СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(12.12–27.12)

2018 № 22

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(12.12–27.12)
№ 22

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

© Національна бібліотека України
імені В. І. Вернадського, 2018

Київ 2018

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

12.12.2018
Telegram получил большое обновление на всех платформах

Разработчики Telegram выпустили глобальные обновления официального клиента для iOS, Android, Windows и macOS. Приложения получили обновленный интерфейс, расширенные настройки диалогов, возможность копирования ссылки на сообщение в закрытых группах и многое другое.

Докладніше

***

12.12.2018
Дмитрий Демченко
Instagram начал тестировать новый тип профилей для блогеров – с аналитикой подписчиков и фильтрацией сообщений

Instagram начал тестировать новый тип профилей, предназначенный специально для блогеров и создателей контента. Об этом сообщает The Hollywood Reporter (AIN.UA).

Новые аккаунты получат встроенную аналитику по подписчикам – Instagram будет показывать прирост (или отток) аудитории в разрезе дня и недели (сколько подписалось и отписалось человек). Кроме этого владельцы таких профилей смогут помечать сообщения, а также устанавливать категории пользователей, которые могут им писать – например, только друзья и бренды.

«Мы хотим еще больше показать, что Instagram – это лучшее и самое удобное место для создания фан-сообществ и развития личных брендов», – отметила менеджер по продуктам Instgram Эшли Юки и добавила, что создатели контента – «важная часть сообщества».

Сейчас функции тестирует небольшое количество блогеров. В компании планируют полноценно запустить новые профили в 2019 году.

***

13.12.2018
Instagram поможет пользователям в развитии аккаунта

Instagram работает над новыми функциями, которые помогут отслеживать развитие аккаунта. Сейчас инструментарий доступен только узкому кругу лиц (например, знаменитостям и популярным блогерам) (InternetUA).

Новые возможности помогут выявить причину появления новых подписчиков, а также увидеть, сколько просмотров собирают посты. Пользователи будут получать ежедневные и еженедельные отчёты об

изменениях в собственной аудитории. Благодаря новой функции создатели аккаунтов также смогут понять, какой контент привёл к увеличению числа подписчиков, а какой – к снижению.

Изменения появятся и в Direct Message. Во-первых, пользователи получат возможность сортировать сообщения по трём категориям: прочитанные, непрочитанные и помеченные. Во-вторых, Instagram начнёт оценивать важность запросов DM и будет отображать первыми самые приоритетные из них.

Новинка станет доступна большему числу пользователей соцсети в 2019 году.

***

13.12.2018
Владельцы iOS лишились одной из важнейших функций

Разработчики популярного сервиса WhatsApp без какого-либо предварительного предупреждения убрали из приложения недавнее обновление (InternetUA).

Совсем недавно состоялся релиз WhatsApp, в котором наконец-то, спустя год обещаний, появилась поддержка стикеров. Тем не менее, отныне пользователям iOS, то есть любых поколений iPhone, возможность их полноценно использовать недоступна. Все дело в том, что компания Facebook, которая отвечает за данный мессенджер, решила убрать из последней версии программы специальную кнопку, позволяющую получать наборы стикеров в магазине App Store.

Для установки сторонних наборов стикеров, а стандартных в WhatsApp всего два, необходимо устанавливать из App Store дополнительное приложение в случае с каждым набором. Компания Apple активно удаляет такое программное обеспечение из своего магазина, потому как оно, как она уверяет, нарушает сразу несколько правил. Компания Facebook никак не может повлиять на эту ситуацию, поэтому из iOS-версии фирменного мессенджера было решено убрать полноценную поддержку сторонних стикеров.

***

13.12.2018
Instagram подвел итоги 2018 года

Платформа отметила, что Heart Eyes были самым распространенным фильтром в Instagram Stories, а стикер с сердечком самым популярным Giphy стикером в Историях. Эмодзи сердца было использовано более 14 млрд раз в течение года (Marketing Media Review).

Instagram-аккаунт под названием Disneyland Tokyo стал самым счастливым местом на земле в 2018 году, так как у него было больше всего эмодзи со смайликом в подписях с геометками.

Трендом нишего коммьюнити была ACMP (автономная сенсорная меридиональная реакция), а популярные темы включали карвинг по мылу, взрывание шаров со слаймом и бритье лица. Самым быстрорастущим хэштегом глобально стал #fortnite, отметив популярность видеоигры Fortnite. В 2018 году пользователи сети слушали K-pop. Крупнейшим вирусным танцевальным челленджем стал #InMyFeelingsChallenge. Среди топ хэштегов правозащитной деятельности лидировали #MeToo (1,5 млн), #TimesUp (597,000) и #MarchForOurLives (562,000).

***

17.12.2018
Глава техподдержки раскрыл внутренние секреты Telegram

Михаил Равдоникас, возглавляющий команду технической поддержки Telegram, рассказал о «внутренней кухне» мессенджера, а также о том, как этот развивается этот проект и каким станет в будущем.

Докладніше

***

18.12.2018
Facebook добавил в Messenger обновления для камеры

В преддверии праздников Facebook добавил три новые инструмента для камеры в Messenger. Во-первых, компания добавила режим «Бумеранга» – зацикленные видео, уже доступные в Instagram и Facebook. В Messenger появился новый режим Selfie, который автоматически размывает фон, делая больший акцент на лице. И в-третьих, сеть добавила новый AR-элемент со стикерами, которые можно наложить на изображения (Marketing Media Review).

***

18.12.2018
В Skype можно будет поделиться экраном одного приложения

Одной из самых востребованных у продвинутых пользователей функцией Skype можно смело назвать инструмент для организации общего доступа к рабочему столу. Скоро он станет чуточку удобнее (InternetUA).

Пользователям предварительной версии Skype предложено протестировать функцию общего доступа к контенту только одного приложения, а не всего рабочего стола целиком. С нею вам больше не придётся сворачивать окна других приложений, содержащие конфиденциальную информацию, скрывать иконки любимых игрушек или менять пошлые обои, просто чтобы обучить кого-то основам использования видеоредактора «Фотографий», например.

Сейчас воспользоваться новой функцией можно в Skype Preview версии 14.37.26.0 или боле новой, после завершения предварительного тестирования она будет отправлена и рядовым пользователям сервиса.

***

19.12.2018
Viber назвал самые «общительные» города Украины

Компания Viber провела исследование активности среди своих пользователей на территории Украины. На сегодняшний день мессенджер установлен у 97 % владельцев всех смартфонов в Украине. В течение 2018 года пользователи продолжали общаться и делиться эмоциями с помощью сообщений, звонков, стикеров и GIF (Marketing Media Review).

Наиболее общительными в Украине оказались жители крупных городов. Активнее всего писали сообщения и звонили в Viber жители Киева – их доля составила 31 % активных пользователей Viber в Украине. На втором месте оказался город Днепр с данными 17 %, а на третьем Одесса – 13,2 %.

Также статистика активности говорит, что в 2018 году в Украине было создано более 4 тысяч сообществ в Viber, участниками которых сегодня являются около 4-х миллионов пользователей мессенджера. Самое многочисленное сообщество в Украине создала и развивает певица Тина Кароль, на которое подписано около 400 тысяч пользователей.

Согласно данным исследования Kantar TNS Cmeter Mobile 2018, Viber в Украине является самым популярным приложением – мессенджер установлен на 97 % смартфонов украинских пользователей.

«Украина является важным рынком для компании, у нас исторически сильные позиции в стране. Много украинцев пользуются приложением достаточно давно, это очень активная аудитория, которая заходит в мессенджер ежедневно, делится фотографиями, гиф, стикерами», – комментирует Яна Рожкова, директор по коммуникациям Viber.

Яна Рожкова отмечает, что компания уделяет много внимания развитию Viber на украинском рынке. В Украине Viber реализует крупные партнерские проекты со звездами, телеканалами, работает с международными и локальными брендами (Тина Кароль, 1+1 медиа, Люкс ФМ, ПриватБанк, ПУМБ и другие). В 2019 году украинских пользователей мессенджера ожидают новые функции, еще больше интересного контента и возможностей для коммуникации.

***

20.12.2018
Вышло обновление Instagram для Android

Разработчики Instagram постоянно работают над улучшениями социальной платформы. Сотрудники платформы подготовили три полезных нововведения. О них рассказали в официальном блоге компании.

Докладніше

***

20.12.2018
Как включить хронологический порядок ленты в Twitter

Спустя полгода обещаний разработчики Twitter все-таки добавили возможность включения хронологического порядка в главной ленте. Пока нововведение доступно только на iOS, но позднее появится в клиенте для Android и веб-версии соцсети (InternetUA).

Хронологический порядок в ленте был с первого дня существования Twitter, но в 2016 году руководство сервиса решило внедрить модную на тот момент функцию «умного» порядка. Специальный алгоритмы показывают пользователю сначала «самые интересные» твиты, которые он пропустил, а только потом остальные посты. Теперь это можно изменить.

Чтобы отключить «умную» ленту, нужно зайти в настройки приложения, выбрать раздел «Настройки контента» и активировать соответствующий переключатель. Кроме того, программа сама предложит вам внести изменения в эти настройки при первом запуске после обновления.

***

25.12.2018
В Telegram появилась новая функция

Telegram запустил специальный инструмент для проведения опросов, который станет удобным дополнением к уже существующим решениям, таким как бот @vote (InternetUA).

Чтобы создать опрос, нужно зайти в меню «Прикрепить», выбрать пункт «Опрос», указать его название и варианты ответа, после чего нажать на кнопку «Отправить».

Опросы можно будет пересылать в другие чаты для увеличения охвата и закреплять в беседе для лучшей видимости.

На данный момент опросы являются анонимными: их участники не раскрываются. В будущем разработчики планируют добавить возможность создавать публичные опросы.

***

25.12.2018
Facebook закрыл проект по борьбе с токсичными высказываниями

Facebook закрыл проект Common Ground, который позволил бы повысить терпимость между пользователями с различными политическими взглядами – в их ленте чаще оказывались бы посты с отличающимся от их собственного

мнением по острым вопросам. Об этом пишет The Wall Street Journal (InternetUA).

Common Ground также предполагал снижение значимости комментариев, порождающих негативные оценки политических событий при формировании ленты новостей пользователей.

Инициатором закрытия проекта стал вице-президент Facebook по общественной политике Джоэл Каплан. По данным издания, он посчитал, что Common Ground приведет к недовольству консерваторов – те могут подумать, что у Facebook есть предубеждения по отношению к их политическим взглядам.

***

25.12.2018
Ирина Фоменко
Почему социальные сети перестали быть актуальными

Термин «социальная сеть» стал бессмысленным набором слов, пишет TechCrunch. Скорее всего, у вас десятки, сотни или, может быть, тысячи друзей и подписчиков на разных платформах. Но соцсети еще никогда не были такими пустыми.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

16.12.2018
Український інститут національної пам'яті виявив у Facebook появу фейкової сторінки

Український інститут національної пам'яті повідомив, що у соцмережі Facebook з'явилася сторінка «Інститут національної пам'яті», яка не має жодного стосунку до офіційної сторінки УІНП і пояснив, як її відрізнити від справжньої (InternetUA).

«Офіційна сторінка Українського інституту національної пам'яті має "галочку" – позначку, яка підтверджує справжність цієї сторінки. Таким чином користувачі можуть відрізнити справжню сторінку інституту від фейкових і бути впевненими, що вся інформація, що публікується в стрічці, достовірна. Оця сторінка, що з'явилася учора – "Інститут національної пам'яті", є фейковою. Просимо поскаржитися та не поширювати від неї дописів», – йдеться у повідомленні.

Наразі створена невідомими сторінка «Інститут національної пам'яті» у Facebook вже недоступна для перегляду.

***

16.12.2018

Перерахуй: Зеленский и его команда запустили новый политический флешмоб

Студия "Квартал 95" запустила новый флешмоб, который касается цен на коммунальные услуги (NewsOboz).

Об этом сообщают на странице «Квартал 95» в социальных сетях, передает NewsOboz.org со ссылкой на Апостроф.

Флешмоб стартовал с обращения Евгения Кошевого, который снял видео, где высказал свое мнение о ценах за газ.

Команда Зеленского призывает пользователей публиковать свои платежки на газ с хештегом #КабмінПерерахуй. Автор лучшей идеи получит возможность побывать на съемках продолжения фильма «Слуга народа» от студии «Квартал 95».

***

19.12.2018

З депутатами Рівненщини можна зв'язатися через соціальні мережі

Громадянська мережа ОПОРА проаналізувала роботу депутатів Рівненської міської ради у соціальній мережі Facebook (період: листопад 2017 року – листопад 2018 року) та порівняла їх активність з минулим роком.

Докладніше

***

21.12.2018

Допис вінницької вчительки про Помісну церкву спричинив релігійний скандал

У Вінниці вчителька математики у закритій групі в соцмережі привітала батьків із створенням помісної української церкви. І ще пожартувала, що їх викликатимуть до школи, як побачать у храмах московського патріархату. Допис потрапив у відкритий доступ і спричинив не лише гнівні коментарі вірян, а й народив чергову жахачку від російських пропагандистів (ТСН).

***

24.12.2018

Стену Трампа высмеяли меткими фотожабами

Президент США Дональд Трамп показал дизайн стены, которая появится на границе с Мексикой. Как он написал в своем Twitter, «стальная ограда»

одновременно «эффективна» и «очень красива». Пользователи сети, тем временем, уже придумали, как перелезть через стену (InternetUA).

По мнению одного из комментаторов, на острые колья сверху можно закрепить пробки, к самой стене приставить лестницу – и человек уже окажется на другой стороне. Другой пользователь предложил накинуть на стену старый матрац, чтобы скрыть острие. Некоторые обратили внимание на то, что пространство между столбами, из которых состоит стена, слишком широкое – и через них можно будет свободно пройти.

В целом же пользователям сети дизайн будущей стены не приглянулся – кто-то сравнил ее с расческой, кто-то с троном из сериала «Игра престолов», а кто-то отметил, что подобный дизайн использовался для строительства деревянных заборов несколько веков назад.

Дональд Трамп заявил о необходимости строительства стены на границе Мексикой для уменьшения нелегальной миграции. На этой неделе (17 – 23 декабря) нижняя палата конгресса США одобрила выделение $ 5 млрд для строительства стены: в поддержку этой инициативы выступили 217 конгрессменов, против – 185.

***

24.12.2018

В анексованому Криму запустили флешмоб «Мусульмани – не терористи»

Ольга Кириленко

В анексованому Криму запустили флешмоб на підтримку кримських татар-мусульман, яких несправедливо звинувачують у злочинах (Громадське).

Діти та дорослі фотографуються з табличкою «Мусульмани не терористи», на якій також присутні фотографії затриманих кримських татар.

Потім надсилають на Facebook-сторінку громадської організації «Кримська солідарність», яка їх оприлюднює.

На сторінці викладено вже понад 50 фото.

***

25.12.2018

«Кораблик на ялинку»: у соцмережах запустили флешмоб на підтримку полонених моряків

Марія Леонова

У соцмережах запустили флешмоб на підтримку полонених українських моряків. Ініціаторами виступили активісти зі Всесвітнього руху патріотів України (Громадське).

Українців та усіх небайдужих закликають прикрашати оселі та новорічні ялинки жовто-блакитними паперовими корабликами.

Фотографію прикрас з хештегом #Жовто_блакитний_кораблик_на_ялинку потрібно виставляти на сторінках у соціальних мережах, а також надсилати Всесвітньому руху патріотів, який публікуватиме результати флешмобу.

Акція триватиме з 25 грудня до 7 січня.

***

25.12.2018

«Заплати за бабусю» – рівнян просять долучитися до всеукраїнського флешмобу

Міжнародний благодійний фонд Lets help оголосив флешмоб #letshelpbabushkas. Саме за цим хештегом можна буде знайти історії допомоги активістів або простих громадян людям поважного віку (Rivne Media).

Небайдужі люди з усіх регіонів України можуть оплатити чеки одиноким людям поважного віку в супермаркетах, магазинах, на базарах. Участь у флешмобі традиційно беруть лідери думок, громадські активісти, а також усі охочі.

Представники фонду кажуть, що за допомогою акції хочуть привернути увагу до скрутного становища українських пенсіонерів. З огляду на мізерну пенсію літні люди часто не можуть собі дозволити навіть мінімальний набір продуктів.

Це вже третій подібний флешмоб. Перші акції пройшли в липні та вересні 2018 року. Учасники розповідають, що багатьом не вірилося в безкорисливе бажанням допомогти: не звикли наші люди до такої доброти й щедрості.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

12.12.2018

Украинская сеть хостелов создала «Telegram-консьержа», чтобы всегда быть рядом с гостями

Сеть хостелов Dream Hostels создала «Telegram-консьержа», чтобы помогать ориентироваться в новом городе и всегда быть рядом с гостями. Консьерж подскажет в какие музеи, кафе, рестораны, клубы лучше пойти или какие события пройдут в городе в ближайшее время.

Докладніше

***

13.12.2018

Исследование: Email занимает 4 место в рекламных расходах брендов

Email занимает скромные 10 % среднего маркетингового бюджета, но продолжает твердо сохранять свою позицию среди других тактик, отмечает исследование Criteo. Платная медийная реклама занимает 16 % бюджетов, социальные медиа – 14 % и традиционный маркетинг 13 %. Контент-маркетинг получает 10 %, SEO – 9 %. На поисковую рекламу выделяют 9 %, на лендинговые страницы/вебсайты 9 % и на аффилированный маркетинг 9 %. Email также занимает хорошую позицию среди тактик по конверсии, которые работают – 41 % используют его для этой цели. Он занимает третье место вслед за социальными медиа (53 %) и платной медийной рекламой (43 %). Поисковую оптимизацию используют 38 %. Исследование отмечает, что онлайн – это второй крупнейший и быстрорастущий канал по расходу рекламы. В прошлом году он составил 34 % от всех рекламных расходов и намерен обогнать ТВ. Глобально, маркетологи называют две стратегии для успеха: увеличение качества для рекламного размещения и предоставление убедительных и уникальных предложений. Email может играть свою роль во всех этих предложениях. Глобально, более 60 % респондентов используют три типа кампаний с повторным вовлечением – повторное вовлечение с помощью приложения, реактивация приложения и повторная покупка. Хотя каждая активность сталкивается с трудностями. К примеру, повторному вовлечению мешают лимитированные каналы и данные. Кроме того, существующие потребители не хотя переходить на другие каналы. При стимулировании повторных покупок брендам сложно изменить ROI (Marketing Media Review).

***

17.12.2018

ТОП-3 совета для создания сильной стратегии в Instagram Stories

Instagram Stories позволяют брендам рассказать историю с помощью видео, графики, популярных продуктов или продуктов, которые проседают в продажах. Ниже три совета, как использовать «Истории» в своей стратегии.

Докладніше

***

19.12.2018

Михаил Сапитон

Facebook таргетирует рекламу по IP-адресу. Даже если отключить определение местоположения

Facebook таргетирует рекламу по местоположению пользователя, даже если юзер отключил отслеживание локации, хранение информации о посещенных местах и удалил из профиля город.

Докладніше

***

20.12.2018
Исследование: больше всего SMM-маркетологов беспокоит ROI

55 % SMM-маркетологов больше всего беспокоит ROI, за ним следует понимание успеха в кросс-канальных активностях (42 %), развитие стратегий для достижения целей бизнеса (39 %) и понимание, какой контент следует размещать (39 %), отмечает исследование Sprout Social's 2018 Social Index.

Докладніше

***

23.12.2018
Ирина Фоменко
Новое о рекламе в соцсетях

Любой, кому когда-либо приходилось обосновывать расходы на социальные сети, поймет, что приятно иметь цифры, на которые можно опираться, пишет IoT Events.

Докладніше

***

23.12.2018
Михаил Сапитон
Facebook разрабатывает криптовалюту для WhatsApp – инсайд Bloomberg

По данным издания Bloomberg, компания Facebook разрабатывает собственную криптовалюту. Электронные деньги планируют использовать в мессенджере WhatsApp. Основной ориентир проекта – рынок заграничных отправлений в Индию. Страна лидирует по количеству международных переводов. За 2017 год в Индию, по данным Всемирного банка, отправили более $69 млрд (AIN.UA).

В Facebook намерены разработать стейблкоин – электронную валюту, курс которой привязан к американскому доллару или другим фиатным активам. Это поможет избежать излишней волатильности. Сейчас над проектом якобы работает блокчейн-команда соцсети, куда входят примерно 40 человек. Возглавляет экспериментальное подразделение Дэвид Маркус, бывший топ-менеджер PayPal. Альткоин еще далек от релиза, поскольку в Facebook прорабатывают стратегию его применения и портфель валют, на который будет опираться стоимость стейблкоина.

В самой соцсети не отрицают существования блокчейн-департамента, но отказываются раскрывать детали его работы. Пока что самый известный стейблкоин-проект – криптодоллар Tether. К нему уже накопилось множество вопросов. Так, создатели проекта отказались проходить внешний аудит,

который бы подтвердил, что каждая выпущенная монета обеспечена фиатными деньгами.

***

24.12.2018
Как оптимизировать сайт под социальные сети

Что такое поисковая оптимизация (SEO) знают практически все, но поисковые системы – не единственный источник трафика на сайт. Одним из таких источников являются социальные медиа.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

12.12.2018
Компьютер вредит детям: названа новая опасность

Головной мозг детей, которые проводят много времени перед экраном компьютера за играми и в интернете, замедляется в развитии (InternetUA).

