СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(28.11–11.12)

2018 № 21

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(28.11–11.12)
№ 21

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

28.11.2018
Facebook запуслил возможность совместного просмотра видео

В Facebook появилась возможность совместного просмотра видео. Новая функция получила название Watch Party. В рамках сервиса любой пользователь социальной сети может пригласить на совместный просмотр какого-либо видео других людей и в его ходе оставлять видные всем зрителям комментарии, управлять воспроизведением, получать статистику просмотров (IGate).

Ранее подобный стриминг был доступен только некоторым сообществам в рамках тестирования, но теперь компания объявила о его запуске для всех официально.

Пользователь, организовавший сеанс, может останавливать ролик, перематывать его, комментировать, добавлять в очередь просмотра еще видео, смотреть, кто в данный момент присутствует на просмотре.

Страницы и группы также получили возможность планировать совместные просмотры для своих подписчиков. Когда трансляция начинается, наиболее вовлеченные фанаты будут получать уведомления о проводимом мероприятии в виде пуша или поста в ленте.

Чтобы воспользоваться Watch Party, необходимо нажать на поле создания поста, потом выбрать этот пункт из предложенных дополнительных функций и затем следовать предоставленным инструкциям.

***

29.11.2018
Instagram запускає функцію для людей зі слабким зором

Instagram запускає опцію, яка дозволить вивчати фотографії людям зі слабким зором (Espreso.tv).

Про це йдеться в блозі соціальної мережі Instagram.

Нова функція буде використовувати технологію комп'ютерного зору для розпізнавання предметів і людей, які зображені на фото. Вона буде працювати на смартфонах тих, у кого підключена функція голосового опису. Люди зі слабким зором зможуть прослухати опис фотографії.

Крім того, Instagram також підключив функцію, за допомогою якої користувачі зможуть самостійно додати описи фотографій. Обидві функції доступні в останньому оновленні програми.

***

29.11.2018
В Facebook появится новая функция

Исследователь приложений Джейн Вонг обнаружила новую функцию, которая может появиться в Facebook. Она позволит пользователям скрывать определённые слова, фразы и даже эмодзи в комментариях в своих timeline (InternetUA).

На опубликованном девушкой скриншоте видна новая вкладка, где отображается список нежелательных слов. При этом запрет коснётся только его инициатора: автор комментария и его друзья будут по-прежнему его видеть.

***

30.11.2018

Михаил Сапитон

YouTube провел массовый запуск Stories. Впервые их анонсировали в прошлом году

С 29 ноября YouTube расширил доступность функции Stories. Теперь короткие видеоролики могут создавать все авторы каналов, набравшие 10000 подписчиков и более, сообщает The Verge (AIN.UA).

Впервые функцию запустили в ноябре 2017 года под именем Reels. Позже ее переформатировали в YouTube Stories. Поначалу возможность создавать Stories была только у ограниченного круга популярных блогеров. В июне представители видеохостинга заявили, что выкатят возможность на более широкую аудиторию.

YouTube Stories отличаются от того, что предлагает Instagram. В видеохостинге они служат возможностью ответить на вопросы подписчиков и показать бекстейдж съемок, а не поддерживать ежедневные обновления. Stories существуют до 7 дней, а не 24 часа, как на других площадках. Они отображаются в мобильных приложениях YouTube для подписчиков и не-подписчиков каналов в разделе «Смотрите далее». На Stories можно отвечать комментариями, голосовать «за» и «против». Авторы каналов могут записать короткие видео из секции «Create Story» в приложении YouTube. Также, они могут отвечать на новые комментарии с помощью коротких роликов.

Stories появятся у пользователей и создателей в течение ближайшей недели.

***

1.12.2018

Instagram разрешил ограничивать доступ к Stories

С 30 ноября пользователи социальной сети Instagram, кто имеет доступ к Stories, получили возможность управлять фотографиям и видео с наложенными поверх текстом и рисунками (или без них), которые исчезают спустя 24 часа после публикации. Принадлежащая Facebook соцсеть сообщила об этом в своем блоге (InternetUA).

Пользователи смогут сформировать список близких друзей (Close Friends) и ограничивать видимость Stories этим списком.

«Сообщество наших пользователей увеличилось, а иногда вы хотите чем-то поделиться не для всеобщего обозрения. С Close Friends у вас появляется возможность поделиться личными моментами с небольшой группой отобранных вами пользователей», – прокомментировала нововведение соцсеть.

Попасть в настройки группы пользователей можно из всплывающего меню в профиле. Список близких друзей видит только владелец аккаунта, подать запрос на добавление в него невозможно.

Если при просмотре чужих Stories пользователь увидит зеленый значок в нижней части экрана, это значит, что автор публикации добавил его в список близких друзей. Нововведение доступно с 30 ноября как для iOS, так и для Android.

***

3.12.2018
Ирина Фоменко
Бывшие ведущие Top Gear создали социальную сеть для водителей

Социальная сеть, основанная Джереми Кларксоном и другими бывшими ведущими Top Gear, начнет помогать пользователям со страхованием, пишет The Telegraph (InternetUA).

DriveTribe будет предупреждать пользователей о необходимом продлении страховки и направит их в компании, предоставляющие такие услуги.

Докладніше

***

3.12.2018
Ирина Фоменко
Skype запускает «живые субтитры» для звонков

Наряду с новостями о получении PowerPoint «живых субтитров» в 2019 году, Microsoft объявила, что аналогичная технология теперь доступна в Skype. Запуск «живых субтитров» приурочили к 3 декабря, Международному дню инвалидов.

Докладніше

***

4.12.2018
Дмитрий Демченко
Что такое Zepeto – самая популярная соцсеть в украинских App Store и Play Market

На первых местах в мировых чартах Play Market и App Store, включая украинские, сейчас находится приложение Zepeto. Несмотря на то, что про него было слышно немного, на данный момент его скачали около миллиона пользователей. Одним из первых на приложение обратило внимание издание Motherboard.

Докладніше

***

5.12.2018

Instagram ждут кардинальные изменения

Разработчики Instagram изменят интерфейс приложений для Android и iOS. Сейчас пользователи листают ленту вертикально, а в скором времени фотографии и видео придётся пролистывать по диагонали, как истории (InternetUA).

Над карточками с контентом будет отображаться карусель из миниатюр с предпросмотром снимков, которая, по замыслу, разработчиков, будет подогревать интерес пользователей и заставлять их листать всё дальше и дальше. Не исключено, что в приложениях появятся и другие нововведения, так или иначе связанные с изменениями в интерфейсе.

***

5.12.2018

Telegram готовится к важному обновлению

Телеграм-канал TG Info рассказал о приближающемся обновлении мессенджера, которое наверняка порадует любителей стикеров. Если разработчики Telegram не передумают, то в скором времени сервис обзаведется анимированными наклейками (InternetUA).

Подтверждением возможного нововведения выступил соответствующий раздел в настройках beta-версии Telegram для iOS. В Android-версии клиента для закрытого тестирования такой кнопки не появилось.

Когда анимированные стикеры появятся в релизных версиях приложений, неизвестно. Обычно бета-версии проходят тестирование в течение двух-трех недель, поэтому Telegram может сделать приятный подарок пользователям к Новому году.

***

6.12.2018

Facebook объяснил, как работает поиск в соцсети

Facebook опубликовал короткое видео, в котором объяснил, какие факторы влияют на результаты поиска в соцсети. В компании заявили, что

хотят быть более прозрачными в том, что происходит, когда пользователи ищут контент на площадке (InternetUA).

Согласно Facebook, основное влияние на результаты поиска оказывает активность пользователей на платформе. При этом их действия за пределами социальной сети никак не влияют на ранжирование.

Когда пользователи ищут контент на Facebook, результаты поиска ранжируются на основании их активности в соцсети и активности сообщества в целом.

В рамках активности пользователя учитываются следующие факторы:

– Чем друзья пользователя делятся с ним;
– Страницы, на которые пользователь подписан;
– Группы, к которым он присоединился;
– События, на которые он подписался или отметил как понравившиеся;
– Публикации, с которым он взаимодействовал в своей новостной ленте;
– Информация, которую он указал в своём профиле;
– Места, которые он помечал;
– Предыдущие поисковые сессии.

Что касается активности всего сообщества Facebook, то здесь учитываются популярность того контента, который пользователь ищет, и то, как давно он был опубликован.

***

11.12.2018

В Skype появился новый статус присутствия

Участникам предварительного тестирования Skype отправлены новые версии приложений для всех платформ. Среди ключевых новшеств обновления упоминается возможность использования нового статуса присутствия и сворачивания окна в системный трей (Украинский телекоммуникационный портал).

Новый статус Recently Active устанавливается автоматически в случае отсутствия активности со стороны пользователя менее часа. Если вы не пользовались Skype более часа, приложение установит статус Away, который был доступен в классических версиях программы и теперь вернулся в современной.

Статус Away можно будет установить и вручную, а вот Recently Active будет применяться только автоматически. Впрочем, в будущем разработчики обещают нам возможность настройки паузы до его включения.

В приложении Skype для Windows 10, устанавливаемом из Microsoft Store, по просьбам пользователей была реализована возможность сворачивания окна в системный трей. Эта функция также была доступна ранее в классической программе. В контекстном меню иконки кроме прочего будет отображаться счётчик непрочитанных сообщений. В планах у разработчиков и устранении

досадного недоразумения с этим приложением: оно отмечало пользователей неактивными, хотя они продолжали пользоваться мышью и клавиатурой.

