К слову, отключение электроэнергии в Украине в декабре 2015 г. списали именно на кибератаку).

Даже если интересующие нападающих объекты к Интернету напрямую не подключены, это не проблема: всегда можно через Интернет забросить, например, вирус одному из сотрудников электростанции, а он, может быть, потом занесет его физически – на флешке, например, в компьютеры внутренней сети.

Кстати, по такой схеме работал знаменитый вирус Stuxnet, который, похоже, был специально создан для уничтожения ядерных центрифуг иранской ядерной программы, и преуспел в этом. Через сеть ошибок в программах он проникал в систему управления и отправлял двигателям центрифуг команды, приводившие к выходу тех из строя. По оценкам эксперта, это отбросило ядерную программу Ирана на два года назад.

Не так давно хакеры сообщали о взломе «умных» машин (перехват управления) и даже самолетов (последнее, правда, под большим вопросом). Даже если организации не имеют выхода в Интернет, но при этом используют компьютеры или мобильные телефоны, они уязвимы.

Как вообще эти все взломы происходят?

Как правило, через ошибки в программах (например, Windows). Если ошибка не исправлена (вот почему важно ставить обновления!) ей можно воспользоваться, чтобы удаленно, через Интернет, проникнуть в систему и запустить на ней любую программу. Ну а дальше – дело техники.

Часто хакеры массово заражают компьютеры для создания «ботнетов» (огромных групп «компьютеров-зомби»). На эти компьютеры устанавливается программа, позволяющая управлять ими удаленно, и после этого «засыпает» в ожидании команд из центра.

«Центр», как правило, использует такие компьютеры для организации DDoS-атак («распределенная атака типа «отказ в обслуживании»). В этом случае не нужно искать уязвимости и писать вирусы – все достигается грубой

силой. Компьютеры-зомби бомбардируют жертву (тот или иной сайт) «мусорными» интернет-запросами, на которые ей приходится отвечать.

Представьте, что на сайт, рассчитанный на обработку 10 запросов от пользователей в секунду, внезапно обрушивается лавина из 1000 запросов в секунду. Обычно это приводит к резкому замедлению работы, а затем компьютеры и сетевое оборудование просто «сходят с ума».

Железо можно «убить» удаленно. А человека?

Не так давно хакеры показывали способы взлома электронных капельниц и кардиостимуляторов. Но эти методики пока достаточно ограниченные.

Для массового убийства людей потребуется удаленно устроить аварию на каком-то крупном объекте: атомной электростанции, химзаводе и т. п.

А такое случалось? Вооют ли уже государства в Интернете?

Пока, к счастью, об инцидентах, явно спровоцированных кибератаками и повлекших гибель множества людей (или даже отдельных людей), неизвестно.

Есть два «но». Первое – если таковые и были, они вполне могли не попасть в прессу. Второе – учитывая темпы компьютеризации, вероятность подобных ситуаций в будущем только растет.

Государства уже давно воюют и шпионят друг за другом в Интернете, правда, об открытой войне речи все-таки не идет. Самыми активными на этом поприще традиционно считают Россию, Китай и США.

Хотя страны время от времени обвиняют друг друга в кибератаках, надо понимать, что все эти обвинения во многом голословны – из-за природы Интернета невероятно сложно определить, кто заказал ту или иную DDoS-атаку или написал хитроумный вирус. Тем не менее, о кибервойнах иногда объявляют: например, хакеры группировки Anonymous объявили войну «ИГ».

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Касаткіна** Тетяна

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.