СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(18–31.07)

2016 № 10

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(18–31.07)
№ 10

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

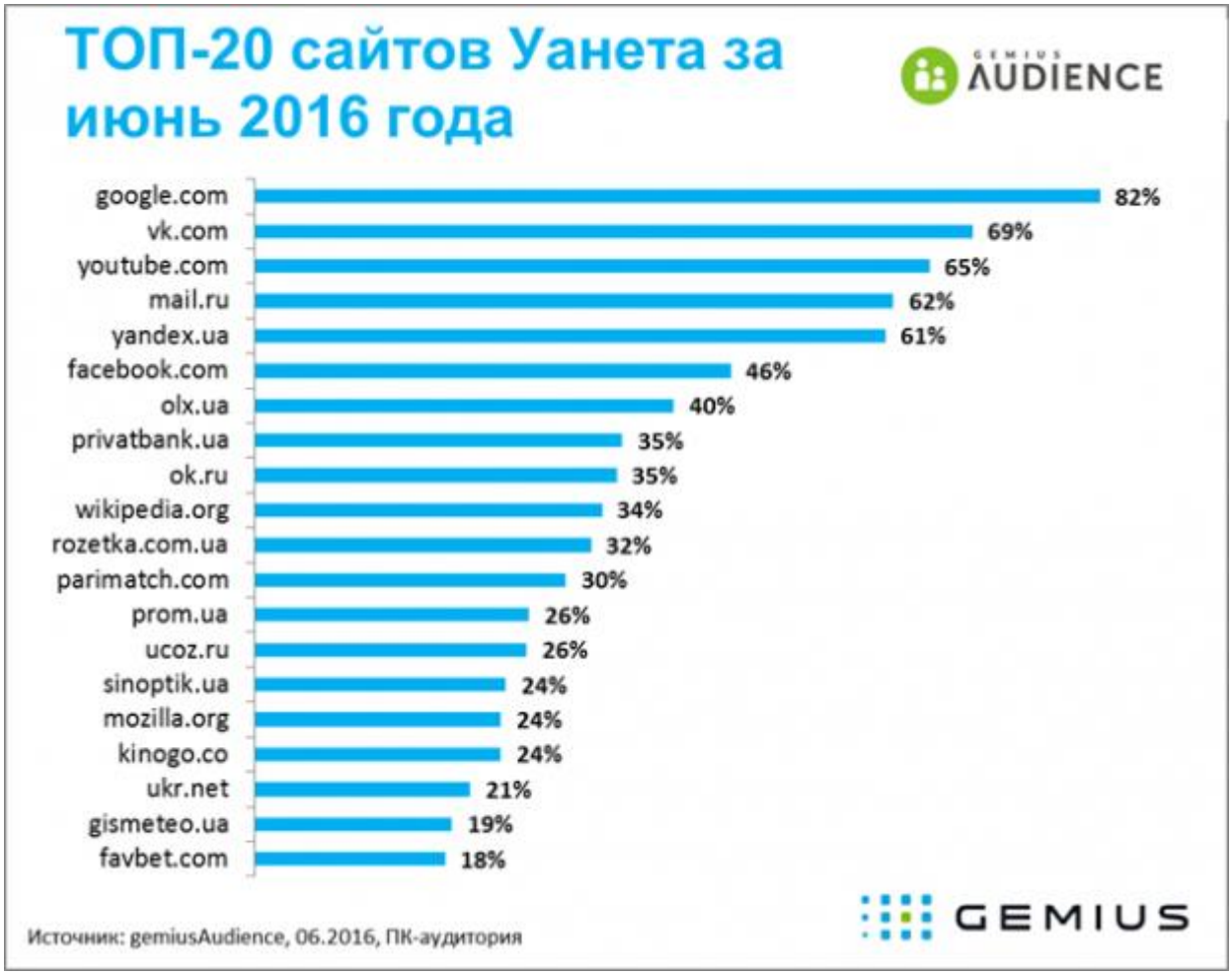
Київ 2016

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

19.07.2016
20,2 млн українців хоча б раз на місяць користуються Інтернетом

У червні 20,2 млн українців щонайменше раз на місяць користувались Інтернетом. Такими є результати дослідження компанії Gemius за минулий місяць, пише UkrainianWatcher.



Окрім того, до трійки сайтів-лідерів за показником відвідуваності, як і раніше, увійшли Google, «ВКонтакте» та YouTube. У червні пошуковиком Google скористались 15 млн користувачів (82 % усієї інтернет-аудиторії України). Друга позиція дісталась соцмережі «ВКонтакте» (69 %), третя – відеохостингу YouTube (65 %).

У ТОП-20 сайтів уанету відбулись зміни: сайт Parimatch.com піднявся на 6 позицій, Ukr.net та Gismeteo.ua – на одну. Favbet.com, Kinogo.co, Mozilla.org і Sinoptik.ua опустилися в рейтингу. У першій десятці змін немає.

***

26.07.2016

Удовлетворенность пользователей социальными медиа упала, особенно Facebook

По данным нового исследования American Customer Satisfaction Index, удовлетворение пользователей категорией социальных медиа упала на 1,4 % до 73 % по сравнению с прошлым годом. Facebook потерял 9 % до 68 %, Twitter упал на 8 % до 65 %. Единственными, кто улучшил свои показатели, были Wikipedia, YouTube и Google+, каждый из них возрос на 1 %. Удовлетворенность Pinterest и Instagram упала на 3 % до 76 % и 74 % соответственно. LinkedIn потеряла 4 %, пишет Marketing Media Review.

По данным ASCI, падение Facebook было вызвано манипуляциями с лентой новостей и подозрениями в том, что сеть подавляет консервативный контент, а на Twitter повлиял отказ от хронологической ленты. Пользователи высоко оценили социальные медиа с позиции простоты навигации и пользования на мобильных девайсах, но исследование обнаружило, что респонденты не довольны свежестью контента, вопросами приватности и количеством рекламы.

***

20.07.2016

В Украине запущена социальная сеть для встреч по интересам

Команда украинских стартаперов запустила социальный сервис Wooower, призванный объединить людей с общими интересами для последующих встреч в реальной жизни, пишет IGate.

Идея создания такого проекта родилась у 3D-дизайнера В. Чувашова несколько лет назад, когда тот столкнулся с дефицитом живого обмена опытом в профессиональной области.

На разработку настольной и мобильной версии сервиса команде понадобилось около 2 лет и чуть более 35 тыс. долл. Отдельного приложения Wooower пока нет.

«Чтобы воспользоваться поиском компании для совместного времяпровождения, достаточно указать то чем вы собрались заняться, привязав ее к месту на карте и роду занятий (к примеру, путешествия). Это займет не более 30 секунд», – рассказывает В. Чувашов – «С этого момента предложенная “активность” будет видна другим пользователям, в первую очередь тем, кто сам находится поблизости и интересуется подобной темой».

В настоящее время функционал позволяет добавлять два типа событий: «Активность» (сюда выкладывают публикации о том, кто куда идет, кто и где катается и тому подобное) и «Мероприятие» (масштабное событие, как фестиваль или концерт). Кроме того на площадке можно создавать

приватные мероприятия с возможностью приглашать конкретных пользователей.

Пока что основная аудитория сервиса сосредоточена в столице. В большинстве своем это люди от 17 до 35 лет.

***

22.07.2016

55 % украинцев заходят на YouTube ежедневно – исследование

Темпы развития видеохостинга YouTube в Украине, где он официально был запущен в 2012 г., выше общемировых. Так, время просмотра видео на сервисе увеличивается на 70 % в год, сообщает пресс-служба «Google Украина», пишет «Телекритика».

Как показало исследование профиля пользователей видеохостинга – YouTube Audience Profiling Study 2016, 83 % украинских интернет-пользователей посещают сервис минимум раз в месяц, а 55 % из них – ежедневно. 70 % из тех, кто заходит на YouTube каждый день, – молодые люди в возрасте от 16 до 24 лет.

Также исследование показало и рост просмотра видео с мобильных устройств – 49 % украинских YouTube-пользователей подключаются к сервису через смартфоны.

Чаще всего украинцы смотрят видео дома (96 %), 18 % делают это в офисе, школе или другом учебном заведении, а 20 % – в дороге или другом месте вне дома. Более половины пользователей YouTube (59 %) смотрят видео на сервисе вечером или перед сном.

По данным исследования, основными мотивами для использования видеохостинга украинцы назвали желание расслабиться и сбежать от каждодневной рутины (37 %). Вторая по популярности причина – желание развлечься или же найти вдохновение (36 %). Еще 36 % смотрят видео, связанные с хобби или интересами.

Кроме того, украинские пользователи стремятся получить на YouTube необходимую им информацию (52 %) и образование (47 %), а 29 % – найти информацию, которая поможет в решении той или иной задачи.

Цель исследования YouTube Audience Profiling Study 2016 – выяснить, как используется и воспринимается YouTube пользователями разных стран, а также определить его роль в поиске информации и досуге. Размер выборки по Украине – 1251 респондент в возрасте 16+.

***

20.07.2016

«ВКонтакте» вернула граффити

Социальная сеть «ВКонтакте» адаптировала сервис граффити для отправки в личных сообщениях. Об этом говорится в блоге соцсети, пишет InternetUA.

Для того чтобы воспользоваться функцией, необходимо в диалоге открыть вложения и воспользоваться пунктом «Граффити».

«В 2007 г. «ВКонтакте» запустила сервис граффити – люди заходили друг к другу на страницу и оставляли рисунки на стене», – вспоминают в соцсети.

В настоящее время сервис доступен пользователям клиентов «ВКонтакте» для Android и Windows Phone, а в скором времени появится iOS и на сайте.

***

19.07.2016

«ВКонтакте» ответила на просьбу адаптировать соцсеть для незрячих

Социальная сеть «ВКонтакте» работает над внедрением специальных функций для слабовидящих и незрячих людей, сообщил «Газете.Ru» пресс-секретарь соцсети Е. Красников, пишет InternetUA.

Ранее на сайте петиций Change.org появилось обращение к пресс-службе «ВКонтакте» с просьбой адаптировать сайт для людей с ограниченными возможностями.

«Команда “ВКонтакте” благодарит Антона Тулякова, автора петиции на Change.org, за то, что он обратил внимание на ряд недоработок в новом дизайне сайта. Мы уже связались с Антоном и пригласили его принять участие в тестировании специальных возможностей полной версии сайта и мобильных приложений “ВКонтакте”», – сообщили в соцсети.

***

19.07.2016

Facebook позволил сохранять видео и смотреть их в оффлайне

И хотя функция намечалась только для пользователей Индии в рамках инициативы социальной сети по борьбе с плохим проникновением Интернета, теперь она доступна для всех пользователей Android. Необходимо зайти в выпадающие меню любого видео и выбрать «сохранить видео», пишет Marketing Media Review.

Функция не позволяет загрузить видео прямо на телефон, а сохраняет его в приложении Facebook для просмотра в оффлайне. Это значит, что доступ к ним можно получить только через приложение. В 2014 г. YouTube предоставил возможность смотреть видео в оффлайне на мобильных девайсах, а недавно Amazon Prime представил подобную функция для iOS и Android.

***

20.07.2016

Twitter дозволив верифікувати акаунти за допомогою онлайн-форми

Соціальна мережа мікроблогів Twitter презентувала онлайн-процедуру верифікації облікових записів. Тепер не потрібно зв'язуватись з кимось із представників соцмережі, достатньо залишити заявку на підтвердження акаунту, заповнивши відповідну форму, пише UkrainianWatcher.

У Twitter відмічають, що верифікація акаунту користувача або організації підтверджує його достовірность. Обліковий запис може бути верифікований і надалі бути відміченим спеціальною позначкою, якщо він становить суспільний інтерес. Як правило, до таких відносять акаунти громадських діячів та організацій у галузях музики, телебачення, кіно, моди, політики, релігії, журналістики, медіа, спорту, бізнесу.

Для того, щоб заповнити форму заявки на верифікацію, акаунт має містити перевірений номер телефону та e-mail, інформацію про користувача або організацію (для користувачів – ще й дата народження), фото (profile та header), посилання на веб-сайт.

***

21.07.2016

Facebook Messenger достиг миллиарда пользователей

Ежемесячная аудитория мессенджера Facebook Messenger достигла 1 млрд, пишет InternetUA.

Социальная сеть отметила популярность визуального контента среди пользователей приложения. По данным Facebook, каждый месяц отсылается более 17 млрд фотографий с помощью мессенджера. Также более 22 млн GIF-файлов пользователи отправляют через приложение ежедневно.

Сервис поддерживает 250 комплектов стикеров, в общей сложности предоставляющих на выбор 4 тыс. изображений. Каждый день пользователи делятся друг с другом более 380 млн цифровых «наклеек».

«Я очень благодарен всем тем людям по всему миру, которые пользуются мессенджером. Мы с нетерпением ждем, когда к нашему сообществу присоединится следующий миллиард», – прокомментировал достижение миллиарда пользователей вице-президент Facebook Messenger Д. Маркус.

Facebook Messenger стал вторым по популярности iOS-сервисом после основного приложения соцсети. В свою очередь Android-пользователи загрузили приложение более 1 млрд раз.

***

26.07.2016
Instagram запустил видеоканалы

Пользователям сети по всему миру стал доступен персонализированный канал «Эти видео вам понравятся», сообщает Marketing Media Review.

Канал можно найти в разделе «Поиск и интересное», где собраны фото и видео авторов, которые могут быть интересны пользователю, но на которые он еще не подписался. Кроме того, появилась возможность найти видео по конкретным темам – Олимпийские игры в Рио, Каннский кинофестиваль, музыкальный фестиваль Coachella, Новый год и прочее.

Поиск подстраивается под предпочтения пользователя: чем больше он лайкает, тем точнее алгоритм подбирает контент, который может его заинтересовать. А если какие-то посты кажутся неинтересными, можно нажать на «Реже просматривать такие посты» в выпадающем меню.

Персонализированный канал «Эти видео вам понравятся» первоначально был запущен для аудитории в США. Таким образом соцсеть рассчитывала побудить пользователей просматривать больше органического видео. Кроме того, увеличение числа просмотров видео поможет компании привлечь создателей контента к использованию платформы

***

27.07.2016
Почему Твиттеру не становится лучше

Сервис микроблогов Twitter, видимо, пережил время роста своей популярности, так и не достигнув доходности. Помимо традиционных финансовых проблем, детище Д. Дорси начало терять аудиторию, а также интерес со стороны рекламодателей. Почему так происходит, разбирался Sostav.ru, пишет МедиаБизнес.

Twitter, пожалуй, одно из самых непростых с точки зрения экономической судьбы социальных медиа. Несмотря на высокий потенциал по росту аудитории, сервису ни разу за свою 10-летнюю историю не удалось закончить год без убытков. В прошлом году, несмотря на рост выручки, компания все равно закончила год более чем с полумиллиардным в долларах убытком.

Эксперты связывают убыточность сервиса с несколькими причинами. Во-первых, компания достаточно поздно стала монетизироваться – лишь пять лет назад в этом направлении были сделаны первые шаги, а вменяемые рекламные форматы появились всего пару лет назад. При этом до сих пор нет достаточно глубоких механизмов оценки эффективности рекламы, что отпугивает бренды.

Еще одна причина хронической убыточности – это огромные инвестиции в различные стартапы: с 2008 г. Twitter купил в общей сложности 22 проекта. Руководство Twitter не раз обвиняли в «разбазаривании» средств инвесторов, вера которых в проект снижается год за годом. Для растущего проекта это были бы временные трудности. Главный вопрос в том, что Twitter перестал быть растущим проектом.

По итогам прошлого года аудитория Twitter сократилась с 307 до 305 млн пользователей. Эксперты отмечают, что для рынка соцмедиа 9-процентный годовой рост аудитории равен нулевому с учетом высокой динамики в сегменте. Таким образом, можно констатировать, что Twitter пропустил свой пик популярности, и теперь убедить инвесторов и рекламодателей в привлекательности площадки будет намного труднее.

Антикризисные усилия топ-менеджмента пока не приносят ощутимых результатов. После возвращения к операционному управлению Д. Дорси Twitter ввел много новых функций – как стратегических, так и пользовательских – например, таргетинг по эмодзи, новые возможности для видеоконтента, стикеры-хэштеги. Но, как ни странно, нововведения лишь усугубили ситуацию.

Одним из ключевых моментов, отпугнувших аудиторию, стала смена алгоритма показа новых сообщений: записи пользователей теперь отображаются не в хронологическом порядке, а по релевантности. Новость о грядущих переменах вызвала бурную реакцию у пользователей сервиса. В сети моментально распространился хэштег #RIPTwitter, ставший лидером по количеству упоминаний в микроблогах. А в Рунете даже появилась петиция с требованием к Twitter не запускать новый алгоритм.

Теряют веру в площадку и рекламодатели, особенно после обнародованного недавно исследования, согласно которому эффективность Twitter не так высока, как в презентациях: 56 % размещенных в сервисе ссылок ни разу не кликались, а это значит, что число переходов по ссылкам невелико по сравнению с другими крупнейшими соцмедиа. Это плохие новости и для брендов, и для СМИ.

Вместо того, чтобы решать насущные проблемы, руководство Twitter этим летом развернуло масштабную пиар-кампанию, включая видеорекламу, в которой рассказывается, зачем заводить аккаунт в этом сервисе. По словам представителей Twitter, около 90 % населения земли знают бренд с синей птицей, но при этом не понимают, в чем заключается основная функция сервиса.