***

11.12.2018

В Instagram з'явилися голосові повідомлення

Instagram запустив функцію голосових повідомлень в Direct: щоб записати їх, досить затиснути кнопку і диктувати текст.

Як зазначає видання Tech Crunch, раніше потрібно було починати пряму трансляцію, щоб поговорити (Еспресо).

Одержувачі можуть прослухати аудіоповідомлення в будь-який час. Запис може тривати до однієї хвилини, надіслати повідомлення можна як одному співрозмовнику, так і в групу, а соцмережа зберігає всі повідомлення, тож їх можна прослухати у будь-який час.

Функція стала доступною по всьому світу відразу на iOS і Android.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

29.11.2018

МІП: Верифіковано сторінки ЗСУ та представництв України за кордоном у Facebook

29 листопада 2018 року, на запит Міністерства інформаційної політики України до Європейського офісу Facebook, було верифіковано офіційні сторінки військ у складі Збройних Сил України та сторінки дипломатичних представництв України за кордоном.

Докладніше

***

30.11.2018

Меланья Трамп заявила о необходимости «давать отпор» в соцсетях

Первая леди США Меланья Трамп заявила, что несмотря на ее призывы к подросткам быть добрыми в соцсетях, иногда бывают исключения. Об этом сообщает The Hill (InternetUA).

«Простите, но иногда необходимо давать отпор», – заявила Меланья, отвечая на вопрос в ходе мероприятия в Университете Либерти в городе Линчберг.

Кампания «Будь лучшим», запущенная по инициативе первой леди, ставит приоритетной задачей борьбу с травлей в интернете. Также она

посвящена борьбе с употреблением опиоидов и поведению в социальных сетях. Как отмечает издание, кампания неоднократно подвергалась критике, так как муж Меланьи, президент США Дональд Трамп часто резко высказывается о своих противниках в твиттере.

***

6.12.2018

Держкомтелерадіо: У соцмережах поширено відеоролики про переваги стратегічного курсу України в ЄС

У соціальних мережах поширено відеоролики, які у стислій і виразній формі інформують про переваги стратегічного курсу України в ЄС. Останні два присвячені новим можливостям для малого і середнього бізнесу щодо розвитку торгівлі, отримання кредитів та пошуку нових бізнес-партнерів, а також реформуванню державної служби (Урядовий портал).

Відеоролики виготовлені ТОВ «Український інститут розвитку медіа» на замовлення Держкомтелерадіо. Ролики, які у виразній і водночас стислій формі популяризують здобутки європейської спільноти і перспективи, що відкриває для українців членство в ЄС, розміщено на сторінці Держкомтелерадіо у Фейсбуці.

***

2.12.2018

Флешмоб допомоги пенсіонерам стартував в Україні

В Україні розпочалася благодійна акція #LetsHelpBabushkas. Її мета – допомогти пенсіонерам, які опинилися у скрутному становищі (Новий формат).

Доєднатися до флешмобу може кожен українець: потрібно оплатити чек літніх людей в супермаркеті та викласти фотозвіт із хештегом #LetsHelpBabushkas у соцмережі.

За даним хештегом вже можна знайти велику кількість дописів та фото зі старенькими, які приємно здивовані такій благодійності.

***

9.12.2018

У соцмережах триває флешмоб на підтримку Олега Сенцова

У соціальних мережах продовжується масовий флешмоб #LetSentsovGetSakharov. Серед його учасників – європейські політики та громадські діячі (uatv).

Вони вимагають відпустити бранця Кремля на церемонію вручення премії імені Сахарова, яке відбудеться у Страсбурзі 12 грудня.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

29.11.2018

Twitter рекламирует флагманский аккаунт в наружной рекламе Нью-Йорка

Twitter запустил наружную рекламу на Таймс-сквер в Нью-Йорке, чтобы прорекламировать свежий и дерзкий тон флагманского аккаунта @Twitter. На билбордах демонстрируются реальные твиты из аккаунта. Их цель – отразить «более легкую и разговорчивую природу» бренда Twitter. Среди сообщений «Кто не спит?» и ретвит Стивена Кинга: «Граффити – это Twitter улиц». Платформа отметила 14-кратный рост ответов на твиты @Twitter со времени смены стратегии и углубления бренда в диалог. Другие бренды, такие как Netflix, Burger King и Wendy's применили тот же подход и начали общаться в сети с позиции пользователя, а не компании (Marketing Media Review).

***

30.11.2018

YouTube планирует открыть бесплатный доступ к оригинальному контенту

YouTube меняет политику предоставления оригинального контента: видеосервис намерен сделать его просмотр бесплатным и открытым, но с перерывом на рекламу (Телекритика).

С 2015 года оригинальный контент YouTube был доступен только для пользователей, имеющих подписку на потоковый сервис YouTube Premium. Однако сейчас в компании собираются объединить текущие премиум-каналы и существующие рекламные предложения в единый сервис – Premium Originals, который к 2020 году будет предоставлять бесплатный оригинальный контент.

«2018 год стал годом прорыва для YouTube Premium и YouTube Originals. YouTube Premium стал доступен в 29 странах, мы выпустили более 50 сценариев и шоу, собрали восемь номинаций «Эмми» и более 30 других наград. В 2019 году мы продолжим инвестировать в производство сценарных программ и переведем YouTube Originals на модель доступа при поддержке рекламы», – рассказал официальный представитель компании.

***

3.12.2018

Как Facebook и Twitter угадывают интересы пользователей // Эти данные используются для таргетированной рекламы

Представители соцсетей Facebook и Twitter неохотно делятся информацией о том, как работают алгоритмы по сбору личных данных

пользователей. По официальным заявлениям, сайты собирают такие базовые данные, как день рождения, пол, используемые устройства, местоположение, опубликованные посты и лайки (InternetUA).

Кроме того, соцсети могут получать информацию с помощью cookies, ссылок и других приложений, связанных с аккаунтом, пишет Quartz.

Пока алгоритмы полностью не раскрыты, Facebook и Twitter пытаются быть прозрачными хотя бы в отношении результатов работы программы. Просмотреть ваши интересы можно в настройках соцсетей. Как объясняет сайт, эти данные необходимы для выстраивания аудиторий с похожими предпочтениями в магазинах, одинаковым стилем жизни и так далее.

***

4.12.2018

Facebook тайно разрабатывает гибких роботов

В корпорации объясняют, что всего лишь хотят сделать более совершенными свои алгоритмы. Однако журналисты подозревают, что Facebook не ограничивается симуляциями. Для чего соцсети роботы с щупальцами и хоботами – пока неясно.

Докладніше

***

6.12.2018

Facebook потерял лидерство в списке лучших мест для работы в США

Facebook получил 7-е место в рейтинге 100 лучших мест для работы в США в 2019 году, составленном Glassdoor (сервис, на котором сотрудники анонимно могут рассказать о работе компании и условиях труда). Годом ранее соцсеть лидировала в списке (InternetUA).

Это самый низкий рейтинг Facebook в опросе с 2015 года, когда компания заняла 15-е место, сообщает Business Insider.

Компания потеряла позиции после скандалов, связанных с нарушением использования данных пользователей, а также недовольства сотрудников.

Еще в 2017 году 84 % сотрудников заявляли, что «оптимистично относятся к будущему компании», 72 % считали, что «Facebook делает мир лучше». Теперь эти цифры снизились до 52 % и 53 % соответственно, сообщает Business Insider, ссылаясь на данные рейтинга.

Glassdoor выявил частые жалобы со стороны сотрудников, в том числе, на «плохой баланс между работой и личной жизнью».

Тем не менее, количество положительных отзывов в значительной степени превышает отрицательные. Так, 96 % отзывов сотрудников свидетельствуют о том, что они одобряют главу компании Марка Цукерберга.

Некоторые из сотрудников в комментариях призывают «не верить всему негативу, который появляется в прессе».

***

11.12.2018

Facebook запускає «внутрішній блокчейн-стартап». І шукає нову команду

Facebook запускає «внутрішній блокчейн-стартап», в який набирає команду розробників і дослідників (Espreso.tv).

Про це пише The Next Web з посиланням на опубліковані компанією вакансії.

В оголошенні компанії йдеться, що Facebook хоче змусити працювати технологію в масштабі соцмережі, і саме над цим працюватиме нова команда.

«Це невелика, але швидко зростаюча група талановитих людей, захоплених зміною світу», – йдеться у повідомленні. Також Facebook шукає фахівця з маркетингу, який би зміг керувати проектом.

Вперше про створення в Facebook окремого напрямку по роботі з блокчейном повідомили у травні 2018 року. Очільником напрямку став Девід Маркус, який раніше працював в PayPal і займав пост віце-президента при розробці Facebook Messenger. Також Маркус входить до ради директорів кріптоплатформи Coinbase.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

29.11.2018

У Раді Європи боротимуться з інтернет-залежністю

У Раді Європи розглядають довготривале перебування людей у мережі інтернет як залежність – на рівні з наркотичною (InternetUA).

