СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(29.03–11.04)

2017 № 7

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(29.03–11.04)
№ 7

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

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

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2017

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

29.03.2017
Facebook собирается тестировать «гифки» в комментариях

В декабре генеральный директор Facebook М. Цукерберг намекнул, что в социальной сети появятся новые возможности для размещения анимированных изображений. Выяснилось, что компания начнёт тестировать одну из таких функций с апреля (Finance.Ua).

«Все любят хорошие GIF-картинки, и мы знаем, что люди хотят использовать их в комментариях, – сказал представитель Facebook. – Поэтому мы вот-вот начнём тестировать возможность добавлять GIF-изображения в комментарии и поделимся новой информацией, когда сможем, но пока мы не перестаём повторять, что это просто тест».

Неизвестно, как долго продлится тестирование. Судя по всему, цель компании – узнать, нужна ли вообще пользователям такая возможность.

Сегодня, чтобы ответить анимированной картинкой, человек заходит на сторонний сайт и копирует оттуда ссылку в Facebook. Это работает, но требует много лишних действий. Благодаря новой функции пользователи могут начать реже использовать реакции и отдать предпочтение GIF-изображениям.

Новая возможность вряд ли удивит пользователей Facebook. Скорее всего, рядом с кнопками размещения фотографий и стикеров появится ещё одна, отвечающая за «гифки». Компания не рассказала, откуда они будут браться, но, вероятнее всего, это один из популярных сайтов – Giphy или Tenor. Именно их возможности обычно встроены в мессенджеры.

Нововведение станет доступно небольшому числу пользователей, но если обретёт популярность, то анимированные картинки сможет отправлять в комментарии каждый.

***

31.03.2017
Ірина Коркішко
Twitter не рахуватиме @Usernames у ліміті символів при відповідях

Twitter відтепер не рахуватиме ім’я користувача, якому ви будете відповідати, в загальній кількості символів твіту. @Username буде винесено окремо, за рахунок чого користувач може використати всі 140 символів для написання самого повідомлення. Про це повідомляє видання Adweek (Watcher).

Ліміт у 140 символів для Twitter лишається незмінним, проте мережа продовжує розширяти можливості для того, аби вмістити в цей ліміт якомога більше. Останнє оновлення стосується відповідей у Twitter, у рамках яких імена користувачів більше на рахуватимуться в загальному ліміті. Нова версія додатку доступна для веб-версії, iOS та Android починаючи від 30 березня.

Коли ви відповідатимете, поле з іменами тих, кому ви відповідаєте, буде розташовуватись згори, над текстом твіта. Це означатиме, що для відповіді будуть доступні всі 140 символів. Якщо натиснути на поле «у відповідь», можна побачити, кому ви відповідаєте, та контролювати цей список, додаючи, або видаляючи інших користувачів. Водночас, читаючи переписку, можна бачити сам текст, не відволікаючись на імена учасників.

***

3.04.2017

«ВКонтакте» будет показывать в «умной ленте» публикации, понравившиеся друзьям

«ВКонтакте» начала показывать пользователям, включившим новую алгоритмическую ленту новостей, публикации, которые были отмечены как понравившиеся их друзьями. Как рассказал представитель соцсети Е. Красников, обновление доступно всем пользователям, поставившим в ленте новостей галочку на опции «Сначала интересные» (IGate).

Новый алгоритм также выводит записи сообществ и людей, на которых человек может быть не подписан, но их прокомментировал кто-то из друзей.

«Это нововведение должно помочь тем пользователям, у которых бедная лента новостей и они мало на что подписаны», – отметил Е. Красников.

Он добавил, что со временем предложенные записи от друзей «должны стать более релевантными пользователю, так как функция использует интеллектуальную технологии машинного обучения.

Если пользователи не желают делиться с друзьями записями, которые они отметили, они могут отключить функцию в настройках приватности».

***

3.04.2017

Facebook активував тривожну кнопку через теракт у Петербурзі

Соцмережа Facebook активувала функцію «Перевірка безпеки» через вибухи в метрополітені Санкт-Петербурга (Інформаційна агенція «Вголос»).

Завдяки цій функції користувачі соцмережі можуть оперативно повідомити друзям, що вони потрапили у небезпеку, або дізнатися, чи є у зоні надзвичайної ситуації знайомі.

«Перевірка безпеки увімкнена в результаті активності людей на Facebook у зоні надзвичайної ситуації», – зазначено на сайті.

Разом з тим на сторінці «Перевірки безпеки» вказано телефон екстреної служби 112, а якщо перейти за посиланням «Більше інформації», можна отримати останні дані про події у Санкт-Петербурзі з новин Google.

***

3.04.2017

Facebook начал ранжировать в ленте новости по геолокации

В последние несколько недель пользователи приложения Facebook начали замечать иконку с ракетой. Она находится справа от значка с лентой новостей. После нажатия на нее пользователю предлагаются посты, опубликованные теми людьми, на страницы которых он до этого мог вообще не заходить. «Ракетная» лента новостей основана на местоположении пользователя (InternetUA).

Новая опция доступна не всем. В частности, ее заметил журналист Mashable из Хорватии, а также несколько пользователей из Великобритании. Если нажать на «ракету», то можно увидеть те посты, которые популярны у пользователей, находящихся рядом. «Я также вижу новости, соответствующие моим интересам, так что лента также как-то связана с моими отметками “нравится” и друзьями», – отмечает автор статьи. Другими словами, эта лента – нечто схожее с тем, что предлагает Instagram при переходе в раздел поиска.

Вообще Facebook уже давно работает над оптимизацией ленты. Алгоритм отображения новостей сейчас основан, в первую очередь, на том, насколько хорошо пользователь знаком с автором, а также на отметках «Нравится» у самой публикации. Другими словами, посты друзей отображаются над новостями брендов.

***

5.04.2017

«ВКонтакте» приступила к тестированию собственного сотового оператора

«ВКонтакте» приступила к тестированию виртуального мобильного оператора, свидетельствует новый релиз компании. Соцсеть выпустила мобильное приложение VK Mobile, которое связано с ее планами запустить собственного оператора святи (InternetUA).

Чтобы пользоваться VK Mobile помимо SIM-карты виртуального оператора нужно устройство с версией Android 4.4 и новее. Личный кабинет абонента в приложении позволяет управлять услугами связи, говорится в описании клиента. Для использования приложения необходима действующая SIM-карта сети VK Mobile.

С помощью приложения можно пополнить баланс, следить за количеством доступных бонусов, получить детализацию по расходам и управлять услугами.

Информации о способах получить «симку» ни в самом приложении, ни в его описании нет. При его запуске пользователь попадает на страницу закрытого сообщества VK Mobile, для вступления в которое необходимо подтверждение администратора.

Судя по опубликованным в Google Play скриншотам, в сервисе также предусмотрен кэшбек за покупки внутри «ВКонтакте». Позднее скриншот с информацией о кэшбеке был удалён из описания.

В компании подтвердили, что проводят внутреннее тестирование сервиса. Однако обсуждать сроки запуска продаж SIM-карт, тарифы для пользователей и другие детали отказались.

***

6.04.2017
Ірина Коркішко
Facebook дозволив усім сторінкам публікувати платний контент

Facebook розширив доступ до публікації спонсорованого контенту для всіх сторінок мережі. Повідомляє видання Marketing Land (Watcher).

Раніше право на публікацію спонсорованого контенту мали тільки власники підтверджених сторінок і профілів. Завдяки оновленню політики розміщення брендованого контенту, такі пости відтепер будуть позначатися як «оплачені». Додатково Facebook дозволив використовувати логотипи, водяні знаки і графічні оверлеї портягом усього відео. Раніше використання даних атрибутів дозволялось лише протягом перших трьох секунд ролика.

Порушники правил будуть отримувати сповіщення про необхідність внесення змін до відео, але видалятися матеріали не будуть. Натомість, мережа просто приховає їх до моменту внесення необхідних змін.

***

6.04.2017
Facebook будет блокировать интимные фото бывших

Социальная сеть Facebook будет фильтровать распространение интимных фотографий пользователей, выложенных без их ведома, например, из мести бывшему партнеру (From-UA).

Соцсеть не позволяет репостить такие изображения, определяет и удаляет их. Это нововведение касается Facebook, Messenger и Instagram, но не WhatsApp. При этом Facebook не будет искать порнографические изображения напрямую, а станет ориентироваться на сигналы, поступающие через кнопку «Пожаловаться».

Модераторы будут принимать решение о посте, обращая внимание, в частности, изображена на фото сексуальная активность или человек, который на него пожаловался. Если они решат, что речь идет о «порномести», изображение удалят, а пользователя, его запостившего, заблокируют.

Далее в действие вступит программа распознавания изображений, которая обеспечит, чтобы противоречивое фото не циркулировало в сети и блокировалось без участия модераторов-людей. Эта техника подобна той,

которую Facebook и другие уже используют, чтобы предотвратить распространение детской порнографии.

«Очень часто эти изображения выкладывают в соцсетях, пытаясь досадить человеку и его близким. Одна из самых больших проблем – остановить повторную загрузку и циркуляцию этих изображений. Это огромный шаг вперед», – заявляет основатель британской горячей линии «Порномести» Л. Хиггинс.

По словам Л. Хиггинс, с 2015 г. ее организация столкнулась с более чем 6 200 случаями «порномести».

***

10.04.2017

Facebook тестирует бесплатную версию корпоративной социальной сети Workplace

В октябре Facebook представила Workplace – платный социальный сервис для рабочих нужд. Теперь компания с целью расширения пользовательской базы начала тестировать бесплатную версию продукта. Она получила название Workplace Standard, а платный вариант был переименован в Workplace Premium (InternetUA).

«Мы позволяем работать в Workplace большему числу компаний, поэтому для нас это достаточно серьёзный шаг», – сказал менеджер по продукту Facebook С. Кросс (Simon Cross). Он добавил, что не каждое предприятие готово платить за сервис. Поэтому Facebook даёт возможность сперва опробовать бесплатную версию продукта в рамках отдельной команды или подразделения.

В Workplace, как и в Facebook, можно создавать группы и публикации, отмечать людей на фотографиях, делиться файлами и общаться с несколькими членами организации. Для личных переписок и звонков используется система Work Chat, которая представляет собой переработанный Messenger. Также в сервисе есть инструменты вроде аналитической панели.

Workplace позиционируется как офисное онлайн-пространство с чертами Facebook. Личный аккаунт к сервису не привязывается. Для компаний с тысячей пользователей и менее стоимость членства составляет 3 долл. за человека. Если предприятие включает в себя до девяти тысяч работников, то подписка обходится в 2 долл. Компании более чем с 10 тыс. сотрудников платят по 1 долл.

Бесплатный продукт пока только тестируется и доступен не всем. В нём не будут доступны административные и аналитические функции, как платным подписчикам.

***

10.04.2017

Facebook запустила помощник M в Messenger

Социальная сеть Facebook запустила анонсированный еще в 2015 г. цифровой помощник M в приложении Messenger. Новые возможности будут доступны на iOS и Android в США, позже появятся в других странах (ht.ua).

Помощник M использует возможности искусственного интеллекта для анализа диалогов. Анализируя ключевые слова, он может предлагать собеседникам в чате совершать те или иные действия. К примеру, если пользователи обсуждают будущую встречу, помощник M предложит составить план, отметить место встречи на карте и даже вызвать такси. Рекомендации отображаются в окне чата в виде соответствующего логотипа.

Помимо этого, помощник умеет отправлять стикеры, переводить деньги, делиться текущим местоположением, создавать голосования в чатах, вызывать такси через приложения Lyft или Uber. Цифровой помощник поддается обучению, а при желании его можно отключить в настройках.

Facebook Messenger с помощником M доступен в режиме бета-тестирования жителям США. Официальную презентацию стоит ожидать в течение месяца. Со слов разработчиков, в будущем он обзаведется многими полезными функциями и будет абсолютно бесплатным.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

29.03.2017
Facebook запустила сервис для контакта с политиками

Социальная сеть Facebook запустила инструмент, который позволяет пользователям находить своих представителей во власти и связываться с ними по различным каналам. О запуске сервиса под названием Town Hall написал на своей странице основатель и глава Facebook М. Цукерберг (Internetua).

В настоящее время сервис Town Hall доступен только в США. Как пишет Mashable, воспользоваться им можно как в мобильной, так и в веб-версии Facebook. Для этого необходимо найти вкладку Town Hall на странице настроек, зайти в нее и указать адрес проживания. После этого сервис выдаст список представляющих интересы пользователя чиновников и лиц, занимающих выборные должности.