К такому выводу пришли ученые Национальных институтов здравоохранения США, специалисты провели обследование 4400 детей в возрасте от девяти до десяти лет.

Магнитно-резонансная томография (МРТ) показала, что у подопечных, которые длительное время проводили перед экранами наблюдались изменения в структуре тканей мозга. В частности, результаты говорят о том, что у таких детей наблюдается истончение коры головного мозга.

Истончение коры мозга свидетельствует о преждевременном старении в этой области мозга.

Вместе с этим стало известно о том, что у детей, которые увлекаются гаджетами, наблюдается видимое повышение в крови и мозговой жидкости дофамина (так называемого гормона удовольствия).

При повышении содержания в крови дофамина возможны не только физические, но и психические расстройства.

***

15.12.2018

Фотографии в Инстаграме могут рассказать о вас больше, чем кажется

Каждый день 500 млн людей пользуются Инстаграмом. Эта соцсеть давно перестала быть цифровым фотоальбомом, теперь ее используют для продаж, продвижения в интернете и даже как материал для исследований. Оказывается, фото и фильтры в ваших постах могут многое рассказать как о вашей личности, так и о здоровье.

Докладніше

***

16.12.2018

Почему психологи советуют не пользоваться соцсетями в период новогодних праздников

Ученые доказали, что соцсети могут негативным образом сказаться на настроении людей, а также вызвать депрессию (InternetUA).

Во время проводимого эксперимента его участники все праздничные дни провели дома, не выходя на улицу, а периодически посещая свою страницу Facebook.

С каждым новым днем настроение людей ухудшалось. Ведь помимо отсутствия свежего воздуха, они наблюдали, как проводят выходные их друзья, а самим им показать было нечего. Также ученые отметили, что частое пользование соцсетями вызвало понижение самооценки и отрицательно влияло на общее психологическое состояние, выливаясь в продолжительные депрессии. Особенно это характерно для одиноких людей.

В связи с чем, основная рекомендация психологов – не наблюдать за чужой жизнью с помощью различных социальных сетей, а жить своей полноценной жизнью, где найдется время прогулкам и встречам с друзьями. Использование соцсетей желательно свести к минимуму.

***

17.12.2018

Інстинкти і сучасні технології: що робити, якщо дитину цькують у соцмережах

Коли ваша дитина стає жертвою інтернет-цькування (кібербулінг) найпершою і найприроднішою реакцією батьків є роз’єднання дитини і джерела небезпеки. Простіше кажучи, батьки забирають у дитини телефон/планшет/комп’ютер, щиро віруючи в те, що оберігають дитину.

Докладніше

***

20.12.2018

Зависимость от соцсетей оказалась похожа на алкоголизм – ученые

Наркологи из Австралии выяснили, что люди, не способные покинуть социальные сети даже на секунду, страдают от тех же нарушений в работе психики, что и «профессиональные» алкоголики.

Докладніше

***

25.12.2018

Ученые предупреждают: Instagram вредит вашему здоровью

Исследование показало, что женщины все чаще отказываются от приема в пищу важнейших нутриентов и сталкиваются с депрессиями, если они пользуются Instagram ежедневно (InternetUA).

Ученые доказали, что все большее количество молодых женщин страдает от дефицита важнейших питательных веществ из-за следования модным диетам из социальных сетей.

Эксперты предупреждают, что женщины после 20-ти и 30-ти страдают из-за недостатка таких ключевых минералов, как калий, магний и медь. Это особенно плохо для женщин, у которых уже есть дефицит железа, кальция и йода.

Многие представительницы прекрасного пола добровольно отказываются от глютена, молочных и зерновых продуктов, а также сахара. Причиной этого может быть Instagram и другие социальные сети, которые побуждают к неправильному питанию.

Маніпулятивні технології

12.12.2018

Программист получил 2 года тюрьмы за антиукраинские публикации в «ВКонтакте»

Суд заочно приговорил к 2 годам лишения свободы жителя Тернополя Евгения Фука за распространение в социальной сети «ВКонтакте» призывов к России начать военную агрессию в отношении Украины.

Докладніше

***

13.12.2018

Медичним закладам розсилають фейкові розпорядження щодо воєнного стану

Міністерство охорони здоров'я закликає керівництво медичних закладів перевіряти всі розпорядження щодо воєнного стану (Espreso.tv).

«У Центральну міську лікарню ім. Титова, що у Лисичанську Луганської області, надійшов сфабрикований лист начебто від Луганської ОДА з дорученням провести підготовчі заходи у зв'язку із впровадженням воєнного стану. МОЗ України закликає медзаклади по всій країні бути пильними і перевіряти кожен підозрілий лист», – наголосили у відомстві.

Як зазначають у МОЗ, воєнний стан є правовим режимом, вперше запровадженим у 10 областях України, тому пов'язані з ним аспекти можуть стати предметом для маніпуляцій і провокацій з боку ворожих до Української держави структур.

«Провокатори можуть надсилати вказівки під приводом воєнного стану від імені керівних структур різного рівня. Підробки на перший погляд не відрізняються від офіційних листів: вони містять вихідний номер, підпис посадової особи та інші стандартні атрибути офіційних звернень. Такі листи можуть направлятися як в окремі медзаклади або обласні управління охорони здоров'я з метою підірвати системну роботу», – застерігають у МОЗ.

***

17.12.2018

Журналисты обвинили Facebook в заказе фейковых новостей

Несколько бывших и действующих фактчекеров, нанятых Facebook для выявления фейковых новостей, заявили, что компания использовала их только для отвода глаз и на самом деле ничего не сделала для борьбы с недостоверной информацией.

Докладніше

***

18.12.2018

Звіт: Активність російської «фабрики тролів» в соцмережах США триває

Спроби Росії вплинути на вибори в США в 2016 році через соцмережі були спрямовані на чорношкірих американців і мали на меті зниження явки виборців-демократів.

Докладніше

***

20.12.2018

Прокурор Вашингтона подал в суд на Facebook

Полученные компанией данные якобы могли быть использованы для влияния на результат выборов президента в США в 2016 году (InternetUA).

Генеральный прокурор столицы США города Вашингтон (округ Колумбия) подал судебный иск против компании Facebook. Иск касается предоставления доступа к данным пользователей Facebook компании Cambridge Analytica, передает Голос Америки со ссылкой на The Hill.

Полученные компанией данные якобы могли быть использованы для влияния на результат выборов президента в США в 2016 году, вмешательства в их течение.

«Facebook не защитил приватность своих пользователей и обманул их относительно того, кто имел доступ к их данным и как эти данные использовались. Facebook подверг риску манипуляций данные пользователей, позволив таким компаниям, как Cambridge Analytica и другим, доступ к личным данным без согласия пользователей», – говорится в представлении генпрокурора Вашингтона Карла Расина.

Как подчеркнул прокурор, иск ставит целью заставить Facebook исполнять собственные обещания по защите приватности пользователей.

Спецслужби і технології «соціального контролю»

12.12.2018
Ирина Фоменко
Главным провокатором французских протестов оказался Facebook

Райан Бродерик и Жюль Дарманин опубликовали отчет в BuzzFeed о французский протестах, которые активисты транслировали в прямом эфире в Facebook. Репортеры описывают движение «желтых жилетов» как петлю обратной связи, начавшейся в Facebook в так называемых «группах гнева», вызвавшей бурные протесты в реальном мире, которые, в свою очередь, снова обсуждали в социальной сети.

Докладніше

***

12.12.2018
Група тернопільських студентів через Telegram налагодила наркобізнес

Житель Миколаївської області організував у Тернополі наркобізнес. Собі у помічники він взяв восьмеро осіб. Усі – молоді хлопці та дівчата віком від 18 до 24 років. Деякі з них – студенти місцевих вишів.

Докладніше

***

12.12.2018

Зберігай спокій та фільтруй інформацію: Як українцям протистояти війні фейків // Сучасна війна ведеться не тільки зброєю - перевагу над ворогом намагаються набути й у інформаційному просторі

Юлія Гуш

Більше чотирьох років в Україні говорять про інформаційну війну з боку Росії та необхідність якось їй протидіяти. Дезінформація, фальсифікація, жонглювання штампами та кліше, навала інтернет-тролів, поширення фейків – заради домінування в інформаційному просторі можуть згодитися будь-які методи.

Докладніше

***

13.12.2018

Владимир Кондрашов

СБУ поймала майнеров криптовалют, которые финансировали сепаратистов

В Едином государственном реестре судебных решений появились подробности дела о финансировании терроризма сотрудниками интернет-магазина. Свежее определение суда не только проливает больше света на эту историю, но даже называет фигурантов уголовного дела.

Докладніше

***

14.12.2018

Пенсионера приговорили к 3 годам условно за сепаратизм в «Одноклассниках»

Луцкий городской районный суд Волынской области приговорил 64-летнего жителя Волынской области к 3 годам лишения свободы с установлением однолетнего испытательного срока условно за сепаратистские публикации в российской социальной сети «Одноклассники». Об этом говорится в сообщении прокуратуры Волынской области, передают Українські Новини (InternetUA).

В частности, мужчина публиковал призывы к изменению границ территории и государственной границы. «Гражданин, используя компьютерное оборудование и средства мобильной связи, зарегистрировал электронную страницу под сетевым псевдонимом в российской социальной сети “Одноклассники” и размещал там публичные призывы о необходимости “освобождения” войсками Российской Федерации территории Украины от проукраински настроенного населения», – говорится в сообщении.

После разоблачения обвиняемый искренне раскаялся в содеянном, активно способствовал раскрытию преступления – и суд учел это при определении ему меры наказания.

***

15.12.2018

Владимир Кондрашов

В СБУ подтвердили, что российские тролли покупают аккаунты украинцев в соцсетях

Служба безопасности Украины подтвердила, что скупкой аккаунтов украинцев в социальных сетях под видом маркетингового агентства занималось скандально известное российское «Агентство Интернет Исследований», больше известное как «ольгинская фабрика троллей».

Докладніше

***

15.12.2018

Поведение китайцев в соцсетях повлияет на их рейтинг

Китайские власти анонсировали скорый запуск черного списка для пользователей, критикующих действия правительства в социальных сетях, либо оскорбляющих других людей. Об этом пишет South China Morning Post (InternetUA).

Теперь за каждое действие в интернете пользователи получат отзыв в свой социальный рейтинг, а абсолютно все сайты, работающие в Китае, должны «проявлять нулевую терпимость к нарушителям». Кроме того, в скором времени пользователей обяжут регистрироваться по настоящим паспортным данным.

По словам замдиректора Министерства киберзащиты Китая Лю Лехуна, такие действия позволят обеспечить целостный вид китайского интернет-пространства.

Постоянная система социальных кредитов в Китае заработает с 2021 года. За каждое правонарушение, даже самое мелкое, рейтинг граждан снизится – вплоть до того, что они не смогут найти работу, ходить в обычные супермаркеты и летать на самолетах.

Сейчас эта система уже тестируется в китайском регионе Синьцзяне с преимущественно мусульманским населением на границе с Киргизией. Система влияет на все возможности человека – от права пользоваться государственными услугами до возможности начать бизнес или устроиться на работу.

При этом гражданам с высоким социальным рейтингом китайская система предлагает ряд привилегий, например, проходить паспортный контроль без очереди, тогда как людям с низким рейтингом просто откажут в полете.

***

17.12.2018

YouTube удалил 7,8 млн видео и 224 млн комментариев в третьем квартале 2018 года

Еще в апреле YouTube выпустил ежеквартальный отчет YouTube Community Guidelines Enforcement Report о соблюдении принципов сообщества (iLenta.com).

На днях компания расширила отчет дополнительными данными, такими как количество удаленных каналов, удаленных комментариев и причину, по которой видео или канал были удалены.

С июля по сентябрь 2018 года YouTube удалил 7,8 миллиона видеороликов, 81 % или 6,4 млн из них были впервые обнаружены автоматизированными системами на базе алгоритмов искусственного интеллекта. Из обнаруженных 74,5 % были удалены так быстро, что даже не успели получить ни одного просмотра. Кроме этого, было удалено 1,7 млн каналов и более 224 млн комментариев.

Более 90 % каналов и более 80 % видео, которые были удалены в сентябре 2018 года, были удалены за нарушение правил в отношении спама или контента для взрослых. Такое нарушение, как пропаганда насилия или экстремизма, встречалось лишь в 0,4 % удалённых видео.

Что касается комментариев, то их было удаленно более 224 миллионов. Все удаления связаны со спамом или не были одобрены авторами тех каналов, где они были опубликованы.

***

18.12.2018

Кремль витратить 300 мільйонів доларів на блокування Telegram

У 2019 році Роскомнадзор планує впровадити нову технологію боротьби із забороненими сайтами і сервісами, в тому числі з Telegram.

Докладніше

***

18.12.2018

Facebook та Instagram заблокували сторінки Національного корпусу

Сторінки заблокували за публікації з акції «Ні – кремлівським окупантам!» (Espreso.tv)

Про це йдеться на сайті Нацкорпусу.

Ці публікації в адміністрації соцмережі розцінили як «ворожі висловлювання».

Проте, у політсилі запевняють, що публікації не містили заборонені законом символи, гасла та зображення.

«Акція за участю Нацкорпусу і Нацдружин відбулася в Києві біля Адміністрації президента з вимогами до української влади розірвати дипвідносини з РФ, обмежити діяльність російського бізнесу в Україні на час війни тощо. Зазначимо, що ні на фото, ні на відео, ні в тексті опису заходи, опублікованих на Facebook, не було жодного забороненого законом символу, гасла і зображення», – повідомляють у Нацкорпусі 18 грудня увечері.

Вони зазначили, що східноєвропейський офіс Facebook знаходиться у Москві. «Facebook давно повинен працювати з українським сегментом саме з Києва. Як і інші IT-кампанії», – заявили у Нацкорпусі.

***

18.12.2018

С помощью специального устройства правоохранители получат доступ к личным данным

СБУ закупило устройство для взлома смартфонов. С его помощью можно добыть практически все данные. Специальных навыков для использования не требуется (InternetUA).

17 декабря управление Службы безопасности Украины в Запорожской области заказало у ТОВ «Эпос» мобильное рабочее место криминалистической экспертизы мобильных устройств UFED Touch 2 стоимостью 172 тысяч гривен, пишут «Наші гроші».

UFED Touch 2 используется в криминалистических исследованиях. С его помощью можно извлекать, декодировать и анализировать доказательные данные, полученные из различных моделей мобильных устройств. От пользователя не требуется специальных навыков, лишь физический доступ к устройству и время.

UFED Touch 2 создан израильской компанией Cellebrite. Среди «клиентов» фирмы спецслужбы США и Российской Федерации.

***

18.12.2018

В Чехии оборудование Huawei и ZTE назвали угрозой безопасности

Чешское национального агентства по цифровой и информационной безопасности (Czech National Cyber and Information Security Agency, NCISA) предостерегло операторов от использования ПО и оборудования китайских производителей Huawei и ZTE, заявив, что они могут угрожать безопасности страны.

Докладніше

***

22.12.2018

Цьогоріч в Україні засудили 15 людей за антиукраїнську діяльність в соцмережах

Українські суди у 2018 році винесли 15 обвинувальних вироків стосовно власників та адміністраторів антиукраїнських спільнот у соціальних мережах, у яких поширювалися заклики до повалення державної влади і масових заворушень, повідомив прес-центр СБУ (InternetUA).

Загалом СБУ цьогоріч здійснює розслідування 83 кримінальних проваджень проти власників та адміністраторів таких спільнот. У рамках цих проваджень 23 особам оголошено про підозру в діях, спрямованих на повалення державної влади, у посяганні на територіальну цілісність України та у створенні терористичних груп та організацій, а 15 особам суди винесли обвинувальні вироки. При цьому подробиці про ці вироки в повідомленні СБУ відсутні.

Також СБУ повідомила про «превентивні заходи» стосовно ще 220 адміністраторів таких спільнот, що дозволило вберегти їх від скоєння вищезгаданих злочинів.

***

27.12.2018

Правительство Индии требует, чтобы компании убрали сквозное шифрование

Правительство Индии хочет обязать технологические платформы – такие как Facebook, WhatsApp, Twitter и Google – удалять контент в течение суток, если его признают «незаконным», и создать «автоматизированные инструменты» для удаления такой информации в будущем.

Докладніше

Проблема захисту даних. DDOS та вірусні атаки

12.12.2018

Кіберполіція попереджає про шкідливий вірус та радить як його знешкодити

Створене шкідливе програмне забезпечення, націлене на користувачів операційної системи MS Windows. Спеціалісти з кіберполіції 11 грудня почали фіксувати факти розповсюдження цього шкідливого програмного забезпечення.

Докладніше

***

12.12.2018

Троян DanaBot отправляет спам-сообщения для распространения угроз

Компания ESET сообщила об обнаружении новых функций трояна DanaBot, которые выводят угрозу за пределы категории банковских троянов. Согласно исследованию специалистов ESET, операторы DanaBot недавно экспериментировали с функциями сбора электронных адресов и отправки спама, которые могут использовать учетные записи электронной почты жертв для дальнейшего распространения вредоносных программ.

Докладніше

***

12.12.2018

NYT: данные 500 млн клиентов Marriott украли китайские хакеры

Предварительные результаты расследования хакерской атаки на сеть отелей Marriott свидетельствуют о том, что за нападением может стоять китайская разведка. Об этом пишет The New York Times со ссылкой на источники (InternetUA).

По их словам, хакеров, получивших доступ к личным данным порядка 500 млн гостей, подозревают в сотрудничестве с Министерством госбезопасности КНР. Чиновники минюста США планируют предъявить злоумышленникам новые обвинения. Для этого будет рассекречена часть конфиденциальных данных, которые будут свидетельствовать о попытках китайской стороны создать базу данных с информацией о чиновниках в составе правительства США.

По словам официального представителя китайского МИДа Гэн Шуана, КНР отвергает подобные обвинения.

***

12.12.2018

Ирина Фоменко

За вредоносный контент пользователей скоро ответят интернет-площадки

В этом году сервис-провайдеру Prodigy предъявили иск за клевету за размещение пользователем определенного контента на одной из досок объявлений. Анонимное лицо обвинило фирму, ведущую операции с ценными бумагами, в мошенничестве в связи с первоначальным публичным предложением, пишет Fast Company.

Докладніше

***

12.12.2018

Владимир Кондрашов

Медицинские данные детей центра кардиохирургии были на грани «утечки»

Украинские хактивисты обнаружили серьезные проблемы с безопасностью, которые могли повлечь за собой утечку в открытый доступ около 2,2 терабайт медицинской информации, принадлежащей столичному Центру детской кардиологии и кардиохирургии.

Докладніше

***

13.12.2018

Android-троян научился обходить двухфакторную аутентификацию

Лукас Стефанко, эксперт в области кибербезопасности антивирусной компании ESET, узнал о существовании нового Android-трояна, который научился миновать двухфакторную аутентификацию и воровать денежные средства пользователей PayPal. Вредоносная программа скрывается под видом утилиты для оптимизации энергопотребления смартфонов и распространяется посредством скомпрометированных ресурсов и альтернативных магазинов приложений (InternetUA).

После установки троян сканирует устройство на предмет присутствия приложения PayPal, запрашивает доступ к специальным возможностям, а потом скрывает свою пиктограмму с рабочего стола. После этого пользователю отправляется уведомление с рекомендацией войти в учетную запись PayPal под предлогом проверки данных с целью обеспечения безопасности.

Как защититься от Android-трояна

Если жертва подчиняется, авторизуясь в приложении, в дело вступают специальные возможности устройства, которые имитируют нажатия на экран и таким образом переводят со счета 1000 долларов/евро в зависимости от региона нахождения. По словам Стефанко, весь процесс занимает не более 5 секунд и не предполагает сколь-нибудь эффективного способа вмешаться в него. А поскольку троян не занимается подлогом, дожидаясь, пока пользователь сам откроет приложение PayPal, то даже двухфакторная аутентификация не оказывает каких-либо препятствий.

Несмотря на то, что троян, в первую очередь, рассчитан именно на пользователей PayPal, в случае отсутствия на устройстве официального приложения платежного сервиса, тот обращается к фишингу. Он загружает оверлейные компоненты, которые перекрывают экраны авторизации в приложениях Google Play, WhatsApp, Skype, Viber и Gmail и предлагают жертве ввести данные ее банковской карты.

***

13.12.2018

Владимир Кондрашов
Киберполиция вышла на след продавца вирусов

Причерноморское управление киберполиции Департамента киберполиции Национальной полиции Украины вышло на след гражданина Украины, который осуществляет распространение и сбыт вредоносных программ.

Докладніше

***

13.12.2018
Приложения из App Store отслеживают все передвижения пользователей

Приложения из магазина App Store каждые 2 секунды отслеживают перемещения пользователя (InternetUA). Об этом сообщает The New York Times.

В издании провели независимое расследование и рассказали о наблюдениях. Оказалось, что приложения даже не уведомляют пользователей о таком «присмотре». Таким образом, компания знает местоположение практически всех пользователей в режиме реального времени.

Приложения из App Store, которые следят за каждым шагом, в настройках требуют доступ к геолокации. Такие программы отслеживают где вы бываете в течение дня или в конкретный промежуток времени. Знают, как долго вы бываете в конкретном месте, где бываете чаще всего и даже маршрут домой. И хотя они измеряют активность благодаря пройденному маршруту, основываясь на картах, эти данные не должны сохраняться, особенно на серверах яблочной корпорации.