Про це йдеться серед пріоритетів робочої програми головування Португалії у так званій групі Помпіду – платформі Ради Європи зі співробітництва у боротьбі зі зловживанням наркотиками та їхнім незаконним обігом, повідомляє власний кореспондент Укрінформу у Страсбурзі.

«Нова програма португальського головування на 2019-2022 роки включає також пріоритетність щодо онлайн-залежності, яка нещодавно була визнана медичною спільнотою як патологія», – заявили у Раді Європи.

За даними дослідження Національної лабораторії медицини та Національного інституту здоров'я США, захворювання на інтернет-залежність руйнує життя, спричиняє неврологічні ускладнення, психологічні розлади та соціальні проблеми.

Програма групи Помпіду з подолання цієї проблеми включає плани співпраці з Google та іншими приватними компаніями, щоб визначити шляхи зменшення обсягу часу, які онлайн-залежні проводять в інтернеті, що нині часто порівнюється із вживанням наркотиків.

***

4.12.2018

Вчені пояснили, чому соцмережі корисні для підлітків

Крім депресій, заздрості та залежності, які є частими наслідками життя в Інтернеті, соціальні мережі також надають людям вагому психологічну підтримку.

Докладніше

***

2.12.2018

Чому Інтернет є відображенням нашої психіки?

Ще 20 років тому на Інтернет покладали великі надії. Люди думали, що вже через декілька років Інтернет змінить світ на краще. Зараз же ми не в захваті від мережі. Ми звинувачуємо її у всіх бідах, думаємо, що без неї було б набагато краще. Чому наше відношення до технологій так сильно змінилося?

Докладніше

Маніпулятивні технології

28.11.2018

Міноборони закликає співгромадян не вестися на фейки та довіряти інформації з офіційних джерел

Міністерство оборони України звертає увагу, що Російська Федерація у традиційній для себе манері продовжує підвищувати градус ненависті до всього українського, у зв'язку з чим помітно збільшилася кількість російських фейків та вкидів в інформаційному просторі на військову тематику, зокрема, у соціальних мережах та стрічках новин деяких засобів масової інформації.

Докладніше

***

28.11.2018

Попытка №2: антиукраинская SMS-атака повторилась в Польше

После того, как жителям Сумской области массово пришли SMS с требованием явиться в воинскую часть, авторы провокации решили закрепить успех. Такие же SMS были разосланы пользователям в Польше в районах, граничащих с Украиной (InternetUA).

О том, что за спам-атакой стоят одни и те же лица, свидетельствует очень похожий текст посланий. В польских SMS указывалось дословно следующее: «Мужчины 18-65 лет, проживающие в Дукле, обязаны прибыть в управление 27 ноября на 10.00 в связи с кризисной ситуацией в Украине». Сообщения были разосланы якобы от имени Центра государственной безопасности.

В Польше уже подтвердили, что официальные органы SMS-предупреждений не рассылали. Кто стоит за провокацией, выясняют спецслужбы и полиция.

***

29.11.2018

Фейки та паніка в українському інтернет-просторі: хто в цьому винен

У Сумській області розсилали підробні повідомлення про мобілізацію. Повідомлення подібного змісту отримали й мешканці Харківської області. Меседжі з пропозицією з'явитися до військової частини розсилали на мобільні телефони начебто від імені Міністерства оборони України, повідомила прес-служба Військової служби правопорядку Збройних сил.

Докладніше

***

4.12.2018

Знайдено 40 фейкових соцсторінок для поширення паніки у прикордонній з РФ області

У Чернігівській області в соціальних мережах виявили понад 40 фейкових сторінок зі змістом, направленим на поширення панічних настроїв серед місцевих жителів. Про це повідомила прес-служба Чернігівської облдержадміністрації, передає УНН.

«У соціальних мережах виявлено більше 40 фейкових сторінок, зміст яких носив провокаційний характер та був направлений на поширення панічних настроїв серед жителів Чернігівщини», – йдеться в повідомленні.

Крім того, за даними відповідних служб, упродовж останньої доби на територію України не допущено 6 осіб – громадян Російської Федерації.

2Загалом ситуація на кордоні з Росією у межах Чернігівської області є контрольованою», – додали в ОДА.

***

5.12.2018

755 тыс. твитов об Украине. В Vox Ukraine проанализировали работу российской «фабрики троллей» с 2010 года

Начиная с января 2010 года 1369 аккаунтов, связанных с российской «фабрикой троллей», сгенерировали 774 957 твитов об Украине. Об этом говорится в исследовании аналитической платформы Vox Ukraine (InternetUA).

До аннексии Крыма Twitter-боты почти не проявляли активности. Максимальное количество публикаций за 2010-2013 годы зафиксировано в день выборов в Верховную Раду осенью 2012 года – 90.

Более массово аккаунты из выборки начали твитить в конце мая 2014-го: перед президентскими выборами (23 мая) было опубликовано 263 сообщения. В следующие полгода количество твитов не падало меньше отметки 115 в день.

«Настоящий “Twitter-шторм” разразился 18 июля 2014 года, на следующий день после катастрофы MH17. В тот день аккаунты “натвитили” более 44 тыс. сообщений, а на следующий – более 25 тыс. 297 аккаунтов продвигали информацию о якобы виновности Украины в крушении Boeing с помощью хештегов #ПровокацияКиева (22,3 тыс. упоминаний), #КиевСбилБоинг (22,1 тыс.) и #КиевСкажиПравду (21,9 тыс.)», – пишут исследователи.

В Vox Ukraine выяснили, что более чем 200 аккаунтами руководили централизованно. Кроме того, ряд клиент-сервисов были созданы под конкретную задачу – распространение пропаганды.

Помимо автоматически распространявшихся сообщений, аккаунты занимались репостами публикаций российских СМИ, в основном агентств «РИА Новости» и ФАН.

***

5.12.2018

Как украинцам не стать жертвой информационных диверсий

Что такое «сливные бачки» в Интернете? Как информация оттуда попадает в качественные СМИ? И как украинцам не стать жертвой информационных диверсий и распространителей паники во время войны с Россией?

Докладніше

***

6.12.2018

Россия пыталась вмешаться в дебаты о сетевом нейтралитете в США

Российские хакеры и сотрудники «фабрики троллей» оставили 500 тыс. комментариев в социальных сетях во время общественного обсуждения

изменений принципов сетевого нейтралитета в США. Об этом рассказал председатель Федеральной комиссии по связи США (FCC) Аджит Пай, пишет Engadget (InternetUA).

Всего за период обсуждения – с декабря 2017 года по июнь 2018 года – пользователи оставили около 22 млн комментариев в поддержку сетевого нейтралитета, однако лишь 17,4 % из них были настоящими.

В мае 2017 года на сайт FCC, где проводились финальные дебаты на эту тему, была совершена DDoS-атака, однако виновные в ней до сих пор не раскрыты.

Российские власти пока не комментировали заявление FCC.

***

7.12.2018

Фейковые новости и как с ними жить

Битва с дезинформацией превращается в соревнование между платформами распространения новостей и тем, кто этими платформами злоупотребляет.

Докладніше

***

9.12.2018

Пророссийские Twitter-аккаунты причастны к разжиганию протестов во Франции

Сотни связанных с Россией аккаунтов в социальных сетях, в частности, в Twitter, причастны к разжиганию уличных протестов «желтых жилетов», которые потрясли Францию. Об этом сообщает издание The Times.

Докладніше

Спецслужби і технології «соціального контролю»

29.11.2018

Фейковий акаунт Путіна у Twitter, що мав мільйон прихильників, закрили

Соціальна мережа Twitter повідомила про закриття англомовного акаунта, який нібито належав президенту Росії Володимиру Путіну і мав мільйон прихильників, передає УНН.

«Ми зупинили дію @putinRF_eng за імітування на основі достовірних даних, отриманих від російських офіційних осіб», – йдеться в повідомленні.

У Twitter повідомили, що фейковий акаунт Путіна з'явився в 2012 році. Його оформили як офіційний сайт російського президента, а кількість фоловерів налічувала мільйон людей.

Про закриття було оголошено у ніч на 29 листопада. Офіційних коментарів від прес-служби Путіна ще не надходило.

***

28.11.2018

СБУ змусила закарпатського депутата видалити антиукраїнські дописи у Facebook

Працівники Управління СБУ в Закарпатській області оголосили офіційне застереження чинному депутатові Хустської районної ради від «Опозиційного блоку», екс-заступнику голови Хустської РДА за часів режиму Януковича Віталію Дулкаю через його антиукраїнські дописи у Facebook (InternetUA).

Як інформує «Закарпаття онлайн», на депутата до правоохоронних органів поскаржився місцевий активіст Віталій Грегор.

У відповіді силовиків йдеться про те, що вони вжили заходів щодо Віталія Дулкая, а саме – оголосили застереження. Підставою такого рішення стало багаторазове поширення депутатом на своїй особистій сторінці в Facebook публікацій російською мовою із сепаратиською і україномобською тематикою, зокрема про те, що Україна є «территориальным недорозумением», а учасники Революції Гідності – «стадом баранов».

Управління СБУ повідомило, що депутата «офіційно застережено від вчинення будь-яких дій, які можуть призвести до скоєння злочинів проти основ національної безпеки України». Після цього Віталій Дулкай видалив ці дописи.