Затем пользователь может подписаться на обновления всех или некоторых людей из списка или выбрать опцию «связаться», которая позволит написать личное сообщение в Facebook, отправить письмо по электронной почте, позвонить выбранному человеку или просто зайти на его страницу. Соцсеть также предложит написать или позвонить своему представителю, если пользователь добавит его в ленту и поставит лайк той или иной записи политика.

Mashable отмечает, что сервис позволяет гражданам высказать свое беспокойство по поводу тех или иных решений власти, включая политику

новой американской администрации. Этот шаг также можно рассматривать как часть плана М. Цукерберга по укреплению гражданского сообщества.

***

11.04.2017

На каналі YouTube Чернівецької обласної служби зайнятості розміщені відеорезюме шукачів роботи

Для зручності та оперативного підбору кандидатів на вакантні посади на каналі YouTube Чернівецької обласної служби зайнятості розміщені актуальні відеорезюме шукачів роботи. Про це повідомляє в. о. директора Чернівецького обласного центру зайнятості Л. Кожолянко (Час).

«Сьогодні в кожному центрі зайнятості наші фахівці порадять, як гідно представити себе роботодавцю, та допоможуть у складанні відеорезюме й організації онлайн-співбесід. Роботодавець за таким резюме може побачити реальну людину, а співбесіди онлайн дають змогу істотно економити час та кошти при підборі фахівців. Це в рази підвищує ефективність працевлаштування шукачів роботи», – зазначає Л. Кожолянко.

У центрі зайнятості переконані, що, переглядаючи саме таке резюме, роботодавець зможе побачити кандидата й одразу ж скласти перше враження про нього, оцінити його перспективність, уміння висловлювати думки та презентувати себе. Після перегляду такого резюме він вирішить, чи запрошувати людину на співбесіду.

Переглянути відеорезюме шукачів роботи можна на каналі YouTube Чернівецької обласної служби зайнятості за посиланням https://www.youtube.com/playlist?list=PLGiETICtPzBJT78tgfyD1kj8_fPIFqnz_.
Також за професійним складом безробітних відеорезюме можна переглянути на сторінці Чернівецького обласного центру зайнятості http://www.dcz.gov.ua/chn/control/uk/publish/article?art_id=40332&cat_id=40241.

Крім того, служба зайнятості створює та постійно поновлює банк даних резюме випускників професійно-технічних закладів області. З ними можна ознайомитися за посиланням https://www.youtube.com/playlist?list=PLGiETICtPzBJGaCPbd4LeyISORqMwTfma.

***

7.04.2017

Для розшуку людей і речей чернігівські поліцейські створили офіційні групи у соцмережах

Правоохоронці Чернігівського відділу поліції для більш ефективного розшуку осіб, які переховуються від поліції, а також для впізнання осіб, які скоїли кримінальні правопорушення, створили офіційну групу «Їх розшукує поліція Чернігова». Такі групи з’явились у Facebook, «ВКонтакте» та Viber. За

повідомленням поліцейських, у цій групі періодично писатимуть про осіб, які або офіційно перебувають у розшуку, або в ході пошукових дій встановлюється їх місцеперебування. Також тут будуть розміщені фото осіб, безвісти зниклих і невпізнаних. Із метою місцезнаходження вкрадених у містян речей викладатимуть як орієнтування фото вкраденого майна. До складу учасників групи можуть входити всі жителі міста, області та держави. Допомога суспільства в розкритті злочинів вітається. Правоохоронці просять учасників груп обговорювати інформацію по суті та ставитись із повагою та розумінням до мети створення спільноти. Якщо ви володієте тією або іншою інформацією, знаєте місцезнаходження розшукуваного або бажаєте надати допомогу із встановлення безвісти зниклого, пишіть адмінам або в коментарях. Правоохоронці гарантують конфіденційність (ЧЕline).

***

31.03.2017
Facebook тестирует функцию сбора средств на благотворительность

Социальная сеть Facebook испытывает функцию Personal Fundraisers, которая позволяет совершеннолетним пользователям сервиса собирать деньги на благотворительность. Об этом компания сообщила в своем блоге (IGate).

В апреле нововведение пройдет бета-тестирование в Соединенных Штатах Америки. Изначально Facebook ввел шесть категорий «основных финансовых потребностей», на которые пользователи смогут собрать средства.

В эти категории вошли образование, медицинская и ветеринарная помощь, помощь в чрезвычайных ситуациях (к примеру, стихийное бедствие), личные чрезвычайные ситуации (пожар или авария), а также похороны. Собирать деньги можно в течение суток.

«Поскольку пользователи видят профили на Facebook, они знают, кто именно организовал сбор средств, кому они будут направлены и кто участвует в кампании еще», – сообщение в блоге Facebook.

Также в соцсети рассказали, что по мере тестирования компания надеется расширить количество категорий и автоматизировать процесс рассмотрения заявок. Пользователи сервиса смогут вносить денежные пожертвования прямо в Facebook.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

4.04.2017
Мешканці Кіровоградщини зможуть оформляти кредити через Viber

В Україні запустили новий сервіс оформлення розстрочки в популярному месенджері Viber. За допомогою бота «Оплата частинами», мешканці Кіровоградщини, які є клієнтами ПриватБанку, просто в месенджері зможуть

оформити бажану суму в кредит, а також знайти товари, на які діє програма безпроцентної розстрочки (Persha.kr.ua).

Новий сервіс банку доступний всім власникам платіжних карток ПриватБанку.

«Тепер у Viber розстрочку на оплату будь-яких покупок можна оформити за хвилину без паперів і відвідання відділення банку», – говорить керівник Бізнесу з роботи з торговими підприємствами ПриватБанку Є. Васильцов.

Для використання бота досить вибрати в пошуку месенджера паблік-акаунт «Оплата частинами» та натиснути на кнопку потрібної операції. За допомогою бота можна дізнатися про доступний ліміт використання сервісів розстрочки «Оплата частинами» та «Миттєва розстрочка», оформити кредит, отримати інформацію щодо вже укладених договорів та одержувати новини про вигідні пропозиції торговельних мереж.

ПриватБанк – перший український банк, що запустив сервіс оформлення кредиту та отримання інформації за кредитними договорами в чатах найпопулярніших месенджерів – Facebook, Telegram і Viber.

***

4.04.2017

Николай Вязов

Facebook хочет превратить WhatsApp в средство для мобильных платежей

Популярный мессенджер WhatsApp, принадлежащий крупнейшей в мире социальной сети Facebook, может стать средством осуществления цифровых платежей – сообщило информационное агентство Reuters (24news.com.ua).

По его данным, компания Facebook может инициировать соответствующий эксперимент на протяжении следующих шести месяцев.

Новая возможность будет в первую очередь ориентирована на пользователей WhatsApp из Индии – Facebook, как известно, рассматривает эту азиатскую страну в качестве одного из наиболее динамичных и перспективных рынков.

«Мы всерьез рассматриваем возможность трансформации мессенджера WhatsApp в многофункциональный инструмент, который, среди прочего, позволит проводить мобильные платежи, заменяя тем самым привычные пластиковые карты», – заявлял журналистам в феврале 2017 г. Б. Эктон, соучредитель WhatsApp.

По словам Б. Эктона, необходимые для осуществления проекта переговоры с властями Индии уже были проведены. Пока что не известно, будет ли Facebook расширять географию проекта за территорию Индии, или платежное средство на основе WhatsApp будет эксклюзивным для этой страны.

***

6.04.2017

«ВКонтакте» сделает аудиозаписи платными

В социальной сети «ВКонтакте» скоро появятся платные функции для прослушивания аудиоконтента. Соответствующее упоминание было обнаружено в приложении мобильного оператора VK Mobile (IGate).

Пользователи нашли в исходном коде Android-приложения текст «Подписка на музыку “ВКонтакте” включена в абонентскую плату». Цена подписки без абонплаты оператора не указана.

Метод работы также не описывается. Как правило, подобные подписки на музыкальные сервисы либо дают полный доступ к музыкальной библиотеке, либо отключают рекламу, которая воспроизводится при бесплатном прослушивании музыки.

***

6.04.2017

YouTube официально запустил собственный сервис онлайн-телевидения

YouTube TV доступен за 35 долл. в месяц. Пока только в США (IGate).

Стриминговый сервис YouTube TV, анонсированный в прошлом месяце, официально начал работу в ряде американских городов. Получить доступ к нему можно по подписке в пяти городах Соединенных Штатов Америки – Нью-Йорке, Филадельфии, Чикаго, Лос-Анджелесе и Сан-Франциско.

Информация о том, что YouTube работает над запуском платформы веб-телевидения, появилась достаточно давно. Пользователи YouTube TV имеют возможность просматривать «живые» трансляции таких каналов, как ABC, CBS, NBC, FOX, ESPN и пр.

Сервис рассчитан прежде всего на «поколение YouTube». Подписчики смогут смотреть материалы на любых устройствах.

В рамках новой службы реализована система облачного рекордера Cloud DVR с безлимитным хранилищем. То есть, подписчики смогут записывать неограниченный объем видеоконтента для последующего просмотра в удобное время.

YouTube TV можно смотреть через специальный веб-интерфейс на компьютере, а также при помощи приложения для устройств под управлением iOS и Android. На телевизорах стриминг поддерживается через Chromecast.

Стоимость подписки на YouTube TV для жителей США составляет 35 долл. в месяц с возможностью использования сразу шести аккаунтов. В эту цену входит также подписка на YouTube Red. Никаких обязательств по использованию сервиса нет – подписчики смогут отказаться от него в любой момент.

О сроках запуска сервиса в других регионах пока не сообщается.

***

10.04.2017

Facebook и еще девять компаний займутся улучшением медиаграмотности читателей

Группа технолидеров и организаций, поддерживающих журналистику, образовали медиаконсорциум News Integrity Initiative, который займется улучшением медиаграмотности читателей и повышением доверия к журналистике, сообщает издание «Мы и Жо» (PRportal).

Организаторами фонда выступили Facebook, Craig Newmark Philanthropic Fund, Ford Foundation, Democracy Funcd, John S. and James L. Knight Foundation, Tow Foundation, AppNexus, Mozilla и Betaworks. Совместно они вложили в News Integrity Initiative 14 млн долл.

Фонд является независимым проектом, управлять которым будет Tow-Knight Center for Entrepreneurial Journalism (Центр предпринимательской журналистики Tow-Knight, цель которого подготовить журналистов к созданию собственных медийных стартапов или к внедрению инноваций в уже существующих СМИ), относящийся к школе журналистики CUNY Graduate School of Journalism.

***

10.04.2017

Facebook готов платить НДС в России

Вслед за крупнейшими интернет-компаниями социальная сеть Facebook встала на учет Федеральной налоговой службы РФ, выразив таким образом свою готовность платить НДС при продаже виртуальных товаров на территории России. Об этом сообщает sostav.ru (МедиаБизнес).

В ФНС уже зарегистрировались такие крупные технологические и интернет-компании как Apple Distribution International, Google Commerce Ltd, Microsoft Ireland, Netflix International B.V. и Wargaming Group Ltd, Bloomberg, Financial Times, LinkedIn и др. Все они либо продают программное обеспечение и компьютерные игры, либо контент, в том числе музыку, фильмы и книги, либо являются сервисами онлайн-бронирования.

В соответствии с Законом, принятым летом прошлого года, все иностранные компании, предоставляющие соответствующие услуги на территории РФ обязаны уплачивать НДС. Так называемый закон о «налоге на Google» обязывает западные компании вставать на учет в налоговом органе и регулярно предоставлять декларацию по налогу на добавленную стоимость. Российские организации уже платят такой налог, поэтому законопроект уравнял их с иностранными игроками.

***

10.04.2017

На YouTube будет сложнее зарабатывать

YouTube пытается побороть проблему кражи видео (IGate).

Пять лет назад программа монетизации контента на YouTube стала доступна всем желающим. Это было поистине грандиозным событием, так как любой пользователь получил возможность опубликовать видео и сразу же начать получать деньги с просмотров. Как результат, появилось большое количество авторов, а сам сервис стал крупнейшей в мире видеоплатформой. Однако, все это повлекло за собой и ряд проблем. Некоторые хитрые пользователи начали выкладывать у себя на каналах чужие видео, получая деньги с просмотров. Для решения этой проблемы в Google решили внести изменения в условия программы для партнеров.

Отныне пользователи не могут начать процесс монетизации своего видео до тех пор, пока на канале не наберется 10 тыс. просмотров. В Google считают, что такого числа достаточно, чтобы собрать достаточно информации о канале и проверить, является ли опубликованные на нем видео легальными.