Будет ли эта кампания успешной – большой вопрос. Как отмечают эксперты, у Twitter наблюдается проблема «перезрелого стартапа»: активные пользователи-миллениалы перешли на более современные инструменты цифровой коммуникации, а совсем молодое поколение просто не знает, что такое Twitter. Учитывая, что оно ориентируется в своем выборе на тренды, а не на пиар, привлечь ее вряд ли удастся таким образом.

Компании надо в корне менять структуру своей работы, но пока этого не видно. Например, не будет устранена одна из главных причин убыточности – руководство Twitter недавно заявило, что будет и дальше активно инвестировать в стартапы. И, конечно, будет продолжать инвестировать в маркетинг и продвижение, скоро будут запущены новые этапы рекламной кампании.

***

29.07.2016
«ВКонтакте» создала альтернативу нашумевшей Prisma

В сети появилось новое приложение, которое обрабатывает фотографии и стилизует их под произведения искусства, как популярные Prisma, Mlvch и другие. Программа под названием Vinci была создана на хакатоне «ВКонтакте». Соцсеть поддержала независимых разработчиков, работавших над проектом, пишет InternetUA.

«ВКонтакте» поддерживает вдохновляющие и инновационные идеи, в том числе и от сторонних разработчиков. Так как обучение и применение глубоких нейронных сетей требует больших вычислительных мощностей, для реализации проекта мы не только предоставили нашу собственную инфраструктуру, но и существенно её расширили», – рассказал TJ А. Рогозов, операционный директор соцсети.

В Vinci есть 20 фильтров, некоторые из которых названы в честь известных художников: Кандинского, Малевича и других. Снимки можно выбирать как из галереи, так и делать их с помощью программы. Стоит отметить, что приложение автоматически наносит свой логотип на изображения, и отключить эту функцию нельзя.

В настоящее время приложение запущено в тестовом режиме. Vinci уже можно скачать на смартфоны под управлением iOS и Android.

***

29.07.2016
В Twitter для Android появилась ночная тема

Несколько месяцев назад разработчики Twitter сообщили, что заняты тестированием ночного режима для Android-версии приложения. Уже сегодня пользователи могут опробовать новую функцию мессенджера, сменив привычную сине-белую палитру красок, на более тёмную. По мнению разработчиков, это нововведение позволит снять напряжение с усталых или сонных глаз пользователей. Найти переключатель нового режима можно в меню настроек, пишет InternetUA.

Разработчики отмечают, что переход к ночному режиму пользователь может осуществлять на своё усмотрение и независимо от времени суток. Ожидается, что в скором времени новая функция станет доступной и на iOS.

***

28.07.2016

Число активных пользователей Facebook превысило 1,7 млрд человек

Число пользователей, которые ежемесячно заходят в социальную сеть Facebook, достигло отметки в 1,71 млрд человек. Об этом говорится в отчете Facebook по итогам II квартала текущего года, пишет InternetUA.

Согласно данным отчета, по сравнению с аналогичным периодом прошлого года этот показатель возрос на 15 %. Что же касается числа пользователей, которые посещают Facebook ежедневно, то в июне 2016 г. оно составило 1,13 млрд человек, показав рост на 17 %.

Отдельно в отчете упоминается количество активных пользователей, которые заходят в соцсеть при помощи мобильных устройств. Ежемесячная мобильная аудитория соцсети составляет 1,57 млрд человек (+20 %), а ежедневная – 1,03 млрд человек (+22 %).

В отчете также содержатся данные о финансовых показателях Facebook за II квартал. Чистая квартальная прибыль Facebook составила 2,06 млрд долларов, увеличившись почти втрое по сравнению с прошлым годом.

***

29.07.2016

Twitter запустил стикеры для всех пользователей.

Социальная сеть добавила новую функцию, которая разнообразит фотографии пользователей, отмечает searchengines.ru. Теперь в сервисе доступна библиотека стикеров с сотнями иконок и эмодзи, которые можно будет помещать на снимки. Возможность добавлять стикеры доступна в приложениях Twitter для iOS и Android. В десктопной версии сервиса их можно лишь просматривать, пишет Marketing Media Review.

По мнению специалистов отрасли, нововведение может принести сервису микроблогов дополнительный доход. К примеру, Twitter может запустить спонсированные стикеры для брендов или платные коллекции стикеров. У конкурентов Twitter, таких как Facebook и Snapchat, стикеры и различные инструменты для редактирования фото доступны уже давно.

***

30.07.2016

Instagram даст больше контроля пользователям над комментариями

Instagram планирует увеличить контроль пользователей над комментариями. Сайт предложит специальные фильтры.

В настоящее время сервис свободно разрешает владельцам аккаунтов удалять комментарии, оставленные другими пользователями, которые по тем или иным причинам их не устраивают, пишет Хроника.инфо со ссылкой на VistaNews.

Но это не всегда работает, так как негативные отзывы могут находиться под публикацией достаточно продолжительное время, пока автор не заметит этого и не решит «ликвидировать» неуместное высказывание. Именно по этим причинам специалисты планируют увеличить систему тщательного контроля.

Издание Washington Post, ссылаясь на представителей Instagram, заявило о следующих нововведениях: теперь подписчики сайта смогут изначально отметить в специальной графе определенные слова или словосочетания, которые система будет блокировать автоматически. Таким образом, комментарии с «запрещенными» фразами не будут высвечиваться в профилях вовсе.

Помимо этого, пользователи будут иметь возможность получать всю необходимую информацию в свои электронные почтовые ящики.

***

31.07.2016

Чем будет заниматься команда Facebook до 2026 года

Издание The Verge опубликовало интервью с основателем и генеральным директором Facebook М. Цукербергом, в котором предприниматель рассказал, какие направления компания планирует развивать в ближайшие 10 лет. Редакция vc.ru рассказывает, чем будет заниматься команда Facebook до 2026 г., пишет интернет-издание «Замкова гора».

1. Подключение к Интернету жителей всего мира

Миссию Facebook М. Цукерберг видит в том, чтобы сделать мир более открытым для коммуникаций.

Он называет три основные проблемы, с которыми сталкиваются жители регионов, не имеющие доступа к Интернету (всего на планете проживает более 4 млрд людей без доступа к сети):

1. Отсутствие инфраструктуры. Даже если у человека есть телефон, он не может подключиться к Интернету. По подсчётам Facebook, такие проблемы испытывают около 1,6 млрд человек. «Для того, чтобы помочь им, нужно построить новые виды сетей – например, раздавать Интернет с беспилотников или спутников», – говорит генеральный директор Facebook.

2. Доступность Интернета. Около миллиарда человек, отмечает М. Цукерберг, живут в регионах, где есть Интернет, но они не могут позволить себе его использовать. Компания видит два решения (и работает, по словам основателя Facebook, над реализацией обоих): удешевление доступа к сети и снижение объёма передаваемых данных.

3. Отношение к Интернету. Около двух миллиардов людей по всему миру, говорит М. Цукерберг, могут себе позволить подключиться к Интернету – но не хотят этого делать или не видят в этом надобности. «Возможно, они никогда не пользовались компьютером, возможно росли без доступа к Интернету. Вы предлагаете им оплатить доступ к сети, но они не понимают, зачем им это нужно. Для таких людей мы реализуем программы бесплатного доступа к интернет-сервисам вроде Free Basics».

2. Запуск программы Aquila

Aquila – проект, который занимается разработкой дронов для передачи интернет-сигнала. Такой летающий аппарат и совершил свой первый полёт 28 июня 2016 г. Размах крыльев дрона превышает размах крыльев пассажирского самолёта Boeing 737 (34 м). При создании дрона использовалось углеродное волокно – за счёт этого устройство, говорит М. Цукерберг, получилось очень лёгким.

Скорость полёта Aquila невысока (по сравнению с другими летающими средствами) и составляет около 40 км/час. «Все мы привыкли, что в небе всё двигается быстро. На самом деле, когда люди создают самолёты, они думают о том, как быстрее доставить пассажира в точку назначения – небольшая скорость полёта тут не даёт большого преимущества. Наша цель – удерживать дрон в воздухе как можно дольше, а для этого приходится снизить скорость, насколько это возможно», – объясняет М. Цукерберг.

В первый полёт команда Facebook планировала удерживать дрон в воздухе в течение 30 минут, но устройство пролетало около 90 минут.

В ближайшее время компания планирует провести ещё один тестовый полёт – и во время него передавать на землю интернет-сигнал.

Скорость передачи данных с помощью дрона, говорит М. Цукерберг, может составить «десятки гигабит в секунду». «Это в 10 раз быстрее, чем любые технологии, существовавшие ранее», – отмечает он.

После того, как все испытания будут завершены, Facebook планирует запустить производство дронов Aquila. Устройства будут летать над сельскими регионами, окраинами крупных городов и зонами стихийных бедствий.

Компания планирует подключить к работе над программой правительства государств и крупнейших телеком-операторов по всему миру. «Мы построим систему и убедимся, что она работает – а затем будем лицензировать других производителей и распространять технологию. Мы не собираемся строить сеть самостоятельно. Но мне кажется, что это всё равно должно быть очень интересно», – говорит основатель Facebook.

3. Развёртывание системы Terragraph

В 2016 г. Facebook представила проект Terragraph – многоузловая беспроводная система, которая призвана обеспечить жителям стабильный доступ к сети в густонаселённых городах. Terragraph, говорит М. Цукерберг, повысит пропускную способность уже существующих оптоволоконных сетей. В дальнейшем, говорит он, возможность мгновенно прогружать

большое количество информации пригодится в сферах виртуальной реальности, обмена видео в режиме реального времени и так далее.

4. Работа над проектом Free Basics

Инициатива Free Basics, которая позволяет людям получить доступ к некоторым интернет-сервисам, не оплачивая доступ к сети, уже запущена в 42 странах. К проекту подключились более 25 млн человек. В будущем компания планирует распространять проект в новых странах – особенно М. Цукерберга интересует Индия, где первый запуск Free Basics провалился из-за проблем с регуляторами. «Это очень важный рынок. В стране живёт миллиард людей, у которых нет доступа к Интернету», – объясняет предприниматель.

5. Искусственный интеллект и робот-дворецкий

В январе 2016 г. М. Цукерберг объявил о своих планах лично создать систему искусственного интеллекта «наподобие Джарвиса из "Железного человека"». В интервью The Verge основатель Facebook отмечает, что разработка двигается: «В ближайшее время я планирую представить демо-версию своего ассистента. Сейчас я могу управлять всеми системами в доме – освещением, отоплением, дверьми.

Ассистент может сделать мне тост. При этом он сам определяет, когда его нужно сделать – выясняет, дома ли я и чем я занимаюсь. Система нуждается в некоторой доработке, но в целом она работает».

По мнению М. Цукерберга, в будущем системы искусственного интеллекта получат наибольшее распространение в двух областях: распознавание образов и обучение. «В обществе ведутся дискуссии о том, может ли искусственный интеллект нанести человеку вред, но мне кажется, что разработки в области распознавания образов всё равно будут чрезвычайно полезны. Слепой человек сможет легко узнать, что находится на экране, повысится безопасность вождения, технологии можно будет применить и в медицине», – говорит предприниматель.

6. Боты

Работу над ботами команда Facebook начала из-за возросшего интереса различных компаний к социальной сети, рассказывает М. Цукерберг. «Бизнес всё чаще использует свою страницу в Facebook как основной канал коммуникации. Пользователи обращаются к представителям компании через её аккаунт в социальной сети, но команда не всегда может отреагировать достаточно быстро. У нас родилась идея создать некоторый искусственный интеллект, который читал бы сообщения и мог предсказывать, что ответила бы команда. Мы захотели найти путь к автоматизации ответов покупателям».

М. Цукерберг отмечает, что существуют кейсы, когда диалоговый интерфейс не может заменить обычное приложение. «Нет, я не думаю, что разговор – лучший способ делать что угодно. Но мне кажется, то, что мы делаем – в 10 или даже в 100 раз лучше существующих сейчас способов взаимодействия с бизнесом. Вы набираете сообщение и практически сразу же получаете ответ, не ждёте часами. Это большой шаг вперёд», – говорит он.

7. Виртуальная и дополненная реальность

«Виртуальная реальность – очень важное для нас направление. По нескольким причинам. Во-первых, наша миссия состоит в том, чтобы дать возможность любому человеку на Земле поделиться своим опытом и помочь другому понять, что происходит в мире», – объясняет М. Цукерберг.

«Людям нравятся смартфоны, но это ещё не конец. Они с нами всё время, пользоваться ими более естественно, чем компьютерами, но виртуальная и дополненная реальности обещают быть ещё более естественными. Телефон нужно доставать из кармана, у него есть и другие ограничения. С VR и AR это останется в прошлом».

У вас будут очки или даже контактные линзы. Вы сможете просто посмотреть вокруг и получить всю нужную информацию.

Как отмечает М. Цукерберг, технологии виртуальной реальности уже готовы – создателям осталось только совершенствовать их. Он также говорит, что с виртуальной реальностью проще работать, поэтому компания начала разработку с неё.

С дополненной реальностью ситуация иная – пока Facebook лишь ищет способы внедрить её в человеческую жизнь и решает множество научных вопросов, связанных с ней. В течение 10 лет, полагает предприниматель, технологии дополненной реальности продвинутся до уровня, на котором сейчас находится виртуальная реальность.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

25.07.2016

Порошенко: Піратські ролики допомагають протидіяти інформаційній війні Росії проти України

Президент України П. Порошенко назвав піратські відеоролики важливим внеском у протидію інформаційній війні Росії проти України. Такими словами на своїй сторінці у Facebook П. Порошенко привітав переможця конкурсу «Допоможи ЗСУ піратським роликом», пише UkrainianWatcher.

Як відомо, конкурс відеоробіт на підтримку Збройних Сил України завершився напередодні. На сайті petrimazepa.com тривало голосування за найкращий ролик. Переможним стало відео «Повсталий степ» користувача Тараса зі Львова. Відеоробота опублікована на сторінці П. Порошенка у Facebook.

Друге місце посів відеоролик Army користувача Вінні, яке до появи відео-переможця довгий час було фаворитом.

Відео з назвою «Війна» користувача Грека посіло третє місце.

***

27.07.2016

У Порошенко указали на идею жесткого флешмоба в центре Киева от сил АТО

Спикер Администрации президента по вопросам АТО А. Лысенко на своей странице в соцсети показал идею жесткого флешмоба в центре Киева, который напомнит людям о том, что в стране идет война, пишет Апостроф.

На своей странице в Facebook А. Лысенко опубликовал скриншот поста А. Хартановича, волонтера в зоне АТО.

А. Хартанович предложил записать звуки боя и «врубить» их вечером на Крещатике.

«Чтобы не забывали, что в стране война», – поддерживает его идею пользователь Facebook Я. Полищук.

Как сообщал «Апостроф», ранее в украинском сегменте соцсети Facebook вызвал большой резонанс душераздирающий флешмоб «Я не боюсь сказать».

***

27.07.2016

Сети взорвала реакция СБУ на причастность их сотрудника к ограблению инкассаторов

Пользователи сети бурно отреагировали на известие от Службы безопасности Украины (СБУ) о разоблачении своего сотрудника, причастного к ограблению инкассаторской машины «ПриватБанка» в поселке Купянск-Узловой Харьковской области 21 июля, пишет Апостроф.

«Ничего себе поворот, а УВБ молодцы. Радует, что круговая порука не срабатывает уже», – написала в своем Facebook блогер Е. Монова.

«Ничего себе», «Патриот!», «Хм.. Интересно, имеет ли этот тип причастность к предыдущим нападениям на инкассаторские машины? Много их в Харькове было, в том числе и с убийствами, и я не помню, чтобы какое-нибудь из них раскрыли», «Радует», – пишут украинцы в комментариях к посту блогера.

***

21.07.2016

В сети в восторге от патриотичного поста украинской легкоатлетки

Пользователи социальной сети Facebook с восторгом восприняли пост украинской легкоатлетки О. Саладухи, в котором она выставила фото в

форме сборной Украины и патриотичной подписью: «Пишаюся представляти ці кольори», пишет Апостроф.

Журналист Т. Корниюк обратил внимание на то, что спортсменка родилась в Донецке и несмотря ни на что, по-прежнему выступает за Украину.

«Это Ольга Саладуха. Одна из самых сильных легкоатлеток мира. Она из Донецка, но всегда гордилась тем, что украинка. Не секрет, сделать себе имя в профессиональном спорте стоит бешеных денег. И Ольга не кивала в сторону государства, что мол то ей чем-то обязано. А шла к своей цели. Впереди – Олимпиада в Рио и наши надежды на медаль. Вперед к победе!», – написал журналист.

«Гордимся тобой», – прокомментировал пост известный волонтер А. Боечко. «Меня всегда переполняли чувства, когда одевал желто-голубую форму сборной. Желаю успешного выступления сборной и Вам лично на Олимпиаде!», – написал известный в прошлом украинский хоккеист, экс-капитан сборной Украины В. Бобровников.

***

27.07.2016

Российская православная церковь обзаведется собственным мессенджер

При поддержке Русской православной церкви будет запущен мессенджер, работа над ним уже началась. Об этом сообщает ТАСС со ссылкой на пресс-службу православной соцсети «Елицы», созданной по благословению Патриарха Кирилла, пишет МедиаБизнес.