Данные у Apple потом покупают разные компании и магазины, чтобы размещать эффективную таргетированную рекламу в сети. По наблюдениям The New York Times, среди таких приложений является The Weather Channel, WeatherBug, theScore и еще куча других приложений, в частности для отслеживания погоды.

***

13.12.2018
Дмитрий Сизов
Наемные хакеры спасают IT компании от реального взлома

Согласно новым данным, опубликованным этической хакерской платформой Bugcrowd, внештатные хакеры могут зарабатывать более 500000 долларов в год на поиске уязвимостей и сообщении об этих проблемах компаниям, таким как Tesla и правительственных организациям – типа Министерства обороны.

Докладніше

***

13.12.2018

Хакеры из Ирана взломали почту американских чиновников

Кибератаке со стороны иранской хакерской группы Charming Kitten подверглись американские чиновники. Злоумышленники получили доступ к почтовым ящикам высокопоставленных сторонников и противников иранской ядерной сделки, передает Associated Press (InternetUA).

По данным СМИ, атаке также подверглись арабские ученые-атомщики и иранские общественные деятели.

Издание со ссылкой на экспертов предполагает, что атака может быть связана с новыми санкциями США в отношении Ирана, а за киберпреступлением стоят власти Ирана.

***

14.12.2018

Уязвимость в сервисах Microsoft позволяла взломать любую учетную запись

Индийский исследователь безопасности Сахад Нк (Sahad Nk) обнаружил несколько уязвимостей, позволяющих злоумышленникам взломать учетные записи пользователей сервисов Microsoft, начиная от Office и заканчивая Outlook (InternetUA).

Проводя исследование для сайта SafetyDetective, исследователь смог захватить контроль над поддоменом компании Microsoft (success.office.com). Благодаря неправильной конфигурации поддомена Нк удалось настроить web-приложение Azure, указывавшее на запись CNAME поддомена. Таким образом он не только получил контроль над success.office.com, но также смог получать все отправляемые ему данные.

Далее в игру вступила вторая уязвимость. Приложения Microsoft Office, Outlook, Store и Sway отправляют поддомену success.office.com токены авторизации. Когда пользователь авторизовался в Microsoft Live, сервис login.live.com отправлял токен прямиком на подконтрольный исследователю сервер. Нк было достаточно лишь отправить жертве электронное письмо с ссылкой, после нажатия на которую в его руках оказался бы действительный токен сеанса. В таком случае для взлома учетной записи не понадобилось бы ни имя пользователя, ни пароль.

Поскольку у исследователя был доступ со стороны Microsoft, отправленная жертве ссылка была бы представлена в виде URL-адреса login.live.com, что позволило бы ей обойти спам-фильтры и защиту от фишинга.

Исследователь сообщил Microsoft об уязвимости еще в июне нынешнего года, однако компания исправила ее лишь в ноябре.

***

18.12.2018

Ошибка в Twitter предоставляла доступ к личным сообщениям пользователей

В социальной сети Twitter устранена ошибка, раскрывавшая личную переписку пользователей сторонним лицам. Проблема проявлялась при использовании приложений, запрашивающих PIN-код для завершения процесса авторизации, вместо применения протокола Oauth. В результате, некоторые разрешения, например, на доступ к личным сообщениям, оставались скрытыми для пользователей Twitter (InternetUA).

По словам исследователя Теренса Идена (Terence Eden), обнаружившего уязвимость, проблема заключается в том, как официальный API Twitter обрабатывает ключи и секреты, к которым разработчики приложений могут получить доступ без авторизации.

«Несколько лет назад утекли официальные ключи API Twitter. Это значит, что разработчики приложений, не одобренных Twitter, по-прежнему могут получить доступ к программному интерфейсу», – пояснил специалист.

Для предотвращения злоупотреблений социальная платформа реализовала ряд мер, в частности ограничение URL обратного вызова, то есть одобренное приложение может получить доступ только к предопределенному адресу. Однако, некоторые приложения не используют URL-адрес или не поддерживают функцию обратных вызовов. Для таких случаев Twitter предусмотрела дополнительный механизм авторизации – по PIN-коду.

«Вы авторизуетесь, вам предоставляется PIN, вы вводите PIN в приложение» и программа получает доступ к контенту в Twitter, говорит Иден. Он обнаружил, что в случае с такими приложениями экран OAuth в Twitter по какой-то причине отображает некорректную информацию. В результате пользователи считают, что у приложений нет доступа к частным сообщениям, хотя на самом деле он есть.

Иден передал информацию об уязвимости администрации Twitter. Проблема уже исправлена, а исследователь получил награду в размере $2 940.

***

17.12.2018

Владимир Кондрашов

Количество кибератак на ВСУ за месяц выросло в четыре раза

С момента введения военного положения в десяти областях Украины количество кибератак на ресурсы Вооруженных Сил Украины выросло в 4 раза.

Докладніше

***

17.12.2018

В Генштабе призвали военных не использовать мессенджеры и iPhone в зоне боевых действий

Генеральный штаб Вооруженных сил призывает военнослужащих не использовать интернет-мессенджеры в зоне боевых действий. Об этом на брифинге сказал начальник войск связи Владимир Рапко, передают Украинские новости (InternetUA).

«У мессенджеров типа Telegram и Viber серверы находятся в России, и в принципе на них все и остается, а у WhatsApp и Skype – остается на серверах в США. ...Если вы открыли мессенжер и работаете в нем, то в нем уже есть полностью все данные о вас. Все эти данные могут быть использованы против наших военных, о чем мы и им и говорим», – сказал генерал. Он также рассказал об опасности телефонов iPhone. «Если вы, к примеру, хоть один раз взяли iPhone и нажали отпечаток пальца, поверьте, этот Iphone уже вас давно сфотографировал, и ваши отпечатки уже есть в базе данных», – сказал Рапко.

Таким образом, Генштаб усилил разъяснительную работу среди военных об опасности использования собственного мобильного телефона в зоне боевых действий, а также о недопустимости фотографирования с привязкой к геолокации.

***

18.12.2018

Обнаружен новый опасный вирус на Android

Исследователи в области кибербезопасности из компании Sophos обнаружили вредоносную программу для устройств под управлением Android, которая провоцирует быструю разрядку аккумулятора. На отчет обратил внимание таблоид Mirror (InternetUA).

Вредное ПО было обнаружено в нескольких сервисах из магазина Google Play и получило название Andr/Clickr-AD. Внутри зараженных приложений содержался кликер, который генерировал переходы по рекламным ссылкам и работал вне зависимости от того, запущено приложение или нет. Постоянная активность приводила к быстрой разрядке аккумулятора. Зараженными оказались более 20 приложений, скачанных около двух миллионов раз.

Злоумышленники позиционировали свои программы для рекламодателей как iOS-приложения, что позволяло им увеличивать доходы. На данный момент зараженные программы удалены из Google Play.

Эксперты посоветовали использовать антивирусы, а пострадавшим предложили вернуть заводские настройки, но предупредили об удалении хранящейся информации в случае использования этого способа.

***

18.12.2018

Хакер взламывал компьютеры украинцев и продавал данные в Интернете

Вредоносное программное обеспечение он распространял под видом файла «Amazon.exe». По данному факту проводится досудебное расследование. Злоумышленнику объявлено о подозрении (InternetUA).

Работники Причерноморского управления Департамента киберполиции совместно со следователями полиции Николаевщины разоблачили 28-летнего жителя города Николаева, который осуществлял несанкционированное вмешательство в работу персональных компьютеров пользователей.

Полицейские во время проведения досудебного расследования установили, что вредоносное программное обеспечение злоумышленник распространял под видом файла «Amazon.exe». Основная цель его действий – атака на веб-ресурсы сети Интернет с целью получения доступа к удаленному рабочему столу и осуществления DDoS-атак.

После получения доступа к компьютеру жертвы, злоумышленник продавал его за деньги на хакерских форумах.

По месту жительства злоумышленника полицейские провели санкционированный обыск. В его квартире следователи изъяли его компьютерную технику и телефон, которые злоумышленник использовал для осуществления своей преступной деятельности.

Во время предварительного осмотра техники, специалисты обнаружили в компьютере мужчины административную панель вредоносного программного обеспечения.

По данному факту начато уголовное производство по ч.1 ст.361-1 (создание с целью использования, распространения или сбыта вредных программных или технических средств, а также их распространение или сбыт) УК Украины. Злоумышленнику объявлено о подозрении. Ему грозит до двух лет лишения свободы.

***

19.12.2018

Twitter атаковали правительственные киберпреступники

Twitter сообщила об атаке на социальную платформу, в организации которой подозреваются проправительственные киберпреступники. Согласно информации на странице поддержки, 15 ноября текущего года компания заметила «большое число запросов, поступающих с частных IP-адресов, расположенных в Китае и Саудовской Аравии» (InternetUA).

Злоумышленники воспользовались уязвимостью в форме поддержки, используемой для информирования администрации соцсети о различных неполадках, позволявшей вычислить код страны привязанного к учетной записи номера телефона и проверить данные о блокировке аккаунта.

Twitter не смогла точно сказать, кто стоит за атаками и какую цель преследовали злоумышленники, но в компании не исключают, что данные IP-адреса могут быть связаны с финансируемыми правительством киберпреступниками. Уязвимость была выявлена 15 ноября, спустя день она была исправлена. Администрация платформы уже уведомила владельцев учетных записей, которые могли пострадать в результате инцидента.

Ранее Twitter устранила ошибку, раскрывавшую личную переписку пользователей сторонним лицам. Проблема проявлялась при использовании приложений, запрашивающих PIN-код для завершения процесса авторизации, вместо применения протокола Oauth. В результате, некоторые разрешения, например, на доступ к личным сообщениям, оставались скрытыми для пользователей соцсети.

***

18.12.2018

Мошенники рассылают фишинговые уведомления о невозможности доставить письмо

Исследователь безопасности из SANS ICS Ксавье Мертенс (Xavier Mertens) обнаружил новую фишинговую кампанию, в ходе которой злоумышленники рассылают поддельные уведомления якобы от Office 365 о невозможности доставить сообщение (Центр информационной безопасности).

Жертвы получают уведомление следующего характера: «Microsoft обнаружила несколько неотправленных писем». В уведомлении также есть ссылка «Отправить еще раз» якобы для повторной отправки «неотправленных» писем. После нажатия на ссылку жертва оказывается на поддельной странице авторизации Office 365.

Когда пользователь вводит в форму для авторизации свой пароль, функция JavaScript под названием sendmails() отправляет введенные учетные данные скрипту sendx.php и перенаправляет жертву на настоящую страницу авторизации Office 365.

URL-адрес фишинговой страницы отличается от настоящего и должен вызывать опасения, но большинство пользователей, увидев знакомый экран, не обращают внимания на адресную строку.

***

18.12.2018

Новая версия движка WordPress 5.0 сливала в Google учетные данные пользователей

Спустя всего неделю после выхода крупного обновления движка WordPress команда разработчиков была вынуждена выпустить срочный патч для WordPress 5.0. В обновленной версии WordPress 5.0.1 устраняются семь проблем безопасности (некоторые из них позволяют получить контроль над

сайтом), а также устраняется очень серьезная утечка важных данных (Центр информационной безопасности).

Проблему утечки обнаружили разработчики плагина Yoast SEO – оказалось, что баг приводил к тому, что поисковая система Google индексировала учетные данные пользователей сайта на WordPress.

Используя специальные поисковые запросы в Google, злоумышленник мог найти страницы с учетными данными, где он мог собрать адреса электронной почты и сгенерированные автоматом пароли. Такая уязвимость могла иметь катастрофические последствия, если в руки третьего лица попадали пароли администраторов. В том случае, если пользователь не изменил сгенерированный движком пароль (а так бывает довольно часто), атакующий мог получить доступ к сайту.

Разработчики популярной CMS также добавили в WordPress 5.0.1 поддержку более серьезной проверки MIME для загружаемых файлов.

***

19.12.2018

Дмитрий Демченко

Facebook давала доступ к скрытым данным пользователей «Яндексу» и еще более ста компаниям

Издание The New York Times опубликовало новое расследование о работе Facebook с партнерами. Журналисты изучили 270 документов компании, а также провели интервью с ее бывшими сотрудниками – это более 60 человек (AIN.UA).

The New York Times выяснило, что Facebook заключала партнерства с более чем 150 крупными компаниями, которым давала доступ к скрытой информации своей аудитории. Например, компания разрешила поисковику Bing, который принадлежит Microsoft, видеть имена всех друзей пользователей без их согласия; Netflix и Spotify – читать личные переписки; Sony, Amazon и Microsoft – получать контактные данные пользователей.

По данным издания, «Яндекс» имел доступ к уникальным идентификаторам пользователей Facebook – даже после того, как компания отключила сторонние приложения от доступа к ним.

В Facebook заявили, что ни одно из этих партнерств или функций не давало компаниям доступ к информации без разрешения пользователей. Кроме этого, представители компании рассказали, что такие партнерства позволяли связывать сторонние сервисы с социальной сетью.

***

19.12.2018

Netflix могла иметь доступ к личным сообщениям пользователей Facebook

Американская компания Netflix могла иметь техническую возможность доступа к личным сообщениям пользователей Facebook. Об этом сообщает Variety (InternetUA).

По данным издания, у нее также могла быть возможность удалять сообщения пользователей.

Однако в Netflix заявили, что никогда не прибегали к подобным действиям.

«Мы ни разу не обращались к личным сообщениям пользователей Facebook и не просили о предоставлении доступа к ним», – подчеркнули в компании.

Подобные подозрения появились на фоне публикации газеты The New York Times о том, что Facebook предоставляла компаниям доступ к личным данным пользователей.

***

19.12.2018

Хакеры начали прятать вирусы в мемах

Специалисты в области кибербезопасности из компании TrendMicro обнаружили вредоносный код в опубликованных в соцсети Twitter мемах. О новом методе работы хакеров сообщается в отчете, опубликованном на сайте компании (InternetUA).

Вредная программа под названием TROJAN.MSIL.BERBOMTHUM.AA получала команды из кода, содержащегося в опубликованных в Twitter картинках. Изображения использовались в качестве средства связи с оператором вредоносной программы. После заражения компьютера вирус мог делать снимки экрана жертвы или воровать личные данные.

Злоумышленники создали аккаунт в Twitter заблаговременно: посты появились в нем еще в октябре. На данный момент учетная запись деактивирована. Как происходит заражение устройств жертв и кто контролирует атаки, неизвестно.

Вероятно, преступники использовали такой уникальный способ контролировать атаки из-за того, что антивирусное программное обеспечение в большинстве случаев не помечает обращение к сайту Twitter опасным.

***

19.12.2018

Ирина Фоменко

ЕС расследует отчет о массовом взломе дипломатических каналов связи

Европейский союз открыл расследование о «потенциальной утечке конфиденциальной информации» после сообщения о том, что хакеры взломали

сеть дипломатических коммуникаций. Об этом сообщает Bloomberg (InternetUA).

Используя методы наподобие тех, которые применяет подразделение Народно-освободительной армии Китая, хакеры читали дипломатическую переписку на протяжении трех лет.

«Мы осведомлены об обвинениях и активно расследуем проблему», – заявила пресс-секретарь Европейского совета.

Предполагаемую атаку обнаружила американская компания кибербезопасности Area 1 Security: она включала в себя тысячи сообщений, в которых рассказывается о проблемах администрации Дональда Трампа, о борьбе с Россией и Китаем, а также о ядерных рисках Ирана.

В одной телеграмме европейские дипломаты описали июльскую встречу президента США Трампа и президента России Владимира Путина как «успешную (по крайней мере, для Путина)». В другом подробном сообщении цитируется, что президент Китая Си Цзиньпин на встрече с европейскими официальными лицами в том же месяце обвиняет Трампа в «запугивании» Пекина.

Хакеры, обнаруженные Area 1 Security, якобы взломали систему ЕС посредством фишинговой кампании, направленной на дипломатов на Кипре, после чего они получили доступ к паролям базы данных бирж ЕС.

«Секретариат Совета не комментирует обвинения и вопросы, касающиеся оперативной безопасности», – заявила пресс-секретарь Европейского совета.

***

19.12.2018
Владимир Кондрашов
Украинский гидрометцентр взломали русскоязычные хакеры

Украинский гидрометцентр взломали неизвестные хакеры, понимающие кириллицу. Уязвимость позволила злоумышленникам воровать данные гидрометцентра и получить полный контроль над почтовым сервером учреждения.

Докладніше

***

20.12.2018
У 2018 році Нацполіція викрила тисячу злочинів у сфері кібербезпеки

20 грудня під час підсумкового річного звіту Голова Національної поліції Сергій Князєв високо оцінив роботу Департаменту кіберполіції у 2018 році та розповів про їх основні результати роботи за рік (Урядовий портал).

«У цьому році підрозділом виявлено близько 6 тисяч злочинів, вчинених у сфері використання високих інформаційних технологій. З них майже тисяча – злочини, вчинені у сфері кібербезпеки», – повідомив Сергій Князєв.

Він додав, що серед успішних операцій – затримання організатора бот-мережі Avalanche, викриття учасника міжнародного хакерського угрупування Cobalt, участь в припиненні діяльності міжнародної хакерської групи FIN7.

За словами Сергія Князєва, Національна поліція продовжує налагоджувати тісні зв'язки з правоохоронними органами всього світу. Так, протягом року було підписано договори про взаємодію у сфері боротьби з кіберзлочинністю з поліцією Австралії, Сінгапуру, Катару та ще низки країн. Відтак, в української кіберполіції вже є напрацювання та успішні результати міжнародної співпраці.

«У рамках міжнародної співпраці викрито 8 транснаціональних хакерських угруповань та взято участь у понад 30 міжнародних операціях», – зазначив глава Нацполіції.

Сергій Князєв відзначив також роботу підрозділу, направлену на попередження вчинення злочинів, що могли значно вплинути на роботу держорганів та життя українців. Так, протягом року було попереджено поширення 4 масових кібератак на території України.

***

20.18.2018

Хакери викрили проект ФСБ у соцмережах з пошуку нелояльних до влади людей

Хакерське угруповання Digital Revolution зламало сервери наукового дослідного інституту «Квант», що входить до складу ФСБ (Рубрика).

Про це передає BBC.

Хакери опублікували список папок і адміністраторів серверів «Кванта», а також помістили на сайт НДІ символ свого угрупування – картинку з собаками в капюшонах. Практично відразу ж «Квант2 відключив свій сайт.

У документах хакери знайшли відомості щодо системи штучного інтелекту, який мав самостійно моніторити соціальні мережі.

Так, в одному з документі під назвою «Авнер» описуються системи моніторингу громадської думки та пошуку протестних настроїв у «ВКонтакте», Twitter, Facebook і навіть Instagram.

Аналіз повинен проводитися за допомогою штучного інтелекту.

«Квант» повинен був також розробити систему нейромереж, які можуть шукати «екстремальні віртуальні групи» в соціальних мережах, наприклад, групу «Путін – йди», і самостійно аналізувати пости в них.

В документах «Кванта» також йдеться про те, що НДІ створював аналогічні системи для уряду і спецслужб Казахстану.

***

22.12.2018

В Apple рассказали, сколько раз Украина запрашивала данные пользователей

Американский гигант электронных технологий Apple представил «отчет о прозрачности» за первую половину 2018 года. Там указано, сколько раз Правительство Украины обращалось к компании за персональными данными своих граждан (InternetUA).

Об этом говорится на официальной странице компании.

Всего правительства обратились к Apple 32342 раза – это на 9 % больше, чем за предыдущий период. Доступ требовался к 163823 устройствам.

Чаще всего к компании обращалась Германия – 13704 запроса к 26160 устройствам (42 % всех случаев). Чаще всего поводом была кража чужих данных.

На втором месте США – 4570 запроса к 14911 устройствам. В больше, чем половине, случаев речь шла об основной информации пользователя или контенте. 918 случаев были связаны с финансовым мошенничеством.

Украинское Правительство запрашивало доступ к 2 устройствам и к 2 аккаунтам – непонятно были ли они связаны. Украина получила доступ к одному устройству, в доступе к аккаунтам было отказано.

Россия запрашивала доступ к 2909 девайсам, 3 аккаунтам и 5 раз просила предоставить финансовую информацию. Получила доступ к 536 устройствам, одной учетной записи и в трех случаях – к финансовым данным.

***

22.12.2018

Обнаружена новая уязвимость в Facebook

Исследователь безопасности, известный в Сети как Lasq, опубликовал PoC-код, который может быть использован для создания полностью функционального червя для Facebook.

Докладніше

***

19.12.2018

На Днепропетровщине 20-летний хакер создал и пытался продать вирус через Интернет

Прокуратурой Сумской области сообщено о подозрении 20-летнего жителя Кривого Рога, который создал и распространял через Интернет вирус.

Докладніше

***

24.12.2018

Создана первая программа для экстренного уничтожения данных

Команда CyberYozh security group объявила о релизе Panic Button – первой программы для экстренного уничтожения цифровых данных на компьютерах под Windows.

Докладніше

***

24.12.2018

Появилось приложение, которое отслеживает утечку данных пользователя

FigLeaf – стартап, основанный Славой Коломейчук и Юрием Двойносом, разрабатывает кроссплатформенное приложение, чтобы дать пользователям представление о том, как были затронуты их личные данные.