«В ближайшее время мы добавим процесс проверки для новых авторов, которые подают заявку для подключения партнерской программы. После того, как пользователь накопит на своем канале 10 тыс. просмотров, мы проанализируем их действия на соблюдение наших правил. Если все будет хорошо, мы начнем показ рекламных объявлений на их контенте. Новые правила помогут добиться того, чтобы выручку получали лишь те, кто играет по правилам», – рассказал вице-президент YouTube по управлению продуктами А. Бардин.

Такое изменение в политике YouTube не только позволит уменьшить число пиратского контента, но и позволит самим рекламодателям быть уверенным, что они вкладывают деньги в проверенные каналы.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

7.04.2017

Близько 100 чернігівських школярів – учасники спільнот, в яких заради «лайків» підлітки влаштовують бої без правил

Жорстокі бійки серед дівчат-підлітків у Чернігові могли бути спричинені змаганням у соцмережах за визнання (Високий вал).

Про таке припущення написав на своїй сторінці у Facebook Уповноважений Президента України з прав дитини М. Кулеба.

У соціальній мережі набувають популярності спільноти «ЗАБИВЫ», «ULTRAPIR» та ін., де діти заради лайків б’ють один одного ледь не до смерті.

«У них “змагаються” відео, де чисельна група підлітків у прямому сенсі забивають однолітків. Якщо твій “вайн_батл” набирає більшу кількість лайків і репостів – ти крутий, сміливий переможець. А у деяких спільнотах за перемогу ще й светрик дарують», – написав М. Кулеба.

На стіні таких спільнот розміщені купа відео, на яких молодь влаштовує жорстокі бійки між собою.

«Можливо, учасниці бійки у Чернігові і не змагалися за винагороду, але підозрюю, що на таку жорстокість їх могло “надихнути” змагання в цих мережах», – припустив Уповноважений Президента.

Аби перевірити цю інформацію, «Високий Вал» промоніторив декілька груп, чи дійсно вони направленні на жорстокі побиття.

Як вдалося з’ясувати, до вже згадуваного пабліку «ULTRAPIR» дійсно входить 33 чернігівські школярі. Проте при подальших пошуках виявилося, що чернігівські підлітки активні учасники й інших бійцівських груп. Подібних спільнот у мережі десятки і майже до кожної входять більше 10 хлопців і дівчат з обласного центру.

***

9.04.2017

Вчені з’ясували, як Facebook та Instagram впливають на добробут дітей

Британські вчені з Університету Шефілду підтвердили: чим більше часу діти проводять у соціальних мережах, тим нещаснішими вони почувають себе майже у всіх аспектах життя (Інформаційна агенція «Вголос»).

Відповідно до дослідження, підготованого для інституту The IZA Institute of Labor Economics, перебування в соціальних мережах протягом усього однієї години знижує на 14 % ймовірність того, що діти будуть повністю задоволені життям. Навіть проживання з одним із батьків впливає на благополуччя дитини в три рази менше.

Діти, які більше часу проводять в Facebook і Instagram, почувають себе менш щасливими в тому, що стосується їхньої успішності, зовнішності та сім’ї. При цьому діти, які активно користуються соціальними мережами, в більшій мірі задоволені стосунками із друзями. Крім того, користування соцмережами сильніше впливає на добробут дівчаток, ніж хлопчиків, з’ясували дослідники.

Задля проведення дослідження співробітник Університету Шефілду Ф. Пауелл і його колеги відібрали чотири тисячі дітей у віці від 10 до 15 років і попросили їх оцінити за семибальною шкалою, наскільки вони задоволені різними сферами свого життя.

***

6.04.2017

Смайлы в сообщениях указывают на психические проблемы – ученые

У многих людей в наше время виртуальная жизнь оказывается куда интенсивнее, нежели реальная. Специалисты заявляют, что по манере человека писать сообщения можно сделать некоторые выводы о его характере, передает medikforum.ru. (ria-m.tv).

В частности, говорят эксперты, если человек часто использует слова «плохо» и «боль», это с большой вероятностью говорит о наличии какого-либо недомогания. Кроме того, о проблемах со здоровьем или психологическим состоянием говорят короткие сообщения.

Кроме того, исследователи подметили: пристрастие к использованию смайликов в переписке может быть сигналом психиатрических проблем.

Дело в том, что с помощью значков, выражающих эмоции, люди стремятся наладить контакты с окружающими, пояснили ученые. Их обилие может говорить о нестабильной психике, о низкой самооценке и зависимости от мнения других. А еще использование «улыбок» может сигнализировать о депрессии, которую человек старается скрыть от окружающих.

***

1.04.2017
Ольга Карпенко
Как соцсети воспитали поколение самовлюбленных нарциссов

Статьи о том, как вредны социальные сети, выходят часто и с завидной регулярностью набирают множество репостов и лайков. Недавняя статья А. Эрора для Highsnobiety тому яркий пример: в ней автор жестоко критикует социальные сети за подмену реальной жизни погоней за лайками. И в то же время статья собрала более 100 000 перепостов. Она может показаться высокомерным ворчанием на заезженную тему, но ее наблюдения заслуживают внимания (AIN.UA).

В начальной сцене культового британского фильма «На игле» главный герой Рентон (его играет Э. МакГрегор) разражается нигилистической, но странным образом вдохновляющей тирадой о том, как за годы правления М. Тетчер духовно бедный материализм завоевал Британию.

«Выбирайте жизнь… Выбирайте огромный чертов телек, стиралки, машины, плееры и электрические открывашки», – говорил герой, пускаясь затем в обличение потребительства.

Этот монолог стал идеальным диагнозом для нации, которой 18 долгих лет управляла партия консерваторов, и его запомнят как эпитафию этому определяющему периоду британской истории. Затем, в январе 2017 г., спустя 20 лет вышел сиквел «На игле».

Спустя два десятилетия после оригинала в новом фильме опять-таки есть нарекания Рентона, но адаптированные под современность. «Выбирайте жизнь… Выбирайте Facebook, Twitter, Instagram и надейтесь, что кому-то, где-то не все равно». И хотя этот монолог не так хорош, как в оригинале, а нападки

на социальные медиа кое-где в Интернете прозвали суеверием, мне не приходит в голову что-то, более подходящее для 2017 г.

Спустя десятилетие после расцвета Facebook, вряд ли просто назвать любой другой феномен, который сформировал бы массовую культуру в такой же степени, как социальные медиа.

Они изменили то, как мы общаемся, повлияли на победу Д. Трампа, поместили нас в искажающие реальность информационные пузыри, выработали в нашем мозгу что-то вроде привыкания и угрожают уничтожить традиционные СМИ.

Заниматься перечислением всех аспектов нашей жизни, на которые повлияли соцмедиа, – пустая затея, но есть один аргумент, который я попытаюсь доказать: социальные сети превратили целое поколение в скучных «нарциссов».

От селфи под мудреными углами, которые превращают обычных людей в красавцев, до режиссирования Facebook-ленты так, чтобы она казалась лентой веселого человека: социальные сети взяли неолиберальную мантру самовлюбленности и накачали ее стероидами.

Возможно, эпоха Тетчер и Рейгана и продвигала жадность и эгозим, что и раскритиковал Рэнтон в первом «На игле», но социальные сети вознесли талант человечества к самолюбованию к новым высотам.

Технологические предприниматели Долины и одержимые Snapchat подростки могли бы поспорить, что социальные сети объединяют людей по всему миру (доказать обратное действительно сложно), но эти связи вряд ли стоит путать с общностью.

Все социальные сети наполнены людьми, состязающимися за фолловеров, лайки, твиты и любые другие признаки одобрения, а не радеющими за общие цели.

Это, конечно, не единственная их цель, в сетях зарождается много позитивных начинаний, но все же множество людей используют их исключительно для того, чтобы проецировать во внешний мир идеализированную версию себя: аватар человека, которым они хотели бы стать, а не того, кем являются на самом деле.

Логично, что такой фокус на себе неизбежно приводит к самолюбованию, однако оно выражается не только в сотнях селфи и восприятии любого события как повода придумать новые теги. Каждое событие реальной жизни, пусть и нерелевантное для аудитории соцсетей, воспринимается их пользователями как потенциальный источник саморекламы.

Подумайте над абсолютно бессмысленным поздравлением с Днем рождения, высказанным на Facebook в адрес человека, который там даже не зарегистрирован. Сомневаюсь, что хоть кто-то сможет объяснить, зачем он это делает, вряд ли люди рефлексируют над этим типом поведения. Если рассказывать что-то о себе, это приносит одобрение других, что приятно, так что они продолжают. Каждый лайк и ретвит питает мозг небольшим впрыскиванием дофамина, сравнимым с невероятно малой дозой кокаина.

Вот почему пользователи добавляют #tagsforlikes #likeforlikes и #likes4likes к своим фото в Instagram. Эта тоска по одобрению настолько выражена, что породила целую биржу обмена неискренними знаками признания. Чувства ничего не значат, пока на экран продолжают поступать уведомления о лайках.

Цинизм, который воспитывают соцсети, удивителен. В декабре прошлого года исламский фундаменталист направил грузовик на рождественскую ярмарку на западе города, убив 12 и покалечив 56 человек.

Facebook сразу же включил опцию чекина, которая позволяла пользователям из Берлина сообщать друзьям, что с ними все в порядке. Не буду рассуждать о том, насколько это полезная функция, но что случилось после этого, заставило меня застонать. Самые ненасытные пользователи из моей ленты все ринулись высказывать свои мысли о трагедии, рассказывать миру, что они чувствуют по этому поводу. Не помню, кто конкретно этим занимался, но приведу пример, который до сих пор у меня перед глазами. Один из моих друзей написал: «Со мной все ОК, но по крайней мере, с девятью людьми – нет. И это не ОК».

Да, конечно, массовые убийства – это не ОК, а снег – холодный, а химическая формула диоксида углерода – $CO2$. Какой цели служит подобный пост, кроме желания доказать другим людям на Facebook, что вы – не социопат?

Он написан ради лайков. Комментариев. Ради внимания. Без сомнения, кто-то сейчас читает этот текст и думает, что автор циничен. Но мне кажется, настоящий цинизм – в том, как человеческие трагедии превратились в контент на Facebook и рекламную возможность для его жителей.

Конечно, это часть обычного человеческого поведения: общение, коллективная скорбь, высказывание своего мнения. Единственное, что отличает эту практику от настоящих поминок – использование посредника.

Здесь есть фундаментальное отличие. До цифровой эры это были типы поведения, которые мы практиковали с другими близкими и важными для нас людьми уединенно. Социальные сети – это публичый форум.

Пользователь, которого я процитировал, не просто озвучил свои сожаления об умерших. Он поместил себя в контекст трагедии. Фокус сместился с погибших на его мысли и переживания.

То же самое случилось и после ноябрьской террористической атаки в Париже, когда Facebook дал пользователям возможность применить к аватаркам фильтр в цветах французского флага. Цель этой акции состояла в пустопорожнем выражении солидарности с погибшими, их семьями и всеми французами. Помню, как поспорил с одним таким пользователем, который искренне верил в то, что соболезнование в один клик как-то поможет тем, кто потерял близких.

Как будто кто-то в любой момент истории думал про себя: «Господи, какой ужас, но мне явно полегчает от того, что миллионы людей по всему миру

цепляют флаг моей страны себе на физиономию». Ведь лучший способ избавиться от душевных мучений – это ура-патриотизм.

Но отличается ли эта практика от старой традиции оставлять цветы и свечи на месте трагедий? Да, поскольку в последнем случае это предполагает физическое участие. В этом паломничестве есть почти религиозный аспект, даже если вы просто переходите через улицу. Мельчайший элемент жертвы – в том, чтобы зажечь свечку или положить цветок. Это все же требует больших усилий, чем напечатать пост в Facebook или твит.

Это – анонимный ритуал, ведь никто не знает, кто оставил цветы. Это – полная противоположность горю в социальных сетях, вульгарному поведению, оттягивающему внимание от жертв трагедий на себя. Поведению, которое оплачивается валютой одобрения.

Более того, олдскульное, аналоговое горе невозможно монетизировать в рамках какой-то компании из Долины, создавшей эти фишки, поскольку они вписываются в бизнес-модель.

Я не хочу стыдить людей за инстинктивное, несознательное поведение (и если меня читает друг из Facebook, которого я цитировал – не обижайся, ничего личного). Суть в том, что технологические компании забрались к нам в мозг и перепрошили его.