Окрім того, депутат раніше поширював на своїй сторінці публікації із забороненою комуністичною символікою. На це також поскаржився активіст, проте інформацію за цим зверненням УСБУ скерувала до закарпатської поліції для реагування згідно з підслідністю.

***

28.11.2018

Сотрудники Google протестуют против поисковика с цензурой

Сотрудники Google обнародовали коллективное письмо с требованием закрыть проект создания поисковика поисковой системы Dragonfly со встроенной цензурой (InternetUA).

«Мы выступаем не против Китая, а против технологий, которые поощряют нарушение прав человека... Передача китайскому правительству свободного доступа к пользовательским данным, как того требует китайское законодательство, сделало бы Google соучастником притеснений и нарушений прав человека», – говорится в тексте петиции.

В августе 2018 года несколько крупных изданий сообщили, что Google – поисковик, которой заблокирован в Китае с 2010 года, работает над проектом под кодовым названием Dragonfly. Он предполагает создание поисковой системы со встроенной жесткой цензурой.

Предполагается, что сервис будет автоматически убирать из выдачи ссылки на запросы, заблокированные так называемым «Великим китайским фаерволом», а также выдавать пустую страницу при попытке пользователя ввести запрещенный запрос. Коммерческий старт проекта намечен на 2019 год. Google ждет от властей одобрения на запуск продукта.

***

28.11.2018

Facebook видаляє пости про агресію РФ і напад у Керченській протоці

Facebook видалив низку дописів українських користувачів, що розповідали про ескалацію в Керченській протоці.

Докладніше

***

29.11.2018

ФБР и Google ликвидировали мошенническую схему на миллионы долларов

ФБР, Google и компания по борьбе с ботами White Ops ликвидировали новую рекордную мошенническую схему «3ve» (произносится «Eve» – «канун», «предшествие»). Злоумышленники пытались заработать на фейковых кликах.

Докладніше

***

30.11.2018

Феминистку навсегда удалили из соцсети за одну фразу о мужчинах

Знаменитая писательница Меган Мерфи (Meghan Murphy), известная своими феминистическими настроениями, рассказала, что ее аккаунт в социальной сети Twitter был навсегда удален администрацией. Такое решение сотрудники социальной сети приняли после того, как на странице Меган появился пост с фразой «мужчины – это не женщины». Слова писательницы восприняли как проявление ненависти.

Докладніше

***

2.12.2018

В Бельгии заявили об активности террористов в Telegram

Бельгийские спецслужбы установили, что террористы, которые раньше использовали для своей активности Facebook и Twitter, перешли на использование мессенджера Telegram. Об этом сообщает РИА «Новости» со ссылкой на годовой отчет бельгийской контрразведки VSSE (InternetUA).

Отмечается, что несколько лет назад, в период расширения террористической группировки «Исламское государство», боевики активно распространяли сведения в соцсетях.

«В течение нескольких лет такие компании, как Facebook, Twitter и YouTube, начали реагировать на такие сообщения и быстро удалять их, что привело к частичному перемещению такой пропаганды в более замкнутую среду приложений для обмена сообщениями, таких как Telegram», – говорится в документе.

***

4.12.2018

Марк Цукерберг потерял контроль над Facebook

Член парламента ЕС: Вряд ли можно сомневаться, что монополия над личными данными миллионов людей и новостным потоком создает явную угрозу демократии.

Докладніше

***

3.12.2018

Опубликована переписка убитого саудовского журналиста в WhatsApp

Саудовский журналист Джамаль Хашкуджи обсуждал в личной переписке планы по созданию протестного движения против властей страны, из-за чего его могли убить.

Докладніше

***

3.12.2018

Ирина Фоменко

Крупнейшие производители продвинутых автомобилей «сливают» данные о своих клиентах властям

Китайское правительство использует «подключенные автомобили» (автомобиль с сетевыми возможностями для слежки за гражданами.

Докладніше

***

4.12.2018
Владимир Кондрашов
Депутаты опять пытаются ввести цензуру в Интернете

В Верховной Раде Украины появился очередной законопроект, который под видом борьбы за информационную безопасность продвигает цензуру всемирной паутины для украинцев. Общественные организации уже бьют тревогу.

Докладніше

***

4.12.2018
Спецслужби РФ розсилали віруси в українські суди – СБУ

Співробітники Служби безпеки України блокували спробу російських спецслужб провести масштабну кібератаку на інформаційно-телекомунікаційні системи судової влади України (InternetUA).

Фахівці СБУ зафіксували, що кібератака розпочалася через розсилку електронною поштою заражених вірусом підроблених бухгалтерських документів. Після відкриття файлів на комп'ютери приховано завантажувалось шкідливе програмне забезпечення для несанкціонованого втручання до судових інформаційних систем та викрадення службової інформації.

Співробітники СБ України встановили, що виявлена вірусна програма з'єднувалась з контрольно-командних серверів які мають, зокрема, російські IP-адреси.

За висновками фахівців задум спецслужб РФ полягав у блокуванні сталого функціонування судової інформаційної системи України. Завдяки спільним заходам із Державною судовою адміністрацією та Держспецзв'язку вдалося локалізувати негативні акції кібератаки та попередити її подальший розвиток.

СБ України, як ключова структура із забезпечення національної безпеки, продовжує реалізовувати комплекс необхідних заходів для захисту критичної інформаційної структури держави.

***

5.12.2018
СБУ разоблачила сеть интернет-провокаторов, сеявших панику в соцсетях из-за военного положения

Служба безопасности Украины разоблачила сеть интернет-провокаторов, которые по заданию российских кураторов распространяли панические сообщения относительно введения военного положения в некоторых регионах страны (InternetUA).

Одним из них оказался жителем города Каменское, Днепропетровской области, который писал лживые сообщения о том, якобы после введения военного положения объявили всеобщую мобилизацию.

Кроме того, он распространял фейковые новости о нехватке продуктов в магазинах и очередях на автозаправках, а также рассказывал, якобы для военных нужд изымают машины на еврономерах.

В то же время, провокатор оправдывал Россию, захватившую украинские корабли, следовавшие в Азовское море и распространял публичные призывы к изменению государственной границы.

В настоящее время идут следственные действия – разыскивают провокаторов, сеющих панику. Виновным может грозить до десяти лет тюрьмы.

«Нами уже собран новый список, где около 100 сайтов, которые мы подадим на ближайшее заседание Совета национальной безопасности и обороны, для внесения их в санкционный список и блокирования», – сообщил Александр Климчук, начальник департамента контрразведывательной защиты интересов государства в сфере информбезопасности СБУ.

***

7.12.2018

В Японии запретят использовать оборудование Huawei и ZTE

Правительство Японии планирует запретить закупки для госучреждений оборудования китайских телекоммуникационных компаний Huawei Technologies и ZTE, опасаясь шпионажа со стороны Китая. Об этом сообщает Reuters со ссылкой на источники (InternetUA).

Ранее издание The Wall Street Journal сообщило, что США призывают интернет-провайдеров Германии, Италии и Японии не использовать оборудование Huawei.

По информации издания, Штаты рассматривают вариант предоставления финансовой помощи для развития сетей связи без использования китайского оборудования. Тогда же стало известно об отказе Новой Зеландии в допуске оборудования китайских компаний к строительству 5G-сетей. В августе аналогичное решение с подачи США приняли власти Австралии.

Вашингтон уже несколько лет подозревает Пекин в скрытом шпионаже. Особенно Штаты опасаются угроз от китайских телекоммуникационных компаний в странах, где размещены их военные базы.

***

10.12.2018

Facebook запровадив нові правила проти сексуальних домагань

У нормах спільноти Facebook з’явилися нові правила, які стосуються сексуальних домагань у соцмережі (InternetUA).

Згідно з новими нормами, Facebook забороняє публікувати:

– Контент, в якому вбачаються явні ознаки сексуального домагання: пошук статевих партнерів чи пропозиція статевого акту, переписки з сексуальним підтекстом та зображення оголеного тіла.

– Відео статевого акту та інший порнографічний контент, стриптиз-шоу чи еротичні танці.

– Неявні сексуальні домагання: висловлювання з сексуальним підтекстом. Наприклад фраза «Хочу розважитися сьогодні ввечері», до якої слідували ще кілька натяків на секс. Також заборонений сексуально-провокаційний сленг та натяки з сексуальним підтекстом, наприклад, згадка про пози при статевому акті.

Користувачі Facebook обурилися, що це може обмежувати їхнє право на вільне спілкування і що вони навіть не зможуть обговорювати сексуальну орієнтацію. Однак у компанії відповіли, що немає приводів для хвилювання, повідомив The Verge. Перш ніж Facebook видалить повідомлення сексуального характеру, на нього повинні подати скаргу інші користувачі. Автоматично видалятися нічого не буде. Нова політика стосується контенту, який публікують у групах, особистих сторінках, коментарях та навіть особистих повідомленнях в Messenger.

Проблема захисту даних. DDOS та вірусні атаки

28.11.2018

Эксперты назвали самый безопасный мессенджер

Эксперты компании Artezio проанализировали функционал свыше 20 мессенджеров и назвали Топ-8 самых безопасных мобильных приложений для обмена мгновенными сообщениями. Некоторые достаточно популярные площадки оказались небезопасными для пользователей (InternetUA).