Мессенджер станет «важным звеном единой коммуникационной платформы Русской православной церкви, создаваемой разработчиками «Елицы» для удовлетворения потребностей верующих в интерактивном общении и непрерывной связи прихожан с Церковью», отметили в пресс-службе.

В новом мессенджере, помимо привычных функций, таких как передача текстовых, аудио- и видеосообщений, будут и специальные. В частности, расширенными возможностями будут обладать священнослужители. «Представители разных уровней церковной иерархии смогут оперативно доносить важную информацию до широкой аудитории – прихода, благочиния, епархии или всей Церкви», – рассчитывают разработчики.

Поводом для создания мессенджера стали запросы пользователей соцсети «Елицы», в которой зарегистрировано более 100 тыс. пользователей, включая около тысячи священнослужителей. Официальные страницы в сети имеют 63 епархии и 45 архиереев. Фундаментом мессенджера станет накопленная соцсетью база из 18 тыс. православных храмов и их общин.

«Потенциальной аудиторией социальной сети и мессенджера по нашим оценкам могут стать от 7 до 10 млн человек», – отметил директор по развитию сети «Елицы» И. Суслин.

***

27.07.2016

У Папи Франциска вже більше 30 мільйонів шанувальників в Twitter

На акаунт Папи в “Twitter” підписалося понад 30 мільйонів користувачів Інтернету. Акаунт @Pontifex в даний час займає в соціальній мережі 26 місце, якщо порахувати передплатників на всі дев’ять мовних версій, пише видання «Голос українською».

Більшість користувачів Twitter стежать за іспаномовним профілем Франциска – 12 млн. На англомовну версію підписано майже 10 млн, італійськомовну – майже 4 млн, німецькомовну – понад 360 тис. Цікаво, що великою популярністю користується латиномовна версія – на неї підписалися понад 620 тис. чоловік.

Кількість користувачів, які стежать за “папським” профілем в Twitter росте дуже швидко. У порівнянні з квітнем 2015 р. вона зросла на третину. З тих пір кожен день акаунт в середньому отримував 20 тис. нових користувачів.

Папа Франциск з часу свого обрання, 13 березня 2013 р., написав понад 700 твітів. Аккаунт @Pontifex був створений в грудні 2012 р. під час понтифікату Бенедикта XVI.

***

26.07.2016

5 Facebook-профилей самых популярных ученых

Ученые – не всегда люди публичные. Тем не менее, многие из них не только занимаются исследованиями, но и активно популяризируют науку – регулярно участвуют в телешоу, пишут книги и рассказывают о своей работе в соцсетях. Портал Inverse рассказал о профилях известных ученых и популяризаторов науки в Facebook, пишет Rabota.ua.

1. Стивен Хоккинг

www.facebook.com/stephenhawking/

Страница одного из самых известных современных физиков С. Хокинга собрала больше 3,5 млн лайков. Правда, как указывается на странице, наполнением профиля занимается его команда. Здесь можно найти новости о его работе, информацию о новых проектах, интервью, фото. Иногда и сам ученый пишет посты, подписывая их – SH. Например, последний авторский пост касался сожалений С. Хокинга о потенциальном влияния Brexit на сферу научных исследований в Великобритании.

2. Нил Деграсс Тайсон

www.facebook.com/neildegrassetyson

Практически такое же количество подписчиков собрал Facebook-профиль известного популяризатора науки, директора Нью-Йоркского планетария Н. Тайсона. У него 3,4 млн подписчиков. Здесь также можно найти новости, ссылки на интервью, отрывки выступлений и анонсы событий с ученым. В основном посты размещает медиа-команда ученого, хотя некоторые сообщения постит и сам физик.

3. Митио Каку

www.facebook.com/michiokaku

Физик М. Каку, автор известных научно-популярных книг, в частности «Физика будущего», на своей странице в Facebook также размещает свои интервью, видео выступлений, участия в дебатах с небольшими комментариями.

4. Ричард Доукинз

www.facebook.com/RichardDawkinsBooks

У известного эволюциониста Ричарда Доукинза, автора популярной книги «Эгоистичный ген», также есть страничка в Facebook. Правда, ее ведет издатель Р. Доукинза. В то же время, здесь достаточно детально совещается публичная деятельность Р. Доукинза – публикуются интервью с ученым, статьи про науку, подготовленные его фондом, видео выступлений и информация о его книгах.

5. Джейн Гудолл

www.facebook.com/janegoodall/

Известный приматолог Д. Гудолл на своей странице делится информацией о своей активистской деятельности, новостями фонда Джейн Гудолл, личными фото, а также рассказами о шимпанзе и изучении этих животных.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

20.07.2016

Менее трети пользователей соцсетей считают новости топовым контентом для своей ленты

Миллионы людей используют социальные сети каждый день, но далеко не все вовлечены в медиа или брендированный контент. Об этом свидетельствует исследование, проведенное компанией Adobe на основании ответов 5 тыс. респондентов по всей Европе, сообщает The Drum, пишет Телекритика.

Согласно опросу, менее одной трети опрошенных поставили новости на первые места в рейтинге того контента, который им интересен в соцсетях.

18 % отметили различные спецпредложения и скидочные программы, информацию о которых бренды размещают в соцсетях, а 7 % – рекламные материалы.

Также исследование показало: менее половины европейцев считает, что социальные сети учатся более грамотно предлагать пользователям релевантный контент и рекламу. 34 % отметили, что их раздражает реклама от брендов, на которые они не подписаны, и почти столько же (33 %) не возражают против такой рекламы, если она для них релевантна.

При этом Facebook продолжает сохранять лидирующие позиции по вовлеченности пользователей в бренды. По данным Adobe, 90 % опрошенных ответили, что используют эту социальную сеть, чтобы следить за брендами и взаимодействовать с ними.

***

21.07.2016

81 % женщин совершают покупки под влиянием социальных сетей

Новое исследование Influence Central отметило, что именно такой процент женщин часто покупают продукты, которыми поделились в социальных медиа. 72 % отмечают, что возможность читать рекомендации о продукте в соцсетях позволяет им избежать покупок новых продуктов «вслепую», а для 81 % обзоры продуктов оказывают влияние на способ совершения покупок. Кроме того, 86 % женщин согласны со следующим утверждением: «Контент в социальных медиа стал главным источником онлайн-исследований, когда я думаю над совершением покупки», пишет Marketing Media Review.

CEO Influence Central отметила, что конвергенция мобильных девайсов и социальных сетей дают новое определение коммерции. «Каждый день, пользователи заходят в социальные сети, где видят изобилие восторженных рекомендаций от первого лица, часто с фотографией продукта, ссылками и информацией о локации магазина. Более того, эти рекомендации сопровождаются убедительными фото и видео, идеями использования, рецептам и лайфхаками. И эта снежная лавина, спровоцированная адвокатурой от первого лица, приводит к новому продукту или узнаваемости о бренде».

Для сравнения, только 64 % опрошенных отметили, что больше знают о продукте после просмотра рекламы на ТВ. И только 1,9 % признались, что ТВ-ролики оказывают влияние на их покупательское решение. Аналогично, только 2,2 % решают купить продукт, если видели статью или упоминание о продукте в печатных СМИ. Тем не менее, социальные медиа медленно отвоевывают свою долю на рынке ecommerce. В 2014 г. на долю Facebook, Twitter, Instagram и Pinterest пришлось только 1,7 % всех e-commerce продаж.

***

19.07.2016

Рекламная технология Snapchat распознает объекты на фото

«Эфемерный» мессенджер Snapchat запатентовал рекламный механизм, который будет распознавать объекты на фотографиях для обслуживания спонсорских фильтров. Новая технология определит, что изображено на «снэпах», и предложит пользователю наложить поверх картинки стикер или фильтр от рекламодателя, пишет InternetUA.

Как уточняет The Verge, компания подала патентную заявку еще в январе прошлого года, а ранее в этом месяце она была опубликована на сайте Бюро США по патентам и торговым маркам (USPTO). Систему можно назвать дополнением к геофильтрам Snapchat, которые позволяют наложить кастомный фильтр в зависимости от местоположения. Обычные пользователи могут стилизовать фото бесплатно, а рекламодатели, которые хотят создать фильтр для продвижения продукта или бренда, должны заплатить.

К примеру, если новый механизм Snapchat «увидит» на снимке чашку кофе или меню, он предложит пользователю разместить рядом стикер от кофейного бренда или ресторана. Кроме того, в патентной заявке упоминается автоматизированная система аукционов, которая позволит рекламодателям делать ставки и выкупать права на определенные объекты.

Спонсорские фильтры – это очередной маркетинговый инструмент, который может помочь Snapchat существенно нарастить выручку к следующему году.

***

19.07.2016

Facebook позволит разработчикам приложений привлекать только активную целевую аудиторию

Социальная сеть Facebook анонсировала запуск нового инструмента для разработчиков приложений, призванного решить проблему с привлечением именно той аудитории, которая будет активно пользоваться мобильным продуктом и тратить в нем деньги, а не просто устанавливать его, пишет «Телекритика».

Как сообщает интернет-издание Cossa, новая функция называется App Event Optimization и позволяет рекламодателям более точно достигать ценных пользователей, взаимодействующих с приложением после его установки.

Чтобы использовать инструмент, у разработчиков должен быть установлен Facebook SDK. Функционал также доступен в Facebook’s Power Editor и Facebook API.

В Facebook считают, что инструмент очень важен для бизнеса мобильных приложений, так как, согласно исследованиям, 90 % всего времени, проводимого пользователями в мобайле, приходится именно на приложения, 58 % мобильных покупок в США также совершаются в приложениях. Вместе с тем другие исследования показывают, что через месяц после установки приложения в среднем только 6 % людей продолжают им пользоваться.

App Event Optimization дает возможность выбрать, на какое действие внутри приложения таргетировать, чтобы максимально эффективно достичь аудитории, склонной к определенному алгоритму поведения. Например, это может быть завершение регистрации, процесс покупки, добавление товаров в корзину, просмотр контента и т. д.

***

21.07.2016

Во «ВКонтакте» разъяснили сообщения о «платной музыке»

Социальная сеть «ВКонтакте» не планирует вводить плату за прослушивание аудиозаписей в своих мобильных приложениях и в браузерной версии сайта. Об этом сообщили «Газете.Ru» в пресс-службе соцсети, пишет InternetUA.

Представитель компании сообщил, что «ВКонтакте» планирует тестировать различные возможности монетизации в сотрудничестве с партнерами-мейджорами и United Music Agency (UMA), но конкретных условий сотрудничества не раскрыл.

«Важно отметить, что для наших пользователей эти условия предусматривают свободу доступа ко всему аудио и видео контенту, который есть в социальной сети», – отметили в пресс-службе.

***

22.07.2016

«Одноклассники» запустили услугу платной блокировки баннерной рекламы

Социальная сеть стала взимать деньги за блокировку рекламы. Месяц без рекламы будет стоить около 100 р., сообщает roem.ru. «По просьбе пользователей мы запустили отключение рекламы за деньги. В настоящее время функция доступна для всех. Отключить рекламу можно на неделю, 15 дней или месяц. Также можно включить автоматическое продление функции. При выключенной рекламе пользователю не будут доступны баннерные блоки справа, а также реклама в ленте. В ОК уже работает скрытие рекламы – можно скрыть объявление, если оно не нравится. Мы предполагаем, что отключение рекламы позволит не видеть рекламу тем пользователям, которым она не релевантна и не интересна, увеличит

лояльность пользователей, при этом не скажется на рекламной конверсии», – прокомментировал С. Боярский, менеджер по развитию бизнеса ОК, пишет Marketing Media Review.

Реклама на видео убираться не будет. При этом, по данным comScore, соцсеть держится на первом месте по видеопотреблению в Рунете – 3,073 млрд в месяц против 1,210 млрд у «ВКонтакте».

***

28.07.2016

Фильтры, время публикации: Как крупнейшие бренды используют Instagram.

Половина из 500 самых успешных и крупных брендов пользуются Instagram, отмечает Marketing Media Review со ссылкой на rusability. При этом по данным недавнего исследования от TrackMaven платформа обеспечивает им самые высокие показатели вовлеченности по сравнению с другими соцсетями. Только у 123 брендов из списка Fortune 500 в 2013 г. был аккаунт в Instagram (24,6 %). Сегодня их уже 250 (50 %), к тому же у 1,4 % есть аккаунты для дочерних брендов. Среди других интересных выводов:

✓ 99 % реакций на публикации крупнейших брендов – лайки, при этом только 1 % – комментарии.

✓ У постов с хэштегами или вопросительными знаками более высокие показатели вовлеченности.

✓ В среднем у постов с восклицательными знаками показатели вовлеченности меньше.

✓ 89 % фото от брендов из списка Fortune 500 публикуется без фильтров.

✓ Juno, Lark и Clarendon – самые популярные фильтры.

✓ Самые эффективные фильтры (по соотношению показателей вовлеченности к средним данным) – Mayfair, Hefe и Ludwig.

✓ 88 % фото крупнейших брендов публикуется между 9:00 и 21:00.

✓ В среднем у постов, опубликованных с 22:00 до 03:00, эффективность выше.

✓ Чаще всего самые успешные бренды публикуют контент в рабочие дни.

✓ Записи, опубликованные в воскресенье, немного эффективнее, так как привлекают в 1,1 раз больше пользователей.

***

28.07.2016

Facebook заявив про брак місць для розміщення реклами

Фінансовий директор Facebook Д. Вейнер сказав, що з 2017 р. кількість реклами, яку соцмережа покаже кожному користувачеві, не буде значним

фактором у прогнозуванні виторгу компанії. На думку видання Recode, у Facebook, який заробив на рекламі в II кварталі 2016 р. 6,2 млрд дол., закінчуються рекламні місця, пише Finance.ua.

Recode вважає, що Facebook не може збільшувати кількість реклами, яку компанія покаже кожному користувачеві в своєму флагманському продукті. «Оптимальний обсяг реклами – це поєднання мистецтва і науки, – заявив Д. Вейнер. – Ми розважливо підходимо до роботи і хочемо бути впевненими в тому, що в стрічці кожного користувача збалансовано основний і рекламний контент».

В ідеалі Facebook має збільшувати кількість користувачів і створювати ефективнішу рекламу, яка буде приносити більше грошей, вважає видання. База користувачів соцмережі продовжує зростати. У другій чверті 2016 р. до Facebook приєдналося 60 млн осіб. Але з рекламою все трохи складніше, вважає Recode.

Компанія має довести, що реклама, розміщена у Facebook, приносить гроші, або пропонувати більше відеореклами високої якості. Із цим можуть виникнути складності. Велика частина реклами Facebook розміщується на мобільних пристроях, проте відеоролики на них продавати досить складно.

Однак проблема Facebook із розміщенням реклами всередині соцмережі може виявитися не такою вже серйозною, висновує автор матеріалу. Флагманський продукт хоч і не єдине, але основне джерело доходу Facebook. Звичайно, у компанії є й інші продукти, на яких ведеться рекламний бізнес, наприклад, Instagram. Також їй належать майданчики, де соцмережа зможе розміщувати рекламу в майбутньому (Oculus, Messenger, WhatsApp).

***

28.07.2016

Соцсеть Instagram презентовала новый функционал для бизнес-аккаунтов

Мессенджер Instagram презентовала новые функции для бизнеса. В частности, пользователи бизнес-аккаунтов смогут размещать на своей странице интерактивные контактные номера телефонов и прочие электронные адреса почтовиков для оперативной связи с другими посетителями интернет-сети. Об этом рассказал на своей странице в Facebook ведущий специалист в области онлайн-маркетинга Д. Кулак, пишет HiTech-News.ru.

«На сегодняшний день воспользоваться новым функционалом в соцсети Instagram смогут пользователи, только проживающие на территории Северной Америки. Однако мне удалось подключить услугу кликабельных номеров телефонов и адресов почты для отечественных бизнес-аккаунтов», – отметил на своей странице маркетолог.

Благодаря нововведению, пользователи сети Instagram смогут, не выходя из мессенджера, совершать звонки или отправлять почту по указанным в бизнес-аккаунтах номерам или адресам. Это, как отмечают специалисты, сможет в некоторой степени повысить рейтинг посещаемости соцсети в качестве интернет-площадки для продвижения товаров и услуг.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

19.07.2016

Твиты и соцсети станут лекарством вечности: новый способ для бессмертия

Доктор Х. Рахнама с Медиалаборатории Массачусетского технологического института хочет оживлять людей. Речь идет не о клонировании тел, а о создании виртуальной цифровой личности, основанной на письменных данных, которые писал человек в течение жизни. Так, в принципе, оживить можно любого, главное, чтобы для этого хватило информации, пишет InternetUA.

Такая концепция называется «дополненная вечность», и у нее есть целое движение сторонников. Целью доктора является с помощью искусственного интеллекта превратить цифровой отпечаток человека на цифровую личность, способную отвечать на вопросы, участвовать в разговорах и любыми другими способами имитировать разговорный стиль индивидуума.

Х. Рахнама вместе с исследователями из университета Райерсон описывает свою цель как «преодоление пропасти между жизнью и смертью с помощью перевода в вечность нашей цифровой личности». Ученый уже на основе этих алгоритмов планирует создать цифровые личности таких выдающихся деятелей, как Л. Толстой, А. Смит и З. Фрейд. Информации для этого вполне достаточно: полное собрание сочинений Л. Толстого, например, насчитывает 90 томов.