Они создали поколение самовлюбленных нарциссистов – нас. Регистрация в сети может быть бесплатной, но долговременное ее использование имеет свою цену.

Маніпулятивні технології

3.04.2017
Вікторія Жуган
Хто і як виловлює фейки у Facebook

Як роботи допомагають боротися з пропагандою та хто відловлює фейки у Facebook? Про це Радіо Свобода розповів виконавчий директор американського видання PolitiFact Е. Шерокман (Радіо Свобода).

PolitiFact спеціалізується на перевірці фактів, що мовою журналістів називається «фактчекінгом». Редакція із 10 осіб аналізує заяви і Д. Трампа, і Б. Обами, інформацію про вірус Ебола і критику системи «Обамакер». Критики закидають, що видання перевіряє в основному республіканців, тоді як у PolitiFact стверджують: однакову увагу приділяють обом партіям.

Із грудня 2016 р. PolitiFact займається фактчекінгом для Facebook. Тоді соцмережа вперше дозволила користувачам позначати публікації як неправдиві або сумнівні, щоб такі матеріали мали менше шансів потрапити у новинну стрічку.

До Києва виконавчий директор американського видання PolitiFact Е. Шерокман приїхав заради участі у Digital Disruption Forum. Подія проходить 3–4 квітня і зібрала медійників із близько 20 країн.

– Чи можуть роботи побороти дезінформацію?

– Думаю, що так. Раніше ми перевіряли в основному меседжі виборчих кампаній і заяви політиків. Тепер для Facebook ми також досліджуємо фейкові новини. За ці кілька місяців ми зрозуміли, хто їх створює, які є типи цих матеріалів і на яких веб-сайтах їх тиражують. Комп'ютер точно зможе все це відслідкувати.

Інша річ, у якій технології може допомогти, розкручувати перевірені новини... Скажімо, пошук у Google іноді видає найбільш популярний результат. А він не обов'язково є достовірним. Я вважаю, що роботи пошукових систем повинні краще ранжувати видання, які заслуговують на довіру.

– Ваша організація використовує роботів?

– Так, і це безкоштовні програми, доступні в Інтернет. Наприклад, ресурс Mapchecking.com дає змогу визначити кількість учасників мітингів за фотографією. Його формула враховує площу і кількість осіб на метр квадратний. За допомогою таких ресурсів можна спростувати заяви речника Д. Трампа Ш. Спайсера про те, що за його інавгурацією спостерігала «найчисельніша аудиторія в історії» (Ш. Спайсер 21 січня звинуватив журналістів у заниженні кількості учасників інавгурації, щоб применшити «величезну підтримку» нового президента під час присяги. – Ред.).

Або ж ресурс ClaimBuster, який здатен у прямому ефірі розшифровувати виступи політиків і позначати фрази, які варто перевірити.

– Яка ваша роль у відслідковуванні фейків у Facebook?

– Користувачі можуть поскаржитися, що матеріал неправдивий. Коли набирається достатня кількість скарг, PolitiFact разом зі ще трьома американськими фактчекінговими організаціями (Snopes, Factcheck.org, ABC News. – Ред.), а також The Associated Press, отримує список усіх таких публікацій.

Тоді ми вирішуємо, які посилання перевіряти, адже не всі із них фейки. Обираємо матеріали, які порушують стандарти найбільше і які набирають значної популярності. Фокусуємося в основному на політиці – користувачі також часто зголошують розважальні матеріали.

– А якщо мій друг-програміст із Росії створить робота, який надішле у Facebook достатню кількість скарг на наше з Вами інтерв'ю?

– Так, це проблема. Або ж, скажімо, ви підтримуєте Г. Клінтон і позначаєте всі матеріали про Д. Трампа як фейки. Чи навпаки.

Чим більше ми розуміємо, як працюють тролі і розповсюджувачі фейків, тим більше усвідомлюємо, наскільки важлива роль людини. Якщо ми маємо справу з російською пропагандою або російські тролі масово позначили якісь матеріали як фейки – є гарні новини. Перевіркою займаємося ми, незалежні фактчекери. Якщо виявиться, що матеріал зголосили несправедливо, ніяких змін в алгоритмі не відбудеться.

– Тобто про війну роботів проти роботів поки не йдеться?

– Наші дослідження показують, що всі люди висловлюються по-різному. Англійська мова дуже складна, одна кома може змінити весь зміст. А якщо

подивитися на президента Д. Трампа – він часто говорить без підготовки, перескакує з однієї думки на іншу. Комп'ютер не в стані зрозуміти, що ж він мав на увазі.

У випадку з Facebook «покарання» дійсно суворе: позначка «фейк» лишається при матеріалі назавжди. Якщо пізніше хтось захоче її поширити, то зробить це разом із попередженням про сумнівність змісту. Думаю, у таких рішеннях Facebook точно хоче покладатися на людей і не зловживати системою.

У PolitiFact ми не прагнемо бути «поліцією думок», люди можуть поширювати що завгодно. Ми ж тільки хочемо пересвідчитися, що це достовірна інформація. Ми використовуємо роботів на повну, але читачам важливо знати, що всім керує людина. Зазвичай людям одразу хочеться знати, ЗМІ сказали правду чи ні. Вони не хочуть почекати десять хвилин чи годину, не кажучи вже про день. Насправді ж робота над перевіркою одного матеріалу може зайняти від однієї до кількох діб. І ось тут на допомогу приходять роботи.

– Фактчекінг допоможе виграти інформаційну війну?

– Аудиторія вже сама вимагає фактчекінгу! Зараз кожен може бути «журналістом», аби тільки був смартфон чи комп'ютер. Я це говорю і згадую про Арабську весну, світ дізнався стільки всього завдяки соцмережам. Кожен може опублікувати якусь інформацію – і дезінформацію також. Питання тільки, як оцінювати її вартість. 50 років тому треба було мати друкарський верстат, супутникову чи радіоантену. А тепер усі ці перешкоди зникли. Тому популярність фактчекінгу так зросла, люди намагаються зрозуміти, що правда, а що ні.

Але у сьогоднішніх умовах фактчекінг – це дорога й екстравагантна забаганка. У нас у редакції 10 осіб, ми публікуємо 150 матеріалів на місяць. А Washington Post стверджує, що ставить новий матеріал щохвилини. А отже, саме комп'ютери дозволять скоротити час нашої роботи від одного дня до шести годин, наприклад. Таким чином, боротьба проти фейків набиратиме обертів.

***

6.04.2017

Основатель eBay инвестирует 100 млн долл. в борьбу с фейковыми новостями

Благотворительный фонд основателя компании eBay П. Омидьяра в ближайшие три года вложит 100 млн долл. в независимые журналистские расследования и борьбу с пропагандой ненависти и фейковыми новостями, пишет Forbes со ссылкой на заявление самого бизнесмена, сделанное во время международного форума Skoll World Forum (Sostav.ua).

Первые 4,5 млн долл. будут направлены в Международный консорциум журналистов-расследователей (ICIJ), который в 2016 г. опубликовал масштабное расследование о владельцах панамских офшоров. Среди других

организаций, которые получат деньги П. Омидьяра, значатся Латиноамериканский альянс за гражданские технологии и неправительственная правозащитная организация «Антидиффамационная лига».

П. Омидьяр не в первый раз оказывает финансовую поддержку СМИ и организациям, занятым разоблачением коррупции и сосредоточенным на защите прав человека. Так, в 2013 г. основатель eBay инвестировал 50 млн долл. в журналистский проект экс-колумниста The Guardian Г. Гринвальда First Look Media.

Фейковые новости становятся глобальной проблемой, поэтому на борьбу с ними поднимаются все новые и новые СМИ, организации и влиятельные люди. Так, в конце прошлого года Facebook, Twitter, газеты New York Times, Washington Post, Telegraph, Le Monde, издание BuzzFeed News, телеканалы CNN и Al Jazeera, агентство AFP, Agence France-Presse и ряд других СМИ присоединились к проекту First Draft News, финансируемому компанией Google, целью которого является борьба с распространением фейков, в том числе в социальных сетях.

***

6.04.2017

Есть работа: требуется команда «эльфов» для борьбы с «кремлеботами»

Бывший сотрудник латвийского дипломатического ведомства собирает команду, готовую противостоять «кремлеботам» и «ольгинским». И. Бисениекс, который раньше работал в латвийском МИД, объявил о наборе команды «эльфов», которые будут бороться с фейками и пропагандой кремлевских «троллей» в социальных сетях и электронных масс-медиа, сообщает Диалог UA (From-UA. Новости Украины).

«Главная цель, которую я ставлю, – это awareness raising, повышение информированности людей, которые ежедневно пользуются Интернетом», – говорит И. Бисениекс.

По его словам, нужно добиться активности энтузиастов, которые могут коротким и приемлемым способом донести до людей актуальную информацию.

И. Бисениекс считает, что бороться с каждым комментарием и высказыванием «троллей» – бессмысленное занятие, поскольку выполнить данное физически невозможно. Да и не нужно это, поскольку «тролли» преследуют цель не доказать правду, а задеть, спровоцировать, вызвать какую-то эмоцию.

«Наоборот, надо регулярно давать людям рекомендации, показывать, где можно купить корректные, а не фейковые знания о том, чем они интересуются», – считает И. Бисениекс.

Спецслужби і технології «соціального контролю»

30.03.2017

В Украине готовят перечень запрещенных сайтов, которые угрожают национальным интересам

Министерство информационной политики начало составлять список сайтов, угрожающих нацинтересам страны. Об этом сообщает пресс-служба ведомства (ЧАС.UA).

Министр информационной политики Украины Ю. Стець заявил, что в рамках обязанностей, возложенных Доктриной информационной безопасности Украины, была создана рабочая группа, работающая над анализом правовых норм законодательства, которые запрещают распространение информации, представляющей угрозу национальным интересам Украины.

«Мы создали список правовых норм, содержащихся в различных законодательных актах и Уголовном кодексе Украины, которые регламентируют и четко определяют информацию, являющуюся запрещенной для распространения. На основании этих норм мы оцениваем материалы, которые распространяются отдельными сайтами и тем самым создают угрозу национальным интересам Украины, разжигают межнациональную вражду или призывают к нарушению конституционного строя», – сказал заместитель министра Д. Золотухин.

В ведомстве сказали, что после изучения и анализа материалов члены экспертного совета при МИП выскажут свои предложения относительно подходов и критериев оценки информации на основании этих правовых норм.

«Работа над списком конкретных сайтов осуществляется под грифом “Для служебного пользования” с целью предупреждения спекуляций со стороны российских и пророссийских СМИ и спецслужб», – отмечается в сообщении.

***

30.03.2017

В окупованому Криму затримали татарина за публікацію в соцмережі

30 березня окупаційна влада Криму затримала ще одного місцевого активіста – Р. Бекірова – начебто за розміщений ним у соцмережах «заборонений матеріал» (Інформаційна агенція «Вголос»).

Про це повідомив у Facebook адвокат Е. Смедляєв.

«Щойно був затриманий активіст Р. Бекіров, його звинувачують у тому, що нібито він розмістив “ВКонтакте” заборонений матеріал. 20.29 КоАП РФ (створення та поширення екстремістських матеріалів. – Ред.)», – написав адвокат.

***

3.04.2017

Путін назвав «достатніми» нинішні обмеження Інтернету в Росії

Президент РФ В. Путін назвав достатніми нинішні обмеження в російському Інтернеті. Про це російський лідер заявив на з'їзді Загальноросійського народного фронту, повідомляє «Дождь» (LB.ua).

Путін зазначив, що не варто критикувати китайський варіант обмежень в Інтернеті.

«Нам не слід критикувати те, що робиться в Китаї. 1,5 млрд осіб. Підіть спробуйте ними покерувати. Колись Наполеон сказав: "Китай спить, і дай боже, щоб він спав якомога довше". Китай вже давно прокинувся, і цими процесами треба управляти», – зазначив він.

За словами В. Путіна, держава не повинна одноосібно формувати правила роботи Інтернету, тому що це питання потрібно вирішувати в діалозі з суспільством.

«У нас є обмеження: це пропаганда суїцидів, це дитяча порнографія, це пропаганда тероризму, розповсюдження наркотиків і т. д. Багато хто вважає, що цього недостатньо, потрібно ще жорсткіше. На мій погляд, поки що досить», – сказав він.

«І це вже треба акуратно, цивілізовано і технологічно відпрацювати в Інтернеті, от і все. А все, що не заборонено, все можна», – сказав президент РФ.