В проведенном аналитическом исследовании эксперты изучили качество шифрования и возможность раскрытия информации, степень защиты личных данных юзеров, функциональность базовых систем хранения и другие составляющие. Всего было исследовано более 30 критериев. Первое место досталось сервису Signal, преимущество которого заключается в двухфакторной идентификации и способе шифрования. Второе место отошло американскому мессенджеру Wickr, который отлично подходит для корпоративного пользования. Третье место у Telegram. Четвертая строчка у приложения Confide.

Пятая позиция досталась Viber, а шестая – Line. На седьмом месте WhatsApp, а замыкает Топ iMessage. Эксперты посоветовали обходить стороной Facebook Messenger. Данная платформа имеет слабую защиту и лишена возможности удалять комментарии.

***

28.11.2018

Владимир Кондрашов

В Украине взялись за создание Национального центра управления сетями

Согласно плану мероприятий по реализации Стратегии кибербезопасности Украины на 2019 год, в следующем году в Украине будет создаваться вторая очередь Национального центра оперативно-технического управления сетями (InternetUA).

Об этом стало известно на заседании Национальной комиссии, осуществляющей госрегулирование в сфере связи и информатизации.

Пунктом 26 плана мероприятий по реализации Стратегии кибербезопасности Украины на 2019 год предусматривается привлечение НКРСИ (по согласию) к созданию Национального центра оперативно-технического управления сетями телекоммуникаций Украины (вторая очередь).

– Стоит отметить, что представители аппарата НКРСИ уже принимают участие в деятельности рабочей группы по решению этого вопроса, – добавили в Нацкомиссии.

Национальная комиссия согласовала без замечаний разработанный в Госспецсвязи проект распоряжения Кабинета Министров Украины «Об утверждении плана мероприятий на 2019 по реализации Стратегии кибербезопасности Украины».

***

28.11.2018

Uber оштрафовали за утечку данных миллионов пользователей

Сервис заказа такси Uber оштрафован в Голландии и Великобритании почти на 1,2 млн долларов за крупную утечку данных, которая произошла в 2016 году (InternetUA).

В Управлении уполномоченного по информационным вопросам (ICO) Великобритании уточнили, что штраф для Uber составит 385 тысяч фунтов стерлингов (490 тысяч долларов). Голландский регулятор намерен взыскать с сервиса 600 тысяч евро (678 тысяч долларов).

Ранее стало известно о том, что злоумышленники украли персональные сведения (имена, адреса электронной почты и телефонные номера), принадлежащие 57 млн пользователей Uber по всему миру. Среди них – 2,7 млн пользователей и 82 тысячи водителей в Великобритании, а также 174 тысяч клиентов из Голландии.

Кроме того, была украдена информация о 7 млн водителей, включая номера 600 тысяч водительских удостоверений в США. В Uber утверждают, что хакерам не удалось получить доступ к номерам социального страхования, данным кредитных карт и маршрутам передвижения клиентов.

Инициаторам атаки заплатили выкуп в размере 100 тысяч долларов, оформив его как премию за раскрытие уязвимостей. По закону компания была обязана сообщать о взломе государственным регуляторам и водителям, чьи номера лицензий попали к преступникам. Вместо этого компания заплатила хакерам, чтобы они удалили данные и хранили молчание.

***

29.11.2018

Восемь приложений из Google Play с миллиардами загрузок оказались вредоносными

Как минимум восемь приложений из Google Play, имеющих в общей сложности более двух миллиардов загрузок, оказались задействованы в демонстрации мошеннических рекламных объявлений.

Докладніше

***

29.11.2018

На українських правозахисників здійснили кібератаки в перший день воєнного стану

На приватні та корпоративні Google-акаунти працівників 28 листопада надійшли повідомлення про те, що вони були атаковані зловмисниками, яких підтримує уряд. Назви організацій не називаються з метою безпеки. Як повідомляє Лабораторія цифрової безпеки, схожі повідомлення українські користувачі масово отримували у 2015-2016 роках, і подальше розслідування показало, що за ними стояли групи хакерів Fancy Bear, яких пов’язують із урядом Російської Федерації (InternetUA).

В компанії Google зазначили, що таких атак як ця зазнають менше ніж 0,1 % користувачів Gmail. Утім, як саме здійснюється така атака не повідомляють, щоб про це не дізнались зловмисники.

Лабораторія цифрової безпеки закликала користувачів, які отримали таке сповіщення, не панікувати, але переглянути свої налаштування безпеки. В першу чергу – перевірити, з яких пристроїв ви залогінені у свій акаунт, а також останні події безпеки у своєму обліковому записі. Лабораторія також готова надати безкоштовні консультації українським журналістам, активістам та правозахисникам.

***

29.11.2018

Додаток-шпигун: У Нацгвардії розповіли, як Кремль «рахує» українських військових

Військових застерігають від використання мобільного додатку «ДМБ Таймер», який може отримувати доступ до всіх можливостей електронного пристрою (InternetUA).

Про це Depo.Харків повідомили у Східному оперативно-територіальному об'єднанні Національної гвардії України.

У ОТО зазначили, що останнім часом серед військовослужбовців-строковиків набув популярності мобільний додаток «ДМБ Таймер».

«Цей додаток, який хлопці встановлюють на свої гаджети, не тільки рахує час до звільнення в запас, а й збирає всю особисту інформацію, яка міститься у телефоні або планшеті, – сказано в повідомленні. – Мобільний додаток "ДМБ Таймер", створений в Росії, при реєстрації нового користувача вимагає вказати повні анкетні дані – рід військ, підрозділ, звання, та пропонує занести до свого списку товаришів по службі різного призову».

Крім того, після встановлення програмного забезпечення на смартфон додаток отримує доступ майже до всіх можливостей електронного пристрою.

***

29.11.2018

Компания Dell пострадала от атаки и вынуждена сбросить пароли пользователей

Представители Dell сообщили о компрометации, произошедшей в начале ноября 2018 года: 9 ноября было обнаружено неавторизованное проникновение в сеть компании, произошедшее в тот же день. Атакующие пытались извлечь информацию о пользователях Dell.com (подчеркивается, что до финансовой информации преступникам добраться не удалось), включая их имена, email-адреса и хешированные пароли (InternetUA).

При этом представители Dell не сообщают, о каком именно алгоритме идет речь. К примеру, если пароли хранились в MD5, взломать их будет очень легко, такие пароли едва ли защищены лучше, чем хранящиеся в формате простого текста.

Пресс-релиз компании гласит, что злоумышленники, вероятно, преуспели и сумели извлечь каике-то данные из сети Dell, хотя пока никаких доказательств этого обнаружено не было (расследование, впрочем, еще продолжается). Не сообщается и точное число пострадавших пользователей, а представители компании подчеркивают, что во время инцидента и вовсе мог не пострадать никто. Тем не менее, представители Dell приняли решение обнулить все пароли пользователей Dell.com, Premier, Global Portal и support.dell.com в качестве меры предосторожности.

Сообщается, что компания уже уведомила о произошедшем правоохранительные органы и привлекла к расследованию инцидента сторонних киберкриминалистов. Предварительно можно предположить, что утечка была не слишком серьезной и могла коснуться только некоторых

пользователей официального сайта, где можно купить продукты Dell и пообщаться на форумах.

***

30.11.2018

Одна из важных функций Android может оказаться вне закона

Функция трекинга, лежащая в основе многих продуктов Google и ОС Android в том числе, противоречит европейскому законодательству о персональных данных. На это обратила внимание группа пользователей из Норвегии, которая подала жалобу в местное ведомство защиты прав потребителей.

Докладніше

***

30.11.2018

Facebook рассматривал возможность продажи данных другим компаниям

Издание The Wall Street Journal опубликовало весьма любопытную информацию, согласно которой внутри Facebook в период с 2012 по 2014 обсуждалась возможность продажи данных подписчиков другим компаниям. В итоге от этой идеи соцсеть решила отказаться (IGate).

По данным журналистов, в Facebook рассматривали данную возможность сразу после неудачного выхода на биржу, который имел место быть в 2012 году. В редакцию издания попали переписки, в которых сотрудники социальной сети обсуждали продажу пользовательской информации, как один из способов увеличения доходов. WSJ не уточняет, на каком уровне происходили эти обсуждения, но если речь идет о топ-менеджменте, это может стать большим ударом по репутации Facebook.

Вопрос о продаже данных поднимался и позже вплоть до 2014 года. В Facebook рассматривали возможность сотрудничества с компаниям, рекламный годовой бюджет которых составляет не менее $250 тысяч.

О письмах стало известно в ходе судебного разбирательства между Facebook и стартапом Six4Three, который создал приложение, отыскивающее в соцсети фотографии пользователей в бикини. Разработчики приложения обратились в суд после того, как Facebook ограничил им доступ к данным, которые считаются открытыми.

Впрочем, в Facebook опровергли информацию, опубликованную The Wall Street Journal: «Как мы неоднократно подчеркивали, предоставленные Six4Three документы являются лишь маленькой частью истории. Этот фрагмент вводит в заблуждение без основного контекста. Мы можем опровергнуть все эти ложные обвинения».

***

2.12.2018

Михаил Сапитон

Хакеры похитили 500 млн аккаунтов отельной сети Starwood. У нее три отеля в Украине

Отельная сеть Starwood, с 2016 года принадлежащая Marriott International, заявила о масштабной утечке (AIN.UA).