Докладніше

***

24.12.2018

Microsoft опубликовала рекомендации, как защититься от киберпреступников

В первую очередь Microsoft рекомендует защищать систему от вирусов и шпионского программного обеспечения – регулярно сканировать компьютер и не устанавливать нелицензионный софт. Следует настроить автоматическое обновление важных приложений, в том числе, браузера. Компания советует ни при каких обстоятельствах не отключать защитник Windows Defender. Необходимо защищать беспроводной маршрутизатор паролем, с осторожностью использовать внешние накопители, не скачивать приложения с подозрительных сайтов, не нажимать на всплывающие окна и не переходить по неизвестным ссылкам, которые приходят по электронной почте (InternetUA).

Важно надежно защитить конфиденциальную информацию. Фишинг – одна из наиболее распространенных киберугроз, которой подвергаются пользователи в предновогодний период. Вредоносное ПО способно похищать данные банковских карт и снимать средства со счетов. Прежде чем вводить персональные данные на сайте, следует убедиться в том, что он безопасен – адрес веб-страницы должен начинаться с https. Microsoft настоятельно рекомендует не отправлять конфиденциальную информацию, номер телефона или банковской карты в ответ на запросы неизвестных отправителей в мессенджерах, электронной почте или соцсети.

Активным пользователям социальных сетей Microsoft рекомендует внимательно относиться к личным настройкам. Не следует добавлять в друзья подозрительных пользователей и открывать им доступ к своей странице.

***

25.12.2018

Удаленные работники названы одной из главных угроз безопасности бизнеса

В последние годы во всем мире растет популярность удаленной работы. Для бизнеса найм дистанционных сотрудников выгоден по целому ряду причин (InternetUA):

– Пропадает необходимость арендовать офис
– Открываются более широкие возможности для найма
– Снижается текучка кадров
– Повышается производительность

Для самих удаленных сотрудников работа на дому также удобна и выгодна. Как минимум, тем, что обеспечивает дополнительную свободу и снижает расходы на транспорт. В общем, все довольны.

Эту идиллию рушат эксперты по безопасности. По их мнению, удаленные работники являются едва ли не главной причиной утечек и дыр.

Недавно компания CybSafe провела опрос среди британских IT-компаний и выяснила, что за последние два года 80 % из них прибегали к работе с дистанционными сотрудниками. При этом за прошлые 12 месяцев треть компаний столкнулась с утечками данных именно в результате действий удаленных работников.

Основатель и генеральный директор CybSafe Оз Алаше считает, что именно человеческий фактор всегда был и будет главной угрозой безопасности. По его словам, прибегая к помощи дистанционных работников, компании также должны усиливать меры безопасности. Почти четверть компаний, опрошенных CybSafe, не предпринимали даже базовых мер, вроде установки антивирусного программного обеспечения. Открывая доступ к системе удаленным сотрудникам, они никоим образом не заботились о защите особо чувствительных данных.

«В то время как удаленная работа может быть чрезвычайно выгодной для компаний, угроза связанных с ней утечек данных серьезно недооценивается. Большинство бизнес-лидеров предполагает, что люди, работающие удаленно, сами знают, как соблюдать меры безопасности. Но количество утечек, вызванных действиям дистанционного персонала, указывает, что это не так. Учитывая, что удаленная работа станет еще популярнее по сравнению с предыдущим годом, проблема станет серьезнее, если компании не начнут принимать меры», – говорит Алаше.

***

25.12.2018

Кіберполіція викрила чоловіка у незаконному втручанні в бази даних державних установ

Обіймаючи посаду в компанії, яка обслуговувала державні установи (в тому числі і військові частини), чоловік незаконно отримував доступ до

інформації, яка містилася в базах цих установ. Наразі поліцейські перевіряють інформацію щодо продажу зловмисником інформації.

Докладніше

***

25.12.2018

Уязвимость в Twitter позволяет отключить настройки безопасности

Специалист в области кибербезопасности Ричард де Вер (Richard De Vere) раскрыл информацию об уязвимости в социальной платформе Twitter, предоставляющей возможность отправлять сообщения с чужих учетных записей, публиковать изображения или видео, а также отключать функции безопасности, в частности, двухфакторную аутентификацию (InternetUA).

Как пояснил эксперт изданию Computerweekly, речь идет о логической ошибке в коде, которая раскрывает номер мобильного телефона, привязанный к учетной записи. Зная номер телефона, злоумышленник может производить различные действия, в том числе отключить двухфакторную аутентификацию, и полностью перехватить контроль над аккаунтом. Де Вер продемонстрировал журналистам процесс эксплуатации уязвимости, однако попросил не раскрывать подробности, поскольку проблема еще не исправлена. Он полагает, что некоторым мошенникам уже известно об ошибке, и они активно пользуются ею в рамках своих схем.

По мнению де Вера, устранение проблемы потребует от Twitter значительных усилий, поскольку компании придется отключить важную часть функционала, связанную с ошибкой.

***

26.12.2018

Многие детские приложения из Google Play оказались вымогателями и шпионами

Google уделяет недостаточно внимания обеспечению безопасности детей, использующих Google Play. По словам группы потребителей, обратившихся с жалобой в Федеральную комиссию торговли США, разработчики некоторых игр и приложений используют запрещенные механизмы контроля за несовершеннолетними пользователями.

Докладніше

***

27.12.2018

Каких электронных писем стоит опасаться в новогодние дни

Рождество, Новый год и зимние праздники любят все. Можно отдохнуть от работы, развлечься в кругу семьи или друзей, подышать глотком свободы.

Но на этот период, как правило, приходится пик удаленного мошенничества. Особенно возрастает поток спама. Что более важно – среди рассылок можно нарваться на мошеннические.

Докладніше

ДОДАТКИ

Додаток 1

12.12.2018

Telegram получил большое обновление на всех платформах

Разработчики Telegram выпустили глобальные обновления официального клиента для iOS, Android, Windows и macOS. Приложения получили обновленный интерфейс, расширенные настройки диалогов, возможность копирования ссылки на сообщение в закрытых группах и многое другое (InternetUA).

Полный список изменений Telegram 5.0 для Android:

– Поддержка кастомных локализаций, созданных через платформу перевода мессенджера translations.telegram.org с возможностью применения переходом по ссылке;

– Поддержка Instant View 2.0 с большим количеством типов контента. А также повторный конкурс на разработку Instant View шаблонов;

– Возможность закреплять сообщения в «избранном» и обычных группах;

– Новая система подтверждения адреса электронной почты для двухэтапной аутентификации, работа с кодами вместо перехода по ссылке из — электронного письма;

– Новый вид профилей (пользователей, групп, каналов) с упрощенной настройкой уведомлений и звуков, и быстрым доступом к общим медиа;

– Обложки альбомов в плейлистах и «Общая музыка»;

– Возможность закреплять сообщения в обычных группах и «Избранном»;

– Новый пункт в меню «Пожаловаться».

Полный список изменений Telegram 5.1 для iOS:

– Поддержка кастомных локализаций, созданных через платформу перевода мессенджера translations.telegram.org с возможностью применения переходом по ссылке;

– Поддержка Instant View 2.0 с большим количеством типов контента. А также повторный конкурс на разработку Instant View шаблонов;

– Возможность закреплять сообщения в «избранном» и обычных группах;

– Новая система подтверждения адреса электронной почты для двухэтапной аутентификации, работа с кодами вместо перехода по ссылке из электронного письма;

– Возможность выбора несколько чатов для быстрого удаления, или пометки их как «прочитанные»;

– Возможность отметить все сообщения как «прочитанные»;

– Новый пункт в меню «Пожаловаться»;

– Более 400 незначительных улучшений.

Полный список изменений Telegram Desktop 1.5:

– Поддержка кастомных локализаций, созданных через платформу перевода мессенджера translations.telegram.org с возможностью применения переходом по ссылке;

– Масштабирование интерфейса для больших экранов, до 300%, и до 150% для Retina экранов на macOS;

– Запрос на использование микрофона для осуществления звонков;

– Лимит описания у медиа был увеличен до 1024 символов;

– Возможность ускорения аудио и видеосообщений в два раза;

– Отображение видеосообщений вместе с аудиосообщениями в общих медиа;

– Возможность добавления комментария при быстрой переотправке постов с канала;

– Просмотр всех медиа из превью ссылок Instagram или Twitter;

– Возможность использовать прокси, настроенные в системе;

– Воспроизведение аудио после завершения звонка, если оно играло до этого;

– Возможность вызова панели эмодзи при вводе описания к медиа;

– Возможность закреплять сообщения в обычных группах и «избранных сообщениях»;

– Возможность изменить счётчик количества непрочитанных сообщений на количество непрочитанных чатов;

– Библиотека libtgvoip обновлена до версии 2.4;

– Разблокировка бота теперь приравнивается его рестарту, с отправкой команды /start;

– Изменена работа ускорения аудиосообщений (теперь ускоряется в 1.7 раз а не в 2 раза);

– Обновлены иконки загрузки медиа;

– Обновленные эмодзи.

(вгору)

Додаток 2

17.12.2018

Глава техподдержки раскрыл внутренние секреты Telegram

Михаил Равдоникас, возглавляющий команду технической поддержки Telegram, рассказал о «внутренней кухне» мессенджера, а также о том, как этот развивается этот проект и каким станет в будущем (InternetUA).

За последние несколько месяцев в версии Telegram для iOS было найдено и устранено около 1500 багов, а в ноябре это приложение перешло на использование нативного для iOS языка Swift, благодаря чему стало работать быстрее и стабильнее. Параллельно с этим разработчики совершенствуют приложение для Android, полностью переделывают веб-версию и работают над внедрением в мессенджер новых функций.

С недавних пор пользователи могут сообщать в поддержку Telegram о противоправном контенте не только через мобильные и десктопные приложения, но также через веб-версию сервиса. Для сообщений о контентом с насилием над детьми запущен отдельный почтовый ящик stopCA@telegram.org, а отчёты о предпринятых мерах публикуются на канале @stopCA по аналогии с отчётами о блокировке террористического контента на @ISISwatch.

Разработчики Telegram изменили подход к борьбе со спамом. По внутренней статистике, спамбот, выявляющий рассылку однотипных сообщений, ошибается лишь в 0,2 % случаев, а 90 % пользователей, которые не заслуживают полной блокировки, требуется подождать 24 часа, прежде чем они снова смогут общаться с другими людьми.

Мошенники, привыкшие обманывать людей, применяют ту же схему в общении с поддержкой Telegram. Равдоникас рассказал, что модераторы критически подходят к жалобам пользователей на блокировку. По его словам, криптомошенники иногда прикидываются учителями, на которых пожаловались дети, дизайнерами-инвалидами, которые общались с клиентами, многодетными родителями, которых в шутку засыпали жалобами друзья, и прочими экзотическими персонажами.

В поддержке Telegram работают волонтёры, не получающие за это зарплату или какое-нибудь другое вознаграждение. Одни трудятся ради опыта и престижа, а других подпитывает вера в то, что помогают менять мир к лучшему. Они общаются друг с другом в специальном чате, где для каждой проблемы или жалобы заводится карточка, и можно оставлять комментарии о ходе её решения.

В скором времени техподдержка начнёт использовать инструмент под названием Heimdall. Эта система будет работать как интерактивный справочник: пользователь сможет получать информацию о возможных способах решения возникшей проблемы, и если не найдёт ответ на свой вопрос, будет перенаправлен на сотрудника поддержки. Прежде, чем внедрить эту систему, разработчикам и поддержке предстоит адаптировать её для разных стран мира.

Равдоникас сравнил Telegram с живым организмом, в котором Павел Дуров – ДНК, разработчики – белки, модераторы – иммунная система, а техподдержка – нервная система. Сотрудники поддержки подают сигналы в мозг организма и оповещают его обо всех событиях, которые происходят внутри и снаружи. Они помогают ему осознавать, кто он и как ему следует взаимодействовать с окружающим миром.

(вгору)

Додаток 3

20.12.2018
Вышло обновление Instagram для Android

Разработчики Instagram постоянно работают над улучшениями социальной платформы. Например, во второй половине ноября команда показала новый дизайн, который улучшит взаимодействие с другими пользователями и заодно сделает личные профили более красивыми. Бизнес-страницы станут более удобными: подписчики без проблем смогут связаться с представителями компании или оформить заказ. Развитие площадки продолжается – пришло время для ещё более плотного общения с друзьями.

Сотрудники платформы подготовили три полезных нововведения. О них рассказали в официальном блоге компании (InternetUA).

Музыкальные истории

Теперь подписчики могут отвечать на вопросительные стикеры в историях с помощью треков из музыкальной библиотеки. Схема простая: вы просите подсказать друзей композицию под определённое настроение или событие. Подписчики делятся треками, их варианты отображаются в отдельном списке. Прослушать композицию получится сразу же. А если песня понравится – можно создать фото или видео с ней на фоне.

Соответствующая иконка находится в меню создания вопроса.

Улучшенные лайвы

Теперь стикеры с вопросами доступны и во время трансляций – авторы увидят то, что интересует их подписчиков. Реакция на вопросы или просьбы сделают общение более тесным и полезным.

К слову, зрители увидят формулировку вопроса, так что неловкостей из-за перехода между разными темами не возникнет.

Таймер моментов

Коллекция стикеров пополнилась таймером обратного отсчёта в историях. Например, можно разделить радость из-за наступающего Нового года или рассказать подписчикам, через сколько вы ждёте доставку пиццы. Дату наступления события указываем во время создания стикера.

Как утверждают разработчики, особенности уже доступны для пользователей, поэтому можно проверять.

(вгору)

Додаток 4

25.12.2018
Ирина Фоменко
Почему социальные сети перестали быть актуальными

Термин «социальная сеть» стал бессмысленным набором слов, пишет TechCrunch. Скорее всего, у вас десятки, сотни или, может быть, тысячи друзей

и подписчиков на разных платформах. Но соцсети еще никогда не были такими пустыми (InternetUA).

Конечно, Facebook, Twitter или LinkedIn не рухнут за одну ночь. Они имеют внутреннюю ценность с другими функциями – социальные графики, цифровые резюме, организация мероприятий... Но концепция широких сетей социальных связей с элементом вещания мертва.

От сообществ на основе интересов к вашему соседу

Если вы достаточно активно работали в Интернете, у вас могут быть приятные воспоминания об интернет-форумах. Фрагментация была ключевой: можно быть активным на нескольких сайтах и не упоминать другие увлечения. Это похоже на общение с гостеприимной группой друзей, потому что у вас схожие интересы.

Потом появился Facebook. Поначалу речь шла также о сообществах, основанных на интересах, но затем он открыл для всех возможность выйти за пределы университетов. Друзьями на Facebook становятся не потому, что вы разделяете хобби, а потому, что вы уже давно знаете этих людей.

Facebook постоянно подталкивает вас к добавлению новых друзей с помощью печально известной функции «Вы можете их знать». Знать кого-то – это одно, а говорить о чем-то – это другое. Теперь вы не можете сказать «нет» своей лучшей подруге в старшей школе, даже если не видели ее пять лет.

Слишком большой, чтобы быть успешным

Одним из ключевых столпов социальных сетей является функция вещания. Вы можете написать сообщение, поделиться фотографией, снять историю и транслировать их своим друзьям и подписчикам. Но вещание не масштабируется.

Большинство социальных сетей сейчас являются публично торгуемыми компаниями – они всегда гонятся за ростом. Рост означает больший доход, а доход – что пользователи должны видеть больше рекламы.

Лучший способ принуждать вас смотреть рекламу – заставить тратить больше времени на сервис. Если вы смотрите несколько видео на YouTube, то увидите больше рекламных роликов. И есть два способа заставить вас проводить больше времени в социальной сети – принудить вас возвращаться чаще и оставаться дольше.

А 2018 год стал годом дешевых трюков. Чтобы заставить вас заходить чаще, компании теперь отправляют FOMO-уведомления с неполной, непропорциональной информацией.

Социальные сети просят вас не просто открыть приложение – теперь они хотят направить вас к другим частям сервиса. Почему вы не нажимаете на этот ярко-оранжевый баннер, чтобы открыть IGTV? Посмотри на эту блестящую кнопку!

Взрослые американцы в настоящее время тратят почти шесть часов в день на потребление цифровых медиа – и телефоны составляют более половины этого показателя. Учитывая, что социальные сети должны каждый раз давать

вам что-то новое, они хотят, чтобы вы следили за как можно большим количеством людей и подписывались на все каналы YouTube.

Частные сообщества

За централизацией всегда следует децентрализация. Теперь, когда мы зашли в тупик социальной сети, пришло время построить собственный цифровой дом.

Групповые переписки играют ключевую роль, когда речь идет о связи с дальними членами семьи. Но вы можете создавать свои собственные группы на основе интересов. Социальные сети, которые не стали слишком большими, все еще имеют возможность трансформироваться.

Если вы проводите свой отпуск, создавая идеальную историю в Instagram, вы должны быть более циничными. Либо вы хотите сделать из этого карьеру и стать звездой Instagram, либо вам следует подумать об отправке фотографий и видео напрямую в ваши группы. В противном случае вы просто участвуете в гнилой системе.

Если вы хотите прокомментировать политику и жизнь в целом, вам следует обсудить эти темы с окружающими вас людьми, а не с вашими друзьями в Facebook. Положите телефон обратно в карман и начните разговор.

(вгору)

Додаток 5

19.12.2018

З депутатами Рівненщини можна зв’язатися через соціальні мережі

Сьогодні важливим способом комунікації з виборцями є спілкування у соціальних мережах. Звичайно, інформування на сторінках соцмереж не є обов’язковим і не передбачається законодавством. Однак такий спосіб комунікації дає можливість додаткового двостороннього зв’язку між депутатом та виборцями (Rivne Media).

Громадянська мережа ОПОРА проаналізувала роботу депутатів Рівненської міської ради у соціальній мережі Facebook (період: листопад 2017 року – листопад 2018 року) та порівняла їх активність з минулим роком.

Загалом, серед 42 депутатів Рівненська міська ради налічує 33 місцевих обранці, які зареєстровані у соціальній мережі Facebook та чию персональну сторінку можна ідентифікувати.

7 депутатів мають дві зареєстрованих сторінки: приватної особи та сторінка своєї приймальні чи округу (або ж як публічної особи):

– приватна сторінка Миколи Бляшина та публічна сторінка Миколи Бляшина;

– сторінки Євтушенко Святослав та «Громадська приймальня Євтушенка Святослава»;

– Володимир Кудрін та відкрита група «Володимир Кудрін – депутат Рівнеради, виборчий округ №38»

– Олександр Курсик та «Виборчий округ #21. Депутат Курсик Олександр»

– Любов Романюк та група «Любов Романюк – депутат в.о. №1 м. Рівне»

– Tetyana Chubay та «Депутат РМР Тетяна Чубай»

– Олександр Чубай – Aleksandr Chubay, Aleksandr Chubay та Нотаріальний сервіс Рівненщини.

16 депутатів активно використовують соціальну мережу для інформування про свою діяльність, а також забезпечують двосторонній зв'язок, відповідаючи на коментарі та коментуючи дописи.

Зокрема, це Микола Бляшин, Сергій Васильчук, Олександр Довжаниця, Святослав Євтушенко, Володимир Кудрін, Олександр Курсик, Віталій Павелків, Сергій Паладійчук, Ірина Пилипчук , Назарій Поліщук , Любов Романюк, Роман Стасюк , Святослав Стельмащук, Олександр Чубайта Роман Яворський . Також активно інформує про свою діяльність Олексій Муляренко, який одночасно виконує обов'язки депутата Рівненської міської ради та голови Рівненської обласної державної адміністрації.

Зокрема, двоє депутатів стали активно використовувати власну сторінку на Facebook для інформування виборців про свою роботу, тоді як минулого року взагалі не були активними користувачами соцмережі. Це заступник міського голови Рівного Сергій Васильчук та Ірина Пилипчук , які інформують про свою роботу та виконані доручення виборців. Також на сторінці депутатів можна зустріти чимало репостів та дописів колег, які безпосередньо стосуються їх депутатської діяльності.

Дехто з місцевих обранців не лише інформують про свою депутатську діяльність, але й позначають своїх колег, журналістів та громадських активістів в своїх дописах, охоплюючи таким чином якомога більшу аудиторію, оскільки ці дописи відображаються в життєписі всіх позначених осіб. Особливо помітна Facebook-активність у Миколи Бляшина, голови Рівненської облдержадміністрації Олексія Муляренко, секретаря міської ради Сергія Паладійчука, Любов Романюк, Назарія Поліщука та Святослава Стельмащука.

17 депутатів (у минулому році їх було лише 11) у розділі «Місця роботи» вказують Рівненську міську ради: Микола Бляшин, Богдан Гапяк, Святослав Євтушенко, Назарій Загоровський, Володимир Кудрін, Ольга Криж , Олександр Курсик, Анатолій Лащук, Василь Немеш, Олександр Нестерук, Назарій Поліщук, Ірина Пилипчук, Володимир Попик, Любов Романюк, Святослав Стельмащук, Олександр Чубай та Роман Яворський.

Контент наповнення сторінок депутатів також досить різний. Троє депутатів охоче вітають виборців зі святами: Святослав Євтушенко, Олександр Нестерук, Віталій Павелків. Крім цього, значна частина депутатського корпусу Рівнеради «репостить» новини з інших сторінок (зокрема, зі сторінок своїх фракцій та їх лідерів): Володмир Попик, Олександр Довжаниця, Олег Карпяк, Олександр Крюков, Андрій Кузьмич, Анатолій Лащук, Василь Немеш,

Олександр Нестерук, Петро Пожарський, Стасюк Роман, Сухий Юрій та Чубай Тетяна

Досі залишаються не активними облікові записи: Богдан Гапяк, Маріян Года та Ольга Криж – жодного власного допису впродовж року; Людмила Туровська , Назарій Загоровськийта Мітін Юрій – один допис впродовж року; Олександр Крюков за останній рік двічі змінив власні світлини; Ігор Ковалець поширив два дописи сторінки «Об'єднання «Самопоміч» – Рівне.