***

4.04.2017

В РФ инетрнет-компании выступили против внесудебной блокировки пиратских сайтов

Предложение министра культуры В. Мединского защитить российское кино, упростив процедуру блокировки сайтов с нелицензионным контентом, критически встречено участниками рынка. Об этом сообщает газета «Ведомости» со ссылкой на письмо Российской ассоциации электронных коммуникаций (РАЭК) спикеру Государственной думы В. Володину. В ассоциацию входят более 100 интернет-компаний, таких как Mail.ru Group, Google, eBay, Ozon, Rambler & Co, РБК, Microsoft и др. (Четверта Влада).

«Мы хотим, чтобы, когда законопроект поступит на рассмотрение в Госдуму, у депутатов уже была информация о нашей позиции», – заявил директор РАЭК С. Плуготаренко. По его словам, письмо господину Володину ушло 3 марта, а копия направлена в комитет Думы по информационной политике. Его руководитель Л. Левин пообещал учесть позицию отрасли.

«Внесудебный порядок опасен тем, что решение принимается административным органом, который в отличие от суда не является независимым», – говорится в пиьсме РАЭК. Владелец сайта не может реализовать свое конституционное право на защиту, поскольку не участвует в процессе. Внесудебный порядок предлагается применить к экономическим

спорам, а не для защиты прав и свобод человека или обеспечения безопасности государства, что, по мнению РАЭК, создает опасный прецедент. В ассоциации также опасаются, что, если поправки Минкульта будут поддержаны, то другие участники рынка тоже могут требовать введения внесудебных процедур для защиты своих прав.

Как сообщал «Ъ», Минкульт готовит законопроект о защите национальных фильмов в интернете, ужесточающий механизм блокировки пиратских сайтов. Согласно идее, поддержанной кинематографистами, доступ к интернет-страницам с российскими фильмами, размещенными там без ведома правообладателя, будут ограничивать без суда за пару дней. Предложение может быть внесено в Госдуму в виде поправок к законопроекту о блокировке «зеркал» пиратских сайтов.

***

4.04.2017

Плохие новости: силовики берут под контроль ЖЖ, ожидается зачистка блогеров

Плохие новости. В очередной раз оказались правы скептики, советовавшие менять ЖЖ на автономный блог.

Как известно, в конце декабря 2016 г. серверы ЖЖ переехали в Россию, пишет в ЖЖ блогер Н. Подосокорский (From-UA Новости Украины).

А. Носик тогда доходчиво объяснил, какие практические последствия это будет иметь для простых пользователей: «Идея перетащить серверы ЖЖ в Россию, “поближе к пользователям”, не нова: она впервые посетила моего друга Э. Полсона в октябре 2006 г., когда компания <суп> заключила с владельцами платформы договор о поддержке кириллического сегмента. В ту пору мне хватило 5 минут, чтобы на пальцах объяснить наивному американскому другу юридические последствия и угрозы такого шага для авторов, комментаторов и читателей ЖЖ. Так что платформа осталась там, где была, на Западном побережье США, и просуществовала там последующие 10 лет.

За этот период в России успели пересажать не меньше тысячи человек за посты, реплики, лайки, шеры, ретвиты и кросспосты в социальных сетях. Но ни одно из обвинительных заключений не основывалось на пользовательских данных, полученных силовиками от администрации сервиса LiveJournal Inc в штате Калифорния. В моём собственном уголовном деле есть переписка сыскарей с той самой администрацией, где содержится вежливый, но категорический отказ в предоставлении моих персональных данных, поскольку запрос не содержал никаких юридических оснований для их раскрытия. Больше оснований для таких отказов нет. Поскольку ЖЖ теперь физически хостится на территории России, вся конфиденциальная информация пользователей сервиса доступна отечественным спецслужбам в режиме реального времени, в соответствии с требованиями СОРМ-2 и СОРМ-3 к российским площадкам».

В середине февраля главным редактором Живого Журнала стал А. Королев, работавший до этого в должности заместителя директора вещания на пропагандистском телеканале RT.

Наконец, сегодня, после часового перерыва всем пользователям ЖЖ в ультимативной форме было предложено подписать новое соглашение. Особо примечательны в нем следующие пункты:

1.1. <...> Использовать Сервис вправе только физические лица, достигшие 14-летнего возраста.

Это, я так понимаю, ответ на участие школьников в недавних акциях протеста в Москве и регионах?

5.1. Технические данные, передаваемые Сервису программным обеспечением Пользователя, а также иные данные, передаваемые Пользователем Сервису, будут доступны Администрации и могут использоваться последней по своему усмотрению незапрещенными законом способами, в том числе для таргетинга демонстрируемой Пользователю рекламы.

То есть любые наши данные могут использоваться как и где угодно.

6.1.1. Администрация оставляет за собой право удалить Аккаунт и Блог если доступ к Блогу не осуществляется Пользователем более 6 месяцев подряд или был ограничен в течение того же срока в связи с нарушением Соглашения.

То есть стоит вам, к примеру, не дай Бог заболеть или уехать в продолжительную командировку или на стажировку в другую страну, где нужна полная погруженность в ваше занятие и нет времени на соцсети, администрация ресурса через полгода удалит ваш блог, даже если вы вели его десять и более лет.

6.3. Администрация обращает внимание Пользователя, что в соответствии с ч. 3 ст. 10.1 Федерального закона Российской Федерации № 149-ФЗ Администрация обязана независимо от волеизъявления Пользователя хранить и предоставлять по законным запросам уполномоченных органов:

6.3.1. информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений Пользователей и информацию о совершивших перечисленные действия Пользователях – в течение одного года с момента окончания осуществления таких действий.

То есть любому менту или чинуше предоставят по первому требованию любую информацию о вас – все ваши подзамочные посты, личные сообщения и т. д. и т. п.

7.4. Администрация обращает внимание Пользователя, что если доступ Блогу (странице Блога) составит более трех тысяч пользователей сети «Интернет» в течение суток, на Пользователя будут распространяться требования ст. 10.2 Федерального закона Российской Федерации № 149-ФЗ.

То есть если раньше администрация ресурса сопротивлялась этому идиотскому закону и даже скрыла количество подписчиков у тех блогеров, у

кого оно превышало 2500, то теперь в проскрипционный список будут заносить всех более-менее читаемых блогеров уже автоматически.

9. Размещая Контент, Пользователь:

9.1.3. Обязуется отмечать Контент, не допустимый в соответствии законодательством РФ для распространения среди детей (от 0 до 18 лет), как материал для взрослых, используя функциональность Сервиса.

Представляете, что теперь под каждым постом с ненормативной лексикой или с какими-то намеками на эротику или насилие (понимать это можно очень широко) надо ставить маркировку: 18+. Это же наверняка будет касаться постов с упоминанием алкоголя и курения и т. п. Открывается широчайший простор для произвола и цензуры. Сетевые мизулины найдут крамолу почти в любой записи. Напомню, что госпожа Мизулина, которая пересела из депутатского в сенаторское кресло, к примеру, два года назад предлагала поставить маркировку 18+ на фильмы «Хоббит» и «Властелин колец», поскольку в них содержатся сцены насилия.

9.2. Пользователю запрещено:

9.2.7. размещать рекламу и/или политическую агитацию, если иное специально не установлено отдельным соглашением между Пользователем и Администрацией;

То есть если вы будете пиарить Путина, ОНФ и «Единую Россию», то это в порядке вещей, а вот если напишете пост в поддержку Навального или будете агитировать прийти на митинг оппозиции, то это сочтут «политической агитацией» и вас забанят.

Размещать рекламу, зарабатывая тем самым на блоге, теперь тоже запрещено. Возможно, это немного и очистит топ ЖЖ от мусора, но убьет к нему интерес у тех немногих, кто вообще пытался в последнее время работать на этой площадке.

10.5. Администрация вправе ограничить доступ Пользователя к любой из функций Сервиса, а также ограничивать или запрещать использование API, размещение ссылок на сторонние ресурсы, и предпринимать иные действия, направленные на защиту Сервиса от воздействия факторов, представляющих, реально или потенциально, угрозу для Пользователей, нормальной работы Сервиса и политике Администрации. Администрация реализует указанные меры по собственному усмотрению и не несет ответственности за возможные негативные последствия таких мер для Пользователя или третьих лиц.

10.6. Администрация вправе по своему усмотрению и без предварительного уведомления Пользователя дополнять, сокращать или иным образом изменять функциональность Сервиса и порядок его предоставления.

Ссылки на сторонние сайты теперь тоже размещать нельзя?! А любую функцию вам смогут ограничить без предупреждения, каких-либо объяснений и просто когда сочтут нужным.

12. Реклама.

12.1. Если иное специально не установлено отдельным соглашением между Пользователем и Администрацией, Администрация может без

дополнительного уведомления и без какой-либо компенсации Пользователю размещать рекламу на Сервисе, включая страницы Блогов/Сообществ.

12.2. Администрация вправе в любое время изменять способ, вид и количество рекламы, размещаемой на Сервисе.

12.3. Участие Пользователя в рекламируемых на Сервисе акциях и мероприятиях, а также приобретение Пользователем рекламируемых на Сервисе товаров, работ или услуг порождает права и обязательства исключительно между Пользователем и лицом, реализующим соответствующий товар, работу, услуг или проводящим акцию или мероприятие.

12.4. Размещение Пользователем на Сервисе Контента рекламного характера (обещание осуществить такое размещение) не влечет никаких обязательств для Администрации.

12.5. Администрация вправе отправлять Пользователю по указанным им адресам электронной почты информацию, касающуюся Сервиса, а также рекламу третьих лиц.

То есть вы будете вести блог, а вас будут засыпать рекламой и спамом какого угодно качества и объема, которые будет везде, включая ваш почтовый ящик.

В январе я ссылался на прогноз SMM-аналитиков относительно деградации ЖЖ в 2017–2018 гг.: «Livejournal окончательно потеряет статус ТОПовой блог-площадки. Серьезное снижение популярности, дальнейший отток авторов на другие площадки». Но тогда я не думал, что убийство ресурса произойдет так быстро. И вот, пожалуйста, в крышку гроба ЖЖ сегодня был забит последний гвоздь. Однако скептикам, которые хоронили ЖЖ и пропагандировали Facebook, не стоит очень уж торжествовать, поскольку очевидно, что после убийства живого журнала – Facebook, Twitter, YouTube и другим аналогичным сервисам в России тоже останется существовать недолго.

***

5.04.2017

Щоб потрапити в США, доведеться поділитися паролями соцмереж

Влада США планує вжити ще більш жорстких заходів по відношенню до тих, хто бажає отримати американську візу (Знай.ua).

Уже незабаром Сполучені Штати Америки можуть ввести додатковий захід перевірки для іноземців, які хочуть в’їхати на територію країни.

Зокрема їм доведеться повідомляти паролі для соцмереж, телефонні контакти, дані про фінанси, а також розповідати про свій світогляд, передає The Wall Street Journal.

За інформацією видання, зараз можливі доповнення жваво обговорюються в адміністрації президента Д. Трампа. У разі прийняття нововведення можуть зачепити претендентів на отримання візи з усіх країн світу, включаючи союзників.

У Білому домі також хочуть збільшити час співбесіди в посольствах для претендентів на візу та розширити список людей, яких слід перевіряти ретельніше.

***

4.04.2017
Німці почнуть штрафувати соціальні мережі

Німецька влада схвалила законопроект, яким передбачено накладати штрафи на соціальні мережі, повідомляє replyua.net з посиланням на Укрінформ (Replyua).

Штрафні санкції будуть накладати за те, що адміністрація соцмереж не буде виконувати належним чином зобов'язання щодо знищення забороненого контенту, зокрема, мова йде про записи і коментарі, які спрямовані на розпалювання ненависті. У Німеччині вирішили юридично зобов'язати представників соцмереж боротися з таким контентом через те, що на добровільній основі видаляється мінімум записів. Зокрема у Twitter видаляють лише 1 % відповідного контенту, у Facebook – трохи менше половини. Щоправда кращі показники має сайт YouTube, на якому знищується до 90 % забороненого контенту.

Згідно з ухваленим 5 квітня законопроектом передбачається, що штрафи не будуть накладатись за одноразові правопорушення. Що ж стосується розмірів фінансових стягнень, то вони можуть сягати до 50 млн євро. Деякі правозахисники вже висунули застереження, що, намагаючись уникнути штрафних санкцій, адміністратори соцмереж будуть видаляти занадто багато матеріалів, що значно обмежить свободу слова у веб-просторі.

***

8.04.2017
Twitter відкликав позов до влади США через Трампа

Компанія відмовилася від позову, спрямованого через вимоги розкрити особисті дані користувача або групи користувачів (Корреспондент.net).