Хакеры, которые с 2014 году имели доступ к внутренней сети бронирования номеров, скопировали и попытались удалить записи более чем о 500 млн постояльцев. 8 сентября 2018 года, сотрудники Satrwood опознали вмешательство в фирменные сервисы, перекрыли доступ, а 19 ноября – расшифровали данные обратно.

В Starwood пообещали уведомить всех, кто пострадал в ходе взлома по почте и запустили специальный сайт. Первые письма разослали 30 ноября. Клиентам в США, Канаде и Великобритании также предложат бесплатную годовую подписку на сервис по обнаружению мошеннических операций с данными WebWatcher.

По информации сети, у клиентов утекли имена, адреса, телефонные номера, email-адреса, паспортные данные, информация аккаунта, год рождения, пол, сведения о дате заселения/выселения. В зашифрованном виде утекли и данные кредитных карточек – но о том, имеют ли злоумышленники доступ к ключам шифрования, не сообщается.

Посетители отелей Marriott не пострадали – в компании используется другая система бронирования.

В собственности Starwood находятся сети W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts. В Украине расположены три отеля компании: Sheraton Hotel Kyiv, Aloft Kiev, а также 11 Mirrors, который является частью сети Design Hotel. Всего же сеть Marriott International располагает 6700 объектами в 129 странах мира.

***

2.12.2018

Минобороны Британии подозревает российских журналистов в шпионаже

Высший уровень безопасности был введен для британских военных баз после того, как телевизионная группа российского канала снимала сюжет возле 77-й армейской бригады в графстве Беркшир (InternetUA).

Об этом сообщает издание Mail on Sunday.

77-я армейская бригада занимается кибербезопасностью, работает в соцсетях и даркнете.

21 ноября корреспондент «Первого канала» Тимур Сиразиев и оператор Дмитрий Волков снимали базу из машины, вплотную подъезжали к ее территории, а также были замечены возле солдатских казарм в деревне Эрмитаж. На следующий день в эфире телеканала вышел сюжет о британской «фабрике троллей под Лондоном».

Так, командование баз должно сразу же обращаться в полицию, если рядом с их местом дислокации будут замечены данные журналисты. В предупреждении содержится ориентировка на Сиразиева, который возглавляет бюро «Первого канала» в Лондоне. Военных просят не вступать с журналистом в разговоры.

***

3.12.2018

В Нидерландах хакеры запустили новый вирус SamSam

В Нидерландах из-за нового вируса-вымогателя SamSam за последние месяцы пострадали десятки компаний, пишет NU.nl (InternetUA).

После получения доступа, вирус шифрует данные системы. Для ее разблокировки жертвы должны перевести на счет мошенников от нескольких сотен до сотен тысяч евро.

Сумма убытков от вируса неизвестна. Не разглашаются также названия компаний, которые пострадали от вируса.

В отличие от уже известных вирусов WannaCry и GandCrab, SamSam атакует компьютеры и требует деньги не сразу после заражения.

Вирус старается как можно глубже проникнуть в систему и распространиться, и только потом дает о себе знать. Специалисты по интернет-защите говорят, что это новая тенденция.

***

4.12.2018

Михаил Сапитон

Масштабная утечка в Quora – хакеры похитили данные 100 млн аккаутов

Сервис для обмена знаниями Quora рассказал о масштабной утечке, которая произошла 30 ноября. Хакеры украли данные около 100 млн пользователей. В число похищенных сведений могли входить юзернеймы, email-адреса, IP-адреса, зашифрованные версии паролей, настройки, персонализированные сведения.

Докладніше

***

4.12.2018

Группа киберпреступников Sednit снова атакует пользователей

ESET продолжает исследовать вредоносное программное обеспечение Zebrocy группы киберпреступников Sednit. Целями атак Zebrocy становятся посольства и министерства иностранных дел, расположенные в Центральной Азии, а также в странах Центральной и Восточной Европы.

Докладніше

***

4.12.2018

С помощью интернета заключенные в США шантажировали сотни военнослужащих

Сотни служащих Вооруженных сил США стали жертвами вымогательства со стороны заключенных исправительных учреждений (InternetUA).

Как сообщает Следственное управление ВМС США (Naval Criminal Investigative Service, NCIS), с помощью пособников на «воле» заключенные тюрем Южной и Северной Каролины выискивали военнослужащих на сайтах знакомств и в соцсетях, под вымышленными именами заводили с ними романтические отношения в Сети и обменивались откровенными фотографиями. Затем под видом отца вымышленной личности они связывались с жертвами, заявляли, что «ребенок» несовершеннолетний и обмен с ним откровенными фото является нарушением закона.

В некоторых случаях «отец» соглашался не подавать жалобу, если военнослужащий выплатит ему денежное вознаграждение. Иногда мошенники выдавали себя за сотрудников правоохранительных органов, требующих денег для семьи потерпевшего «ребенка».

Вышеописанный вид мошенничества приобрел большую популярность за последние годы. Как показывает отчет NCIS, подобную схему могут реализовать даже заключенные с ограниченным доступом к Интернету.

«С помощью одного лишь смартфона и нескольких нажатий клавиш заключенные исправительного учреждения Южной Каролины совместно с сообщниками на свободе преследовали сотни людей», – говорится в отчете NCIS.

По данным Следственного управления, жертвами вымогателей стали 442 служащих Армии США, ВВС, ВМС и Корпуса морской пехоты. В общей сложности шантажисты заработали порядка $560 тыс.

***

5.12.2018

Британия обнародовала доказательства продажи личных данных пользователей Facebook

Парламент Великобритании опубликовал 250 страниц внутренней переписки менеджмента Facebook Inc. в качестве доказательства предоставления ряду компаний специального доступа к пользовательским данным с целью их продажи, сообщает Financial Times (InternetUA).

Исходя из личных бесед топ-менеджмента соцсети, включая основателя Facebook Марка Цукерберга, компания внесла в «белые списки» ряд фирм, включая Netflix и Airbnb, для распространения им личных данных пользователей.

В отчете парламентского комитета по цифровым технологиям, культуре, медиа и спорту говорится, что Facebook пытался сделать все возможное, чтобы пользователи не узнали, что их звонки записываются, а текстовые сообщения собирались во время обновления мобильных устройств на системе Android.

Внутренние документы были предоставлены парламентариям Британии в рамках иска компании Six4Three LLC против Facebook.

Пресс-секретарь Facebook заявила, что «документы, собранные для дела, являются лишь частью истории и представлены таким образом, что это вводит в заблуждение без дополнительного контекста».

***

5.12.2018

Eset: наиболее активными в Украине остаются инфицированные сайты, рекламное ПО и майнеры

Eset представляет основные тенденции распространения компьютерных угроз в ноябре 2018 г. Согласно данным, полученным с помощью системы быстрого оповещения Eset LiveGrid, наиболее активным в Украине остается программное обеспечение, которое перенаправляет жертву на инфицированные сайты, рекламное программное обеспечение и угрозы для скрытой добычи криптовалюты.

Докладніше

***

5.12.2018

Пользователей предупредили о новом виде мошенничества в Сети

Консультанты по разблокировке файлов, которые были зашифрованы после атаки программ-вымогателей, могут вступать в сговор с их создателями (InternetUA).

К подобным специалистам обращаются компании, у которых нет резервной копии данных, и при этом не желающие платить злоумышленникам.

Консультанты нередко начинают «работать» заодно с вымогателями. Например, компания Dr. Shifro в 2016 году сообщила о запуске «уникального алгоритма по восстановлению данных», который на самом деле был связан с мошенниками.

По данным экспертов, автор сервиса получает $1300, а специалист – $1000 за восстановление заблокированных файлов.

Согласно исследованию Check Point Research, индустрия программ-вымогателей составляет около $5 млрд, так как эти вирусы не сложно создать, но тяжело обнаружить.

***

7.12.2018

Хакеры используют вредоносное расширение Chrome для атак на университеты

Специалисты команды ASERT компании Netscout раскрыли подробности фишинговой кампании, в рамках которой злоумышленники используют вредоносное расширение для Google Chrome в атаках на университеты в США, а также некоммерческие организации в Азии. Как полагают специалисты, организатором кампании является спонсируемая правительством киберпреступная группировка, судя по оставленным злоумышленникам следам, речь может идти о Северной Корее. Операция, получившая название «Stolen Pencil», активна по меньшей мере с мая 2018 года (InternetUA).

С помощью фишинговых писем злоумышленники заманивали жертв на сайты, имитирующие официальные ресурсы научных организаций, на которых размещался PDF-документ. Для его просмотра пользователю предлагалось загрузить из Chrome Web Store расширение под названием Auto Font Manager (в настоящее время уже удалено из интернет-каталога). С помощью программы злоумышленники могли похищать пароли и файлы cookie.

Как установили исследователи, для осуществления фишинговых атак использовалась инфраструктура, ранее замеченная в кампании по взлому сетей высших учебных заведений через RDP-подключение. Хотя специалисты не связывают операцию «Stolen Pencil» с какой-либо определенной группировкой, по мнению опрошенных изданием ZDNet экспертов, речь может идти о группе Kimsuky (она же Velvet Chollima), известной своими атаками на научные организации.

Судя по всему, злоумышленников пока интересует только кража учетных данных и возможность сохранения доступа к скомпрометированным сетям. Исследователи не нашли свидетельств хищения данных, но не исключают, что в будущем цели злоумышленников могут измениться.