9 депутатів не можливо ідентифікувати їх сторінки у соціальній мережі, оскільки профілі з такими ж іменами та прізвищами не містять фото депутата, не вказано місця роботи та приховані дописи із життєпису. Тому, однозначно не можна стверджувати, чи є ці місцеві обранці у соціальній мережі. До цього списку входять: Олександр Бабат, Олег Дзецько, Анна Іванова, Галина Кульчинська, Роман Петролюк, Юрій Осіпчук, Тамара Тимощук, Людмила Чирак та Анатолій Чугуєвець.

Що ж, активне ведення сторінки у соцмережі не є нормою чи обов'язком. Проте, отримуючи мандат, депутати автоматично стають публічними персонами і громадськість хоче знати, що ж роблять їх місцеві обранці.

ОПОРА нагадує, що використання соціальних мереж не є основним показником роботи депутата, однак звертає увагу, що Facebook можна розглядати як інструмент для додаткової можливості депутатові виконувати свої обов'язки. Зокрема, завдяки Facebook можна щоразу інформувати громадян про графік приведення особистого прийому громадян, оприлюднювати проміжний та річний звіти про результати роботи, щоб робити свою діяльність ще більш відкритою і публічною, а головне – двосторонньо комунікувати з виборцями.

(вгору)

Додаток 6

12.12.2018

Украинская сеть хостелов создала «Telegram-консьержа», чтобы всегда быть рядом с гостями

Сеть хостелов Dream Hostels создала «Telegram-консьержа», чтобы помогать ориентироваться в новом городе и всегда быть рядом с гостями. Консьерж подскажет в какие музеи, кафе, рестораны, клубы лучше пойти или какие события пройдут в городе в ближайшее время (Marketing Media Review).

Telegram-консьерж работает круглосуточно и всегда готов помочь, если кто-то потерялся или нужно заказать ночью такси. А для потенциальных гостей он забронирует место в хостеле или предложит пообщаться с другими путешественниками в чате.

Чтобы воспользоваться сервисом, нужно зайти в Telegram и указать город, в котором находится пользователь, а дальше перейти в канал, где будет сразу предложена основная информация и появится возможность напрямую связаться с консьержем.

Цель проекта – дать путешественникам больше, чем просто проживание, стать ближе и поддерживать с ними общение 24/7, даже если гость выехал из хостела. В будущем, количество городов в сервисе будет увеличиваться по мере появления новых хостелов. На данный момент услуга доступна в Киеве, Львове, Варшаве и Братиславе, на этапе запуска – Полтава, Запорожье, Рахов и Прага.

«Общаться со своими гостями и делиться самыми важными новостями из жизни отелей в режиме “здесь и сейчас” – тренд гостиничного бизнеса. Мы, как крупная сеть, стремимся следовать этим трендам, в первую очередь для удобства наших гостей. На данном этапе, стараемся как можно быстрее реагировать на сообщения от гостей и помогать с личными вопросами в большинстве каналов коммуникации. Создание “Telegram-консьержа” было логичным шагом, поскольку он дает возможность гостю получить ответы на большинство вопросов сразу», – рассказывает руководитель отдела маркетинга Ольга Кашпур.

Сейчас сервис еще дополняется, но уже есть возможность им пользоваться.

(вгору)

Додаток 7

17.12.2018

ТОП-3 совета для создания сильной стратегии в Instagram Stories

Instagram Stories позволяют брендам рассказать историю с помощью видео, графики, популярных продуктов или продуктов, которые проседают в продажах. Ниже три совета, как использовать «Истории» в своей стратегии (Marketing Media Review):

Добавляйте интерактива «Историям»

«В формате Stories есть много функций, которые могут добавить интерактива рекламному контенту, особенно когда речь заходит о призыве к действию. Увеличить вовлечение помогут визуальные подсказки, которые указывают на желаемое действие, – отметил глава креативной студии Smartly.io Хосе Санчес. – Для контента Stories без видео интерактив позволит бренду быть узнаваемым в рекламе. Если это формат карусели, можно использовать более длинный рассказ и создать визуальный элемент, который прослеживается в трех фреймах, чтобы придать истории один брендинг».

Сообщение должно быть ясным

«Самое важное – это ясность: удостоверьтесь в том, что ваше главное преимущество продукта или услуги передается быстро и просто, отмечает Санчес. Для Stories в видеоформате важно, чтобы они были простыми и краткими, менее 15 секунд. Кроме того, хотя для формат Stories звук не обязателен и 60 % пользователей выключают его, это значит, что половина все равно смотрит со звуком, поэтому лучше встроить звук».

«Истории» должны быть своевременными

«И наконец, независимо от того, насколько интересной или интерактивной может быть реклама в Stories, важно, чтобы она находила отклик у аудитории. Во время праздников, даже если у бренда нет сезонного предложения, компания все равно должна говорить им о том, что происходит в их жизни в данный период. Это может быть просто праздничный декор на заднем фоне рекламе. Нечто простое, с чем несезонный продукт, к примеру, подгузники, может найти отклик с потребителями в эту пору года».

(вгору)

Додаток 8

19.12.2018

Михаил Сапитон

Facebook таргетирует рекламу по IP-адресу. Даже если отключить определение местоположения

Facebook таргетирует рекламу по местоположению пользователя, даже если юзер отключил отслеживание локации, хранение информации о посещенных местах и удалил из профиля город (AIN.UA).

На это в блог-посте на Medium обратила внимание Александра Королева, сотрудница Университета Южной Калифорнии. Выключив все вышеперечисленные опции, отказавшись от чекинов, отметок о посещении мест и выключив трекинг в WhatsApp, Instagram и Messenger, она все равно получала таргетированную по ее месту жительства рекламную информацию. Объявления сопровождались приписками «для живущих возле Санта-Моники» или «… Лос-Анджелеса» – в этих городах Королева проживает и работает соответственно.

Как поясняется на соответствующей странице, Facebook собирает информацию об IP-адресах, Wi-Fi точках и Bluetooth-подключениях устройств. Королева пожаловалась, что соцсеть вводит пользователей в заблуждение – при отключении трекинговых служб, Facebook не уведомляет о дальнейшей слежке. Она считает, что компания должна предоставить по-настоящему действенные механизмы противодействия трекингу вместо бесполезных опций.

В комментарии изданию Gizmodo представители Facebook подтвредили опасения Королевой:

«У людей нет возможности полностью отказаться от использования их местоположения в рекламе. Мы используем данные на уровне почтового индекса и города, которые собираем при помощи IP-адресов и другой информации вроде чекинов. Это нужно, чтобы убедиться, что мы предоставляем людям лучший сервис – от показа Facebook на правильном языке, до отображения близлежащих событий и рекламы локального бизнеса».

Поскольку отказаться от таргетированной рекламы по местоположению нельзя, можно лишь запутать систему при помощи VPN-сервисов. Они маскируют реальный IP-адрес под источник из другой страны. Как отмечают в MacRumors, остается лишь удалиться из соцсети и полностью стереть данные –

но и в таком случае, Facebook хранит «теневые профили» со сведениями о людях, которые не используют соцсеть.

(вгору)

Додаток 9

20.12.2018

Исследование: больше всего SMM-маркетологов беспокоит ROI

55 % SMM-маркетологов больше всего беспокоит ROI, за ним следует понимание успеха в кросс-канальных активностях (42 %), развитие стратегий для достижения целей бизнеса (39 %) и понимание, какой контент следует размещать (39 %), отмечает исследование Sprout Social's 2018 Social Index. Только 14 % могут определить доход, полученный от социальных медиа. Маркетологи рассматривают эти платформы в нематериальном смысле, для увеличения осведомленности о бренде (80 %), роста вовлеченности сообщества (65 %), роста трафика на сайт (54 %) и генерации лидов/продаж (41 %). При создании видео для сетей рекламодатели должны помнить о том, что пользователи ищут аутентичного контента, а не рекламы, которая продвигает продукт. Исследование обнаружило, что предпочтения маркетологов и пользователей расходятся. SMM-маркетологи ищут образовательный контент (61 %), контент, который рассказывает историю (58 %) и вдохновляет (53 %), а потребители ищут скидки/распродажи (73 %), демонстрацию новых продуктов/услуг (60 %) и обучающие видео (59 %) (Marketing Media Review).

Маркетологи могут создавать видеоконтент, который они хотят, но среди топ-факторов, которые заставляют пользователей смотреть видео – продолжительность (61 %), подпись или описание видео (51 %) и является ли видео роликом (40 %). Если пользователи видят, что им продают что-то, они менее склонны смотреть контент, отмечает исследование. «Видео для сетей не должны служить только целям бренда, но предлагать реальные истории, людей и ситуации», – отметили в компании.

Сотрудники в роли адвокатов бренда – это новый маркетинг инфлюенсеров и 71 % компания используют своих сотрудников в качестве лидеров мнений, только 19 % продолжают использовать программы с лидерами мнений.

Почти половина респондентов (45 %) отметили, что обращались к компаниям в социальных медиа. Среди топ-причин: вопросы (57 %), жалобы (45 %) и похвала (34 %).

Facebook остается доминирующим каналом, 97 % назвали сеть самой полезной платформой, 83 % также используют Instagram, только 13 % – Snapchat. Половина потребителей (51 %) используют Instagram, 30 % – Snapchat. В исследовании приняли участие 1,253 потребителей и 2,060 маркетологов. Исследование проводилось в апреле и мае 2018 года.

(вгору)

23.12.2018
Ирина Фоменко
Новое о рекламе в соцсетях

Любой, кому когда-либо приходилось обосновывать расходы на социальные сети, поймет, что приятно иметь цифры, на которые можно опираться, пишет IoT Events (InternetUA).

Если в вашем аккаунте в Twitter 200 подписчиков, и благодаря ретвитам 100 человек нажали и подписались на вашу рассылку, тогда да, вам повезло. Если у вас 10 миллионов подписчиков, но нет подобной активности, возможно, пришло время задуматься.

Без предоставления контекста и без четких целей статистика не имеет смысла.

Когда взаимодействие не является таковым?

Взаимодействие – это слово, которое часто встречается в социальных сетях, но что оно на самом деле означает? С точки зрения социальных сетей, кто-то «взаимодействует» с вами, если предпринимаются такие действия, как ретвит, лайк, комментирование или обмен информацией. Это следующий шаг от скроллинга чего-либо.

Причина, по которой само по себе взаимодействие бессмысленно, заключается в том, что оно не дает вам никакого контекста. Итак, вы получили 100 комментариев к этому посту в Facebook – это хорошо или плохо?

Оценивать взаимодействие нужно относительно числа подписчиков или показов. Давайте посмотрим на пример:

На момент написания этого материала было 72 репоста, 696 лайков и 18 комментариев. Отлично! Но так ли это? На странице LEGO в Facebook – 11124653 подписчиков. Уровень взаимодействия относительно числа подписчиков – 0,00000059 %. Не выглядит так впечатляюще, правда?

Аналитика Facebook и аналитика Twitter делают эту арифметику простой для вас, так как они показывают впечатления/охват и, в случае с Twitter, переходят к следующему шагу и рассчитывают для вас коэффициент взаимодействия.

Взаимодействие приводит к действию?

Когда вы планировали твит или статус Facebook, или что бы это ни было, чего вы хотели достичь? Да, социальные сети – это больше, чем просто продажи, но в конечном итоге вы делаете это с определенной целью. Если эта цель состоит в том, чтобы просто заставить людей смеяться, тогда хорошо, но если вы действительно хотите, чтобы люди жертвовали на благотворительность, или делали подробные доклады, или участвовали в конкурсе, то вы должны это измерить. Тип взаимодействия тогда так же важен, как и его общий уровень.

Посмотрим на примере учетной записи в Twitter. Для блогера, например, конечная цель – генерировать трафик и клики. Стоит отметить, что лайки и ретвиты не имеют прямого отношения к этому:

Как вы можете видеть, первый твит классифицируется как «top tweet». У него рациональное количество ретвитов и лайков и более широкий потенциальный охват, чем у второго твита. Люди явно больше заинтересованы в картинке торта, чем в переходе по ссылке, так как во втором посте, в котором только один лайк и нет ретвитов, кликов в восемь раз больше.

В следующий раз, когда вы планируете кампанию в социальных сетях, подумайте о контексте и целях, а не просто о красивых фотографиях и ретвитах.

(вгору)

Додаток 11

24.12.2018

Как оптимизировать сайт под социальные сети

Что такое поисковая оптимизация (SEO) знают практически все, но поисковые системы – не единственный источник трафика на сайт. Одним из таких источников являются социальные медиа (соцсети, блоги и т. д.) (IGate).

Для того, чтобы сайт получал и удерживал посетителей из социальных сетей, его также нужно улучшать, этот процесс и называется оптимизацией под соцсети (SMO).

Чем SMO отличается от SMM

И SMO и социальные медиа-маркетинг направлены на то, чтобы получать клиентов в социальных сетях, но это два разных метода. Здесь снова будет уместно вспомнить о SEO, как известно, поисковое продвижение включает два ключевых этапа: внешнюю и внутреннюю оптимизацию. Для продвижения в соцсетях SMO и есть внутренней оптимизацией (работа над самим сайтом), а SMM – внешней (раскрутка на внешних площадках).

Как оптимизировать сайт

Поработайте над юзабилити

Первое, что следует обеспечить для собственных посетителей – удобный и привлекательный сайт. Нужно завоевать расположение еще на этапе знакомства, и тогда к вам с большей вероятностью вернутся. Для пользователя крайне важен интуитивно понятный интерфейс, визуальный дизайн.

Размещайте действительно информативный и увлекательный контент

Выражение «Краткость – сестра таланта», для SMO крайне актуально. Читатель с большей охотой поделится небольшим текстом на актуальную и волнующую его тему, чем увесистым и содержательным лонгридом. Но бывают и исключения, если статья действительно несет ценную информацию для ЦА, еще и написана близким и понятным языком, она вполне может стать вирусной.

Предоставьте возможность делиться информацией в соцсетях

Еще одна важная деталь, необходимая чтобы привлекать новых пользователей из социальных медиа – возможность репостить информацию. Для этого необходимо добавить кнопки «поделится» для любых соцсетей, где есть ваша ЦА.

Разрешите посетителям оставлять комментарии

Наличие комментариев под статьями вызывает доверие у читателей. Это отличный способ завоевать лояльность. Одна из причин, почему соцсети стали популярными – возможность делиться собственным мнением с остальными, даже незнакомыми людьми. Подобную возможность вы можете предоставить и на собственном ресурсе.

Конечно, негативные отзывы будут, некоторым не понравится ваш сайт, а некоторые просто пытаются привлечь внимание кричащим негативным заявлением. Но если на них аргументированно отвечать, обрабатывая любые возражения, то от подобных комментариев также будет польза – вы повысите лояльность читателей.

Не дайте читателям скучать

Однообразие – вот с чем нужно бороться. Чтобы не наскучить посетителям, регулярно публикуйте свежие новости, устраивайте акции и розыгрыши, стимулируйте аудиторию принять дать обратную связь.

Не забывайте про SMM

Можно наилучшим образом оптимизировать ресурс для пользователей, но какой от этого прок, если их не будет. Чтобы такого не допустить, используйте SMM. Создайте собственные паблики или страницы в различных социальных сетях, обзаведитесь целевой аудиторией, после чего постепенно переманивайте ее на сайт: публикуйте анонсы новых материалов, делитесь новостями, сообщайте об акциях и т. д. В комплексе SMM и SMO дают гораздо лучший результат.

(вгору)

Додаток 12

15.12.2018

Фотографии в Инстаграме могут рассказать о вас больше, чем кажется

Каждый день 500 млн людей пользуются Инстаграмом. Эта соцсеть давно перестала быть цифровым фотоальбомом, теперь ее используют для продаж, продвижения в интернете и даже как материал для исследований. Оказывается, фото и фильтры в ваших постах могут многое рассказать как о вашей личности, так и о здоровье (InternetUA).

Мы нашли результаты таких исследований любопытными и делимся ими с вами.

Что могут рассказать цвет и фильтр

– Ученые из Сонгюнгванского университета проанализировали профили 179 человек (всего 25394 фотографии). Исследование уделяло внимание цвету

как одному из ключевых элементов стиля. Они заметили, что люди в отношениях выкладывают снимки ярких цветов чаще, чем пользователи без пары. Также яркие фильтры и фото используют экстраверты и люди, склонные к нарциссизму.

– Исследователи из Гарвардского и Вермонтского университетов проанализировали 43950 фотографий пользователей Инстаграма и выяснили, что люди с депрессией чаще выкладывают снимки. Также на их фото встречается больше лиц, а вот фильтры они используют реже. Кроме того, на снимках людей с депрессией преобладают темные, синие и серые оттенки, а также черно-белые фото.

Что может рассказать тема фотографии

– Не любите бесконечные фотографии еды в Инстаграме? Оказывается, они могут приносить пользу. Исследователи пришли к выводу, что когда люди делятся снимками своей еды и рецептами блюд, им проще придерживаться правильного питания и даже худеть. Таким образом, профиль в Инстаграме выступает в качестве журнала питания, а лайки и комментарии друзей мотивируют пользователей и дальше выбирать здоровую пищу.

– Некоторые эксперты считают, что люди, которые выкладывают много фотографий со своей половинкой, пытаются таким образом маскировать проблемы в отношениях. А подписи в духе «моя девочка» и «мой мужчина» могут говорить о чувстве собственничества.

Что еще можно узнать о вас по вашему профилю

– Люди младше 25 лет менее склонны улыбаться на фото профиля. Эту особенность выявили исследователи из Колледжа информационных наук и технологий в Пенсильвании и Королевского колледжа Лондона.

– Пользователи Инстаграма, которые чаще отмечают друзей на фотографиях, менее склонны к одиночеству. В то же время люди, выкладывающие фото, которые не обращены ни к кому и не подталкивают к обсуждениям, ощущают себя более одинокими.

– Селфи не обязательно говорят о нарциссизме. Можно выделить три группы любителей селфи: «собеседники», «автобиографы» и «саморекламщики». Первые делятся своими фото, чтобы вовлечь друзей и подписчиков в обсуждение, например люди, которые фотографируются со значками «Я проголосовал(а)». «Автобиографы» делают селфи, чтобы запечатлеть памятные моменты из жизни. Они не прочь показать их другим людям, но в первую очередь делают селфи для сохранения воспоминаний, а не ради лайков. «Саморекламщики» же любят документировать почти все в своей жизни, стараясь выставить себя в выгодном им свете. К ним можно отнести представителей семейства Кардашьян.

(вгору)

Додаток 13

17.12.2018

Інстинкти і сучасні технології: що робити, якщо дитину цькують у соцмережах

Захист власної дитини – це здорова реакція батьків. Часто ми захищаємо дитину, орієнтуючись на інстинкти. Логіка у цьому є. Бо це – перевірені мільйоном років моделі поведінки. Але проблема у тому, що ці моделі може й добрі, але кардинально змінились обставини і те, що було добре мільйон років не спрацьовує сьогодні. Я навіть скажу більше – досвід вашого доінтернетного дитинства уже не дуже пригодиться дитині (InternetUA).

Коли ваша дитина стає жертвою інтернет-цькування (кібербулінг) найпершою і найприроднішою реакцією батьків є роз'єднання дитини і джерела небезпеки. Простіше кажучи, батьки забирають у дитини телефон/планшет/комп'ютер, щиро віруючи в те, що оберігають дитину.

І вони отримують результат. Але це – результат переважно у самопереконанні. Нібито дитина тепер у небезпеці і батькам можна заспокоїтись. Проблема цькування вирішена. Але – ні.

Соціальні мережі розвиваються і без вашої дитини. І не сьогодні-завтра цькування у Інтернет може вилізти у реальне життя – через ігнорування дитини у школі, розповсюдження чуток чи просто «косі погляди» й усмішки. Врешті-решт, не розуміння дитиною чим завершилась проблема у соціальних мережах (перепалка, викладення компромату, реакція друзів і т.д.) також тиснутимуть на дитину.

Батькам варто пам'ятати, що дитина, позбавлена періодичного (на рівні з її однокласниками) доступу до інтернет-мережі, сьогодні ризикує опинитись в ізоляції. По-перше, технічно – дитина вибуває зі спілкування зі своїми однолітками у соцмережах. По-друге, світоглядно – вона не володіє інформацією, яку обговорюють в Інтернет однокласники, а тому у реальному світі зменшуються «точки дотику» групи та дитини. Просто пам'ятайте, що для підлітків віртуальний світ – одна з важливих частин їхнього реального життя.

Саме тому, для дитини позбавлення спілкування у соціальних мережах, може бути гіршим покаранням, ніж сам кібербулінг у них. У результаті, наступного разу ви можете не дізнатись про її проблеми, бо вона переживатиме, що її знову за них покарають. Або дитина знайде можливість виходу в інтернет і без вашого дозволу.

Це не означає, що нічого не треба робити при кібербулінгу. Це говорить про те, проблема значно глибша. І її не вирішити методами «зроби що небудь, щоб було спокійне сумління». Протидія кібербулінгу потребує значно більше зусиль, ніж просто висмикнути з розетки комп'ютер.