В этом и заключается особенность технологии при массовом использовании: качество цифровой личности напрямую зависит от количества написанного в течение жизни текста. Алгоритмам понадобится масса информации для воспроизведения дикции, страстей и личностных черт, составляющих индивидуума. То есть, чем больше твитов и записей в соцсетях оставить, тем выше шансы получить вечную жизнь.

***

18.07.2016

Подростки более склонны к манипуляции своими фотографиями в Instagram

Социальные сети – кладезь информации для социологов, психологов и прочих исследователей человеческой натуры в том или ином формате, пишет InternetUA.

Специалисты из Университета штата Пенсильвания в целом исследовали 2 млн учётных записей в Instagram и пришли к определенным выводам.

К примеру, оказалось, что подростки чаще удаляют непопулярные фото и заново публикуют те, которые им больше нравятся. Считается, что это обусловлено тем, что молодое поколение сильнее жаждет быть в центре внимания. Также подростки чаще оставляют комментарии и «лайкают» фотографии других.

При этом данная группа пользователей публикует меньше фотографий и они менее разнообразны по тематике, нежели у взрослых пользователей. Кроме того, исследователи пришли к выводу, что «лайк» в Instagram для пользователей является менее важным, нежели в Facebook или Twitter, поэтому люди чаще отмечают понравившиеся им фотографии, чем записи в других социальных сетях.

***

28.07.2016

Психологи сообщили, как социальные сети влияют на образ жизни людей

Социальные сети оказывают значительное влияние на жизнь современных людей, говорят британские ученые, которые обнаружили положительное воздействие соцсетей на образ жизни пользователей, пишет «Комментарии:» со ссылкой на planet-today.ru.

«Люди, которые хотят, например, похудеть, часто подписываются на всевозможные сообщества, посвященные здоровой пище, физическим тренировкам и разнообразным диетам. Печальная сторона этого явления состоит в том, что обычно, этим все и ограничивается. Но, определенный положительный эффект от ежедневного созерцания таких материалов все-таки есть», – говорят сотрудники Бирмингемского университета, которые изучали воздействие соцсетей на психику людей.

Оказалось, что подписчики посвященных здоровому образу жизни сообществ, которые просто смотрят картинки, не выполняя, при этом, никаких реальных действий, все равно постепенно приобщаются, таким образом, к мыслям, что быть стройным и здоровым – социальная норма, а не нечто фантастическое. Шаг за шагом, контент, популяризирующий здоровую

пищу и физические тренировки, делает свое дело и меняет сознание людей. Это подтверждается серией экспериментальных исследований, осуществленных учеными.

***

30.07.2016
«Селфі» негативно впливають на стосунки, – вчені

Дослідники Університету штату Флорида Д. Ріджуей і Р. Клейтон дослідили найпоширеніші селфі в Instagram, і виявили, що активне віртуальне життя і «селфі» шкодять стосункам, пише Espreso.tv.

Про це повідомляє офіційний сайт Університету.

За результатами дослідження науковців довели, селфі-пристрасть ставить під загрозу ваші відносини з партнером. У парах, які ведуть активне життя у соціальних мережах, сварки через ревнощі виникають значно частіше. Це може пояснюватися тим, що закохані витрачають забагато часу на «моніторинг» сторінок один одного, тим самим, скорочуючи час для реального спілкування. Це і підриває довіру у стосунках. Психологи вважають, що селфі 4–5 разів на день можуть вважатися проявом нарцисизму та схильністю до зради.

Маніпулятивні технології

29.07.2016
Російські інтернет-тролі агітують за Дональда Трампа

Росія використовує своїх інтернет-тролів для агітації за кандидата на пост президенти США Д. Трампа. Групи тролів – це добре скоординовані компанії, проплачені Кремлем. До такого висновку дійшов журналіст видання The New Yorker А. Чен, пише UkrainianWatcher з посиланням на Business Insider.

Журналіст поспілкувався з колишніми російськими онлайн-провокаторами і з'ясував, що завдання, яке ставиться перед ними – поширювати інформаційні вкиди про політику у буденні неполітичні судження американців в соціальних мережах. «Російську інформаційну війну можна розглядати як найбільшу в світовій історії операцію з тролінгу, котра знищує демократичність Інтернету як джерела інформації», – пише А. Чен.

Редактор The Daily Beast М. Вайсс додав, що група тролів з Москви готує інформаційні викиди і поширюють їх серед ЗМІ по всьому світу для того, щоб демонізувати сприйняття демократичних країн. «Мета тролінгу – сприяти розколу у різноманітних західних громадських об'єднаннях, в тому числі у НАТО, посіяти розлад між союзниками, щоб послабити позиції США

в очах спільноти у Європі, Азії, Африці, Латинській Америці», – вважає М. Вайсс.

На 58-х президентських виборах США Росія активно підтримує кандидата від республіканців Д. Трампа, який неоднозначно висловлюється щодо російської агресії на території України і називає Росію своїм союзником. В свою чергу, республіканець є фаворитом росіян на майбутніх президентських виборах.

Як відомо, в історичному районі Петербурга – Ольгино – розташовано ТОВ «Агентство Інтернет-Досліджень», яке займається інтернет-пропагандою. Сотні співробітників безперервно пишуть коментарі, розміщують картинки, обливають брудом Україну, Америку і Європу і гноблять незгодних росіян, створюючи таким чином видимість громадської думки.

***

21.07.2016

Как работает информационный пузырь

За последние несколько лет информационный пузырь (он же «Пузырь фильтров» или Filter bubble) превратился из чего-то вроде городской легенды в суровую реальность, с которой мы сталкиваемся каждый день. Если раньше о нем говорили исключительно эксперты и интернет-активисты, то сегодня многие люди и организации осознают серьезность проблемы. К примеру, недавно издание The Wall Street Journal продемонстрировало, как работает пузырь на фоне предвыборной гонки в США. Впрочем, обо всем по порядку (IGate).

Что такое информационный пузырь

Если говорить кратко, то информационный пузырь – следствие вездесущей персонализации. Сегодня Интернет очень тщательно следит за тем, какую информацию мы потребляем. Конечно же, это делается не из злого умысла. Google, к примеру, следит за нашими интересами, чтобы вовремя предлагать нам наиболее востребованную рекламу. Впрочем, этим занимаются все поисковые системы. Вы, наверняка, замечали, как после поиска информации о профессиональной фотографии вам повсюду начинает попадаться реклама фотокамер и аксессуаров для них.

Аналогичным образом работают социальные сети, формирующие ленту на основе интересов пользователя. Буквально каждое ваше действие, каждый просмотр и каждый лайк анализируются умным алгоритмом, который отныне будет отсеивать все, что вам не нравится и подбрасывать больше приятной и комфортной информации.

Что плохого в информационном пузыре

Информационный пузырь катастрофически ограничивает ваше мировоззрение. Алгоритмы персонализации представляют собой «ленивое мышление», воплощенное в программном коде.

Человеку от рождения свойственно больше верить той информации, которая совпадает с его точкой зрения. Само собой, ни о какой объективности при таком восприятии окружающего мира не может быть и речи. Чтобы избавиться от ленивого мышления и начать смотреть на мир шире, человеку приходится прилагать сознательные усилия. Но сегодня из-за преследующих нас программных алгоритмов сделать это не так-то легко.

Мы просто заходим в Facebook и оказываемся в море комфортной информации, всецело соответствующей нашим убеждениям и желаниям. Убежденный либерал не увидит здесь статей, обеляющих и отстаивающих консервативную точку зрения. Убежденный хоплофоб никогда не прочитает материал, поддерживающий идею легализации оружия.

По сути, каждый пользователь превращается в эдакого ручного хомячка, заботливо защищенного от окружающего мира пузырем «умных» алгоритмов. Корм для каждого подобран индивидуально.

Наглядная демонстрация информационного пузыря

Недавно издание The Wall Street Journal решило наглядно продемонстрировать, как именно работает информационный пузырь в Facebook. Редакция создала две диаметрально противоположные ленты – синюю и красную, в соответствии с цветами противоборствующих главных партий в США. В синюю ленту попадает контент, наиболее явно соответствующий настроениям либеральных демократов. В красную – контент для консервативных поклонников Д. Трампа.

Если вы либерал, то не будете видеть того, что видит консерватор и, соответственно, наоборот. Даже одни и те же события будут преподнесены этим группам людей по-разному. «Тэд Круз отказался поддержать Дональда Трампа», – повествует синяя лента. «Тэд Круз был освистан, после того как отказался поддержать Дональда Трампа», – уточняет красная.

«Яблоко от яблони далеко не падает, – пишет демократическое издание Occupy Democrats в синей ленте. – Этот твит от Трампа доказывает, что он такой же козел, как его отец».

«Первые сто дней президентства Трампа будут ЭПИЧНЫМИ! – заявляет Right Wing News в красной ленте. – Трамп анонсировал лучшую новость, что вы могли слышать со времен Рейгана».

Информационный пузырь – работает. И, пожалуй, единственный способ не превратиться в одного из консервированных хомячков М. Цукерберга – взвешенно подходить к своей активности в социальных сетях. Думайте, сомневайтесь, контролируйте эмоции – и будете свободны.

***

20.07.2016

Реакция человека Путина на убийство Шеремета вызвала гнев в сети

В сети с гневом отреагировали на заявление официального представителя МИД России М. Захаровой в связи с гибелью украинского журналиста П. Шеремета, пишет Апостроф.

«В Киеве взорван автомобиль, в котором находился Павел Шеремет. Профессионал, не боявшийся говорить власти, что о ней думает. Разной власти, в разные времена. И за это его уважали. Украина (не страна, а система) становится братской могилой журналистов и журналистики», – написала в своем Facebook.

Пользователи Twitter отреагировали на заявление М. Захаровой массой нелицеприятных комментариев.

Зарубіжні спецслужби і технології «соціального контролю»

27.07.2016

ФСБ собирается взять Интернет под тотальный контроль

Директор российского ФСБ А. Бортников считает, что для борьбы с терроризмом нужно взять под контроль Интернет, пишет GuildHall.

Об этом он заявил, выступая 27 июля на открытии 15-го совещания руководителей спецслужб, органов безопасности и правоохранительных органов, сообщают «РИА Новости».

Он добавил, что «использование бандитами Интернета для распространения своих агрессивных идей» является серьезной проблемой с точки зрения противодействия планам террористов.

«Необходимо решить проблему бесконтрольности и анонимности глобального виртуального пространства, которыми активно пользуются террористы», – сказал А. Бортников.

По его словам, в первую очередь, речь идет о постоянном мониторинге национальных информационных пространств на предмет выявления и блокирования террористических киберугроз, а также о незамедлительном реагировании на соответствующие обращения со стороны стран-партнеров по борьбе с терроризмом.

***

21.07.2016

У Білорусі вводиться контроль над дзвінками по Viber і Skype

У Білорусі з 18 вересня запроваджується повний контроль над IP-телефонією. Якщо пояснювати простими словами, IP-телефонія – це голосове або відео спілкування через Інтернет. Наприклад, його підтримують такі додатки, як Viber і Skype, пише MediaSapiens.

Відповідні норми прописані в «Положенні про систему протидії порушенням порядку пропуску трафіку на мережах електрозв'язку», опублікованому на національному правовому інтернет-порталі Білорусі.

Як пояснює видання «Белорусский паризан», оператори та інтернет-провайдери будуть зобов'язані виявляти трафік IP-телефонії та блокувати його при виявленні порушень порядку пропуску.

Порушенням вважається схема при використанні так званих GSM-шлюзів, які переводять звичайні дзвінки в Інтернет і навпаки.

Крім того, положення торкається використання популярних інтернет-месенджерів, в тому випадку, коли користувач телефонує через Інтернет на міські або мобільні номери (використовуючи, наприклад, сервіс Viber Out), або користувачеві дзвонять в месенджер зі звичайного/стільникового телефону. У разі порушення оператори за вказівкою НЦОТ зобов'язані призупинити надання послуги абоненту і блокувати трафік.

Також посилюється порядок контролю за абонентами і створюється «Реєстр абонентських номерів». Це державна інформаційна система, яка використовує «з метою отримання, зберігання, збору додаткової інформації, аналізу та надання інформації про факти, які свідчать про порушення порядку пропуску трафіку, в тому числі про користувачів послуг, яким їх було надано». У разі виявлених порушень і «підозрілої поведінки» абонентські номери (не абоненти) потрапляють до Реєстру. Оператори визначають підозрілу поведінку самостійно на підставі практики протидії порушенням порядку пропуску трафіку і передають інформацію в НЦОТ. Якщо інформація підтверджується, абонентський номер блокується.

Положення висуває і більш жорсткі вимоги до роботи дилерів/повірених операторів електрозв'язку. Зокрема, там йдеться про те, що такі компанії повинні здійснювати збір персональних даних співробітників, а також проводити ідентифікацію абонента із застосуванням засобів фото- і відеофіксації при наданні йому послуг і зберігання зазначених відомостей не менше 6 місяців.

***

22.07.2016

В Крыму добиваются закрытия сайтов-анонимайзеров

Прокуратура аннексированного Севастополя через суд хочет заблокировать доступ к специальным сайтам-анонимайзерам, через которые можно заходить на уже заблокированные ранее сайты, сообщает пресс-служба ведомства, пишет «Телекритика».

«В ходе мониторинга выявлены 9 сайтов-анонимайзеров, которые предоставляют доступ к заблокированным сайтам, содержащим материалы экстремистского характера, которые направлены на разжигание социальной, расовой и религиозной розни», – говорится в сообщении.

В связи с этим прокуратура подала в Гагаринский районный суд 9 исковых заявлений о признании информации, которая размещена на выявленных сайтах-анонимайзерах, запрещенной к распространению с целью последующего блокирования доступа к ней.

***

25.07.2016

В Китае запретили публиковать новости в Интернете без одобрения властей

Администрация по киберпространству Китая запретила нескольким крупным веб-порталам (Sina Corp., Tencent Holdings, Sohu.com, NetEase Inc. и другие) писать оригинальный новостной контент, об этом сообщает Bloomberg, пишет InternetUA.

Как следует из заявления ведомства, упомянутые интернет-компании «серьезно нарушили» местные нормы интернет-регулирования, разместив много оригинальных новостей, из-за чего это привело к «значительным негативным последствиям».

Теперь интернет-СМИ разрешено публиковать те заметки, которые были размещены китайскими СМИ, зависимыми от государства. За несоблюдение норм медиа-компаниям будет выписан большой штраф.

Теперь им запрещено публиковать материалы о текущих событиях: актуальные новости политики, экономики и общества.

Это не первая ограничительная мера интернет-регулятора Китая. В начале июля местным онлайн-СМИ запретили публиковать новости, основанные на информации из социальных сетей.

***

25.07.2016

Роскомнагляд заблокував сам себе

Російський наглядовий орган вирішив виконати рішення суду за червень 2013 р. і заблокував ряд ресурсів компанії Comodo, пише MediaSapiens.

Компанії Comodo є одним з найбільших постачальників сертифікатів SSL в світі – протоколів, що забезпечують захищений обмін даними. Тому по суті Роскомнагляд заблокував свого постачальника SSL-сертифікатів, пояснює Geektimes.

Зараз ці ресурси вже прибрали зі списків блокування, але ще 23 липня сайт Роскомнагляду по https доступний не був.

Як повідомлялося, Роскомнагляд заблокував сайти із закликами бойкотувати вибори в Держдуму. Вимоги заблокувати сайти надійшли в Роскомнагляд від Генеральної прокуратури. «Зазначені у вимозі публікації містять матеріали агітаційного характеру з метою популяризувати серед

населення Росії ідею бойкоту виборів до Державної думи Російської Федерації», – ідеться в повідомленні.

***

19.07.2016

В Бразилии третий раз за год заблокировали WhatsApp

Суд Рио-де-Жанейро в третий раз за последние 12 месяцев предписал операторам связи заблокировать мессенджер WhatsApp на территории всей страны. Об этом сообщает The Next Web со ссылкой на бразильский портал Globo.com, пишет InternetUA.

Как и в предыдущих двух случаях ограничения доступа (в мае 2016 г. и декабре 2015 г.), решение связано с отказом администрации сервиса выдать властям информацию о пользователях, которые фигурируют в деле о наркоторговле.

Издание полагает, что, как и в предыдущие разы, блокировка будет отменена спустя несколько дней. Однако длительная неработоспособность WhatsApp может сказаться на пользователях, которые приедут в Бразилию ради Олимпийских игр.

Кроме того, суд обязал компанию Facebook (ей принадлежит WhatsApp) выплачивать по 50 тыс. долл. в день до исполнения решения о предоставлении информации властям. Бразильские правоохранительные органы хотят получить данные о переговорах двух подозреваемых, использующих мессенджер. С помощью содержания переписки полиция собиралась выйти на след группировки наркоторговцев, которые действуют в Бразилии, Боливии, Парагвае и Испании.

***

28.07.2016

Бразильский суд заблокировал $11,7 млн на счетах Facebook

Федеральный суд в Бразилии вынес решение заблокировать 38 млн реалов (11,7 млн долл.) на счетах компании Facebook, которая владеет мессенджером WhatsApp. Об этом пишет ТАСС со ссылкой на портал UOL (InternetUA).

Сообщается, что вердикт суда связан с отказом представителей мессенджера открыть правоохранительным органам доступ к переписке пользователей.