***

10.12.2018

Хакеры взломали сайт Linux.org

Сайт коммьюнити разработчиков Linux вывели из строя из-за нового кодекса поведения Contributor Covenant за авторством трансгендера Коралайн Ада Эмке (Coraline Ada Ehmke).

Докладніше

***

10.12.2018

Уязвимости в распространенных протоколах IoT ставят под угрозу множество предприятий

Компания Trend Micro, без ложной скромности называющая себя «мировым лидером в области решений для кибербезопасности», на днях предупредила о необходимости пересмотреть вопросы обеспечения безопасности в связи с обнаружением существенных конструктивных недостатков в двух популярных протоколах межмашинного взаимодействия (M2M), а также уязвимых реализаций этих протоколов. Речь идет о протоколах Message Queuing Telemetry Transport (MQTT) и Constrained Application Protocol (CoAP). Как сказано в отчете Trend Micro, подготовленном совместно с Миланским политехническим институтом, выявленные слабые места увеличивают риск промышленного шпионажа и атак со стороны злоумышленников (InternetUA).

Всего за четыре месяца исследователи Trend Micro идентифицировали более 200 миллионов сообщений MQTT и более 19 миллионов сообщений CoAP, которые «утекли» через уязвимости. Как утверждается, используя простой поиск по ключевым словам, злоумышленники могут обнаружить эти утечки производственных данных, выявляя информацию об активах, персонале и технологиях, которые могут быть использованы для целенаправленных атак.

В исследовании показано, как злоумышленники могут удаленно контролировать конечные точки IoT или выполнять DoS-атаки, используя проблемы с безопасностью, заложенные при разработке, реализации и развертывании устройств, использующих эти протоколы.

«Проблемы, которые мы обнаружили в двух наиболее распространенных протоколах обмена сообщениями, используемых сегодня устройствами IoT, должны стать для организаций поводом серьезно и всесторонне взглянуть на безопасность своих операционных сред», – так оценил ситуацию Грег Янг (Greg Young), вице-президент Trend Micro по кибербезопасности. По его словам, вышеназванные протоколы были разработаны без учета требований безопасности, но они все чаще встречаются в критически важных средах и приложениях.

***

11.12.2018

Google+ закриють через витік даних 52 млн користувачів

Компанія Google вирішила припинити існування своєї соціальної мережі Google+ у квітні (Espreso.tv). Про це повідомляє Reuters.

«Причиною відповідного рішення стала вже друга помилка в системі конфіденційності, яка відкрила доступ до даних 52,5 млн акаунтів, таких як імена, електронна пошта, стать і вік. При цьому, за твердженням компанії, поки ніяких свідоцтв того, що хтось встиг скористатися цим доступом, немає», – йдеться в повідомленні.

Помилка містилася в оновленому ПО, яке надали для скачування в листопаді. При цьому програмісти змогли усунути неполадку через тиждень. Але сторонні додатки могли запросити імена і вік користувачів, рід діяльності, адреса електронної пошти.

При цьому додатки не отримували фінансових даних, номери паспортів, паролі та іншу інформацію, яку зловмисники могли б використовувати в корисливих цілях. Запит міг бути зроблений навіть в тому випадку, якщо користувач приховав свій профіль з публічного доступу.

Водночас в Google заявили, що не знайшли доказів того, що чиїсь особисті дані були використані третіми особами.

***

11.12.2018

Хакеры рассылают пользователям электронные письма с угрозами

Исследователи из группы ProofPoint обнаружили новую кампанию хакеров-шантажистов. Злоумышленники принуждают жертв скачивать вирус на свой компьютер. Исследование опубликовано в блоге компании (InternetUA).

Киберпреступники рассылают пользователям электронные письма с угрозами. В них они сообщают о взломе компьютера и утверждают, что обладают записями веб-камеры, где юзер смотрит порно.

В качестве доказательства к письму прикрепляется файл, якобы содержащий фрагмент видеозаписи. Однако на самом деле этот zip-архив содержит троян Azorult, крадущий данные с компьютера. Также он загружает известную программу-вымогатель GandCrab.

Эксперты уверены, что такая тактика шантажистов еще опаснее для пользователей, чем прочие. Даже если юзеры не испугаются угроз, они, скорее всего, захотят проверить, действительно ли видео с их участием существует. Это приведет к заражению компьютера двумя различными типами вредоносных программ.

***

11.12.2018

Facebook ждет миллиардный штраф за нарушение приватности

Марка Цукерберга и его компанию сопровождают скандалы, связанные с утечками данных. Теперь нарушениями крупнейшей соцсети занялась Федеральная торговая комиссия США (InternetUA).

Facebook ждет десятизначный штраф, рассказал Fortune профессор Джорджтаунского университета Дэвид Владек. Он знает, о чем говорит: Владек работал в Федеральной торговой комиссии (FTC) и в 2009 году наложил на соцсеть взыскание за безответственное обращение с данными пользователей.

С профессором Джорджтаунского университета согласны другие бывшие члены FTC. Скорее всего, вопрос будут решать в суде.

Власти США пока только тестируют юридические инструменты, которые можно применять в случаях с утечками данных. И полны решимости.

Но проблема в том, что для крупных корпорацию даже такой большой штраф не имеет большого значения. «Руководители Facebook, похоже, давно подсчитали, что штраф, даже на $1 млрд, – это цена быстрого роста, и компания вполне может его себе позволить. Расчет окупился: Facebook не только превратил пользовательские данные в рекламную золотую жилу, но и использовал их, чтобы подавить конкурентов и сохранить монополию», – считает журналист Fortune Джефф Джон Робертс.

В то же время утечки данных через Facebook задевают интересы тысяч человек. У многих из них в США есть простой и бесплатный способ засудить компанию – с помощью чатбота-юриста.

***

11.12.2018

С Госохраны уволили военнослужащего за «слив» информации в соцсети

Управление государственной охраны Украины уволило военнослужащего за «слив» информации с автоматизированной информационно-поисковой системы (АИПС) МВД Украины в соцсети (InternetUA).

Об этом сообщает пресс-служба ведомства.

«В Управлении государственной охраны Украины провели служебное расследование с целью установления факта возможной причастности военнослужащих охранного ведомства к распространению в одной из социальных сетей информации с автоматизированной информационно-поисковой системы (АИПС) Министерства внутренних дел Украины. По результатам служебного расследования из рядов Госохраны уволен один военнослужащий за ненадлежащее исполнение служебных обязанностей», – говорится в сообщении.

Материалы, собранные в ходе служебного расследования, были направлены в Военную прокуратуру Украины с целью приобщения их к материалам уголовного производства.

Ранее главный военный прокурор Украины Анатолий Матиос заявил, что сотрудник УГО продавал ряду лиц закрытую информацию, которую потом политтехнологи использовали для влияния на личную жизнь чиновников и журналистов.

***

11.12.2018
Ирина Фоменко
Ваш смартфон шпионит за вами и продает полученную информацию

Миллион точек на карте обозначают автомагистрали, переулки и велосипедные дорожки, каждая из которых совпадает с маршрутами пользователей мобильных телефонов.

Докладніше

ДОДАТКИ

Додаток 1

3.12.2018
Ирина Фоменко
Бывшие ведущие Top Gear создали социальную сеть для водителей

Социальная сеть, основанная Джереми Кларксоном и другими бывшими ведущими Top Gear, начнет помогать пользователям со страхованием, пишет The Telegraph (InternetUA).

DriveTribe будет предупреждать пользователей о необходимом продлении страховки и направит их в компании, предоставляющие такие услуги. Соцсеть использует данные, собранные с помощью функции MyGarage – она дает возможность пользователям получить сведения об их машинах или тех авто, которые они хотят приобрести.

DriveTribe основана два года назад Джереми Кларксоном, Ричардом Хаммондом и Джеймсом Мэйем, бывшими ведущими Top Gear. Перед запуском соцсеть получила 6,5 млн долларов финансирования от 21st Century Fox и 5,5 млн долларов от инвесторов, в том числе от инвестиционной компании Breyer Capital (один из первых инвесторов Facebook).

В августе Регистрационная палата Великобритании выяснила, что за первые два года компания потеряла 12,5 млн фунтов стерлингов.

DriveTribe будет предлагать членские сделки от коммерческих партнеров на основе данных о владельцах автомобилей. Также DriveTribe будет собирать информацию о пользователях во время того, как они находятся за рулем, например, данные местоположения и манеры вождения.

Среди проектов, запланированных на следующий год, – анализ тональности текста, где будут использоваться такие носимые устройства, как Fitbits и Apple Watches. Девайсы должны «измерять, как чувствуют себя водители», чтобы сделать вождение более «здоровым».

По словам главного исполнительного директора Джонатана Морриса, DriveTribe планирует сотрудничать с компаниями по групповому

використанню автомобилей – пользователи смогут сдавать в аренду собственные транспортные средства.

(вгору)

Додаток 2

3.12.2018
Ирина Фоменко
Skype запускает «живые субтитры» для звонков

Наряду с новостями о получении PowerPoint «живых субтитров» в 2019 году, Microsoft объявила, что аналогичная технология теперь доступна в Skype. Об этом сообщает TechCrunch. Запуск «живых субтитров» приурочили к 3 декабря, Международному дню инвалидов (InternetUA).