(вгору)

Додаток 14

20.12.2018

Зависимость от соцсетей оказалась похожа на алкоголизм – ученые

Наркологи из Австралии выяснили, что люди, не способные покинуть социальные сети даже на секунду, страдают от тех же нарушений в работе психики, что и «профессиональные» алкоголики (InternetUA).

Их выводы были представлены в журнале AJP.

– Мы нашли не только сходства, но и различия между любителями соцсетей и спиртного, что нужно учитывать при борьбе с этими феноменами. К примеру, уменьшение импульсивности действий поможет и тем, и другим зависимым, тогда как ослабление нарциссизма больше поможет людям, не способным оторваться от телефона, – объясняет Майкл Лайверс (Michael Lyvers) из университета Бонда (Австралия).

В последние годы ученые всерьез заинтересовались двумя новыми формами зависимости, о которых часто говорят обыватели – «телефонной» и «интернет»-наркоманией. Их изучение показывает, что в данном случае простые люди часто бывают правы. У некоторых их носителей действительно наблюдаются особые изменения в поведении, характерные для реальных наркоманов, и на них действуют те же факторы риска.

К примеру, в прошлом году ученые обнаружили, что их жертвами чаще всего становятся импульсивные люди, плохо контролирующие свои желания. Подобные характеристики, как показывают наблюдения ученых, являются отличительной чертой алкоголиков и реальных наркоманов, не способных самостоятельно избавиться от пагубной привычки.

Подобные открытия заставили Лайверса и его команду провести небольшой эксперимент, в рамках которого они сравнили то, как развитие алкоголизма и зависимости от социальных сетей меняет психику и манеру работы мозга человека.

Для этого они собрали группу из 150 добровольцев, живущих в Австралии и согласившихся пройти несколько развернутых опросов на предмет того, какую роль занимают социальные сети в их жизни. Параллельно ученые изучили результаты аналогичных опросов среди алкоголиков, проходивших реабилитацию в разных больницах страны.

Изменения мозга при интернет-зависимости аналогичны тем, которые наблюдаются при употреблении алкоголя и кокаина, свидетельствуют результаты исследования.

Эти опросы показали, что алкоголизм и зависимость от социальных сетей в целом были очень похожи друг на друга. Как оказалось, и для той, и другой проблемы были характерны высокие уровни нарциссизма, импульсивности и алекситимии – дефицита рефлексии и эмоций.

Небольшие различия в выраженности этих нарушений все же присутствовали, однако в целом, по словам ученых, они примерно одинаково влияли на поведение алкоголиков и любителей социальных сетей. Это можно использовать для борьбы и с тем, и с другим феноменом.

Что интересно, в отличие от тяги к спиртному, имеющей явно выраженный «мужской» характер, зависимость от социальных сетей была

одинаково характерна для представителей и того, и другого пола. Как надеются ученые, дальнейшие наблюдения помогут им понять, почему это так.

(вгору)

Додаток 15

12.12.2018

Программист получил 2 года тюрьмы за антиукраинские публикации в «ВКонтакте»

Суд заочно приговорил к 2 годам лишения свободы жителя Тернополя Евгения Фука за распространение в социальной сети «ВКонтакте» призывов к России начать военную агрессию в отношении Украины (InternetUA).

Об этом говорится в приговоре суда от 5 декабря, передают Українські Новини.

Указано, что 34-летний уроженец Ростовской области России Фук до 24 января 2017 года проживал в центре Тернополя и работал программистом.

В период с 12 мая по 22 июня 2015 года обвиняемый в социальной сети «ВКонтакте» создал личный аккаунт, через который сознательно размещал публичные призывы к свержению конституционного строя в Украине.

Так, Фук на «стене» своего аккаунта умышленно распространил для ознакомления публикации, в которых содержатся призывы к Российской Федерации осуществить военную агрессию в отношении Украины и таким образом свергнуть ее конституционный строй.

В частности, в размещенных публикациях от 22 июня 2015 года содержится высказывание: «Россия должна бороться за то, чтобы никакой Украины на ее границах не было, а была Новороссия и Малороссия».

Также он активно репостил сепаратистские публикации с сайта Sharij.net.

Более того, установлено, что подсудимый скорее всего примкнул к боевикам самопровозглашенных «республик» на Донбассе, так как в частной переписке, исследованной в суде, он выражал такое намерение.

Суд признал Фука виновным и приговорил к 2 годам лишения свободы без конфискации имущества.

(вгору)

Додаток 16

17.12.2018

Журналисты обвинили Facebook в заказе фейковых новостей

Несколько бывших и действующих фактчекеров, нанятых Facebook для выявления фейковых новостей, заявили, что компания использовала их только для отвода глаз и на самом деле ничего не сделала для борьбы с недостоверной информацией. Об этом пишет The Guardian (InternetUA).

Особенно журналисты возмущены тем, что соцсеть, вероятно, организовала целую информационную компанию против миллиардера и

мецената Джорджа Сороса, который неоднократно резко высказывался о Facebook. Как ранее выяснили журналисты New York Times, для очернения Сороса нанятая Facebook пиар-фирма использовала антисемитскую и конспирологическую риторику о том, как «евреи контролируют весь мир», в том числе, финансируют движения против Facebook.

«Как мы можем доверять Facebook, когда он распространяет те же слухи, которые нанятые им же фактчекеры признают ложными новостями?» – анонимно заявил один из нынешних фактчекеров компании.

В 2016 году Facebook обвинили в предоставлении площадки для ботов, распространяющих недостоверную политическую рекламу накануне президентских выборов в США. После этого соцсеть пообещала решить проблему, учредив целый комплекс мер по выявлению и удалению фейковых аккаунтов, а также публикуемых ими новостей. Так, Facebook начал сотрудничать с десятками независимых фактчекеров и СМИ с мировым именем. В настоящее время Facebook работает примерно с 40 медиа по всему миру, включая Associated Press, PolitiFact и Weekly Standard. Компания утверждает, что количество фейковых новостей падает, но некоторые как из бывших, так и из нынешних партнеров в проекте разочаровались.

«Руководители Facebook не воспринимают проблему всерьез. Главное, что их волнует – это как сохранить лицо и не потерять доход», – говорит Брук Бинковски, экс-редактор сайта Snopes, который в течение двух лет сотрудничал с Facebook. Напомним, Марк Цукерберг не явился на заседание международного комитета по фейковым новостям в Лондоне.

Фактчекеры также отметили, что Facebook требует уделять основное внимание разоблачению негативных новостей о своих рекламодателях, но при этом игнорировать фейки о важных социальных проблемах. Компания эти обвинения отрицает.

(вгору)

Додаток 17

18.12.2018

Звіт: Активність російської «фабрики тролів» в соцмережах США триває

Спроби Росії вплинути на вибори в США в 2016 році через соцмережі були спрямовані на чорношкірих американців і мали на меті зниження явки виборців-демократів (Українська правда).

Про це йдеться у звітах, підготовлених для Комітету Сенату США з розвідки, пише The New York Times.

В рамках кампанії впливу в соціальних мережах на вибори 2016 року Росія доклала екстраординарні зусилля, спрямовані на афроамериканців, використовувала цілий ряд тактик, щоб спробувати знизити явку виборців-демократів і розгорнула бурхливу активність в Instagram, сказано у звіті

підготовленому компанією з кібербезпеки New Knowledge спільно з дослідниками з Колумбійського університету і Canfield Research LLC.

У документі стверджується, що російська присутність в Instagram була недооцінена і могла бути настільки ж ефективною або більш ефективною, ніж в Facebook.

У звіті також говориться, що дії із втручання тривають на декількох платформах.

Наприклад, одна з них спрямована на те, щоб вплинути на думку про Сирію і підтримати Башара Асада, президента Сирії і російського союзника в цьому жорстокому конфлікті.

Другий звіт складений фахівцями з Оксфордського університету спільно з компанією Graphika, яка спеціалізується на аналізі соцмереж.

В обох звітах підкреслюється, що російське «Агентство інтернет-досліджень» (фабрика тролів) створювало облікові записи в соціальних мережах під вигаданими іменами практично на всіх доступних платформах. Головна мета полягала в тому, щоб підтримати Дональда Трампа, спочатку в праймеріз Республіканської партії, потім на загальних виборах, і далі вже на посаді президента з моменту його інавгурації.

Створивши акаунти, таким чином ніби вони належать американцям, «Агентство інтернет-досліджень» поширює свої повідомлення не тільки через Facebook, Instagram і Twitter, які привернули найбільшу увагу, але також і YouTube, Reddit, Tumblr, Pinterest, Vine і Google+. Для атаки на Сполучені Штати використовувалися майже виключно високотехнологічні інструменти, створені американськими компаніями.

Видання відзначає, що нові звіти в значній мірі підтверджують зроблені раніше висновки: кампанія була спрямована проти кандидата в президенти США Хілларі Клінтон і на підтримку Трампа, а також на поглиблення існуючих розбіжностей в американському суспільстві.

(вгору)

Додаток 18

12.12.2018
Ирина Фоменко
Главным провокатором французских протестов оказался Facebook

Райан Бродерик и Жюль Дарманин опубликовали отчет в BuzzFeed о французский протестах, которые активисты транслировали в прямом эфире в Facebook. Репортеры описывают движение «желтых жилетов» как петлю обратной связи, начавшейся в Facebook в так называемых «группах гнева», вызвавшей бурные протесты в реальном мире, которые, в свою очередь, снова обсуждали в социальной сети. Об этом сообщает The Verge (InternetUA).

«”Группы гнева” мобилизовались в октябре после распространения петиции Change.org, касающейся налога на бензин. Петиция привела к акции на Facebook, которая повлекла за собой протесты, уже четыре недели проходящие

по всей Франции. К настоящему времени погибли три человека, еще сотни получили ранения и тысячи были арестованы», – сообщается в докладе. – «Протестующие, собранные небольшими, децентрализованными группами Facebook, вышли на улицы Парижа, транслируя насилие своим друзьям, смотрящим из домов».

«Социальная сеть залила бензином пожар, который горел во Франции с первых дней президентства Макрона», – пишут авторы отчета.

Некоторые эксперты усомнились в том, что роль Facebook в акциях протеста завышена. Макс Рид считает, что в Нью-Йорке мало доказательств связи, установленной в BuzzFeed.

«Совершенно нелепо так думать о беспорядках, в которых сотни людей получили ранения, особенно если вы критик Facebook или скептик. Посмотрите, что Facebook приносит в стабильные демократии! Посмотрите, как Facebook сбивает с толку хороших граждан! Проблема в том, что для этого конкретного обвинения очень мало доказательств. Мы знаем, что за последний год Facebook различными способами корректировал сортировку новостных лент. Мы знаем, что некоторые из протестующих использовали Facebook, чтобы организоваться. Но еще слишком рано кричать, что “этот зверь родился почти полностью из Facebook”, как это делает BuzzFeed», – утверждает Рид.

«Нельзя сказать, что Facebook не имел отношения к протестам. Кажется, существует консенсус в отношении того, что социальная сеть является предпочтительной организационной платформой для «желтых жилетов”. Но идея о том, что массовое возмущение больше связано с “властью социальных сетей”, чем с реальной французской политикой, как утверждает Бершидский, кажется очень ошибочной и более чем безответственной», – заявил Макс.

«Некоторые предполагают, что все парижане руководствуются теориями о фейковых новостях и заговорах в Facebook и не имеют образования. Было бы ошибкой так думать», – написала 7 декабря утром глава парижского бюро Guardian Анжелика Крисафис в Twitter.

Рид утверждает, что мы должны рассматривать Facebook не как «причину», а как «условие» – как часть фона, на котором происходят события, хотя и влияющего на них способами, которые трудно изолировать.

Конечно, кажется очевидным, что французские протестующие действуют из-за искреннего недовольства своим правительством. И, как отмечает Рид, бесполезно постоянно спрашивать себя, происходили бы эти протесты в каком-то теоретическом мире, где никогда не создавался Facebook. «В той степени, в которой мы можем выделить и измерить влияние Facebook на общество, становится ясно, что его эффект более важен на макроуровне, чем на индивидуальном поведенческом», – пишет Макс.

Четыре года назад Facebook уличили в изменении новостной ленты для манипуляции эмоциями пользователей. По данным исследования, люди, которые видели много положительных постов, вероятно, будут создавать больше положительных публикаций. Слишком рано отвергать идею о том, что

французские «группы гнева» не мобилизовали свою аудиторию подобным образом.

(вгору)

Додаток 19

12.12.2018

Група тернопільських студентів через Telegram налагодила наркобізнес

Житель Миколаївської області організував у Тернополі наркобізнес. Собі у помічники він взяв восьмеро осіб. Усі – молоді хлопці та дівчата віком від 18 до 24 років. Деякі з них – студенти місцевих вишів (InternetUA).

За словами Михайла Димиди, начальника підрозділу протидії наркозлочинності в області, діяльність даної групи вони почали документувати ще на початку року. Пік їхньої активності припав на початок літа.

На фасадах будинків, приміщень та в інших місцях вони розміщували приховану рекламу про продаж наркотиків. Через месенджер Telegram «бізнесмени» приймали замовлення, а після того, як отримували підтверджуючі документи про оплату товару, вказували місця, де захований товар.

Схованки були в різних частинах обласного центру – в під'їздах, підвалах, під підвіконням, між батареями, в пачках з-під цигарок та в пляшках з напоїв.

Розповсюджували вони марихуану не лише в Тернополі, але й в Хмельницькому, Вінниці, Львові, Івано-Франківську, Запоріжжі, Житомирі, Рівному, Києві, Чернівцях та Луцьку. В усіх цих обласних центрах організатор також мав своїх помічників.

Серед товарів була марихуана різних сортів. Грам сировини коштував 220 гривень. За попередніми даними, помічники в місяць заробляли від своєї діяльності близько 30-50 тисяч гривень, а от організатор мав від такої незаконної справи майже сто тисяч гривень.

Оперативники встановлюють, хто постачав групі наркотики. Наразі відомо, що товар надходив до продавців поштою.

Під час санкціонованих обшуків правоохоронці виявили та вилучили електронні ваги, мобільні телефони, банківські картки, пристрої для вживання марихуани, аерозольні балончики та клейкі стрічки, якими позначали товар та малювали рекламу, комп'ютерну техніку, близько 17 тисяч гривень та майже 3 кілограми наркотичної сировини.

Чотирьох учасників злочинної групи оперативники затримали. Їм обрали міру запобіжного заходу у вигляді тримання під вартою з правом внесення застави у розмірі 576 тисяч гривень. По решті підозрюваних тривають слідчі дії, зазначають у поліції.

(вгору)

Додаток 20

12.12.2018

Зберігай спокій та фільтруй інформацію: Як українцям протистояти війні фейків // Сучасна війна ведеться не тільки зброєю - перевагу над ворогом намагаються набути й у інформаційному просторі

Юлія Гуш

Більше чотирьох років в Україні говорять про інформаційну війну з боку Росії та необхідність якось їй протидіяти. Дезінформація, фальсифікація, жонглювання штампами та кліше, навала інтернет-тролів, поширення фейків – заради домінування в інформаційному просторі можуть згодитися будь-які методи (Depo).

Деякі російські фейки свого часу перетворилися на меми. «Новини» про двох рабів та вбивство українськими школярами снігурів не висміяв хіба що ледачий. Але разом з тим наслідки розповсюдження фейків не такі вже й кумедні: вони не тільки надають неправдиву та викривлену інформацію, а й підвищують напругу в соціумі, сіючи паніку та розбурхуючи ненависть і нетерпимість.

«Найяскравіші фейки в соцмережах в 2018 році пов'язані з введенням воєнного стану в Україні, – розповіла голова правління Інформаційного центру "Майдан Моніторинг" Наталія Зубар. – Вірусного поширення в соцмережах та "Вайбері" набув текст про нібито запровадження тотальної цензури в Інтернеті, в якому згадується "федеральний уряд". Він дослівно повторює вірусний текст, який розповсюджувався в Російській Федерації в другій половині 2017 року у відповідь на ухвалення обмежувальних законів. Цікаво, що поширення тексту не зупинила відсутність в Україні "федерального уряду"».

Були ще й інші фейки, пов'язані з воєнним станом. Вони виглядали як накази місцевих органів влади або МВС про конфіскацію автомобіля на потреби війська. Накази поширювалися у вигляді нібито сканів документів, що містили численні та явні граматичні помилки. Також у них були фактичні помилки у прізвищах посадовців.

«Інформаційна безпека – це така штука, яка робить нас трішки параноїками, – пояснює тренерка з медіаграмотності, доцент кафедри управління соціальними комунікаціями Харківського національного економічного університету ім. Семена Кузнеця Ганна Старкова. – Важливо не впадати в крайнощі, все має бути з розумом. А її ввімкнення – особиста відповідальність кожного. Звісно, воєнне положення вносить свої корективи. З чіткого усвідомлення, що воно таке та як працює, я б і радила почати роботу над власним інформаційним полем».

За словами Старкової, у цій ситуації важливо не обмежуватися одним джерелом інформації. Вона зазначила, що у своїй роботі мусить постійно моніторити усі офіційні сайти та заяви перших осіб як України, так й інших держав. Тому важливо, щоб спожиті дані відповідали фактам. При цьому достовірність офіційної інформації не важко перевірити. Наприклад, закони стають обов'язковими до виконання лише після публікації в газеті «Урядовий

кур’єр», це зазначено в Законі України «Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності». Що стосується офіційної інформації, Старкова радить, по-перше, дочекатися публікації у відповідних джерелах. По-друге, спробувати самостійно розібратися у документі. Як приклад вона наводить Указ президента про введення воєнного стану в Україні.

(вгору)

Додаток 21

13.12.2018

Владимир Кондрашов

СБУ поймала майнеров криптовалют, которые финансировали сепаратистов

В Едином государственном реестре судебных решений появились подробности дела о финансировании терроризма сотрудниками интернет-магазина. Свежее определение суда не только проливает больше света на эту историю, но даже называет фигурантов уголовного дела (InternetUA).

Напомним, как мы ранее уже сообщали, собственника, коммерческого директора и директора интернет-магазина, специализирующегося на продаже оборудования для майнинга, СБУ подозревает в финансировании террористов на временно оккупированных территориях Донецкой и Луганской областей. Предприниматели, по версии следствия, с помощью криптовалют Bitcoin и Ethereum финансировали «Народную дружину Донбасса и Павла Губарева» и «Донецкую народную республику».

Согласно определению суда, опубликованному десятого декабря, Служба безопасности Украины установила, что пять граждан страны с февраля 2018 года по настоящее время, в городе Днепр создали схему по предоставлению систематической материальной помощи с использованием криптовалют «Bitcoin» и «Ethereum» представителям «Донецкой Народной Республики». Украинцы переводили электронные денежных средств на электронные кошельки, используемые представителями указанной террористической организации, чем осуществляют содействие ее деятельности.

Один из подозреваемых является физическим лицом-предпринимателем) и владельцем Интернет-сайта «Miner Tech» (www.minertech.org), с использованием которого предоставляет услуги по продаже, обслуживанию технологического оборудования, предназначенного для «Майнинг» (генерации) криптовалюта и осуществляет незаконную конвертацию криптовалют.

Кроме ФЛП, в деле фигурирует также собственник ООО «Стратум 24», которое осуществляет незаконные операции по обналичиванию электронных криптовалют на территории Днепропетровской области в интересах представителей «ДНР». По полученным данным, руководители Интеренет-ресурса «Miner Tech», поддерживая связь с собственником ООО «Стратум 24»,

периодически использовали возможности этого предприятия (stratum24.com) для конвертации электронных криптовалют.

6 ноября во время проведения обыска по месту фактического местонахождения ООО «Стратум 24» в Днепре оперативники изъяли 20 стартовых пакетов «Vodafone», 17 сим-карточек операторов мобильной связи с условными рукописными цифровыми обозначениями на каждой из них (сим-карты зачем-то были пронумерованы), 14 сим-карточек, запакованных в полиэтиленовый пакет, 6660 долларов США, счетчик банкнот и детектор валют.

(вгору)

Додаток 22

15.12.2018

Владимир Кондрашов

В СБУ подтвердили, что российские тролли покупают аккаунты украинцев в соцсетях

Служба безопасности Украины подтвердила, что скупкой аккаунтов украинцев в социальных сетях под видом маркетингового агентства занималось скандально известное российское «Агентство Интернет Исследований», больше известное как «ольгинская фабрика троллей» (InternetUA).

Соответствующее сообщение было опубликовано на официальной странице Службы безопасности Украины в Facbook, передает InternetUA.

Напомним, как мы ранее сообщали, около месяца назад украинскому консультанту по кибербезопасности Егору Папышеву удалось проникнуть на «российскую фабрику троллей» и узнать некоторые подробности работы «кремлеботов» изнутри. Папышева привлекло объявление некоего «рекламного агентства» с предложением заработка именно украинским пользователям – они предлагали собственнику аккаунта установить программу, через которую удаленно могли бы управлять профилем. Используя недостатки в системе коммуникации кремлеботов, консультанту по кибербезопасности удалось проникнуть внутрь сети и узнать, как налажена работа на фабрике троллей. Как оказалось, на российских ботофермах используют специальный софт для работы с социальными сетями, обучают сотрудников и готовят площадку для очередной информационной волны, «арендуя» реальные аккаунты украинцев в соцсетях.

В свежем сообщении Службы безопасности Украины говорится о том, что «Агентство Интернет Исследований» собиралось использовать аккаунты украинцев для дестабилизации ситуации в стране.