***

26.07.2016

Facebook і Twitter розкрили переписку підозрюваних у підготовці терактів на Олімпіаді в Ріо-де-Жанейро

Facebook і Twitter надали бразильській поліції дані переписки користувачів соцмереж, яких підозрюють в участі в ісламістських угрупованнях та підготовці терактів на Олімпіаді в Ріо-де-Жанейро, пише venturebeat, пише UkrainianWatcher.

«Компанії почали надавати інформацію про зміст діалогів, а також про те, де саме відбувались ці обговорення», – пояснив представник суду.

Натомість, у Facebook і Twitter ситуацію не коментують, хоча їхні представники зазначили, що компанії мають нульовий рівень толерантності до діяльності, яка пов'язана з тероризмом та іншими злочинами.

Завдяки інформації Facebook і Twitter бразильській поліції вдалось знайти підозрюваних в участі в ісламістських угрупованнях та арештувати щонайменше 12 осіб.

Як заявили бразильські слідчі, затримані в рамках «Операції Хештег» є прихильниками ісламістської держави. За допомогою месенджерів вони обговорювали спроби нападів на час проведення цьогорічної Олімпіади в Ріо-де-Жанейро, яка почнеться 5 серпня.

***

31.07.2016

АНБ пытается взломать российских хакеров

Американские хакеры из АНБ, вероятно, пытаются взломать российские хакерские группировки, чтобы выяснить их причастность к взлому серверов Демократической партии США. Об этом сообщает ABC News со ссылкой на источники в американской разведке, пишет InternetUA.

Глава управления операциями по законному доступу АНБ Р. Джойс ранее не стал комментировать взлом демпартии, однако отметил, что у АНБ есть технические возможности и разрешения для того, чтобы «взломать в ответ» причастные хакерские группировки.

Р. Джойс добавил, что приоритетной задачей для АНБ в настоящее время является выяснение того, кто ответственен за взлом.

Р. Де, бывший генеральный юрисконсультант АНБ, также отметил, что АНБ может работать совместно с ФБР в рамках расследования и сфокусировать на российских хакерских группировках.

***

30.07.2016

WhatsApp хранит сообщения пользователей после удаления чатов в мессенджере

Самый популярный в мире мессенджер WhatsApp сохраняет историю переписки даже после ее удаления. Это обнаружил эксперт в области информационной безопасности Д. Здзиарски, пишет InternetUA.

По словам Здзиарски, WhatsApp для iOS удаляет не все данные о переписке пользователей после того, как они очищают чаты в мессенджере. Он обнаружил, что в последней версии приложения даже после удаления чатов программа хранит архив переписки онлайн-чатов и мгновенных сообщений (чат-логи). Данные сохраняются в памяти самого устройства, а также в облаке iCloud, кроме того, его можно получить через резервную копию устройства Apple на сопряженном компьютере.

В апреле WhatsApp усилил шифрование данных, которыми пользователи обмениваются через мессенджер. В результате чего шифрование распространилось не только на текстовые сообщения, но и на передаваемые фото- и видеоматериалы, а также на сообщения из групповых чатов. Система обеспечивает защиту от перехвата данных в процессе их передачи.

Хранение чат-логов WhatsApp позволяет получать доступ к переписке спецслужбам, если им понадобится прочитать сообщения. Они могут добиться этого, даже при условии, что переписка была удалена из приложения.

Примечательно, что архив сообщений мессенджера, в отличие от передаваемых данных, не шифруется.

***

29.07.2016

Жителя Кіровоградщини засудили за розповсюдження в Інтернеті сепаратистських матеріалів

До кримінальної відповідальності притягнули росіянина, жителя обласного центру, який поширював через Інтернет матеріали деструктивного характеру із закликами до вчинення дій з метою зміни меж території та державного кордону України, пише InternetUA.

Про це Новинам Кіровоградщини повідомили у прес-службі прокуратури області.

У лютому 2016 р. 63-річний чоловік розмістив в Інтернеті на власній сторінці у соціальній мережі «Одноклассники» текст із публічними закликами до зміни меж територій або державного кордону України. Суд визнав чоловіка винним у вчиненні кримінального правопорушення за ч.1 ст.110 КК України (посягання на територіальну цілісність і недоторканність України) та засудив до 3 років позбавлення волі зі звільненням від відбування покарання строком на 1 рік.

Чоловік повністю визнав свою провину в умисному розповсюдженні сепаратистських матеріалів, щиро розкаявся та уклав угоду про визнання винуватості.

***

31.07.2016

Кропман В.

Спецслужбы Турции взломали шифрованные чаты 40 тысяч гюленистов

Турецкие спецслужбы задолго до попытки государственного переворота смогли идентифицировать среди турецких граждан десятки тысяч сторонников исламского проповедника Ф. Гюлена, которого Анкара считает главным идеологом неудавшегося путча. Об этом 30 июля сообщила немецкая медиакомпания n-tv со ссылкой на анонимного турецкого чиновника, пишет Deutsche Welle.

По информации чиновника, разведслужба MIT, начиная с мая 2015 г., перехватывала электронную переписку сторонников Ф. Гюлена, которые использовали для конспирации приложение ByLock, позволяющее обмениваться зашифрованными сообщениями. Таким образом, было идентифицировано почти 40 тыс. предполагаемых гюленистов, среди которых было около 600 высокопоставленных военных.

Спецслужбе так и не удалось в этом массиве переписки найти доказательства подготовки путча. В то же время, как утверждает источник n-tv, многие из участников зашифрованных чатов позднее приняли участие в попытке госпереворота. По информации американской газеты The Wall Street Journal, разведка передала Генштабу список из 600 имен предполагаемых гюленистов среди военных за четыре дня до попытки путча. Предполагалось, что они будут отстранены от своих должностей во время заседания военного руководства в августе. Турецкие спецслужбы считают, что кто-то слил эти планы армейского руководства путчистам.

По данным The Wall Street Journal, группа аналитиков MIT, помимо слежки за чатами гюленистов, внимательно изучала записи проповедей имама, надеясь вычислить тайные сообщения в его словах и жестах. К примеру, в марте этого года аналитики нашли на канале YouTube видео, в котором Ф. Гюлен впервые появился в одежде цвета хаки - такой же расцветки, которая используется в турецкой армии. В разведке пришли к выводу, что это был некий сигнал его сторонникам в армии, но так и не смогли понять какой.

При этом группа Ф. Гюлена создавала серьезные проблемы для турецких спецслужб. Как выяснила WSJ, сам он давно отказался от использования телефона и каких-либо иных средств связи, передавая устно указания людям, которые посещали его дом в США. Все попытки Анкары добиться от Вашингтона запрета на въезд сторонников Ф. Гюлена в США оказались безрезультатными.

Проблема захисту даних. DOS та вірусні атаки

20.07.2016

Депутатская авантюра с хранением конфиденциальных данных в облаках может дорого обойтись стране

Идея народных депутатов «перевести государственный сектор» на облачные сервисы является достаточно модной, пишет InternetUA.

Облачное хранилище – модель онлайн-хранилища, в котором данные хранятся на многочисленных распределённых в сети серверах, предоставляемых в пользование клиентам, в основном, третьей стороной. В отличие от модели хранения данных на собственных выделенных серверах, приобретаемых или арендуемых специально для подобных целей, количество или какая-либо внутренняя структура серверов клиенту, в общем случае, не видна.

На Западе «клаудизация» отдельных сегментов правительственных документов началась давно и интенсивно продолжается.

Лидерами по внедрению облачных технологий являются США, Австралия, страны Евросоюза, Япония. По прогнозам Market Research Media, в период с 2015 по 2020 гг. расходы мировых правительств на облачные технологии будут расти в среднем на 6,7 % в год и достигнут 118 млрд долл. В то же время, уже несколько лет назад США и Великобритания подвергли критике использование облачных хранилищ для конфиденциальных данных, о чем мы расскажем ниже.

Законопроект №4302 «О внесении изменений в некоторые законодательные акты Украины относительно обработки информации в системах облачных вычислений», похоже, исключением не стал.

Но как уже писал InternetUA, текст законопроекта не совпадает с декларируемыми в объяснительной записке целями.

Документом разрешается третьим лицам, нерезидентам, хранить государственные данные за пределами Украины.

Компания Gartner провела анализ использования публичных облаков и пришла к настораживающим выводам. В частности, одни компании за сохранность данных клиентов ответственности не несли, другие могли удалять информацию, если сервисом не пользовались определенное время, а для госструктур, которые работают с персональными данными, выход в открытое облако оказался вообще невозможным.

Приватные, в отличие от публичных облаков, теоретически обещают более высокий уровень безопасности. Однако затраты на хранение информации в них значительно выше.

К слову, альянс HITRUST подготовил отчет по утечке данных, которые хранятся в облаках. Основное внимание они акцентировали на медицинских данных. По их подсчетам, было похищено 21,12 млн записей из

медицинских карт, произошло 495 утечек. Общая стоимость похищенных данных составила 4,1 млрд долл.

Также в законопроекте не прописано распределение ответственности за персональные данные граждан между организацией-собственником облачного сервиса, интернет-провайдером и государством, что способствует появлению зон информационной опасности.

При «переводе» государства в облака необходимо помнить, что никто не застрахован от форс-мажорных ситуаций. Яркий пример, обыски в дата-центре «Парковый», когда представители СБУ и Генпрокуратуры остановили работу облака. В результате, в аэропорту «Борисполь» погасли табло. Кроме того, под угрозой оказалась работа ряда сервисов, связанных с жизнеобеспечением людей, среди которых службы логистических компаний, детские медклиники, банки.

Стоит отметить, что правительственный комитет отклонил данный законопроект, но вмешалась Администрация Президента и решение правительственного комитета было отменено.

О том, что законопроект «сырой» и не соответствует базовому уровню безопасности, говорят и эксперты.

Г. Гулак, к.э.н., эксперт по IT-безопасности, заместитель главы наблюдательного совета Sl Global Service:

«В законопроекте очень слабо прописаны вопросы защиты информации. Например, в статье 9.1 предлагается оценивать уровень защиты информации в системе облачных вычислений в соответствие со стандартом ISO/IEC 27001. Стандарт ISO вообще не является стандартом защиты информации. Это стандарт системы управления информационной безопасности. Он никак не может заменить стандарты, которые определяют критерии оценки безопасности. Они, между прочим, также отсутствуют в законопроекте. Существует всемирно признанный стандарт ISO 15408, который вводит критерий оценки безопасности информационных технологий, но его в тексте документа нет. Как в таком случае говорить о защите информации?

Что касается криптографии, то с ее помощью вы можете обеспечить только конфиденциальность ваших данных. А их целостность – это уже на совести собственника облачного сервиса»...

И. Петухов, глава Комиссии УСПП по вопросам науки и IT:

«Говоря о данном законопроекте, хочу заметить, что ни одна уважающая себя в мире страна не располагает свои национальные информационные ресурсы/базы данных с чувствительной информацией (медицинские данные, данные об образовании, права на собственность, финансовая и другая персональная информация) о своих гражданах за ее пределами, да, еще на неуправляемой ею инфраструктуре…

Защита безопасности и собственности граждан – основная функция государства. А при таком подходе, сами представители государства создают все условия для вероятной «потери» собственности своих граждан!

В законопроекте также не предусмотрена ответственность за утечку информации».

В. Вовк, генерал-майор СБУ, эксперт по вопросам государственной безопасности:

«Украине необходимы реформы и облачные технологии в данном случае – не исключение. Мир движется вперед и мы не должны отставать. Использование облачных технологий позволят качественно и количественно снизить расходы.

Безусловно, риски защиты персональных данных и государственной тайны есть. Но у нас осталось мало государственных тайн. Практически все они имеются в распоряжении России. У нас никогда не было тайн ни от США, ни от РФ. Персональные данные – это более опасный момент. Ведь здесь уже идет речь о каждой конкретной личности. Но подобные риски вряд ли коснутся рядовых украинцев. Скорее тех, кто имеют отношения к международной сфере, у кого есть бизнес за границей.

Поэтому защищать данные нужно более системными мерами. Очень важно не только принятие закона, а то, как он будет внедряться и реализовываться. Но я не вижу особых рисков. РФ и без всяких облаков может получить любую нашу информацию».

А. Шкрум, народный депутат от «Батьківщини», автор законопроекта №4302:

«В законопроекте много не доработок. Когда мы его разрабатывали, то брали опыт других стран, потому что у нас такого никогда не было. Поэтому однозначно его нужно будет дорабатывать после первого чтения. Кроме того, сейчас в законопроекте присутствуют непрозрачные механизмы. В частности, нужно прописать механизм отбора поставщика облачных технологий, данные должны храниться не на одном сервере. Законопроект должен быть максимально прозрачным».

Очевидно, что если народные избранники не хотят подвергать риску персональные данные граждан, то им еще предстоит нелегкая работа над законопроектом. Ведь если не позаботиться о надлежащим уровне безопасности, то несанкционированное использование данных станет серьезной проблемой и, как отмечают эксперты, страна может попасть под внешнее управление.

***

20.07.2016

Взломанные 3D-принтеры могут использоваться для промышленного саботажа

3D-принтеры могут использоваться не только для создания различных объектов, но и для промышленного саботажа, утверждают исследователи из Нью-Йоркского университета. К примеру, взломанный хакерами принтер, используемый для изготовления автозапчастей, может выпускать

комплектующие с невидимыми на этапе производства дефектами. Такая ситуация может привести к отзывам продукции из продажи и многочисленным судебным искам, пишет InternetUA.

Значительное количество современных 3D-принтеров подключены к Интернету, что позволяет удаленно управлять устройством. Злоумышленники могут воспользоваться данной возможностью и незаметно внести изменения в процесс производства. Скажем, уменьшить прочность изделия. Как правило, столь незначительные дефекты невозможно распознать даже при помощи ультразвуковой акустоскопии.

Если речь идет об использовании дефектных комплектующих для автомобилей и самолетов, подобный саботаж может угрожать жизни людей. В настоящее время многие авиастроители используют 3D-принтеры для изготовления запасных комплектующих. Потенциал для саботажа может только увеличиться, если производители будут заключать аутсорсинговые контракты с ненадежными исполнителями, предупреждают исследователи.

Более того, риск использования подключенных к Интернету 3D-принтеров выходит за рамки промышленного производства. К примеру, хакеры могут взломать принтер и похитить с него файлы, являющиеся интеллектуальной собственностью.

Для минимизации риска ученые рекомендуют отключить используемые принтеры от Интернета и хранить все файлы в зашифрованном виде.

***

20.07.2016

Банки рассказали о новейших способах обмана доверчивых граждан

Мошенники придумывают новые способы, чтобы выманить данные кредитных и платежных карт у доверчивых граждан. Представляем вашему вниманию три варианта, которые были самыми распространенными в последнее время (InternetUA).

1. Рассылка спама

Недавно многие пользователи сети получили письма, в которых говорилось о возникшей задолженности перед банком. И хотя люди ни разу не обращались в банк за кредитом, у многих возникло желание открыть вложенный файл или позвонить по указанному телефону.

«Внутри файла был вирус, – говорят специалисты. – А при звонке на номер мобильного телефона у вас, скорее всего, попытались бы выведать данные вашей кредитной карты. Якобы для проверки в базе данных».

2. Звонок робота

Также мошенники начали использовать роботов. Как рассказали в НБУ, в этой схеме держателям платежных карточек звонят не мошенники, а запрограммированные ими роботы, которые от имени «банка» просят

предоставить информацию о платежной карте или логин/пароль от веб-банкинга, необходимые для осуществления платежа.

«Данные платежной карты (полный номер карты, срок ее действия, код CVV/ CVV-2, пин-код к карте, логин/пароль для входа в веб-банкинг) являются конфиденциальными, и вы не должны их предоставлять другим лицам (в том числе работникам банков, в которых вы открыли карточные счета). Работники банка ни при каких обстоятельствах не будут и не имеют права звонить клиенту с запросом такой информации», – еще раз напоминают в НБУ.

3. Охота за отдыхающими

Еще один способ выманить деньги – это сыграть на вашей же жадности. Как говорится в разосланном предупреждении одного из банков, мошенники используют размещенные в Интернете частные объявления, в которых предлагают скидки от 50 % на отели и авиабилеты. Автор представляется родственником сотрудника авиакомпании, который имеет хорошие скидки, или говорит, что его поездку пришлось отменить и т. д.

Доверчивый покупатель переводит деньги на карту посредника, а в ответ получает ваучер с бронью на свое имя. Проверяет бронь на сайте отеля – все в порядке.

На самом же деле мошенник украл карту и хочет ее обналичить. Он находит супервыгодные тарифы или горящие туры и пишет о них в соцсетях. Когда доверчивый человек соглашается на выгодное предложение, мошенник платит за отель или билет краденой картой. Настоящему держателю карты приходит SMS о списании денег с карты. Он обращается в банк, банк – к поставщику услуг. Бронь аннулируется.

Поэтому банкиры советуют пользоваться только проверенными сайтами отелей и посредников с мировым именем.

***

19.07.2016

Искусственный интеллект готовится взять на себя роль защитника от кибератак

В настоящее время сложилась такая ситуация, что хакеры располагают в среднем 312 сутками на то, чтобы использовать уязвимости «нулевого дня» до тех пор, пока эти уязвимости не будут выявлены экспертами по кибербезопасности и не устранены программистами. В связи с этим руководство Управления перспективных исследовательских программ Пентагона DARPA приступает к реализации новой программы, целью которой является определение того, сможет ли искусственный интеллект взять на себя работу по обнаружению и устранению уязвимостей в программном обеспечении, тратя на это несколько секунд или минут времени, пишет InternetUA.