Компанія Twitter Inc 7 квітня відкликала свій позов проти Міністерства внутрішньої безпеки (МВБ) США, поданий до суду Сан-Франциско після того, як американська влада зажадала розкрити особисті дані користувача або групи користувачів, що стоять за аккаунтом @ALT_uscis. Про це повідомила американська газета The Recorder.

Назва аккаунта розшифровується як «Альтернативна Служба громадянства та імміграції США» (Alternative U.S. Citizenship and Immigration Services). Власники облікового запису розміщують у соціальній мережі повідомлення із критикою на адресу політики президента Д. Трампа і надають допомогу біженцям із країн, на які поширюється дія міграційного указу президента.

Рішення про відкликання позову в компанії пояснили тим, що Митно-прикордонна служба США, що входить до складу структури МВБ, відмовилася від вимог, що пред'являлися Twitter Inc., надати логін, номер телефону, поштову адресу й IP-адресу власників аккаунта.

Раніше у Twitter @ALT_uscis було розміщено запис із текстом першої поправки до Конституції США, яка, зокрема, передбачає свободу слова.

***

10.04.2017

WikiLeaks обнародовала новую порцию конфиденциальных документов ЦРУ

В рамках проекта Vault 7 организация WikiLeaks опубликовала новый массив конфиденциальных документов Центрального разведывательного управления США. Предыдущая часть, получившая название Marble («Мрамор»), была обнародована 31 марта (Центр информационной безопасности).

Новая публикация называется Grasshopper («Кузнечик») и содержит 27 документов, в которых идет речь об одноименной платформе, предназначенной для создания вредоносного ПО для Microsoft Windows.

Grasshopper включает различные модули, позволяющие сотрудникам ЦРУ создавать кастомизированные «импланты», способные демонстрировать разное поведение в зависимости от определенных функций и возможностей, предусмотренных в процессе сборки. Как отмечается, модули Grasshopper не могут засечь крупнейшие антивирусные решения, в том числе продукты «Лаборатории Касперского» и Symantec.

Один из механизмов, используемых ЦРУ, называется Stolen Goods. Ряд его компонентов позаимствован у банковского вредоносного ПО Carberp, чей исходный код утек в Сеть в 2013 г.

***

10.03.2017

В Госдуму РФ внесли законопроект о регистрации в соцсетях по паспорту

Депутат Госдумы России В. Милонов внес законопроект, запрещающий детям младше 14 лет пользоваться соцсетями. Документ опубликован на сайте Госдумы РФ (LB.ua).

Предлагается разрешить регистрацию в соцсетях только при предъявлении документа, удостоверяющего личность.

«Это позволит защитить подростков от вредной информации, привлекать к ответственности распространителей запрещенных материалов и решать проблему "фейковых страниц"», – говорится в пояснительной записке.

В. Милонов объяснил необходимость принятия таких жестких мер возросшей популярностью «групп смерти» и «тлетворным влиянием трудных подростков и детей из неблагополучных семей на своих сверстников».

При этом законопроект также запрещает использовать соцсети для организации несанкционированных митингов.

«Организаторы таких мероприятий находят через соцсети граждан, готовых за определенную сумму поучаствовать в незаконной акции. В связи с этим проектом предлагается ужесточить административную ответственность за организацию несанкционированных митингов посредством социальных сетей», – считает автор законопроекта.

В. Милонов также предлагает внести поправки в Трудовой кодекс РФ и запретить пользоваться соцсетями на работе. Также предлагается запретить «рекламу оккультно-магических услуг и народной медицины» и установить «особые требования» для благотворительности.

26 марта по всей России прошли массовые митинги с требованием борьбы с коррупцией. Поводом стало расследование Фонда борьбы с коррупцией оппозиционера А. Навального, который опубликовал материалы о «коррупционной империи» премьер-министра РФ Д. Медведева под названием «Он вам не Димон». Участники митингов требовали реакции российских властей на расследование.

Тем не менее, на федеральных телеканалах и государственных СМИ РФ протесты особо не освещали, а по всех городах прошли массовые задержания участников акций.

После протестов начала появляться информация о том, что власти РФ пойдут на ужесточение интернет-законодательства, поскольку митинги были анонсированы именно в соцсетях.

Проблема захисту даних. DDOS та вірусні атаки

30.03.2017

ПриватБанк почав виявляти зломщиків соцмереж

Система протидії шахрайству ПриватБанку тепер може автоматично визначати шахрайські транзакції, що здійснюються за допомогою злому акаунтів соціальних мереж, месенджерів або Skype. Як повідомили в банку, у разі визначення загрози переказу коштів на зламані акаунти соцмереж банк повідомить про це клієнту або попросить підтвердити транзакцію за допомогою телефонного дзвінка чи SMS (Утренний город).

«Ми оперативно налаштували нашу антифрод-систему під порівняно молодий для України спосіб шахрайства, що дозволяє зупинити його масове поширення, – говорить керівник Напрямку внутрішнього контролю та fraud-менеджменту ПриватБанку О. Соколовський. – Щодня за допомогою антифроду ми допомагаємо не втратити свої гроші майже двом десяткам клієнтів, які стали жертвами злому акаунтів соцмереж своїх знайомих».

Як зазначають спеціалісти банку, найчастіше шахраї зламують соціальні мережі «ВКонтакте» та «Одноклассники». Отримавши доступ до чужого облікового запису, хакери починають розсилати повідомлення від імені жертви його друзям і знайомим з проханням терміново переказати гроші на рахунок мобільного телефону або картку з різних приводів.

***

30.03.2017

Арестован хакер, угрожающий удалить 300 млн аккаунтов пользователей iPhone

По данным издания Motherboard, речь идет об участнике хакерской группировки Turkish Crime Family, шантажировавшей Apple (Finance.Ua).

По данным NCA, 20-летний житель Великобритании задержан с целью проведения допроса. Согласно предполагаемому ордеру, арест связан с расследованием дела о шантаже компании Apple группировкой Turkish Crime Family.

Неделей раньше, напомним, группа хакеров заявила, что располагает доступом к более чем 300 млн аккаунтов Apple. Это и учётные записи iCloud, и электронная почта доменов icloud и me.

Взломщики заявили, что они планируют совершить атаку 7 апреля, если Apple не заплатит выкуп. Они потребовали у корпорации 100 000 долл. для каждого из семи членов организации или подарочные карты iTunes номиналом 1 млн долл. для немедленной перепродажи в размере 60 % от оригинальной стоимости.

В Купертино заявили, что серверы и базы данных компании не были взломаны, и предположили утечку данных у сторонних сервисов, таких как LinkedIn. Издание ZDNet получило от одного из участников хакерской группировки массив данных доступа к 54 аккаунтам iCloud. Все они оказались рабочими: журналистам удалось связаться с 10 владельцами, предупредить их об опасности и попросить поменять пароль.

Представители группировки подтвердили журналистам, что парень, о котором идет речь, не выходил с ними на связь с 28 марта. «Его теперь обвиняют в создании и управлении всей группой. Его друг был у него дома во время ареста, снял практически все на камеру и прислал нам», – сообщили участники группировки.

Turkish Crime Family прислала журналистам ссылку на видео предположительного обыска и фотографии ордера. NCA не подтвердила, является ли арестованный тем же человеком, чье имя указано в ордере.

***

5.04.2017

ФБР арестовало белого хакера за пособничество преступникам

ФБР арестовало создателя популярной шпионской программы NanoCore Т. Хаддлстона (Finance.Ua).

Т. Хаддлстон обвиняется в пособничестве преступникам. Программист никогда не применял свое изобретение, а продал его злоумышленникам. В результате вредоносный софт стал главным инструментом крупных взломов в 10 странах.

Специалист выставил программу на продажу на площадке HackForums с предупреждением о том, что NanoCore не является вредоносным софтом и не должна использоваться в этом качестве. Программа была разработана в качестве бюджетного инструмента для удаленного администрирования, которым могли бы пользоваться компании, не имеющие возможности приобрести дорогостоящее ПО.

Издание отмечает, что создатель программы пытался предотвратить атаки, совершенные с помощью проданного софта. Он использовал еще одно свое изобретение – программу Net Seal – для отключения недобросовестных пользователей от NanoCore. Однако власти утверждают, что Net Seal может быть еще одним подтверждением того, что Т. Хаддлстон взаимодействовал с хакерами.

На данный момент в отношении создателя софта ведется расследование. Его отпустили из-под стражи, но запретили покидать дом и пользоваться Интернетом.

Т. Хаддлстон известен среди так называемых белых хакеров – взломщиков, которые тестируют различные системы на прочность, сообщают о существующих брешах «жертвам» и получают вознаграждения за найденные уязвимости.

***

30.03.2017

В Германии создадут киберкомандование

Структура создается во исполнение решений НАТО и канцлера А. Меркель, назвавшей защиту Германии от кибератак одним из главных приоритетов (Экономические известия).

В Германии в начале апреля появится Кибернетическое и информационное командование. Об этом сообщает Reuters, информирует news.eizvestia.com.

Новая структура будет располагаться в Бонне. Ее изначальная численность – 260 человек, но к июлю планируется довести ее до 13,5 тыс. человек, включив в состав стратегическую военную разведку и центры связи. К 2021 г. число сотрудников службы достигнет 14,5 тыс. человек, 1,5 тыс. мест зарезервированы для гражданских контрактников.

Министр обороны ФРГ Урсула фон дер Ляйен уже назвала имя начальника нового киберкомандования – им станет генерал-лейтенант Л. Ляйнхос.

Как отмечает агентство, структура создается во исполнение решений НАТО и канцлера А. Меркель, назвавшей защиту Германии от кибератак одним из главных приоритетов. В качестве главного противника рассматривается Россия, которая, как полагают в Берлине, пытается при помощи пропаганды и дезинформации дестабилизировать немецкое общество.

7 января Федеральное ведомство по охране конституции ФРГ заявило, что в кибератаке на ОБСЕ в декабре 2016 г. имеется след «российских хакеров». По словам главы ведомства Х.-Г. Маассена, у экспертов есть улики, указывающие на причастность группировки APT 28 (другим названием считается Fancy Bears), которую связывают с Россией.

***

31.03.2017
Володимир Корчинський
Екс-кандидат у президенти США заявив про хакерську атаку з Росії

Сенатор від Республіканської партії США та колишній кандидат у президенти країни М. Рубіо заявив, що члени його виборчого штабу зазнали хакерських атак, ймовірно, з російських IP-адрес. Про це він повідомив під час слухань комітету з розвідки американського Сенату, передає УНН із посиланням на Deutsche Welle (Українські Національні Новини).

М. Рубіо також розповів, що в липні 2016 р., після того, як він вийшов із президентських перегонів та заявив про намір переобиратися в Сенат, члени його штабу були «атаковані з IP-адрес із невідомого місця в Росії», однак хакери зазнали невдачі.

При цьому сенатор відзначив, що впевнено говорити про те, звідки велися атаки, ґрунтуючись тільки на IP-адресах, неможливо, оскільки хакери можуть легко їх підробити.

М. Рубіо, який свого часу був суперником Д. Трампа в праймеріз, заявив про завершення своєї президентської кампанії після поразки в рідному штаті Флорида у березні 2016 р.

***

31.03.2017
Хакери зламали Facebook Олланда і запросили на вечірку з приводу його відставки

30 березня хакери зламали сторінку Facebook президента Франції Ф. Олланда. Після злому сторінки, хакери розмістили запрошення на захід під назвою «вечірка в честь відставки Франсуа Олланда», яку призначили на 7 травня (Інформаційна агенція «Вголос»).

Про це повідомляє Europe1.

Це запрошення було на офіційній сторінці Ф. Олланда протягом години, потім його видалили.

Захід організований активістами руху «За відставку Франсуа Олланда». Відмітку про те, що згодні піти на зустріч, поставили 12 тис. користувачів соцмережі. Водночас представники руху в Facebook причетність до злому аккаунта президента заперечують. Тим не менш, Facebook-сторінка руху наводить скріншот поста Ф. Олланда. «Тепер офіційно ми отримали підтримку Франсуа Олланда (без жартів)», – йдеться в повідомленні.

***

2.04.2017

Пользователи Skype стали мишенями атак вымогателей через вредоносную рекламу

Ряд пользователей в последние дни жаловались на рекламу в приложении Microsoft Skype, которая содержит вредоносный код и при запуске приводит к установке приложений-вымогателей. Обсуждение этого появилось в социальной сети Reddit в среду. Автор топика утверждает, что начальная страница Skype содержит фальшивую рекламу якобы критически важного обновления плагина Flash (InternetUA).