– Накануне президентских и парламентских выборов в Украине в 2019 году к гражданам нашей страны от этой российской «фабрики троллей» начали поступать предложения якобы от коммерчески заинтересованных лиц. У них за денежное вознаграждение украинским пользователям предлагается предоставить временный доступ к так называемому рекламному кабинету

аккаунтов в социальных сетях «Facebook» и «Twitter» для якобы распространении через них таргетинговой рекламы и продвижения коммерческих интересов, – объясняют в СБУ. – На самом деле полученные представителями страны-агрессора права доступа к аккаунтам украинцев в социальных сетях будут использованы спецслужбами РФ для проведения разведывательно-подрывной деятельности, манипулирования общественным сознанием, вмешательства в предвыборные процессы, а также распространения антиукраинских материалов, направленных на дестабилизацию общественно-политической обстановки в государстве.

СБУ просит в случае получения предложений продать или передать в аренду свой аккаунт в социальных сетях, сообщать на горячую линию СБУ.

(вгору)

Додаток 23

18.12.2018

Кремль витратить 300 мільйонів доларів на блокування Telegram

У 2019 році Роскомнадзор планує впровадити нову технологію боротьби із забороненими сайтами і сервісами, в тому числі з Telegram (InternetUA).

Про це повідомляє «Російська служба Бі-бі-сі».

Як пише видання, російська влада готова витратити на це до 20 млрд рублів (понад 300 млн доларів). Досі спроби блокувати месенджер Павла Дурова були марними.

Нову технологію блокувань почнуть запускати вже в наступному році. Йдеться про технології DPI (від англійського deep packet inspection – «глибокий аналіз пакетів»).

У провайдера інтернету встановлюється програмно-апаратний комплекс, який аналізує весь трафік і виділяє специфічні пакети, властиві конкретним сайтам або додаткам. Цей же комплекс відсікає і небажаний трафік.

DPI принципово відрізняється від нинішньої системи, за допомогою якої Роскомнадзор намагався заблокувати Telegram.

Зараз доступ до заборонених сайтів блокується за IP-адресою, через що страждають нейтральні ресурси.

Наприклад, навесні 2018 року, борючись проти месенджера Дурова, Роскомнадзор заблокував близько 11 млн IP-адрес, говорив глава відомства Олександр Жаров. Частину з них використовували інтернет-магазини, логістичні компанії і ЗМІ.

На даний момент Роскомнадзор фактично не веде боротьбу з Telegram, стверджують співрозмовники видання. «Цей спосіб був неефективним», – визнає джерело, знайоме з деталями розробки проекту з впровадження нової технології блокування.

«Зараз іде “симуляція” блокування, якісь IP-адреси додаються до реєстру заборонених сайтів, якісь видаляються. У цих умовах аудиторія месенджера в

Росії не просто не впала, а навіть зросла і досягла рекордних значень в 3,4 млн осіб в день», – пише видання.

(вгору)

Додаток 24

18.12.2018

В Чехии оборудование Huawei и ZTE назвали угрозой безопасности

Чешское национального агентства по цифровой и информационной безопасности (Czech National Cyber and Information Security Agency, NCISA) предостерегло операторов от использования ПО и оборудования китайских производителей Huawei и ZTE, заявив, что они могут угрожать безопасности страны (InternetUA).

Huawei, крупнейший в мире производитель телекоммуникационного оборудования, подвергается все большему давлению со стороны западных государств, власти которых подозревают компанию в связях с правительством КНР и кибершпионаже. Китайский вендор неоднократно отвергал обвинения, называя их беспочвенными и несправедливыми.

«Китайские законы предписывают частным компаниям, расположенным на территории страны, сотрудничать с разведывательными службами, поэтому внедрение их оборудования в ключевые государственные системы может представлять угрозу», – говорится в заявлении от имени директора NCISA Душана Навратила (Dusan Navratil). Выдержки из него публикует «Рейтер».

В NCISA отметили, что поводом для заявления стали собственные выводы и сведения союзников.

В ответ пресс-секретарь Huawei заявил, что компания категорически отрицает любые утверждения о том, что она представляет угрозу национальной безопасности. В компании призвали NCISA предоставить конкретные факты, а не бросать тень на репутацию Huawei без каких-либо доказательств.

Huawei всегда считала кибербезопасность приоритетом, и компания была надежным партнером всех основных чешских операторов связи. Китайский вендор вновь отверг предположения США о том, что в оборудовании Huawei могут быть предусмотрены лазейки, позволяющие шпионам из КНР проникнуть в критически важную сетевую инфраструктуру.

«В Китае нет законов или нормативных актов, обязывающих Huawei или любую другую компанию устанавливать в сетевом оборудовании так называемые бэкдоры. Компания никогда не получала подобных просьб от правительственных организаций и никогда не согласилась бы на подобное», – заявил пресс-секретарь.

Комментариев от ZTE на момент публикации не поступило.

Несколько мобильных операторов протестировали 5G в отдельных районах Чехии, а инвестиционная группа PPF, владеющая ведущим чешским провайдером CETIN, подписала с Huawei меморандум о взаимопонимании

относительно сотрудничества в области связи пятого поколения. Аукцион по распределению частот 5G в Чехии запланирован на 2019 год.

Ранее Австралия, а за ней Новая Зеландия не допустили китайских вендоров к 5G-проектам в своих странах, сославшись на риски для национальной безопасности. Из тех же соображений власти Японии недавно утвердили новые принципы госзакупок, фактически запрещающие правительственным организациям закупать оборудование Huawei и ZTE.

(вгору)

Додаток 25

27.12.2018

Правительство Индии требует, чтобы компании убрали сквозное шифрование

Правительство Индии хочет обязать технологические платформы – такие как Facebook, WhatsApp, Twitter и Google – удалять контент в течение суток, если его признают «незаконным», и создать «автоматизированные инструменты» для удаления такой информации в будущем (InternetUA).

Власти также хотят, чтобы они создали инструмент для отслеживания источников контента, что потребует от таких платформ, как WhatsApp, перестать использовать сквозное шифрование.

Новые меры вызвали обеспокоенность у активистов защиты конфиденциальности, которые утверждают, что те будут угрожать свободе слова и позволят проводить «массовый надзор».

Новый закон также потребует от любой платформы с более чем 5 млн пользователей в день назначать «контактное лицо» для «круглосуточной координации с правоохранительными органами и должностными лицами», вести учет всей «незаконной деятельности» в течение 180 дней (или неограниченно по требованию суда) и отправлять ежемесячные уведомления каждому пользователю, информируя их о том, что платформа может немедленно «удалить несоответствующую информацию» и профиль.

MeitY, Facebook, Google и Twitter не ответили на запрос BuzzFeed News о комментариях. WhatsApp, которая имеет более 200 млн пользователей в Индии и будет одной из крупнейших компаний, которую затронет закон, от комментариев отказалась.

Компания неоднократно отказывалась от требований правительства Индии о создании системы отслеживания сообщений. «Мы считаем, что встраивание “отслеживаемости” в WhatsApp подорвало бы сквозное шифрование и частную природу мессенджера, создавая возможность для его неправильного использования», – заявляли в компании.

(вгору)

Додаток 26

12.12.2018

Кіберполіція попереджає про шкідливий вірус та радить як його знешкодити

Створене шкідливе програмне забезпечення, націлене на користувачів операційної системи MS Windows. Спеціалісти з кіберполіції 11 грудня почали фіксувати факти розповсюдження цього шкідливого програмного забезпечення. Загалом воно було націлене на користувачів, які є приватними нотаріусами України (Урядовий портал).

Повідомлення із шкідливими додатками надходили начебто від імені державних установ, зокрема судів різних інстанцій.

Для зараження комп'ютерів користувачів зловмисники використовували декілька видів шкідливого програмного забезпечення (далі – ШПЗ), які мають схожий функціонал. При цьому, використовувались різні методи їх розповсюдження (наприклад, користувачі отримували архівні файли, які зовні виглядали як файли формату .pdf).

Злочинці навіть підробили зміст цих файлів – зовні вони виглядали як відсканований документ, створений від імені державної установи. В деяких інших випадках розповсюдження вірусу відбувалось за допомогою документів формату .docx із вбудованим шкідливим "OLE" об'єктом. Після відкриття документа користувачем, відбувався запуск шкідливого програмного забезпечення. Автоматично відбувалось додавання запису в реєстр операційної системи для його автозавантаження.

Під час поглибленого аналізу спеціалісти з кіберполіції встановили: кожен раз ШПЗ запускалось із теки системного диску за посиланням – :\ProgramData\Microtik\winserv.exe. Виявлене шкідливе програмне забезпечення переходило у прихований режим очікування з'єднання та в повній мірі надавало доступ до ресурсів комп'ютера жертви.

Згідно з результатами аналізу, вказане ШПЗ є модифікованою версією легального програмного забезпечення "RMS TektonIT".

Департамент кіберполіції, задля уникнення зараження своїх комп'ютерів, радить користувачам дотримуватися наступних порад:

По-перше, в жодному випадку не відкривати листи від сумнівних адресатів із сумнівним змістом. Перед відкриттям краще отримати підтвердження у відправника такого листа іншими можливими засобами зв'язку.

По-друге, встановити ліцензійне програмне забезпечення операційної системи та використовувати антивірусні програми.

По-третє,систематично оновлювати операційну систему та програмні продукти.

По-четверте, не надавати доступ стороннім особами до персонального комп'ютера.

Також ви можете самостійно заборонити автоматичний запуск ШПЗ. Для цього потрібно виконати наступні кроки:

– запустіть редактор реєстру. Для цього необхідно натиснути клавішу «Пуск» та внести для пошуку запис «regedit»;

– знайдіть наступну гілку реєстру – HKCU\Software\Microsoft\Windows\CurrentVersion\Run;

– власноруч видаліть знайдений запис такого змісту – «Microtik»;

– на системному диску операційної системи видаліть теку – :\ProgramData\Microtik;

– перезавантажте комп'ютер.

(вгору)

Додаток 27

12.12.2018

Троян DanaBot отправляет спам-сообщения для распространения угроз

Компания ESET сообщила об обнаружении новых функций трояна DanaBot, которые выводят угрозу за пределы категории банковских троянов. Согласно исследованию специалистов ESET, операторы DanaBot недавно экспериментировали с функциями сбора электронных адресов и отправки спама, которые могут использовать учетные записи электронной почты жертв для дальнейшего распространения вредоносных программ (Компьютерное Обозрение).

Вредоносные электронные письма отправляются в ответ на легитимные сообщения электронной почты, найденные в инфицированных почтовых ящиках, создавая впечатление, что их присылают сами владельцы почтовых ящиков. Кроме того, вредоносные электронные письма, присланные из учетных записей, настроенных на отправку подписанных сообщений, будут иметь действительные цифровые подписи.

Электронные письма включают ZIP-файлы, предварительно загруженные с сервера злоумышленников, которые содержат PDF-файлы и вредоносный файл VBS. Выполнение файла VBS приводит к загрузке дополнительных вредоносных программ с помощью команды PowerShell.

На момент написания исследования описанные выше вредоносные функции были нацелены только на Италию.

Кроме появления новых функций, специалисты ESET обнаружили связь DanaBot с другими троянами, в частности GootKit. Проанализировав вредоносный файл VBS на командном сервере DanaBot, специалисты ESET обнаружили, что файл указывает на модуль загрузчика для GootKit. Связь угроз также подтверждается данными телеметрии ESET. Домены DanaBot и GootKit, как правило, используют одинаковый регистратор для своих доменов .co, а именно Todaynic.com, Inc, и в основном используют одинаковые названия серверов – dnspod.com.

За неделю, начиная с 29 октября, телеметрия ESET показала значительное снижение распространения DanaBot в Польше, в ту же неделю в Польше

наблюдалось значительное повышение активности GootKit. Во время этого всплеска угроза GootKit распространялась с помощью того же метода, что и DanaBot в недавних польских кампаниях.

Анализируя DanaBot, специалисты ESET также заметили, что часть настроек DanaBot имеет структуру, как в других семействах вредоносного программного обеспечения, например, Tinba или Zeus.

Исследования специалистов ESET показывают, что DanaBot имеет гораздо более широкий спектр функций, чем обычное банковское вредоносное программное обеспечение. Операторы угрозы регулярно добавляют новые функции, проверяя векторы распространения и, возможно, сотрудничают с другими группами киберпреступников.

(вгору)

Додаток 28

12.12.2018

Ирина Фоменко

За вредоносный контент пользователей скоро ответят интернет-площадки

В этом году сервис-провайдеру Prodigy предъявили иск за клевету за размещение пользователем определенного контента на одной из досок объявлений. Анонимное лицо обвинило фирму, ведущую операции с ценными бумагами, в мошенничестве в связи с первоначальным публичным предложением, пишет Fast Company (InternetUA).

Согласно постановлению Верховного суда штата Нью-Йорк, поскольку Prodigy публиковал руководящие указания для пользователей, использовал модераторов и сканировал на непристойный контент, то он является «издателем» и, следовательно, несет юридическую ответственность за содержание, которое публикуют пользователи.

Конгрессмен Крис Кокс работал с Роном Уайденом над законопроектом, который освободил бы интернет-компании от юридической ответственности за пользовательский контент. Законопроект в конечном итоге стал дополнением к Закону о порядочности в сфере связи, который является частью Закона о телекоммуникациях 1996 года.

Но с 1996 года Интернет сильно изменился. Технологические платформы выросли больше, чем кто-либо мог себе представить, и их используют по-разному, и в хороших целях, и в плохих. Проблема вредоносного контента, публикуемого пользователями, никогда не исчезала – вместо этого она стала намного хуже и, вероятно, вышла из-под контроля.

На сегодняшний день вопрос в том, каким образом регулировать такие компании, как Google, Twitter и Facebook, чтобы они отвечали за контент на своих платформах. Один из наиболее вероятных способов сделать это для Конгресса – пересмотреть Раздел 230.

Раздел 230

Законодательный акт предоставляет так называемые «щит» и «меч» интернет-компаниям. «Щит» защищает технологические компании от ответственности за вредоносный контент, размещаемый на их платформах пользователями. «Меч» дает технологическим компаниям правовое основание для выбора, который они делают при модерировании пользовательского контента.

«Я хотел убедиться, что интернет-компании могут модерировать свои сайты, не будучи обремененными судебными процессами. Я думаю, что все согласятся, что это лучший сценарий, чем альтернатива, когда веб-сайты прячут головы в песок из-за страха быть задавленными ответственностью», – заявил Уайден на заседании палаты представителей в марте.

Многие законодатели, в том числе Уайден, считают, что технические гиганты не спешат обнаруживать и удалять вредоносный пользовательский контент. Они используют правовую защиту, предусмотренную статьей 230, чтобы избежать активной ответственности за пользовательский контент на своих платформах.

«Устаревшая лазейка, которую могут использовать Google и Facebook»

По словам бывшего сотрудника Белого дома Майки Дикерсона, Facebook не сильно отличается от издателя. Когда компании вкладывают свои алгоритмы в процесс принятия решения, какой контент показывать отдельным пользователям, они действуют как издатели.

«С 1996 года большие веб-платформы эволюционировали так, что Раздел 230 больше не подходит. Я думаю, что это устаревшая лазейка, которую Google и Facebook могут использовать», – заявил Дикерсон.

Снятие защиты в Разделе 230 на самом деле может помочь крупным интернет-компаниям и навредить небольшим инновационным предприятиям. По словам Уайдена, если небольшие интернет-фирмы будут подвергаться судебным искам со стороны отдельных лиц и штатов, это может лишить их бизнеса.

Между тем, крупные авторитетные интернет-компании могут позволить себе судебные издержки. И они могут извлечь выгоду, потому что новое юридическое воздействие может создать высокий барьер для выхода на рынок молодых предприятий.

«Существует опасность изменения закона таким образом, что это не улучшит ситуацию для небольших компаний, а скорее приведет к тому, что крупные фирмы будут становиться все сильнее и сильнее», – прокомментировал Дикерсон.

Также есть реальная возможность, что повышение ответственности технологических компаний за пользовательский контент окажет негативное влияние на свободу слова в Интернете. Веб-компании, сталкивающиеся с новой угрозой судебных исков, могут ограничивать или удалять все, кроме самых безопасных видов пользовательского контента.

Крис Кокс считает, что Раздел 230 в целом мог бы провести более четкую грань между веб-платформой и создателем контента. В марте он заявил, что

Конгресс должен вернуться к Разделу 230 и добавить формулировку, объясняющую, что, когда оператор сайта активно запрашивает незаконный контент или иным образом «связан с незаконной деятельностью», он больше не должен пользоваться юридическим иммунитетом, предусмотренным в Разделе. Защита по Разделу 230 предназначена для сайтов, которые действуют как «посредники».

Большинство экспертов убеждены, что лучшим решением проблемы пользовательского контента станет добровольные действия со стороны IT-компаний: удаление токсичного содержания со своих платформ. Дело в том, что Раздел 230 не может заставить их делать это – там нет слов «удалите с вашего сайта в течении 24 часов». Таким образом, для технологических компаний это остается в основном проблемой PR и государственной политики. Единственным реальным рычагом, который есть у Конгресса, является угроза снятия средств защиты в Разделе 230, которыми так долго пользовались технологические компании.

(вгору)

Додаток 29

12.12.2018

Владимир Кондрашов

Медицинские данные детей центра кардиохирургии были на грани «утечки»

Украинские хактивисты обнаружили серьезные проблемы с безопасностью, которые могли повлечь за собой утечку в открытый доступ около 2,2 терабайт медицинской информации, принадлежащей столичному Центру детской кардиологии и кардиохирургии (InternetUA).

Информацию об этом на своей странице в Facebook опубликовал пользователь под ником Lurca Tier.

– Иногда хочется так влупить кому-то больно! В этот раз рука не поднимается в #FRD выкладывать! Но кому-то в Центре детской кардиологии и кардиохирургии нужно очень пересмотреть всё, что связано с сетевой безопасностью! Снимки, базы данных, телефония и еще 25 портов наружу только на одном ресурсе!, – написал Lurca Tier.

Ранее, утром 11 декабря, на странице ведущего разработчика компании ИТ Лаборатория Александра Галущенко появился анонс публикации сведений об инциденте – хактивисты обещали выложить данные в открытый доступ, как это предполагается в рамках флешмоба #fuckresponsibledisclosure, инициированного Украинским киберальнсом.

– Сегодня коллеги опубликуют огромный фак ап с утечкой персональных данных из медицинского учреждения с фотками Ваших костей и внутренних органов. Терабайты информации. Готовьтесь. Будет весело, – написал эксперт.

Однако когда стало известно, чьи именно данные находились в открытом доступе, хактивисты отказались публиковать данные об утечке и сообщили

специалистам медучреждения об обнаруженной уязвимости. По состоянию на 14-00 12 декабря уязвимость уже закрыта.

По данным, которыми располагает наше издание, в открытом доступе находилось около 2,2 терабайт информации о пациентах, включая рентгеновские снимки, записи о пациентах, данные флюорографии, МРТ, УЗИ и т. д.

Сведений о том, что из-за уязвимости данные могли похитить злоумышленники, нет.

(вгору)

Додаток 30

13.12.2018
Владимир Кондрашов
Киберполиция вышла на след продавца вирусов

Причерноморское управление киберполиции Департамента киберполиции Национальной полиции Украины вышло на след гражданина Украины, который осуществляет распространение и сбыт вредоносных программ. По данным киберполиции, данное ПО используется для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи.

Об этом говорится в определении Приморского районного суда Одессы, передает InternetUA.

Основываясь на информации киберполиции, следователем Приморского ОП Одессы 27 апреля открыто уголовное производство по признакам уголовного преступления, предусмотренного ч.2 ст. 361 УК Украины.

В ходе досудебного расследования было установлено, что к совершению указанного уголовного преступления может быть причастен житель Одессы, который распространяет и продает вредоносное программное обеспечение. С этой целью мужчина как пользователь под ником «arsenkooo135» разместил на Интернет форуме bhf.io объявления о продаже скрытого ботнет-майнера «Rarog». В описании объявления пользователем «arsenkooo135» указано что «Rarog» – троян со встроенным модулем майнера и элементами ботнета. Rarog умеет скрывать процесс майнинга от диспетчеров задач и маскируется под драйвер Realtek, копируя заголовки оригинальных утилит. Как указал «arsenkooo135» в объявлении, процесс загрузки осуществляется следующим образом: при первом запуске «Rarog» определяет, заражена ли система. Если система не заражена, он создает скрытую папку в системной директории, копируется в нее и запускается с специальным флагом, уничтожая оригинальный файл. Далее закрепляется в системе - добавляет записи в реестр, создает ярлыки и задачи в системе. После обращается к Rest API машины, аатем получает конфигурацию майнера (CPU / GPU), выгружает соответствующую версию майнера с сервера и запускает в скрытом режиме.

27 октября по месту жительства продавца вирусов был проведен обыск, в ходе которого у подозреваемого изъяли банковские карты (в том числе и карту «Яндекс.Деньги» на имя Arsen Oganesyan), два iPhone, сим-карту, жесткий диск и флешку. Суд наложил на изъятое имущество арест.

Следствие продолжается.

(вгору)

Додаток 31

13.12.2018
Дмитрий Сизов
Наемные хакеры спасают IT компании от реального взлома

Согласно новым данным, опубликованным этической хакерской платформой Bugcrowd, внештатные хакеры могут зарабатывать более 500000 долларов в год на поиске уязвимостей и сообщении об этих проблемах компаниям, таким как Tesla и правительственных организациям – типа Министерства обороны (InternetUA).