В рамках этой новой программы будет устроено соревнование Cyber Grand Challenge, которое будет представлять собой настоящее сражение систем искусственного интеллекта. Эти системы будут стремиться взломать сервера условного противника и, одновременно, защищать свои собственные сервера, «на лету» находя и устраняя недостатки программного обеспечения. Победитель соревнования получит приз в 2 млн долл., 1 млн будет дан обладателю второго места, а за третье место сумма приза составляет 750 тыс. долл.

В результате всего этого руководство DARPA планирует получить систему искусственного интеллекта, пусть и нуждающуюся в дальнейшее доработке, но уже способную в какой-то мере оказать помощь людям в деле защиты сетевого программного обеспечения от кибератак.

В настоящее время «обороноспособность» в области кибербезопасности обеспечивается постоянной работой групп высококвалифицированных специалистов, которые буквально вручную выявляют все признаки угроз и пытаются с ними справиться в режиме реального времени. Это очень сложное и утомительное занятие, а количество сообщений об ошибках в случае сбоев программного обеспечения, каждое из которых требует анализа, может составлять сотни и тысячи.

Внедрение систем искусственного интеллекта в эту область позволит не только избавить людей от работы по мониторингу текущей ситуации. Эти системы могут производить более быстрый и более всесторонний анализ, минимизировать время реакции, автоматически генерируя корректирующие программные коды, устраняющие обнаруженные уязвимости.

Проведение соревнования Cyber Grand Challenge запланировано на 4 августа 2016 г. в Лас-Вегасе. На протяжении 10 часов участники команд смогут только наблюдать за тем, как их «детища» сражаются друг с другом в виртуальном цифровом пространстве. Но самое интересное предстоит испытать командам, которым удастся добраться до финала. Их системы искусственного интеллекта будут действовать в рамках изолированной от мира сети, а на подзащитных серверах будет функционировать совершенно новый и неизвестный им программный код. Это означает, что системе искусственного интеллекта придется самостоятельно определить, изучить язык сетевого общения и логику программного взаимодействия прежде, чем она сможет приступить к обнаружению и устранению уязвимостей.

«Мы собираемся произвести большой научный эксперимент в области искусственного интеллекта и одновременно эксперимент по обеспечению жизнеспособности компьютерных систем. Пока мы даже не готовы представить себе какие результаты нам удастся получить» – пишут представители DARPA, – «Но даже убедительная победа в соревновании Cyber Grand Challenge станет лишь первым шагом на длинном пути развития искусственного интеллекта. Следующим шагом станет выступление победителя на конференции хакеров DEF CON 2016, где искусственному

интеллекту уже предстоит противостоять действиям высококвалифицированных людей-экспертов».

***

19.07.2016

Уязвимость в OpenSSH позволяет раскрыть имена пользователей

В OpenSSH выявлена уязвимость, позволяющая злоумышленнику вычислять реального пользователя в системе. Проблема затрагивает большинство современных конфигураций, так как вычисление хэш SHA256/SHA512 занимает больше времени, чем хэш BLOWFISH. Это позволяет по времени выполнения операции определить применялся алгоритм BLOWFISH или SHA256/SHA512 и узнать, существует ли пользователь в системе, пишет InternetUA.

Уязвимость еще не исправлена, однако обнаруживший ошибку ИБ-специалист из Verint Э. Харари отметил, что разработчик OpenSSH Д. Такер в курсе о проблеме и уже работает над ее решением.

При отправке пользовательского ID с длинным, но неправильным паролем (10 килобайт) на OpenSSH сервер, сервер быстрее ответит несуществующим пользователям и медленнее реальным. «Когда SSHD пытается проверить подлинность несуществующего пользователя, он выберет поддельную структуру пароля, жестко зашифрованную в исходном коде SSHD. В этой жестко зашифрованной структуре хэш пароля основан на алгоритме BLOWFISH. Получается, на пароль реального пользователя, использующего хэш SHA256/SHA512, сервер отреагирует медленнее, чем на длинный поддельный пароль (10Кб)», – пишет Э. Харари.

Если злоумышленник сможет вычислить SSH пользовательского ID, следующим шагом будет его проверка в списке раннее скомпрометированных ID и паролей.

***

19.07.2016

Почти 1 млн пользователей Android-устройств стали жертвами мошенников

ИБ-эксперты ESET обнаружили в Google Play восемь поддельных Android-приложений, предназначенных для увеличения подписчиков в социальных сетях. С помощью приложений, названных исследователями Android/Fasurke, злоумышленники похищали личные данные и деньги. В ходе мошеннической кампании программы успели установить от 250 тыс. до миллиона пользователей, пишет InternetUA.

Приложения запрашивали личные данные пользователя, постоянные платные подписки, а также согласие на получение маркетинговых сообщений и рекламы. При запуске программ пользователю предлагалось ввести

название модели мобильного устройства, свое имя и количество подписчиков, которое он хотел бы получить. После старта «процесса увеличения подписчиков» необходимо было пройти так называемую проверку на робота.

Пользователю предлагалось множество различных подарков, купонов и бесплатных услуг в обмен на личную информацию (имя, адрес электронной почты, адрес, телефон, дата рождения и пол). Несмотря на многочисленные негативные комментарии, популярность приложений не спадала.

Компания Google была уведомлена о проблеме и приложения уже удалены из интернет-магазина. Однако, эксперты ESET предупредили, что в Google Play могут существовать другие приложения подобного характера.

***

19.07.2016

Исследователь нашёл метод кражи денег в Instagram, Google и Microsoft

Бельгийский исследователь в сфере информационной безопасности А. Свиннен нашёл способ вытягивания денег из Facebook через сервис Instagram, у Google и Microsoft с применением голосовой системы распределения токенов при двухфакторной аутентификации (2FA), пишет InternetUA.

Большинство использующих 2FA компаний отправляют своим пользователям короткие коды через сообщения СМС. Если пользователь пожелает, то вместо СМС он может получать голосовой звонок, во время которого автоматизированный оператор говорит код вслух. Звонок выполняется на привязанный к учётной записи номер телефона.

А. Свиннен сумел создать аккаунты в Instagram, Google и Microsoft Office 365, а потом привязать их к премиальному номеру телефона вместо обычного. Звоня на этот номер, компании получают за это счёт на оплату. С применением скриптов хакеры могут запрашивать метки аутентификации у всех аккаунтов и зарабатывать на телефонных звонках.

Подсчёты показывают, что за год теоретически можно заработать 2,066 млн евро на Instagram, 432 тыс. евро на Google и 669 тыс. евро на Microsoft. Технические подробности отличаются для каждого сервиса. Информация была отправлена в программы поиска багов соответствующих компаний. От Facebook за это была получена награда в $2000, в Microsoft – $500, в Google – упоминание в зале славы компании.

***

19.07.2016

В результате взлома форума Ubuntu похищены персональные данные более 2 млн пользователей

Компания Canonical опубликовала предупреждение о взломе официального форума дистрибутива Ubuntu. В результате атаки были похищены IP-адреса, логины и адреса электронной почты более 2 млн пользователей ресурса. Об инциденте стало известно 14 июля нынешнего года после того, как один из пользователей сообщил о доступности копии базы данных форума, пишет InternetUA.

Как показало проведенное расследование, злоумышленники проэксплуатировали известную уязвимость в дополнении Forum Runner к используемому на форуме движку vBulletin. Данная проблема позволяла выполнить произвольную SQL-инъекцию. В настоящее время уязвимость уже исправлена.

Согласно уведомлению, атакующие не смогли получить доступ к репозиториям Ubuntu, механизму обновлений и действительным паролям пользователей. Как полагает администрация форума, злоумышленникам также не удалось получить shell-доступ к серверам. Данные в БД модификации не подвергались. Другие сервисы Canonical и Ubuntu скомпрометированы не были.

В целях предотвращения утечки данных в будущем Canonical установила модуль ModSecurity и организовала отслеживание своевременной установки обновлений для компонента vBulletin.

***

18.07.2016

Вымогатели всё чаще атакуют корпоративные сети

Криптографические приложения-вымогатели продолжают представлять собой всё большую угрозу не только для домашних компьютеров, но и для предприятий. С последних можно получить больше денег, так что хакеры уделяют корпоративным сетям всё более пристальное внимание, пишет InternetUA.

Согласно данным из доклада лаборатории Касперского, за последний год число жертв атак вымогателей в корпоративных сетях составило 718 тыс. против 131 годом ранее – рост в пять с лишним раз. На долю корпоративных пользователей приходится каждая десятая атака. Почти в половине атак между 2015 и 2016 годами использовали приложение Teslacrypt, которое стало неопасно в нынешнем мае после релиза ключа для расшифровки зашифрованных им файлов.

Другой значимой угрозой был вымогатель CTB-Locker, через 96 часов после заражения удаляющий файлы. Также в список вошли приложения Scatter, Craki, CryptoWall, Shade, Mor, Aura и Locky. В докладе говорится, что главной целью становятся малые и средние организации. Для них потеря доступа к файлам даже на несколько часов может быть более накладной, чем выплата выкупа.

Несмотря на это, специалисты не рекомендуют платить, поскольку это только повышает аппетиты злоумышленников и ведёт к появлению всё новых вымогателей. Компаниям рекомендуется регулярно выполнять резервное копирование файлов на свои серверы и в облако.

***

18.07.2016

Android-троян мешает пользователям блокировать скомпрометированные карты

ИБ-исследователи из Symantec обнаружили функцию блокировки вызовов в новых версиях вредоносов семейства Android.Fakebank.B. С помощью нововведения злоумышленники могут мешать пользователям просить у банков заблокировать скомпрометированную платежную карту, пишет InternetUA.

Вредноносное ПО Fakebank впервые было выявлено еще в 2013 г. Под видом приложения для Android-устройств вредонос инфицирует систему и пытается похитить деньги жертвы. Fakebank сначала сканирует устройство на наличие конкретных банковских платежных приложений. Затем троян предлагает пользователю удалить приложения и установить вместо них вредоносные версии тех же инструментов.

Новые версии Fakebank не только собирают учетные данные пользователя, но и способны контролировать телефонные вызовы. В случае набора номера банка вредонос отменяет вызов. В настоящее время использование нового Fakebank было замечено в России и Южной Корее. ИБ-исследователи настоятельно рекомендуют пользователям отказаться от установки приложений от непроверенных сторонних производителей.

***

17.07.2016

Cerber стал самым распространенным вымогателем месяца

За последние 30 дней вымогательское ПО Cerber стало самым распространенным, потеснив с лидерских позиций шифровальщиков Exxroute (он же CryptXXX) и Locky. По данным компании Microsoft, за месяц на долю Cerber пришлось 25,97 % случаев инфицирования, тогда как Exxroute был ответственен за 15,39 % вымогательских атак, а Locky – за 12,8 %, пишет InternetUA.

Впервые Cerber был замечен в феврале нынешнего года и за последующие несколько месяцев применялся в значительном количестве атак, в том числе в рамках DDoS-кампании. Атаки были нацелены в основном на пользователей из США, Турции и Великобритании. В конце июня текущего года исследователи Avanan сообщили о вредоносной кампании, направленной на пользователей облачного сервиса Office 365.

Как отмечают эксперты Microsoft, наибольшее количество инцидентов с использованием Cerber зафиксировано в США, Азии и Западной Европе, однако случаи инфицирования встречаются по всему миру. В компании поясняют, что чрезвычайно широкая распространенность Cerber обусловлена использованием многочисленных способов дистрибуции, в том числе в составе наборов эксплоитов (Neutrino, Angler и Magnitude), через скомпрометированные веб-сайты или спам-рассылку.

Чаще всего для инфицирования применяются документы Microsoft Office, содержащие вредоносный макрос или встроенные OLE-объекты. В ряде случаев злоумышленники использовали VisualBasic Script (VBS) и JavaScript для загрузки Cerber с C&C-сервера. Оказавшись на системе, вредонос шифрует файлы жертвы и за их восстановление требует выкуп в размере 0,92 биткойна (примерно 600 долл.). В отличие от остальных вымогателей, в каждую зашифрованную папку Cerber помещает не только инструкции по восстановлению файлов в текстовом формате, но и аудиосообщение.

***

20.07.2016

Обнаружен первый троян для вербовки инсайдеров в компаниях

Исследователи израильской компании Diskin Advanced Technologies обнаружили первое вредоносное ПО, использующее методы социальной инженерии и вымогательство для вербовки инсайдеров в компаниях. Вредонос, получивший название Delilah, чаще всего распространяется через игровые сайты и ресурсы с контентом «для взрослых». Оказавшись на системе, троян собирает конфиденциальные данные, в том числе относящиеся к семье и месту работы, позволяющие злоумышленникам шантажировать жертву, пишет InternetUA.

Помимо сбора персональных сведений, троян способен записывать видеоматериал с веб-камеры пользователя без его ведома. По словам эксперта компании Gartner Research А. Литан, в своих инструкциях злоумышленники требуют от жертвы использовать VPN-сервисы и анонимную сеть Tor, а также удалять историю просмотров в браузере. По всей видимости, это нужно для сокрытия следов несанкционированной деятельности в случае проведения аудита.

В настоящее время троян не продается на черном рынке и доступен только на закрытых хакерских форумах. Судя по количеству ошибок, вредоносное ПО пока находится на стадии разработки. Как отмечают исследователи, использование Delilah требует непосредственного участия авторов вредоносного ПО, в частности в том, что касается применения социальной инженерии для идентификации потенциальных жертв.

За последнее время проблема вредоносного инсайдерского ПО стала довольно актуальной. Как утверждается в докладе компании Verizon, в

большинстве случаев подобные угрозы обнаруживаются только спустя несколько месяцев, а то и лет, после инфицирования системы. А. Литан прогнозирует рост числа инцидентов с использованием Delilah и подобных вредоносов в будущем и рекомендует организациям принять меры по предотвращению возможного заражения.

***

15.07.2016

Українські хакери зламали сервер департаменту міноборони РФ

Українські хакери угруповання Falcons Flame, Trinity, Рух8 і КіберХунта зламали сервери департаменту із забезпечення державного оборонного замовлення Міністерства оборони Російської Федерації. В результаті зламу, хакери отримали дані, які містять документи оборонних контрактів з термінами виконання до кінця 2015 р., пише UkrainianWatcher.

Зламані дані були передані для аналізу волонтерам-розвідникам міжнародного співтовариства InformNapalm.

Волонтери обробили отримані документи і представили їх у вигляді таблиці, де відображені такі параметри: виконавець контракту, ІПН виконавця, номер контракту, терміни, короткий опис контракту, сума.

Як з'ясувалось, оборонний бюджет РФ в 2014 р. становив 2,501 трлн р., у 2015-му – 3,078 трлн р. У 2015 р. на закупівлю нового озброєння Міноборони РФ планував витратити більшу частину всього бюджету, тобто близько 1,74 трлн. Очевидно, що передані для аналізу документи розкривають лише малу частину оборонного бюджету за частиною закупівлі нового озброєння, але і вони є досить інформативними.

Загальна сума контрактів – 81,111,022,793.66 рублів. Найбільша сума контракту – 45,000,000,000.00 рублів, укладений з ВАТ «БСП» на виконання будівельно-монтажних робіт (БМР). Імовірно, даний контракт укладено для будівництва Національного центру управління обороною. Найбільшу кількість контрактів було підписано з ВАТ «Ремдизель» – 51 контракт. Лідером за контрактами є ВАТ «БСП», загальна сума контрактів – 52,751,642,560.59 рублів. Основна діяльність за контрактами: виконання будівельно-монтажних робіт.

Волонтери також оприлюднили контракти на закупівлю нового озброєння, техніки та компонентів для озброєння.

***

21.07.2016

В большинстве антивирусов нашли дыры, которые упрощают взлом

Исследователи из компании enSilo нашли шесть серьёзных проблем с безопасностью, свойственных пятнадцати продуктам таких компаний, как

AVG, «Лаборатория Касперского», McAfee, Symantec, Trend Micro, Bitdefender, Citrix, Webroot, Avast, Emsisoft, Microsoft и Vera Security. Все они напрямую связаны с методами перехвата вызовов других процессов, которые используют антивирусы и средства виртуализации.

В enSilo обнаружили уязвимости, когда изучали, каким образом различные приложения используют технологию под названием hooking и внедряют свой код в другие процессы, чтобы перехватывать, отслеживать и модифицировать выполняемые ими системные вызовы, пишет InternetUA.

Эта технология широко применяется антивирусами для того, чтобы следить за вредоносным поведением приложений. Кроме того, hooking используют для защиты от эксплойтов, виртуализации, мониторинга производительности и сэндбоксинга.

Некоторые дыры, найденные enSilo, позволяют полностью обойти средства защиты Windows и других программ от эксплойтов. В результате злоумышленники получают возможность эксплуатировать такие уязвимости, которые в другом случае были бы труднодоступны, а то и недоступны вовсе.

Другие дыры могут привести к тому, что вредоносная программ останется незамеченной или сможет внедрять собственный код в любые программы, запущенные на компьютере жертвы.