Реклама активирует скачивание HTML-приложения, которое выглядит как достоверное. При его запуске скачивается вредоносный код, который блокирует компьютеры и зашифровывает файлы. Ещё два пользователя пожаловались на эту же проблему в четверг. Один из пользователей выставил исходный код приложения.

Код написан на JavaScript, после запуска первоначальное приложение удаляется и запускается PowerShell, далее скачивается JavaScript Encoded Script (JSE) с уже закрытого домена. Все эти шаги призваны затруднить обнаружение антивирусами.

Есть предположение, что эта реклама является ответвлением кампании по распространению вымогателя Locky, где содержится троян Kovter, который отвечает за вредоносную рекламу. Locky также использует JavaScript, не прибегая к помощи промежуточных приложений.

Неизвестно, сколько доменов используется в нынешней кампании, но явно больше одного. Skype не первый раз становится источником подобной рекламы. В 2015 г. здесь наблюдалась вредоносная реклама на Java и Flash.

***

2.04.2017

Исследование: WhatsApp и другие мессенджеры уязвимее на iOS, чем на Android

Все популярные мессенджеры уязвимы, причем это относится как к версиям для Android, так и для iOS. К такому выводу пришли специалисты компании Solar Security, о проведенном в которой исследовании пишет «Коммерсант» (InternetUA).

С помощью технологии автоматического бинарного анализа компания Solar Security проверила код девяти наиболее популярных мессенджеров: Telegram, WhatsApp, Viber, Facebook Messenger, Signal, Slack, Skype, WeChat и QQ International. В результате проверки было установлено, что критических уязвимостей не содержит только мессенджер Signal под Android. Однако в его коде все же присутствуют шесть ошибок среднего уровня и семь низкого. В коде Facebook Messenger и Slack есть по четыре критических ошибки, в остальных – еще больше.

К самым распространенным критическим уязвимостям мессенджеров на Android относятся слабые алгоритмы шифрования и хеширования, небезопасные реализации SSL, использование пустых паролей. Эти ошибки повышают риск перехвата логинов и паролей, хранящихся на устройстве.

iOS-версии мессенджеров оказались более уязвимы, чем клиенты для Android. Так, в Facebook Messenger для iOS специалисты компании Solar Security обнаружили 12 критических уязвимостей, в Viber – 15, в Skype – 17. Больше всего ошибок было обнаружено в китайских мессенджерах QQ International и WeChat. Как считают специалисты компании, то, что в iOS-версиях приложений содержится больше ошибок, скорее всего связано с тем фактом, что разработчики Android «более внимательно относятся к уровню защищенности», так как «сама Android считается менее безопасной».

Сами мессенджеры информацию о проблемах с безопасностью не подтвердили, отметив, что все продукты регулярно проходят проверку.

***

3.04.2017

НАТО надасть СБУ обладнання для кіберзахисту

До кінця весни Служба безпеки України отримає як допомогу від НАТО спеціальне обладнання для протистояння кібернетичним загрозам. Про це повідомив заступник помічника генсека Північноатлантичного альянсу з питань нових викликів безпеці Д. Шеа в інтерв'ю агентству «Інтерфакс-Україна» (LB.ua).

«Ми на етапі організації доставки його [устаткування] в Україну, його вже придбано. Нам залишилося пройти деякі звичайні адміністративні формальності процедур імпорту/експорту, але ми сподіваємося, що зможемо зробити це дуже швидко. Наша мета полягає в тому, щоб до літа все було встановлено, протестовано і запущено», – сказав він.

Шеа нагадав про роботу трастового фонду Україна-НАТО з питань кіберзахисту.

«НАТО має відповідний трастовий фонд, який очолює Румунія, але донорами цього фонду є багато країн. Ми витратили понад 300 тис. євро, щоб допомогти Міністерству закордонних справ України, а також допомогти українським спецслужбам у навчанні співробітників і поліпшенні обладнання для кращого виявлення і відбиття кібератак», – розповіді він.

***

3.04.2017

Verizon будет продавать Android-устройства с шпионским ПО

Крупнейший по количеству абонентов оператор сотовой связи в США Verizon намерен продавать Android-устройства с предустановленным шпионским ПО для сбора данных пользователей. Компания заключила соглашение со стартапом Evie, разработавшим одноименный лаунчер, о создании приложения AppFlash. Программа представляет собой универсальный поисковик для быстрого поиска приложений и web-контента, предустановленный на домашнем экране всех продающихся через Verizon устройств (InternetUA).

По существу, AppFlash является заменой строки поиска Google. Приложение позволяет осуществлять поиск в Интернете и программах, и не делает ничего такого, чего не умеет Google. Однако теперь данные телеметрии, поисковые запросы, сведения об устройстве, приложениях и онлайн-активности будут отправляться не Google, а Verizon. Подобно другим предустановленным приложениям удалить AppFlash можно, только получив права суперпользователя на устройстве.

Складывается впечатление, будто Verizon заменила предустановленный поисковик с единственной целью – собирать данные о пользователях и продавать их рекламным компаниям. Напомним, на прошлой неделе Сенат США разрешил американским операторам связи без разрешения пользователей продавать их данные.

***

2.04.2017

Британія посилює охорону АЕС і аеропортів через загрозу кібератак

Влада Великобританії посилює охорону атомних електростанцій і аеропортів через зростання терористичної загрози. Про це повідомляє The Telegraph (LB.ua).

За повідомленнями урядових служб, причиною посилення заходів безпеки стала як інформація про розробку терористами вибухівки, яку можна помістити в електронні пристрої, так і побоювання щодо загрози нових кібератак на захищені об’єкти.

Голова департаменту енергетики уряду країни Д. Норман заявив, що ядерні електростанції «повинні бути готові протистояти зростаючій кіберзагрозі».

В уряді країни побоюються, що хакери, кібертерористи і співробітники іноземних розвідок можуть використовувати вразливість в електронних системах безпеки для того, щоб зробити атаки на АЕС.

Крім того, британська влада побоюється зростаючих можливостей терористів з виготовлення бомб, які неможливо виявити за допомогою звичайних заходів охорони.

***

2.04.2017

Вредоносный плагин для WordPress предоставляет хакерам доступ к сайтам

Исследователи компании SiteLock обнаружили вредоносный плагин WordPress под названием WP-Base-SEO, подделанный под настоящий инструмент для поисковой оптимизации WordPress SEO Tools. На первый взгляд файл кажется вполне легитимным, включая ссылку на базу данных плагинов WordPress и техническую документацию. Однако в ходе более подробного анализа эксперты обнаружили зашифрованный с использованием base64 запрос eval (InternetUA).

Eval представляет собой популярную у киберпреступников PHP-функцию, выполняющую произвольный PHP-код. Из-за частого применения хакерами php.net рекомендовал полностью отказаться от ее использования.

Директория плагина содержит два файла. Один из них, wp-sep.php, использует различные функции и имена в зависимости от установки. Второй, wp-seo-main.php, использует «родной» функционал WordPress для присоединения запроса eval к «шапке» сайта. С его помощью злоумышленники получают доступ к ресурсу. Как пояснили эксперты, инициализация запроса происходит при каждой загрузке темы в браузере.

Исследователи обнаружили множество сайтов с установленным вредоносным плагином. Тем не менее, поиск по названию WP-Base-SEO не предоставляет никакой информации. Из этого следует, что данное вредоносное ПО в настоящее время практически не детектируется.

***

4.04.2017

Фишеры атакуют клиентов авиакомпаний

Вице-президент компании Barracuda Networks ИБ-эксперт А. Сидон (Asaf Cidon) сообщил о фишинговых атаках на клиентов авиакомпаний. Злоумышленники рассылают сообщения, содержащие либо заражающее систему вредоносное ПО, либо ссылку на подконтрольный им взломанный сайт. Целью киберпреступников является получение личных и корпоративных учетных данных клиентов авиакомпаний (InternetUA).

За последние несколько недель эксперты Barracuda Networks зафиксировали волну комбинированных атак. В некоторых случаях злоумышленники выдавали себя за представителей туристических агентств или за коллег жертв по работе. По их словам, в письме якобы содержится авиа- или

электронный билет. На самом деле после открытия вложенного документа на компьютер жертвы загружалось вредоносное ПО.

В других случаях письма содержали ссылку на подконтрольные хакерам взломанные сайты авиакомпаний. Такая атака более сложная, ведь сначала злоумышленникам необходимо было взломать сам ресурс. Вдобавок мошенники персонализировали целевую страницу в надежде обманом заставить жертву ввести свои персональные или корпоративные учетные данные.

По словам А. Сидона, вышеупомянутые атаки нацелены на компании, занимающиеся перевозкой, доставкой или производством. Как отметил эксперт, фишинговые атаки на клиентов авиакомпаний являются наиболее эффективными – злоумышленники достигают желаемой цели в 90 % случаев. Согласно уведомлению US-CERT, фишинговые атаки являются точкой входа для получения доступа к конфиденциальной персональной или корпоративной информации.

***

4.04.2017

Смарт-телевизоры можно взломать через эфирный сигнал

С каждым годом появляется всё больше устройств для дома с подключением к Интернету, при этом самым популярным видом таких девайсов остаются смарт-телевизоры. Именно их многие компании считают центром всего «умного» дома. Многие пользователи волнуются о безопасности своих компьютеров и смартфонов, но совсем не заботятся о защите «умного» дома. Исследователь в сфере безопасности Р. Шеил из Oneconsult рассказал об эксплойте, позволяющем контролировать смарт-телевизоры, встраивая код в цифровые, в частности, DVB-T, эфирные трансляции (InternetUA).

Вредоносный код использует уязвимости в веб-браузере, чтобы получить корневой доступ и выполнить практически любую команду. Хакерам достаточно иметь мощную передачу, чтобы достичь совместимых телевизоров, и по крайней мере одна атака пройдёт, а пользователи даже ничего не заподозрят.

Хорошей новостью является то, что DVB-T используется только в некоторых странах, а формат широкополосного телевидения (HbbTV), необходимый для взлома, распространён и того меньше. Кроме этого, телевизор также должен быть настроен на DVB-T-канал и быть подключённым к Интернету.

***

3.04.2017

Доказано: в ваш компьютер могут проникнуть даже через сканер

Ученые Университета им. Бен-Гуриона в Негеве и Института Вейцмана обнаружили, что обычный сканер может стать «черным ходом» в компьютерную сеть офиса (From-UA Новости Украины).

Ученые доказали, что с помощью лазера или смартфона можно закачивать вредоносное программное обеспечение, используя подключенный к компьютеру сканер, если его крышка открыта. Чувствительность сканера к изменениям освещенности оказалась достаточной, чтобы с помощью лазера с расстояния 900 м можно отправить через сканер в компьютер сообщение, запускающее программу, сообщает cursorinfo.co.il.

В другом эксперименте сигнал на сканер подавался смартфоном, который управлялся радиоволнами. Лампочка смартфона мигала в соответствии с заданной учеными программой, меняла освещенность в помещении и запускала через сканер программу в компьютере.

Ученые рекомендуют подключать компьютеры к сканеру через прокси-сервер, однако и этот способ защиты имеет свои недостатки. В частности, ограничивает возможности печати и отправки факсов с удаленных устройств.

***

4.04.2017

Хакеры начали активно использовать вирусы из 90-х

Среди хакеров снова становятся популярными написанные в 1990-х годах три макровируса для Microsoft Office и червь SQL Slammer. Об этом со ссылкой на совместное исследование компаний WatchGuard и Fortinet сообщает Silicon UK (InfoResist).

По словам технического директора WatchGuard К. Нахрайнера (Corey Nachreiner), для организации атак на пользователей сети создатели зловредного программного обеспечения все чаще модернизируют старые программы вместо написания новых и регулярно используют макровирусы.

Представители Fortinet отметили, что засекли неожиданную активизацию червя SQL Slammer в 2003 г., за 10 минут заразившего 75 тыс. компьютеров-хостов и замедлившего общую скорость передачи интернет-трафика. Исследователи утверждают, что нынешние атаки с использованием SQL Slammer в основном исходят из американских университетов, где злоумышленники, скорее всего, ищут старые уязвимые серверы.

Макровирусы и черви получили широкое распространение в конце 1990-х и начале 2000-х годов. Они использовали многочисленные уязвимости в продуктах Microsoft и вынудили корпорацию активнее искать бреши в безопасности Windows и пакетов Office.