Компания, основанная в 2012 году, является одной из немногих так называемых компаний, предлагающих «баг-баунти», которые предоставляют платформу, ориентированную на хакеров для безопасного поиска уязвимостей в компаниях, которые хотят пройти тестирование.

Хакеры работают над четко определенным контрактом для конкретной компании и получают вознаграждение, когда они могут найти изъян в сетевой части компании. Сколько им платят, зависит от того, насколько серьезна решенная ими проблема.

Компании все чаще ищут альтернативы для тестирования кибербезопасности, говорит генеральный директор Bugcrowd Кейси Эллис. По некоторым оценкам, к 2021 году могут остаться открытыми до 3,5 миллионов рабочих мест.

В прошлом году компания увидела крупнейшую выплату за один эксплойт – 113 000 долларов за ошибку, обнаруженную в крупной компании, выпускающей техническое оборудование, сказал Эллис. Согласно данным, выплаты выросли на 37 процентов в годовом исчислении в 2018 году.

Согласно исследованию, половина этических хакеров – или экспертов по безопасности, нанятых для проникновения в сети и компьютерные системы от имени их владельцев – сообщили о том, что они работают на полную ставку. Около 80 процентов сказали, что усилия помогли им найти работу в области кибербезопасности. По словам Эллиса, средние ежегодные выплаты для топ-50 хакеров составили около 145 000 долларов.

По словам Эллиса, хакеры, заработавшие больше всего денег, обладают определенными необходимыми навыками.

«Они нашли определенный класс уязвимости, и они снова и снова идут в разные компании. Они будут разбираться в киберпространстве и пытаться

найти как можно больше возможностей для использования этой уязвимости», – сказал Эллис.

«Они также обладают хорошими навыками разведки и способны понять, что может нанести наибольший ущерб организации. Хорошее понимание того, как работает бизнес или как строится их инфраструктура, действительно полезно», – добавил он.

И в то время как 94 процента охотников Bugcrowd в возрасте от 18 до 44 лет, некоторые все еще в средней или средней школе. Эллис сказал, что стоимость входа низкая и основана на навыках. Около четверти хакеров на платформе не имеют высшего образования.

Компании, пытающиеся взломать

Чтобы защитить себя от кибератак, компании используют ряд методов, позволяющих людям с навыками взлома проверять свою защиту. Некоторые компании используют собственных тестеров проникновения, часто назначая их в так называемые “красные команды”, которые играют роль злонамеренного коллектива, пытающегося уничтожить корпоративные серверы или украсть информацию.

Другие используют консалтинговые фирмы, которые предлагают эту услугу, или такие компании, как Bugcrowd, HackerOne, Synack и Cobalt. Или же они просто делают электронное сообщение с отчетом для любого, кто находит проблемы, чтобы обратиться к ним.

Эллис сказал, что программы по защите от ошибок предлагают более формализованный подход с правилами, которым должны следовать хакеры, например, не перепрыгивать с сервера для тестирования на другие серверы с более конфиденциальными данными.

IJet и Tesla платят хакерам от 1000 до 15000 долларов за поиск проблем, в зависимости от серьезности проблемы. Mastercard выплачивает до 3000 долларов. В октябре министерство обороны заключило контракты с « Взломом Пентагона» для Bugcrowd и HackerOne для их краудсорсинговых программ.

(вгору)

Додаток 32

17.12.2018
Владимир Кондрашов
Количество кибератак на ВСУ за месяц выросло в четыре раза

С момента введения военного положения в десяти областях Украины количество кибератак на ресурсы Вооруженных Сил Украины выросло в 4 раза (InternetUA).

Об этом на брифинге, посвященном первоочередным мероприятиям по кибербезопасности, проводимым в ВСУ, сообщил начальник Войск связи Вооруженных Сил Украины – Главного управления связи и информационных систем Генерального штаба ВСУ генерал-майор Владимир Рапко.

– В четыре раза выросло количество DDoS-атак и случаев распространения вредоносного программного обеспечения с 26 числа, с момента введения военного положения, – заявил Владимир Рапко.

Всего, по словам генерал-майора, только на сайт Минобороны за год зафиксировано более тысячи атак. Одной из последних была DDoS-атака на ресурс Минобороны во время конфликта в Керченском проливе.

– Сайт Министерства – только лицо. Самое главное – чтобы эти атаки не повлияли на работу нашей информационно-коммуникационной сети. Мы используем ресурсы Укртелекома, других операторов связи, и, если атака «положит» их систему, тогда уже будут проблемы. Мы это всё защищаем, – подчеркнул начальник Войск связи Вооруженных Сил Украины.

На данный момент, как рассказал Владимир Рапко, в ВСУ подразделениями кибербезопасности разработаны четкие алгоритмы реагирования на случаи DDoS-атак на сайт Минобороны, все подразделения переведены в боевой режим работы, усилены дежурные смены.

– Некоторые подразделения работают круглосуточно, – отметил генерал-майор.

В Генштабе отмечают активное сотрудничество с ВС США и странами-членами НАТО в плане обмена информацией о самых актуальных угрозах в киберпространстве на базе платформы MISP. Кроме того, сотрудничают военные и с частными структурами – Cisco Talos, ESET Украина и пр.

К сожалению, как отметил генерал-майор Рапко, удержать хороших специалистов по кибербезопасности очень тяжело, как в лавах Вооруженных Сил, так и в стране в целом, ведь зарплаты таких специалистов в частных компаниях в несколько раз выше. Тем не менее, украинские военные в сфере кибербезопасности активно принимают участие в хакатонах и других международных соревнованиях по вопросам кибербезопасности (и даже привозят в Украину призовые места), обучаются в школе НАТО по направлению «кибербезопасность». Также с 2016 года при поддержке НАТО разрабатывается система оперативного управления, связи, разведки и наблюдения (C4ISR).

(вгору)

Додаток 33

19.12.2018
Владимир Кондрашов
Украинский гидрометцентр взломали русскоязычные хакеры

Украинский гидрометцентр взломали неизвестные хакеры, понимающие кириллицу. Уязвимость позволила злоумышленникам воровать данные гидрометцентра и получить полный контроль над почтовым сервером учреждения (InternetUA).

Информацию о том, что Украинский гидрометцентр был взломан, опубликовал на своей странице в Facebook консультант по кибербезопасности Егор Папышев.

– Почту Украинского гидрометцентра давно проломили до администратора сервера, и ее читают неизвестные хакеры. Неизвестные, но, по крайней мере, умеющие читать кириллицу. Сеть этого учреждения, судя по всему, тоже Гидромету уже не принадлежит. Есть надежда, что все поменяется к лучшему, но пока файлик с самыми актуальными конфигурациями dbSettingsHome2.ini гуляет в паблике, – написал Папышев.

В Украинском гидрометцентре нашему изданию сообщили, что знают об атаке, но она якобы произошла ещё полгода назад, уязвимость уже давно закрыта, а делом занимается Департамент киберполиции. Тем не менее, как сообщил Егор Папышев, уязвимость была ещё актуальна по состоянию на 3 декабря этого года.

– Скомпрометирована вся служебная переписка конкретного ведомства. У злоумышленников был полный доступ к размещению информации, её отправке по служебным каналам, – уточнил эксперт в комментарии нашему изданию.

По его словам, хакеры могли использовать доступ к почте для искажения информации и отправки недостоверных сведений, например, в ГСЧС.

– Злоумышленники могли блокировать работу ведомства в тот период, когда оперативная сводка по погодным и другим условиям была очень важна, – уточняет Папышев. – Абсолютно точно хакеры имели возможность не только читать, но и отправлять почтовые сообщения от имени любого сотрудника Укргидрометцентра, включая всё руководство.

(вгору)

Додаток 34

22.12.2018
Обнаружена новая уязвимость в Facebook

Исследователь безопасности, известный в Сети как Lasq, опубликовал PoC-код, который может быть использован для создания полностью функционального червя для Facebook. Код эксплуатирует уязвимость в социальной платформе, позволяющую публиковать спам на страницах пользователей. Что интересно, эта уязвимость уже активно эксплуатируется спамерами (InternetUA).

Lasq обратил внимание на проблему, когда заметил на страницах своих друзей ссылку, которая вела на французский сайт комиксов. При заходе пользователю требуется подтвердить возраст, а затем открывается страница с собственно комиксами и большим количеством рекламных объявлений, при этом ссылка на ресурс публикуется на стене на странице посетителя в Facebook.

Изучая исходный код страницы сайта, эксперт обнаружил подозрительный iframe, наличие которого могло указывать на кликджекинг.

Копнув глубже, Lasq выяснил, что мобильная версия Facebook игнорирует заголовок X-Frame-Options в диалоге общего доступа (в десктопной версии проблема не проявляется), который используется сайтами для предотвращения внедрения кода в iframe, и является одной из основных мер защиты против кликджекинга.

Исследователь сообщил о проблеме администрации Facebook, но в компании отказались рассматривать ситуацию как угрозу безопасности. Как пояснили представители платформы, кликджекинг считается проблемой только в случаях, когда атакующий каким-либо образом изменяет состояние учетной записи (например, отключает функции безопасности или удаляет аккаунт). Однако эксперт не согласен с данной точкой зрения. По его словам, злоумышленники могут воспользоваться данной возможностью не только для рассылки спама, но и для распространения ссылок на вредоносные сайты.

(вгору)

Додаток 35

19.12.2018

На Днепропетровщине 20-летний хакер создал и пытался продать вирус через Интернет

Прокуратурой Сумской области сообщено о подозрении 20-летнего жителя Кривого Рога, который создал и распространял через Интернет вирус (InternetUA).

Об этом ИА «МОСТ-ДНЕПР» сообщили в пресс-службе прокуратуры Сумской области.

«В ходе следствия, проведенного следователями следственного отдела СУ ГУ ЧП в Сумской области, установлено, что юноша создал программу, которая имеет функции удаления, блокирования, модификации и копирования данных, разрушение производительности компьютеров или компьютерных сетей, создание сетевых соединений без ведома и разрешения пользователя.

В дальнейшем с личного электронного почтового ящика подозреваемый посылал вредоносный файл случайным лицам по электронной почте. Такое «письмо счастья» поступило и жительнице Сум. После запуска файла вредоносная программа передала информацию с ноутбука без ведома и разрешения девушки на другой сервер.

В то же время юный хакер разместил в сети Интернет объявление о продаже созданной им вредоносной программы. Вскоре появился желающий приобрести вирус. Свою разработку юноша оценил в 1100 грн. После получения аванса в 550 грн, юноша переслал покупателю желаемый файл», – говорится в сообщении.

Действия подозреваемого квалифицированы по ч. 1 ст. 361-1 (создание с целью использования, распространения и сбыта вредных программных средств, предназначенных для несанкционированного вмешательства в работу

электронно-вычислительных машин (компьютеров), а также их распространение и сбыт из корыстных побуждений) УК Украины.

(вгору)

Додаток 36

24.12.2018

Создана первая программа для экстренного уничтожения данных

Команда CyberYozh security group объявила о релизе Panic Button – первой программы для экстренного уничтожения цифровых данных на компьютерах под Windows (ITnews).

Любое проникновение в компьютер, будь то тайное получение доступа коллегой или извлечение информации сотрудниками правоохранительных органов, запускает немедленное и необратимое уничтожение данных.

Для кого была разработана Panic Button? Эта программа предназначена для всех, кто хочет защитить конфиденциальную информацию от несанкционированного доступа или криминалистического анализа. К этой категории относятся журналисты, предприниматели, чиновники и политики, а также обычные пользователи, которые опасаются атак киберпреступников.

Важно, что Panic Button может активироваться как действиями пользователя (клик по ярлыку или нажатие комбинации заранее заданных клавиш), так и автоматически – в режиме логической бомбы. Пользователь задает в настройках программы определенное действие, невыполнение которого приводит к уничтожению конфиденциальных данных. Таким образом, логическая бомба сработает, если доступ к компьютеру будет получен тайно или принудительно.

Panic Button умеет экстренно уничтожать данные об активности пользователя в операционной системе: информацию о последних просмотренных документах, изображениях и запущенных программах. Также уничтожаются данные об активности в сети – история и кэш браузера, cookies, закладки и сохраненные пароли. Программа работает со всеми популярными браузерами: Chrome, Mozilla, Opera, Edge и Яндекс.Браузер.

Кроме того, при активации Panic Button уничтожает любые файлы, указанные в настройках программы. При желании пользователь может настроить отправку email-уведомлений о срабатывании программы.

Что умеет Panic Button?

– Экстренно уничтожает всю информацию об активности пользователя в системе и в сети;

– Экстренно уничтожает любые файлы, указанные в настройках программы;

– Автоматически срабатывает при несанкционированном доступе к компьютеру;

– Активируется при тайных попытках проникновения в компьютер.

(вгору)

Додаток 37

24.12.2018

Появилось приложение, которое отслеживает утечку данных пользователя

Приложение будет контролировать использование личных данных сайтами и показывать, какая информация уже есть у сторонних сервисов (InternetUA).

FigLeaf – стартап, основанный Славой Коломейчук и Юрием Двойносом, разрабатывает кроссплатформенное приложение, чтобы дать пользователям представление о том, как были затронуты их личные данные.

«Мы хотим расширить возможности пользователей и предоставить им инструменты, позволяющие оставаться наедине с сетью без угроз для себя», – отметил Двойнос в интервью Download.com. По его словам, над FigLeaf работает команда из 100 человек.

Пользователи также получат инструменты для возврата личных данных и смогут определить, кто получал к ним доступ. По словам Двойноса, даже если пользователь решит остаться полностью приватным и не делиться какими-либо данными, он все равно сможет пользоваться интернетом.

Приложение FigLeaf, которое все еще находится в бета-тестировании, сможет определить, были ли взломаны ваши личные данные и кто их использовал. По словам разработчиков, понимание того, насколько вы уязвимы, – это первый шаг к повышению безопасности.

Одним из способов, которым FigLeaf определяет, какие из ваших данных было скомпрометированы – сканирование дарквеба. Когда пользователь вводит свой адрес электронной почты в приложении, он запускает поиск и может посмотреть какие данные о нем есть в сети.

FigLeaf помогает пользователям создавать более безопасные пароли, шифровать и синхронизировать их между устройствами. Еще один инструмент, который предложит FigLeaf, – это создание фиктивной учетной записи, которая подключается к вашей реальной. Пользователь будет выполнять любые онлайн-транзакции с ложной учетной записью, и в случае утечки данных, основные записи будут защищены.

Кроме того, приложение позволяет выбирать, какие веб-сайты или компании могут иметь доступ к вашим данным, просто нажимая переключатель.

(вгору)

Додаток 38

25.12.2018

Кіберполіція викрила чоловіка у незаконному втручанні в бази даних державних установ

Обіймаючи посаду в компанії, яка обслуговувала державні установи (в тому числі і військові частини), чоловік незаконно отримував доступ до інформації, яка містилася в базах цих установ. Наразі поліцейські перевіряють інформацію щодо продажу зловмисником інформації (GoodNews.ua).

Працівники Подільського управління Департаменту кіберполіції, за участі детективів Хмельницького відділу поліції, співробітників СБУ в Хмельницькій області та працівників військової прокуратури Хмельницького гарнізону, викрили 36-річного мешканця Хмельницького у втручанні до комп'ютерної мережі бухгалтерського обліку державних органів та підприємств.

Працівники кіберполіції встановили: чоловік є працівником приватного підприємства, що обслуговує державні об'єкти, в тому числі й військові частини. До його обов'язків входили реалізація, встановлення та обслуговування програмного забезпечення бухгалтерських та облікових систем. Крім того, чоловік реалізовував, встановлював та обслуговував програмне забезпечення бухгалтерських та облікових систем, яке входить до санкційного списку.

Порушуючи вимоги договірних зобов'язань, він таємно отримував доступ до даних працівників цих підприємств, реєстраційних номерів їх облікових карток платників податків тощо.

Проведено обшуки за адресою ведення господарської діяльності та за місцем проживання зловмисника. На персональних комп'ютерах правоохоронці виявили ряд інформації відносно працівників державних установ. Їх направлено на експертизу. Після отримання її результатів буде визначено об'єм, приналежність та перелік інформації, яку отримано в наслідок злочинної діяльності чоловіка.

Триває досудове розслідування розпочате за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України. Зловмиснику загрожує до шести років ув'язнення з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

(вгору)

Додаток 39

26.12.2018

Многие детские приложения из Google Play оказались вымогателями и шпионами

Google уделяет недостаточно внимания обеспечению безопасности детей, использующих Google Play. По словам группы потребителей, обратившихся с жалобой в Федеральную комиссию торговли США, разработчики некоторых игр и приложений используют запрещенные механизмы контроля за несовершеннолетними пользователями. Они грубейшим образом нарушают

закон о неприкосновенности частной жизни детей и тем самым подвергают их серьезной опасности (InternetUA).

В данном случае речь идет о приложениях и играх, публикуемых в семейном разделе Google Play. В соответствии с правилами Google, весь контент, который попадает сюда, должен соответствовать нескольким обязательным правилам. Например, предоставлять полный спектр данных, которые приложения собирают о пользователе. Так родители могут проконтролировать, какая именно информация об их детях накапливается разработчиками, и при необходимости ограничивать ее сбор.

Незаконный сбор данных приложениями

Однако, как сообщается, многие приложения нарушают этот принцип, передавая информацию о несовершеннолетних пользователях третьим лицам. В число сведений, собираемых разработчиками, входили данные служб геолокации, а также личная информация. В общей сложности, подсчитали эксперты, этим занимаются более 70 % приложений и игр из раздела семейного ПО, указывая на то, что Google пренебрегает своими же правилами, не проводя должной проверки.

Вымогательство в приложениях

Еще одним фактором, оказывающим негативное воздействие на детей, является демонстрация специфической рекламы, продвигающей встроенные покупки. Несовершеннолетним намеренно показывают популярных героев мультфильмов плачущими от того, что ребенок не совершает внутриигровых приобретений. По мнению экспертов, это абсолютно недопустимое психологическое воздействие на детей, которое при определенных сценариях может классифицироваться как вымогательство.

(вгору)

Додаток 40

27.12.2018

Каких электронных писем стоит опасаться в новогодние дни

Рождество, Новый год и зимние праздники любят все. Можно отдохнуть от работы, развлечься в кругу семьи или друзей, подышать глотком свободы. Но на этот период, как правило, приходится пик удаленного мошенничества. Особенно возрастает поток спама. Что более важно – среди рассылок можно нарваться на мошеннические. Их следует разделить на несколько категорий и предназначены (InternetUA):

1. Для инсталляции на ПК вирусов, например, ПО для незаконного майнинга цифровых активов.

2. Для кражи данных доступа к криптографическим и электронным кошелькам, профилям в соцсетях.

3. Для банального выманивания средств у доверчивой онлайн-аудитории.

Мошенники часто оперируют испытанным методом и для достижения успеха применяют послания, оформленные геральдикой и атрибутикой

известных компаний, поскольку популярные производители балуют комьюнити новогодними акциями, подарками и скидками.

Сложно разобраться в лавине спама, наполняющего Интернет и почтовые ящики онлайн-публики. Поговорим, как распознавать послания мошенников.

Фейковые опросы и платные призы

Проведение опроса – распространенный способ мошенничества и часто встречается не только в канун новогодних праздников. Спам от имени известных компаний возвещает о фейковом розыгрыше, но требует обязательного участия в опросе или викторине, что интригует доверчивых пользователей.

Как правило, доверчивая аудитория попадается на уловку, позарившись на круглую сумму, обещанную аферистами взамен небольшой комиссии. Легко догадаться, что деньги, переведенные на указанный аферистами счет, потрачены впустую, а часто мошенники получают и платежные данные.

Опасные купоны

Весьма часто спамеры применяют для экспорта вредоносного ПО специальные предложения якобы от известных брендов в виде купонов на предпраздничные скидки и разные акции.

Фейковые онлайн-магазины и финансовые сервисы

В период праздников особенно растет число сайтов-клонов популярных торговых фирм и удаленных магазинов. Мошенники научились «делать» трудно различимые копии. И если вы любитель онлайн-шопинга, нужно внимательно изучить данные партнера, иначе рискуете потерять деньги.

Растет число клонов официальных веб-ресурсов банков и систем удаленных платежей. Мошенники вводят комьюнити в заблуждение разной информацией, и они разглашают платежные данные, что заканчивается потерей сбережений.

Участились в уходящем году случаи создания клонов криптовалютных хранилищ. Первым прецедентом стало появление в мае Electrum Pro – мошеннического клона Биткоин-кошелька Electrum. Уже с осени администрация Google Play вынуждена бороться с поддельными ресурсами аналогичного вида, число которых стабильно растет.

Как избежать рисков

Среднестатистическому обывателю сложно разобраться в технических аспектах онлайн-мошенничества, но простые меры предосторожности помогут сохранить в сохранности свои фидуциарные или криптовалютные сбережения:

– Визуальное сходство с копируемым онлайн-ресурсом вводит в заблуждение. Тщательно изучите сайт.

– Обращайте внимание на детали письма. Наличие вложений или посторонних ссылок является индикатором идентификации вероятного мошенничества.

– Брендовые компании не берут за раздачу призов комиссию – это универсальный стандарт.

– Следите за названием сайта в адресной строке. Мошенники способны применить похожий, но ни в коем случае абсолютно идентичный домен.

– Инсталлируйте на ПК актуальные версии программ со встроенными механизмами защиты.

– Никогда не разглашайте свои платежные реквизиты.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

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
Сайт: http://nbuviap.gov.ua/
http://сіаз.укр/
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.