Некоторые компании, упомянутые в отчёте enSilo, уже устранили замеченные ошибки, но рассчитывать на скорое решение всех проблем не приходится.

Поскольку в список уязвимых продуктов входит Microsoft Detour, в enSilo полагают, что под удар попали сотни тысяч пользователей. Уязвимость в Detour остаётся неисправленной по меньшей мере восемь лет. Ожидается, что её устранят в августе.

***

24.07.2016

Telegram отключил возможность удаления аккаунта по SMS после серии взломов

Telegram отключил возможность удаления аккаунтов при помощи SMS-сообщений. Об этом сообщает Meduza со ссылкой на службу поддержки мессенджера, пишет InternetUA.

До этого популярный мессенджер позволял удалять защищенные аккаунты без знания пароля двухфакторной авторизации, посредством коротких сообщений. Такая опция была предусмотрена на случай, если у владельца аккаунта сменилась SIM-карта или он потерял пароль.

После нескольких случаев перехвата SMS-сообщений для доступа к Telegram функцию отключили. Отныне удалять аккаунты таким способом не получится.

***

22.07.2016

В Google Chrome 52 исправлено 48 уязвимостей

Компания Google представила новую версию своего интернет-обозревателя – Chrome 52. В этом релизе разработчики устранили в общей сложности 48 уязвимостей, 11 из которых были критическими, 6 – средней степени опасности, пишет InternetUA.

В числе критических исправлены CVE-2016-1706, позволявшая обойти sandbox-изоляцию в PPAPI и уязвимость CVE-2016-1707 (подмена URL в iOS). Первая проблема была обнаружена исследователем Pinkie Pie, получившим за ее обнаружение премию в размере 15 тыс долл. Вторую выявил xisigr из команды Tencent Xuanwu Lab. В качестве вознаграждения Google выплатила эксперту 15 тыс. долл. Более подробная информация об остальных девяти уязвимостях буде обнародована несколько позже. Отметим, что уязвимостей, позволяющих обойти все уровни защиты и выполнить произвольный код в на системе, не выявлено.

***

22.07.2016

Франция требует от Microsoft прекратить «чрезмерный» сбор пользовательских данных в Windows 10

Французская Национальная Комиссия по защите данных (French National Data Protection Commission, CNIL) выпустила обращение к компании Microsoft. В нём она требует прекратить «избыточный» сбор данных в системе Windows 10 и отслеживание пользователей через приложения, в том числе браузер Edge, пишет InternetUA.

Microsoft получила три месяца на выполнение требований акта French Data Protection Act и «прекращение избыточного сбора данных и слежения за пользователями без их согласия». CNIL заявляет, что Windows 10 собирает слишком много информации в телеметрии, включая данные о скачивании и установке приложений и даже о проводимом в каждом из них времени. Эти данные CNIL называет лишними для работы системы.

Организация также заявляет, что Windows 10 не хватает надёжной защиты, так как пин-код из четырёх цифр не обладает ограничением на число попыток ввода. Данное утверждение является неверным, поскольку Windows 10 предлагает пользователю ввести капчу после нескольких неудачных попыток ввода пин-кода, а в итоге нужно перезагружать операционную систему.

Также французские власти говорят, что при установке системы автоматически активируется рекламный ID, позволяющий приложениям присылать целенаправленную рекламу, а куки-файлы появляются без предоставления опции заблокировать их.

Microsoft уже выпустила ответ и пообещала обновить политику конфиденциальности для приведение в соответствие с данными требованиями в течение трёх месяцев.

***

22.07.2016

Уязвимость в реализации CGI позволяет осуществить атаку «человек посередине»

ИБ-исследователь VendHQ Д. Ширлинк обнаружил опасную уязвимость, основанную на ошибке 15-летней давности. Уязвимость влияет на большое число дистрибутивов Linux и языков программирования и позволяет осуществить атаку «человек посередине» на веб-серверы. Уязвимость, получившая название Httpoxy, затрагивает веб-приложения на стороне сервера, использующие CGI-интерфейс (Common Gateway Interface) или CGI-окружение, например, FastCGI для PHP, Python и Go, пишет InternetUA.

Д. Ширлинк описывает Httpoxy, как набор уязвимостей, возникнувших из-за простого конфликта имен, связанных с HTTP заголовками, которые небезопасно полагаются на переменную HTTP_PROXY при генерации предаваемых запросов. Данная проблема позволяет злоумышленнику удаленно изменить значение переменной HTTP_PROXY на веб-сервере с помощью специально сформированного HTTP-запроса.

Атакующий может удаленно проэксплуатировать уязвимость, осуществить атаку «человек посередине» и перенаправить трафик на произвольный хост. Злоумышленник также может перехватить и расшифровать трафик, или осуществить DoS-атаку, принуждая уязвимое ПО использовать вредоносный прокси-сервер.

Httpoxy включает целый ряд уязвимостей, влияющих на платформы и языки, включая PHP (CVE-2016-5385), Go (CVE-2016-5386), Apache HTTP Server (CVE-2016-5387), Apache Tomcat (CVE-2016-5388), HHVM (CVE-2016-1000109) и Python (CVE-2016-1000110).

По словам Д. Ширлинка, Httpoxy связана с уязвимостью в сценарии Perl, обнаруженной экспертом Р. Шварцом в 2001. Р. Щварц исправил уязвимость, однако подобные ошибки повторялись множество раз.

***

27.07.2016

Хакерські атаки на енергетичні компанії в Україні спланували у Кремлі – РНБО

У відомстві наголошують, що є всі ознаки участі російських програмістів у розробці різних хак-систем, пише InternetUA.

Підготовка й розробка програм для хакерських атак на українські компанії була спланована в Росії. Про це повідомив керівник Служби з питань інформаційної безпеки Апарату РНБО України В. Петров, передає прес-служба відомства.

В. Петров переконаний, що підготовка хак-атак була спланованою і тривала щонайменше півроку.

«Це був процес, що тривав не менше півроку, внаслідок якого було уражено не лише українські енергетичні компанії – це була лише верхівка айсберга – були уражені також ряд інших великих підприємств, а також один з національних телеканалів», – зауважив експерт.

Зазначається, що сліди хакерських атак, які були здійснені на українські енергетичні підприємства, ведуть до російських серверів, «та є всі ознаки участі російських програмістів у розробці різних систем для цього».

На підтвердження В. Петров називає той факт, що вірус було підготовлено та запущено саме з території РФ свідчить факт, що часові налаштування на комп'ютері, на якому створили цей вірус, збігаються з часовим поясом Москви і Санкт-Петербургу.

Крім того, за словами В. Петрова, прообраз того вірусу, який застосовувався проти енергетичних компаній України 2007 р., активно поширювався на одному з комп'ютерних форумів росіянином.

«Він поширював на спеціалізованому форумі програму, яка пізніше стала вірусом для ураження українських компаній. Тобто, за створенням і походженням цього вірусу стоїть російський громадянин», – сказав В. Петров.

«Росія сьогодні прагне відновити свою геополітичну велич, і тому вона вимушена вдаватись до різноманітних асиметричних способів, зокрема, до пропаганди та кіберзагроз. Ті події, які відбулися в Україні, спрямовані насамперед не проти України, це – демонстрація потенційних можливостей Росії для Заходу», – наголосив В. Петров.

«Атаки на енергетичні компанії – це тривожний дзвінок для нас, але ще більше тривожний дзвінок для країн Європи та тих країн, де інформаційні технології набагато краще розвинені, ніж в Україні», – зауважив він.

***

27.07.2016

США накажут санкциями стоящих за кибератаками

В Белом доме заявили, что Соединенный Штаты введут санкции в отношении стоящих за кибератаками на транспортные системы и системы энергоснабжения США, сообщает InternetUA со ссылкой на Reuters.

Об этом заявила помощник президента США по вопросам внутренней безопасности и борьбы с терроризмом Л. Монако.

По ее словам, санкции будут вводиться «целенаправленно», «когда будут подходящие условия» в соответствии с дальнейшей политикой, проводимой США.

***

27.07.2016
США считают Китай и РФ главными киберугрозами

В США обнародовали новые указания государственным органам относительно реагирования на кибератаки, в которых главными источниками таких возможных нападений названы Россия, Китай, Иран и Северная Корея. Об этом сообщает Радио Свобода, пишет InternetUA.

Как сообщила советник Белого дома по противодействию терроризму Л. Монако, Россия и Китай стали значительно опаснее как кибер-противники. Иран и Северная Корея, добавила она, тоже способные и желают осуществлять разрушительные кибератаки.

В новых указаниях, которые обнародовал Белый дом, определены пять уровней опасности кибернападений. Самый высокий, пятый уровень означает, что нападение представляет критическую угрозу для большого круга жизненно важной инфраструктуры, стабильности власти или жизней американцев.

Также в указаниях впервые публично определена роль федеральных органов власти в расследовании нарушений кибербезопасности в правительственном и частном секторах и в реагировании на эти нарушения.

Документ был обнародован в период, когда в США звучат предположения о вероятности участия хакеров, связанных с государственными структурами России, в похищении электронной переписки работников аппарата Демократической партии.

***

27.07.2016
Законопроект по кибербезопасности нужно тщательно доработать

В марте 2016 г. была утверждена стратегия кибербезопасности, в июле закончили обучение первые киберполицейские. Однако действующего закона о киберзащите страны до сих пор нет, пишет InternetUA.

Парламентский комитет по вопросам информатизации и связи на последнем своем заседании 6 июля 2016 г. порекомендовал народным депутатам принять в первом чтении законопроект №2126а «Об основах обеспечения кибербезопасности Украины».

Законопроект определяет основные цели, направления и принципы государственной политики в сфере кибербезопасности Украины, а также систематизирует полномочия и обязанности госорганов по обеспечению

киберзащиты страны. Вводятся определения таких терминов как: «кібератака», «кіберзахист», «кіберзлочин» и другие.

Ключевые правки в новой версии:

– исключено понятие «национальный сегмент киберпространства» и все связанные с этим положения;

– структурированы положения о национальной системе кибербезопасности, направлений ее работы, принципов координации и взаимодействия;

– доработано содержание понятия «критически важные объекты инфраструктуры»;

– введено понятие национальных электронных информационных ресурсов, что связано с необходимостью киберзащиты массива информации;

– исключены ряд систем, на которые действие Закона не распространяется, в частности, это государственная тайна (другие требования), системы, которые не подключены к Интернету (кроме технологических систем критических объектов), социальные сети и частные веб-ресурсы; также определено, что Закон не связан с содержанием информации.

Дополнительные полномочия и обязанности получает ГСССЗИ, которая становится национальным регулятором по кибербезопасности. Согласно законопроекту Госспецсвязи, «координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем критичних інфраструктурних об'єктів на вразливість».

По мнению юристов, доработанный законопроект был частично усовершенствован.

Б. Дучак, партнер и сооснователь юридической компании Axon Partners:

«Пока народные депутаты не могли поделить проект закона с Госспецсвязью, из текста были исключены противоречивые положения, касающиеся контент-провайдеров. Авторы отказались от идеи приравнять по правовому статусу контент-провайдеров к телекоммуникационным операторам.

Действие закона не распространяется на контент в принципе, поэтому пользователи социальных сетей и блогеры могут вздохнуть с облегчением: цензура этим проектом не вводится».

Ю. Котляров, партнер практики в сфере телекоммуникаций АО Juscutum:

«Если данный законопроект станет законом, то предложенные в нем нормы не обеспечат кибербезопасность страны. С таким подходом Украина к киберугрозам не готова. Законопроект просто не рабочий. Почему?

Во-первых, опять прописаны только декларации. Законопроект переполнен намерениями, целями, принципами. Императивных норм в проекте нет, не понятно, зачем взяли и просто скопировали достаточное

количество положений с решения СНБО Украины от 27.01.2016 г. “О стратегии кибербезапасности Украины”.

Во-вторых, для законопроекта характерна неоднозначность и недальновидность понятийного аппарата. Помимо того, что предложенная терминология не согласовывается с уже существующими смежными определениями, также авторы недальновидны в контексте ограниченности технологий для киберпространства, целей для кибератак.

В-третьих, установленные задачи субъектов национальной системы кибербезопасности не согласовываются с базовыми действующими законодательными актами, которые регулируют деятельность таких органов».

А. Данченко, глава парламентского комитета по вопросам информатизации и связи, автор законопроекта:

«Необходимо помнить, что Украина находится в состоянии гибридной войны. Отсутствие законопроектов, регулирующих кибербезопасность, – это преступление. К сожалению, стратегию кибербезопасности страны утвердили только полтора месяца назад. Без нее разрабатывать какие-то законопроекты было сложно.

Законопроект №2126а – компромиссное решение. В нем описываются элементы стратегии по кибербезопасности, те реперные точки, которые необходимы государству. Что касается нареканий на терминологию, то никто из экспертов мне не показывал письменных подтверждений того, что она, например, не соответствует стандартам НАТО или ЕС».

В тоже время эксперты акцентируют внимание на несовершенстве терминологической системы документа, а также на несогласованности с другими законодательными актами. По их мнению, законопроект требует существенной доработки.

О. Гусев, первый заместитель председателя Комиссии УСПП по вопросам науки и информационных технологий, заместитель главы Правления ИнАУ:

«15 марта принята Стратегия кибербезопасности Украины. Однако ряд положений проекта закона не соответствует этой Стратегии.

Так, несмотря на преамбулу проекта, документ определяет правовые и организационные основы обеспечения защиты, в частности, жизненно важных интересов человека и гражданина, полномочия и обязанности государственных органов, предприятий, учреждений, организаций, лиц и граждан в этой сфере и тому подобное. Но в тексте закона не предусмотрено положений, направленных на практическое обеспечение кибербезопасности личности, зато все внимание сосредоточено на защите интересов государства в этой сфере.

В документе много несогласованных определений, которые впоследствии могут создать неправильную систему отношений. Например, термин «система электронных коммуникаций (коммуникационная система)» не соответствует требованиям Директивы Европейского Парламента и

Совета №2002 / 21 / ЕС от 7 марта 2002 о совместных правовых рамках для электронных коммуникационных сетей и услуг (Рамочная Директива).

Принятие проекта может ввести в стране противоправные подходы лишения операторов телекоммуникаций возможности предоставлять услуги доступа к глобальным сетям передачи данных государственным органам и предприятиям»...

Вопросы обеспечения кибербезопасности чрезвычайно актуальны для Украины. Однако предложенный законопроект, вероятно, имеет уязвимые места, а также не коррелируется с другими законодательными актами. Поэтому остается только надеяться, что после первого чтения парламентарии учтут замечания экспертов и доработают текст законопроекта, не сделав его еще «лучше».

***

27.07.2016

Уязвимость в Twitter Vine позволяла видеть весь исходный код приложения

ИБ-исследователь под псевдонимом Avinash обнаружил серьезную уязвимость в мобильном приложении Twitter Vine, позволяющем создавать короткие (длительностью 6 секунд) видеоролики. Уязвимость позволила эксперту без проблем скачать образ Docker, содержащий полноценный исходный код Vine, пишет InternetUA.

Образ Docker, который должен был быть конфиденциальным, на самом деле оказался доступен всем пользователям. При поиске уязвимости Avinash использовал бесплатную поисковую систему Censys, позволяющую выявлять уязвимости и другие проблемы в сети. С помощью Censys эксперт обнаружил более 80 образов Docker и обратил внимание на образ «vinewww», предполагая, что тот содержит связанную с сайтом Vine информацию.

После запуска «vinewww» с помощью интерактивной оболочки Avinash смог увидеть весь исходный код Vine, ключи API, сторонние ключи и другие секретные данные. Исследователь предоставил Twitter все сведения об уязвимости и в течение пяти минут ошибка была исправлена. За проделанную работу Avinash получил от Twitter 10 тыс. долл.

***

26.07.2016

Старое приложение кражи паролей использовали для промышленного шпионажа

Исследователи из компании McAfee обнаружили взломанный сервер, который использовали как командный сервер для разных приложений для кражи паролей. Целью были несколько организаций в рамках проведения кампании промышленного шпионажа, пишет InternetUA.

Раскрыть действия злоумышленников помогла невнимательность с их стороны, поскольку они не удалили с одного из серверов архив ZIP с установочными файлами. Их анализ вместе с исходным кодом командного сервера позволили узнать компонент ISR Stealer, модифицированную версию инфостилера Hackhound, впервые обнаруженного в 2009 г.

Хакеры использовали IRS Stealer для создания программы кражи паролей из таких приложений, как Internet Explorer, Firefox, Google Chrome, Opera, Safari, Yahoo Messenger, MSN Messenger, Pidgin, FileZilla, Internet Download Manager, JDownloader и Trillian. Распространялась программа в архивах через фишинговые электронные письма с различные компании.

Архивы RAR и Z содержали исполняемые файлы, загружавшие программу кражи паролей. Пароли передавались на командные серверы через HTTP. Серверный компонент IRS Stealer принимал данные только в том случае, если строка user agent имела значение HardCore Software For : Public, специфичное для компонента на стороне клиента. Данные сохраняются в виде файла формата INI.

Кампания была начата как минимум в январе 2016 г. На одном из взломанных сайтов было найдено более десяти командных серверов.

***

26.07.2016

Программист рассказал о способе получить доступ к странице пользователя «ВКонтакте» после разлогина

Пользователь «Хабрахабра» под ником prohodil_mimo рассказал об обнаруженной им уязвимости во «ВКонтакте», которая позволяет злоумышленнику зайти на страницу пользователя после того, как тот вышел со своей страницы, пишет InternetUA.