***

6.04.2017

Шахраї дублюють SIM-картки і фактично отримують доступ до банківських рахунків

Важлива інформація для всіх, хто збирає кошти на допомогу та/або благодійність на банківські картки шляхом розміщення номеру картки та номеру телефону (Утренний город).

На сьогодні існує одна невирішена проблема з безпекою таких благодійних зборів. Ця проблема пов'язана із незахищеністю номерів мобільних операторів, які обслуговуються на умовах передплати. На відміну від номерів, які обслуговуються на умовах контракту, «передплатні» номери не завжди передбачають прив'язку до власника за допомогою паспортних даних.

Почастішали випадки, коли зловмисники використовують шахрайський метод дублювання SIM-картки мобільного оператора. Це робиться доволі легко. Зловмисники телефонують на номер мобільного оператора «жертви» та поповнюють його рахунок на символічну суму (як правило, на 5–10 грн). Далі, знаючи три останні набрані/отримані номери, дату та суму останнього поповнення рахунку, шахраї звертаються до оператора з нібито проблемою втрати SIM-картки та її заміною. При цьому картка, якою користується «жертва», автоматично блокується. На жаль, така схема отримання дублікату SIM-картки мобільного оператора дуже спрощена, і цим самим наражає власників «передплатного» номеру на ризики шахрайства.

Отримавши доступ до мобільного номеру телефону людини та, якщо цей номер використовується у банківській установі як фінансовий (на нього надходять SMS-повідомлення з паролями платежів, підтвердження фінансових операцій тощо), зловмисники фактично отримують доступ до банківських рахунків.

Для запобігання таким шахрайським операціям, ПриватБанк наполегливо просить не публікувати в соціальних мережах ФІНАНСОВІ номери телефонів, які підв'язані під банківські рахунки та картки, в разі, якщо цей номер не є контрактним. Допоки проблема захисту SIM-карток мобільних операторів залишається невирішеною, слідування цьому простому правилу – запорука безпеки грошей клієнтів. Також, при неможливості переведення номеру мобільного на умови контрактного обслуговування оператором, у ПриватБанку радять використовувати для фінансових операцій номери, які знає якомога менше незнайомих людей.

У разі, якщо клієнт запідозрив блокування його мобільного номеру телефону, потрібно якнайшвидше зв'язатися з банком, зателефонувавши на номер цілодобової підтримки 3700 (безкоштовно з мобільних і стаціонарних номерів телефонів) або звернувшись в онлайн-чат на сайті privat24.ua <https://www.privat24.ua/> або pb.ua <https://privatbank.ua/>.

***

6.04.2017

Обнаружен один из самых сложных вирусов для Android

Мы уже настолько привыкли к новостям о новых вирусах для той или иной операционной системы, что, зачастую, даже не обращаем внимание на появившиеся угрозы (iLenta.com).

Несмотря на заверения Google о том, что даже самые опасные вирусы для Android не несут особой угрозы, на официальном сайте для Android-разработчиков появилась статья, сообщающая об одном из самых опасных зловредов.

Вирус был обнаружен специалистами Google и Lookout. По их словам, речь идет об одном из самых сложных и целенаправленных мобильных вирусов, с которыми они сталкивались.

Зловред получил имя Chrysaor. Интересно, что он был разработан в качестве эксплойта для iOS под названием Pegasus и использовался для слежки за борцом за права человека из Объединённых Арабских Эмиратов. Теперь же вирус был модифицирован под Android.

***

7.04.2017
Ірина Коркішко
США співпрацюватиме з Україною в питаннях кібербезпеки

У Конгресі США представлено проект закону щодо співпраці з Україною з питань кібербезпеки, повідомляється на офіційній сторінці Посольства України в США у Facebook (Watcher).

У Конгресі США був представлений проект «Закону 2017 року про співпрацю з Україною з питань кібербезпеки». Цей законопроект визначає, що політикою США є надання допомоги урядові України в удосконаленні власної стратегії кібербезпеки. Напрями, в яких буде здійснюватися допомога, це:

1. Встановлення найбільш сучасних безпекових оновлень на комп'ютерах органів державної влади, у тому числі систем.

2. Програмного захисту, спрямованих на захист об'єктів критичної інфраструктури України.

3. Зменшення залежності України від російських технологій.

4. Сприяння розширенню участі України у програмах обміну інформацією, що пов'язана з проблематикою кібер-безпеки, та міжнародних зусиллях з протидії кібер-загрозам.

5. Сприяння розбудові нашою країною власних спроможностей у сфері кібер-безпеки.

«Реалізація даної законодавчої ініціативи стане важливим внеском у боротьбу України з гібридною війною РФ, що триває і складовою якої є здійснення кібер-атак проти нашої держави», – повідомляє Посольство.

***

9.04.2017
У Viber проблемы: секреты пользователей в опасности

В Viber нашли возможность подслушивать разговоры. Один из пользователей ресурса Habrhabr рассказал о проблеме в популярном приложении Viber (From-UA).

Оказалось, что используя приложение, можно подслушать разговор собеседника, если он осуществляется в одно время с голосовым звонком. Он также отметил, что для прослушивания разговора нужно дважды нажать кнопку «Удержание» на смартфоне.

При этом пользователь также отметил, что узнать о подслушивании разговора пользователь не может. Описание проблемы уже отправлено разработчикам Viber по электронной почте. Однако отреагировали они далеко не сразу.

В последней версии популярного приложения для Android проблема устранена. Однако на iOS и Blackberry прослушивание разговоров все еще возможно.

Как прокомментировали нам сложившуюся ситуацию в компании Viber, проблема на данный момент уже решена.

«Viber очень серьезно относится к вопросам конфиденциальности – мы сосредоточились на решении этой проблемы, как только она была обнаружена. Решение было найдено давно, несколько месяцев назад, однако не было должным образом доведено до сведения пользователя, и мы приносим свои извинения за это», – заявили в компании.

***

11.04.2017

Почему Tor не настолько анонимен, как вы думали

Испанские исследователи сетевой безопасности выявили множество слабых мест у зашифрованной анонимной сети Tor. В частности, использование одних и тех же скриптов, отслеживающих перемещение пользователей, в даркнете и в обычной Сети, подвергает опасности деанонимизации и скрытые ресурсы, а также их пользователей (InternetUA).

Слабые места Tor

Исследователи из испанского университета «Деусто» провели исследование сети Tor и пришли к выводу, что анонимность даркнета значительно переоценивается: слишком многое связывает обычные и закрытые участки всемирной Сети.

«Даркнет не настолько “темен”, как это может показаться», – говорит И. Санчес-Рола (Iskander Sanchez-Rola), исследователь университета «Деусто», занимающийся вопросами безопасности данных и приватности.

Команда И. Санчес-Ролы проанализировала порядка 1,5 млн страниц даркнета и выяснила, что более чем на 20 % этих страниц используются данные, импортированные из обычного Интернета, – изображения, документы и даже файлы JavaScript.

Все это, по мнению исследователей, создает потенциальные риски раскрытия данных, поскольку владельцы этих ресурсов могут отслеживать их загрузку пользователями; например, Google может отслеживать трафик к 13 % доменов, проанализированных группой Санчес-Ролы.

Помимо этого, на 27 % проанализированных сайтов даркнета исследователи выявили скрипты, отслеживающие перемещения пользователей. Примерно треть этих скриптов попали туда из обычной Сети. Источником 43 % скриптов был Google.

По словам И. Санчес-Ролы, если сайт в даркнете использует тот же скрипт, что и какой-либо сайт внешней сети, появляется возможность отследить и даже идентифицировать пользователя, когда он посетит менее защищенный сайт.

Прокси-фактор

Отдельный фактор риска – это прокси-сервисы сети Tor, такие как Tor2Web; по сути, это точки входа в закрытую сеть. Их пользователи рискуют деанонимизацией больше всего. Эти сервисы «видят» пользовательские IP-адреса; наличие же ссылок между даркнетом и Интернетом означает, что посторонние заинтересованные лица также могут получить доступ к информации о пользовательских IP. Если пользователь открывает через прокси страницу в даркнете, на которой присутствуют ресурсы (картинки, скрипты и т. д.), взятые из внешней Сети, его браузер загрузит эти ресурсы через обычные соединения, обходя анонимизацию.

Поэтому, говорит И. Санчес-Рола, для доступа к ресурсам в сети Tor необходимо использовать только специализированный браузер Tor.

Стоит отметить, что браузер Tor основан на коде Mozilla Firefox. В обоих время от времени обнаруживаются уязвимости, в том числе такие, которые позволяют деанонимизировать пользователей Tor.

Исследовательница Сара Джейми Льюис (Sarah Jamie Lewis), написавшая сервис OnionScan, позволяющий отыскивать уязвимости в ресурсах даркнета, утверждает, что до 35 % серверов в Tor могут быть деанонимизированны, однако операторы этих ресурсов не спешат предпринимать какие-либо меры по этому поводу.

По словам Льюис, исследование испанских экспертов – это серьезный повод для того, чтобы перестать использовать следящие скрипты из сторонних источников, которые подвергают риску и сами ресурсы, и их пользователей.

«Исследование показывает одну очень простую вещь: сам по себе Tor не является универсальным средством обеспечения анонимности и (или) защиты собственной приватности, – говорит Д. Гвоздев, генеральный директор компании “Монитор безопасности”. – Одного только слоя защиты не достаточно нигде; это правило работает и в сфере кибербезопасности, и в области безопасности физической. Любая защита должна быть “глубоко эшелонированной”, в противном случае она будет малоэффективной».

***

10.04.2017

Как мошенники и шпионы используют Google Play, Yandex и Twitter

Мошенники внедрили на Google Play бизнес по перепродаже бесплатного приложения Adobe под видом плагина для воспроизведения мультимедийного контента. Об этом сообщают эксперты ESET (Take-profit.org).

В отличие от мобильных банкеров, программ-вымогателей и другого вредрносного ПО, замаскированного под легитимный софт, приложение F11 не имело вредоносных функций.

Мошенники действовали исключительно методами социальной инженерии, убеждая пользователей заплатить 18 евро (или 19 долл.) за изначально бесплатную программу. Статистика загрузок F11 указывает на успешность «бизнеса» – с ноября 2016 г. приложение скачали до 500 000 пользователей.

После загрузки с Google Play приложение выводит на экран инструкции по установке и оплате через PayPal. Мошенники дополнительно предлагают установить мобильный браузер Firefox или Dolphin – эти браузеры поддерживают Flash Player по умолчанию.

По данным ESET, в данный момент приложение F11 удалено из Google Play.

В свою очередь эксперты компании Talos заявили, что облачные сервисы «Яндекса» и Twitter используются для хостинга вредоносных командных серверов и передачи данных недавно обнаруженной вредоносной программой Rokrat, используемой в шпионских целях, сообщает CNews.

Rokrat представляет собой вредоносный инструмент удаленного администрирования (Remote Administration Tool – RAT), который используется в новой кампании, направленной против пользователей из Южной Кореи.

Атака на пользователей начинается с рассылки фишинговых писем с вложенными документами в формате HWP. Это формат крайне популярного в Южной Корее текстового редактора Hangul, поддерживающего корейский алфавит.

Для связи зараженных ПК с командной инфраструктурой Rokrat использует ресурсы известных глобальных сервисов. В частности, исследователи обнаружили семь «зашитых» в код трояна API-токенов Twitter, четыре токена «Яндекса» и один аккаунт хостингового сервиса Mediafire.

Twitter используется для хостинга командного сервера и получения Rokrat команд от своих операторов. Серверы Яндекс и Mediafire – как для хостинга командных серверов, так и для передачи данных.

***

11.04.2017

В Microsoft Word обнаружена опасная уязвимость

Специалисты по информационной безопасности из компании FireEye сообщили, что во всех версиях Microsoft Word обнаружена уязвимость «нулевого дня».

Проблема позволяет загрузить вредоносное ПО на компьютер жертвы (From-UA).

Для проведения атаки злоумышленникам достаточно отправить пользователю вредоносный RTF-документ, распространяемый в виде вложения письма электронной почты. Далее выполняется скрипт Visual Basic, который в итоге предоставляет хакерам загружать вредоносное ПО и получить контроль над компьютером жертвы атаки.

Эта уязвимость позволяет обходить все защитные меры. При этом, в отличие от других подобных атак, в данном случае не требуется запуск макроса. Она работает на компьютерах под управлением всех версий ОС Windows, в том числе Windows 10.

В Microsoft уже проинформированы о существовании проблемы и специальный патч может быть выпущен 11 апреля в рамках «вторника обновлений».

Соціальні мережі
як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, Голосіївський просп., 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.