Уязвимость была обнаружена в API, предназначенном для работы с мобильными приложениями, а конкретно – в способе авторизации OAuth. По словам программиста, злоумышленники могут беспрепятственно воспользоваться «куками» пользователя после того, как он вышел со своей страницы. Для доступа к профилю даже не понадобится вводить верный логин или пароль.

Если пользователь залогинен, ему будет сразу предложено установить приложение, если нет – вначале залогиниться, а уже потом устанавливать. Если приложение уже установлено, то идёт сразу переход на страницу, в хэше которой будет токен. Дальше идёт работа с API.

Самое интересное начинается после выхода из «ВКонтакте». Ваше приложение может иметь ссылку на выход вида vk.com/login.php?op=logout. Это стандартная ссылка на выход из VK. Но после выхода пользователя из VK куки остаются рабочими.

Таким образом, если опять показать страницу авторизации, ввести совершенно другой логин и пароль – вы всё равно сможете пользоваться страницей первого пользователя. prohodil_mimo

Как отметил prohodil_mimo, в самом приложении, подобным образом перехватывающем данные, могут использоваться «самые безобидные» права. Разработчик может не запрашивать доступ к контактам или фото, но всё равно получить возможность открывать как снимки, так и любую другую информацию в профиле.

По словам программиста, в поддержке во «ВКонтакте» ему ответили, что «это не баг, а фича, но, возможно, что-то изменится в будущем».

В разговоре с TJ пресс-служба «ВКонтакте» заявила о том, что разработчик допустил ошибку, а уязвимости на самом деле нет.

«В публикации на “Хабрахабре” допущена ошибка: vk.com/login.php?op=logout – это не ссылка для выхода из “ВКонтакте”. Ссылка логаута для каждого пользователя индивидуальная, это можно проверить, наведя курсором на кнопку “Выход” или скопировав ссылку правой кнопкой мыши на сайте.

Автор публикации действительно мог столкнуться с тем, что ему показывалась форма авторизации при переходе по указанной ссылке – этот баг мы в скором времени закроем. Однако к выходу со страницы это не имеет никакого отношения, и о какой-либо уязвимости здесь речи не идет», - сообщили в пресс-службе «ВКонтакте».

***

31.07.2016

Злоумышленники все чаще используют вымогательское ПО

Компания Cisco опубликовала отчет по кибербезопасности за первое полугодие 2016 г. Согласно документу, в кибератаках злоумышленники чаще всего использовали вредоносное вымогательское ПО. В первом полугодии 2016 г. мошеннические кампании, ориентированные как на предприятия, так и на отдельных пользователей стали более активными и мощными, пишет InternetUA.

Наиболее распространенным в вымогательских атаках является набор эксплойтов для эксплуатации уязвимостей в Adobe Flash. В 80 % случаев использовался набор эксплойтов Nuclear для успешной эксплуатации уязвимостей в Adobe Flash. Злоумышленники также активно использовали в вымогательских кампаниях уязвимости в JBoss в качестве нового вектора.

С сентября 2015 г. по март 2016 г. исследователи отметили пятикратное увеличение HTTPS-трафика, связанного с вредоносной активностью. В основном такой рост наблюдается из-за инъекций вредоносных рекламных сообщений и распространения рекламного ПО. Используя зашифрованное HTTPS-соединение, злоумышленники пытаются скрыть свою активность и обеспечить себе достаточно времени для осуществления атак.

Согласно отчету, пользователи продолжают несвоевременно устанавливать обновления, что позволяет злоумышленникам использовать эксплоиты к известным уязвимостям. Из-за использования устаревшего программного обеспечения значительное количество устройств продолжают быть уязвимыми для разного рода атак. В качестве примера исследователи взяли простой набор устройств Cisco для выяснения «возраста» известных уязвимостей, которые эксплуатируются на различных инфраструктурах. Выяснилось, что 23 % устройств подвержены уязвимостям, датированным 2011 г., а в 16 % обнаружены ошибки, впервые выявленные в 2009 г.

По данным Cisco, злоумышленники начали активно эксплуатировать TLS-протокол, используемый для шифрования сетевого трафика. Это является причиной для беспокойства среди ИБ-экспертов, так как углубленная проверка пакетов становится неэффективным инструментом.

***

31.07.2015

Киберпреступники используют PayPal для распространения одного из вариантов трояна Zeus

Эксперты компании Proofpoint зафиксировали вредоносную кампанию, эксплуатирующую платежный сервис PayPal для распространения банковского трояна Chthonic. В ходе кампании злоумышленники используют взломанные или новые учетные записи PayPal для рассылки электронных сообщений якобы от администрации сервиса с просьбой вернуть ошибочно отправленные на счет деньги, пишет InternetUA.

В сообщении указывается, что на счет пользователя случайно были переведены 100 долл. и эти средства требуется вернуть. К уведомлению прикреплена ссылка на скриншот, предположительно демонстрирующий подробности ошибочной транзакции. На самом деле включенная в письмо ссылка перенаправляет пользователя на страницу katyaflash[.]com/pp.php, с которой на компьютер загружается обфусцированный JavaScript-файл с именем paypalTransactionDetails.jpeg.js. При его открытии на устройство загружается банковский троян Chthonic – один из вариантов вредоносного ПО Zeus. Оказавшись на системе, троян связывается с C&C-сервером и загружает ранее не известный вид вредоносного ПО – AZORult.

«Услуга запроса средств в PayPal позволяет прикреплять к запросу уведомление, в котором атакующий может разместить персональное сообщение или вредоносную ссылку. Здесь действует двойная схема – пользователь либо может стать жертвой обмана и лишиться 100 долл., либо загрузить на свой компьютер банковский троян, или то и другое», – отмечают эксперты Proofpoint.

Масштаб вредоносной кампании совсем невелик. По данным исследователей, переход по вредоносной ссылке был совершен всего 27 раз. Эксперты уже уведомили компанию PayPal о проблеме.

***

30.07.2016

ИБ-исследователи раскрыли подробности работы трояна Mad Max

ИБ-исследователи из Arbor Networks сумели взломать сложный обфусцированный алгоритм генерации доменных имен вредоноса Mad Max. С помощью данного трояна злоумышленникам удалось создать ботнет, инфицировав компьютеры в 16 странах, пишет InternetUA.

Специалисты сумели обнаружить все связанные с вредоносным ПО домены начиная с 2015 г., а также те, которые, предположительно, могли использоваться до 2017 г. Исследование Mad Max раскрыло некоторые важные подробности о трояне, однако эксперты Arbor Networks отложили публикацию информации на более поздний срок.

По данным Virtus Total, вредонос Mad Max может быть обнаружен только с помощью эвристики. По словам экспертов, вредонос загружает на систему несколько DLL-файлов и выполняет их с помощью rundll32.exe. Во избежании детектирования Mad Max использует обфускацию, и его код состоит в основном из фиктивных команд. Обфускация делает Mad Max весьма трудным для обнаружения как с помощью отладчика, так и реверс-инжиниринга. По словам исследователя из Arbor Networks Д. Эдвардса, обфускация становится все более популярной среди злоумышленников.

Несмотря на все сложности, экспертам удалось создать деобфускатор, способный выявлять реальные команды, а не фиктивные. После удаления фиктивных команд, специалисты обнаружили, что Mad Max действительно использует алгоритм генерации доменных имен.

По словам экспертов, вредонос каждую неделю меняет генерируемое новое доменное имя, используя определенный шаблон домена верхнего уровня в зависимости от текущей недели месяца. В частности, троян будет генерировать домен в зоне .com для первой недели месяца, затем перейдет к .org, далее к .info и в конце месяца будет использовать .net.

Mad Max успел инфицировать компьютеры в Бразилии, Канаде, Китае, Финляндии, Франции, Германии, Индии, Италии, Японии, Южной Корее, Норвегии, Тайване, Таиланде, Украине, Великобритании и США.

***

29.07.2016

Автор шифровальщика Petya рассекретил закрытые ключи вымогателя Chimera

Жесткая конкуренция на черном рынке вымогательского ПО может иногда обернуться благом для пользователей. Некто под псевдонимом JanusSecretary, известный как автор вымогательского ПО Petya, опубликовал в открытом доступе 3,5 тыс. ключей для дешифровки файлов,

зашифрованных другим вредоносом – Chimera. В прикрепленном сообщении JanusSecretary также признался, что использовал элементы исходного кода Chimera при создании вымогательского ПО Mischa, пишет InternetUA.

В настоящее время эксперты компании Malwarebytes проводят проверку подлинности ключей и в ближайшем будущем намерены разработать декриптор, позволяющий восстановить зашифрованный контент.

О вымогательском ПО Chimera стало известно в ноябре прошлого года. Вредонос распространяется через письма электронной почты, содержащие ссылки на веб-страницу Dropbox. Оказавшись на системе, Chimera шифрует файлы и требует за их восстановление выкуп в размере 2,45 биткойна. В случае неуплаты вымогатель угрожает опубликовать данные в интернете.

***

28.07.2016

Опасная уязвимость в LastPass ставит под угрозу учетные данные миллионов пользователей

Исследователь из команды Google Project Zero Т. Орманди обнаружил ряд критических проблем в популярном сервисе управления паролями LastPass, позволяющих полностью скомпрометировать учетные записи миллионов пользователей, пишет InternetUA.

Предположительно, проэксплуатировав уязвимости, атакующий может получить полный доступ к паролям жертвы, если та посетит вредоносный сайт. Орманди уже предоставил полный отчет о проблемах разработчикам LastPass. Подробности уязвимостей пока не раскрываются. В настоящее время атак с эксплуатацией данных ошибок не обнаружено.

***

28.07.2016

В мире действуют более ста кибергрупп, специализирующихся на целевых атаках

Исследование, проведённое «Лабораторией Касперского», показало, что количество преступных группировок, целенаправленно атакующих государственные и коммерческие компании, за последние годы возросло в разы, пишет InternetUA.

Речь идёт о кибератаках типа ATP – Advanced Persistent Threats. Группы подготовленных и опытных хакеров специализируются на взломе компьютеров пользователей высокого ранга и рабочих станций организации с целью незаметного хищения ценных данных. Такие атаки могут длиться годами, а масштаб утечек может достигать нескольких Тбайт и даже Пбайт.

Наибольшему риску стать жертвой целевой атаки подвергаются правительственные и дипломатические организации, финансовые компании, предприятия, работающие в энергетической и космической отраслях,

учреждения в сфере здравоохранения и образования, телекоммуникационные и IT-компании, поставщики для вооруженных сил, а также общественные и политические активисты.

По данным «Лаборатории Касперского», ещё несколько лет назад число группировок, стоявших за целевыми кибератаками, составляло около двух десятков. Сегодня в мире активно более 100 групп, организующих кампании кибершпионажа и атаки класса APT, и под их прицел попадают коммерческие и государственные организации в 85 странах мира.

Эксперты говорят, что в последнее время ATP-атаки всё чаще применяются не только для шпионажа, но и для кражи денег. Целевые нападения затрагивают самые разные организации, их жертвой могут стать не только государственные учреждения. Не меньший интерес для злоумышленников представляют крупные компании, обладающие ценной интеллектуальной собственностью или имеющие доступ к большим финансовым активам.

***

28.07.2016

Новая версия трояна Kovter маскируется под обновление для Chrome

Специалисты Microsoft Malware Protection Center предупредили о появлении нового варианта трояна Kovter. Свежая версия Kovter распространяется под видом обновления для Chrome и обладает новым механизмом, усложняющим обнаружение и нейтрализацию трояна. Кроме того, он использует ряд новых цифровых сертификатов, что обеспечивает более высокий процент инфицирования, пишет InternetUA.

Новый вариант Kovter генерирует и регистрирует при установке специфическое расширение. Вредонос создает определенные ключи реестра, позволяющие запустить троян при каждом открытии файла с данным расширением.

Также вредоносная программа использует mshta для выполнения вредоносного скрипта JavaScript. Для обеспечения постоянного запуска скрипта Kovter создает в разных местах серию «мусорных» файлов со специфическим расширением. На завершающем этапе установки троян реализует механизм автозапуска, автоматически открывающий эти файлы.

«Хотя новый вариант Kovter нельзя назвать полностью бестелесным, большая часть вредоносного кода по-прежнему сохраняется только в реестре. Для того чтобы полностью удалить троян с инфицированного компьютера, потребуется удалить все созданные им файлы и внести изменения в реестре», – отметил специалист Microsoft Malware Protection Center Д. Нгуен.

Последние несколько месяцев авторы вредоноса не сидели сложа руки. В минувшем апреле вирусописатели добавили в троян функционал

шифровальщика, а в начале июля стали маскировать его под обновление для Firefox.

***

22.07. 2016

В Android 7.0 Nougat появится встроенная защита от вирусов

В Android 4.4 KitKat компания Google ввела процесс проверки устройства при загрузке на наличие и скрытую работу руткитов и вредоносных приложений. При этом сама система не предпринимала никаких действий, а лишь сообщала пользователю о возможной опасности. Так было до последнего времени, но в Android 7.0 Nougat ситуация кардинально изменится. Если загрузочный образ или раздел повреждён или заражён вредоносным кодом, то система будет либо загружаться в режиме ограниченного использования (при согласии владельца мобильного устройства), либо же не запускаться вообще, чтобы защитить пользовательские данные. Данная функция сначала заработает на моделях, которые будут поставляться с новой версией ОС «из коробки», пишет InternetUA.

Для подавляющего числа пользователей данное нововведение будет крайне полезным, так как предотвратит работу вирусов. Правда, для этого потребуется время от времени делать перезагрузку устройства. При обнаружении опасности, система может отключить доступ к некоторым разделам данных, что, в свою очередь, может привести к необычному поведению устройства. Также это может усложнить жизнь пользователям, использующим сторонние прошивки.

По заверениям Google, каждое устройство с заблокированным загрузчиком будет использовать эту функцию для проверки внесённых в систему изменений. К счастью, с девайсами, у которых загрузчик разблокирован, вроде линейки Nexus, таких проблем с использованием модов и кастомных прошивок возникнуть не должно.

***

26.07.2016

Защитные реле могут использоваться для кибератак на электросети

Защитные реле призваны обеспечить защиту от неисправностей в электрооборудовании, таком как двигатели и генераторы. Цифровые реле являются неотъемлемой частью модернизированных сетей электроснабжения (Smart grid), использующих информационные и коммуникационные сети и технологии для сбора информации об энергопроизводстве и энергопотреблении, пишет InternetUA.

Эксперты компании Mission Secure провели исследование, направленное на изучение уязвимостей в промышленных системах контроля и в оборудовании. Как оказалось, защитные реле являются одним из слабых звеньев электросетей. В процессе работы специалисты изучили реле производства SEL (в частности, SEL751A) и выяснили, что устройства никак не защищены от кибератак. Несмотря на отсутствие знаний о специфике работы электросетей, исследователям потребовалось совсем немного времени для того, чтобы скомпрометировать устройство и получить полный контроль над HMI-интерфейсом.

По словам специалистов, получив контроль над панелью, злоумышленники могут блокировать доступ операторам и администраторам, блокировать возможность ручного управления и осуществлять другие действия.

***

29.07.2016

Более 2 млн пользователей скачали трояны на телефон

В магазине приложений Google Play обнаружили троян, который содержится в 155 программах. По оценкам «Доктор Веб», вирус скачали более 2 млн пользователей, сообщает Grifonsoft.ru со ссылкой на Hi-Tech@Mail.ru.

Троян получил название Android.Spy.305.origin. Приложения, содержащие этот вирус, отображают надоедливую рекламу, мешая нормальной работе устройства. Также вредоносные программы выгружают на сервер злоумышленников личные данные пользователей, в частности, адрес электронной почты.

Как сообщает «Доктор Веб», троян содержится в «живых» обоях, редакторах изображений, клиентах интернет-радио и во многих других приложениях.

По оценкам исследователей, вирус скачали около 2,8 млн пользователей.

Компанию Google оповестили об обнаруженном вирусе Android.Spy.305.origin. Однако некоторые вредоносные приложения все еще доступны для загрузки в Google Play. С полным списком зараженных программ вы можете ознакомиться на странице исследования.

***

28.07.2016

Хакери з РФ можуть атакувати машини для підрахунку голосів у США, – американський експерт з безпеки

Експерт рекомендує створити команди для тестування обладнання, різко зміцнити їх системи захисту і перевести в офлайновий режим, пише "Главком".

Кібератака російських хакерів на комп'ютерні мережі Національного комітету Демократичної партії США вказує на можливість появи в листопаді ще більш серйозних проблем: американські виборчі системи або машини для підрахунку голосів теж можуть виявитися уразливими для подібних атак. Таку думку висловив експерт з безпеки і викладач Урядової школи Кеннеді (Гарвард) Б. Шнайер, пише The Washington Post.

На думку Б. Шнайера, забезпечити захист машин для підрахунку голосів до настання осені. Експерт рекомендує створити команди для тестування обладнання, різко зміцнити їх системи захисту і перевести в офлайновий режим, якщо не вийде гарантувати безпеку при підключенні до Інтернету. На думку Б. Шнайера, в перспективі слід повернутися до виборчих систем із «паперовим слідом», оскільки вони захищені від маніпуляцій.

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Касаткіна** Тетяна

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

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

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

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