Технология позволяет пользователям с плохим слухом читать то, что произносит их собеседник во время аудио- и видеозвонков в Skype. Функцией можно воспользоваться, нажав кнопку (+) и выбрав «включить субтитры».

Опцию можно установить по умолчанию в разделе «Настройки». Для этого кликните на изображения профиля, затем «Настройки», потом «Вызов», затем в разделе «Субтитры во время звонка» нажмите «Показывать субтитры» для всех голосовых и видеозвонков.

После включения «живые субтитры» будут автоматически показываться во время звонка. В Microsoft заявили, что в будущем компания предложит другие варианты просмотра. В частности, Skype скоро позволит пользователям прокручивать надписи на экране и «живые субтитры» в боковом окне.

Microsoft утверждает, что «живые субтитры» на базе ИИ были оптимизированы так, чтобы быть «быстрыми, постоянными и контекстно обновляемыми».

«Живые субтитры» – это один из способов, как Skype пытается облегчить общение своим пользователям. Skype расширил возможности перевода в реальном времени пару лет назад, а в ближайшие недели представит переводы, поддерживающие более 20 языков и диалектов.

При подключении пользователи Skype смогут читать субтитры на выбранном ими языке во время каждого вызова.

Функция надписей на экране и «живых субтитров» доступна в 8 версии Skype на Android (6.0+), планшетах Android, iPhone, iPad, Linux, Mac, Windows и Skype для Windows 10 (версия 14). Разработчики предупреждают, что не на всех устройствах может быть доступна новая функция, поскольку технологию будут внедрять еще на протяжении нескольких недель.

(вгору)

Додаток 3

4.12.2018
Дмитрий Демченко

Что такое Zepeto – самая популярная соцсеть в украинских App Store и Play Market

На первых местах в мировых чартах Play Market и App Store, включая украинские, сейчас находится приложение Zepeto. Несмотря на то, что про него было слышно немного, на данный момент его скачали около миллиона пользователей. Одним из первых на приложение обратило внимание издание Motherboard. Редакция AIN.UA рассказывает, что такое Zepeto (AIN.UA).

Что такое Zepeto

Zepeto – приложение от южнокорейского разработчика SNOW. Это социальная сеть, где пользователи представлены не традиционными профилями, а виртуальными аватарами. Особенность Zepeto заключается в том, что здесь аватары генерируются с помощью технологии распознавания лиц. Затем эти виртуальные фигурки можно кастомизировать: изменять их внешний вид, одежду, дома, а также создавать уникальные приветствия, комбинируя различные фразы с жестами или танцами.

Что нужно делать в приложении

Zepeto ориентирована на общение с другими пользователи, поэтому сервис можно назвать полноценной соцсетью. Пользователи могут подписываться друг на друга – после этого у них появляется возможность обмениваться сообщениями. Есть также вкладка Discover, где можно просматривать незнакомые аватары, новых персонажей можно найти на виртуальной улице.

Пользователи могут также фотографироваться с другими людьми, благодаря функции, похожей на фотокабину. Издание vc.ru отмечает, что именно благодаря этому популярность приложения стала стремительно расти, так как пользователи стали делиться снимками на других платформах. Кроме этого, в приложении можно создавать собственные стикеры со своим аватаром и использовать их при общении с друзьями.

В Zepeto есть виртуальная валюта, за которую пользователи покупают новые движения и приветствия. Заработать виртуальные деньги можно в самом приложении, смотря рекламу или играя в мини-игру Flying Ghost – аналог Flappy Bird.

Будущее соцсети

Zepeto – это по большому счету новая итерация аватар-билдеров и чатов, которые использовали миллениалы много лет назад, считает Motherboard. Издание подчеркивает, что приложение может стать очередной соцсетью-однодневкой, как Allo или Yo. Но у его разработчика есть преимущество – деньги. В этом году SNOW привлек $50 млн, которые планирует потратить на усовершенствование технологий дополненной реальности и распознавания лиц.

(вгору)

Додаток 4

29.11.2018

МІП: Верифіковано сторінки ЗСУ та представництв України за кордоном у Facebook

29 листопада 2018 року, на запит Міністерства інформаційної політики України до Європейського офісу Facebook, було верифіковано офіційні сторінки військ у складі Збройних Сил України та сторінки дипломатичних представництв України за кордоном (Міністерство інформаційної політики).

Як зазначив Міністр інформаційної політики України Юрій Стець, в умовах воєнного стану необхідно користуватися тільки офіційними джерелами інформації та не поширювати факти, не підтверджені офіційними спікерами уповноважених органів влади. «Соціальні медіа будуть використовуватися, щоб дезінформувати населення та посіяти паніку серед українців. Не піддавайтеся – користуйтеся офіційними коментарями», – наголосив Міністр.

Зокрема, було верифіковано такі офіційні сторінки військ у складі Збройних Сил України:

– Військово-морські сили ЗСУ
– Сухопутні війська ЗСУ
– Оперативне командування «Північ»
– Оперативне командування «Захід»
– Оперативне командування «Південь»
– Оперативне командування «Схід»
– Повітряні сили ЗСУ
– Десантно-штурмові війська ЗСУ
– Сили спеціальних операцій ЗСУ

Позначку «верифіковано» також отримали сторінки дипломатичних представництв за кордоном, зокрема, Постійне представництво України при ООН, Постійне представництво України при Раді Європи, посольства та консульства України в 90 країнах Європи, Азії, Америки й Африки.

(вгору)

Додаток 5

4.12.2018
Facebook тайно разрабатывает гибких роботов

В корпорации объясняют, что всего лишь хотят сделать более совершенными свои алгоритмы. Однако журналисты подозревают, что Facebook не ограничивается симуляциями. Для чего соцсети роботы с щупальцами и хоботами – пока неясно (InternetUA).

За последний год Facebook наняла нескольких специалистов по созданию роботов, повторяющих встречающиеся с животном мире механизмы, например, хобот слона, щупальца осьминога или язык ящерицы, сообщает Business Insider.

Среди тех, кого Facebook взял на работу, – инженер-робототехник Джессика Ходжинс. Ранее она работала в Disney, делая движения анимационных персонажей более естественными, отмечает Phys.org.

На данный момент в Facebook есть три вакансии для специалистов из этой области. В первую очередь компанию интересуют люди с опытом работы в биоинженерии, инженерной механике, робототехнике, материаловедении.

Получивших работу пригласят разрабатывать гибких роботов в офисе Facebook в Редмонде, штат Вашингтон.

Для каких целей Facebook нужны гибкие роботы, пока неясно. Ян Лекун, отвечающий за ИИ-направление в компании, пояснял, что корпорация вкладывается в разработку роботов, так как считает эти знания применимыми для совершенствования алгоритмов.

Однако Facebook не просто присматривается к технологии – они действительно собирают гибких роботов, подчеркивает Business Insider. И непохоже, чтобы эти наработки пригодились устройству для звонков со следящей камерой Portal или VR-гарнитур Oculus. О других гаджетах, разрабатываемых в корпорации, широкой публике неизвестно.

Время от времени Facebook объявляет о неожиданных проектах – например, корпорация собиралась создать дронов на солнечной энергии для раздачи интернета в труднодоступных районах. От этой идеи в итоге отказались в пользу разработки телекоммуникационных микроспутников.

(вгору)

Додаток 6

4.12.2018

Вчені пояснили, чому соцмережі корисні для підлітків

Крім депресій, заздрості та залежності, які є частими наслідками життя в Інтернеті, соціальні мережі також надають людям вагому психологічну підтримку.

Дослідницький центр Pew Research опублікував результати масового опитування, за результатами якого 81 % підлітків відчувають зв'язок зі своїми друзями саме завдяки соціальним мережам. Крім того, вони допомагають відчувати підтримку і впевненість (Politeka).

В ході експерименту дослідники Pew Research опитали 743 підлітка у віці від 13 до 17 років. 68 % респондентів сказали, що завдяки соціальним мережам вони відчувають, що у них є люди, які підтримають в складний момент. 69 % відзначили, що соцмережі допомагають їм взаємодіяти з більш широкою і різноманітною групою людей і відчувати себе частиною великого суспільства. Також 69 % підлітків заявили, що використання соціальних мереж робить їх більш впевненими в собі, а 26 % відчувають менше захищеними після взаємодії з іншими людьми в мережі.

На тлі всіх перерахованих вище позитивних ефектів 45 % опитаних підлітків відзначають, що вони відчувають себе пригніченими через все, що відбувається в соціальних мережах. 44 % розповіли, що часто видаляють людей з друзів або скасовують підписку. Основною причиною розірвання зв'язку для

78 % є негатив, який несуть ці люди, а 52 % підкреслили, що ті, з ким вони перестали спілкуватися в онлайні, в тій чи іншій мірі пов'язані зі знущаннями.

43 % підлітків сказали, що вони відчувають тиск і необхідність публікувати те, що буде позитивно їх виділяти в очах інших користувачів, в той час як 37 % відчувають, що вони змушені робити контент, який збирає багато лайків і коментарів.

Також дослідники дізналися, чим цікавляться підлітки в соцмережах. Приблизно в поллвині повідомлень вони розповідають про те, що зробили, в 44 % випадків зачіпають тему сім'ї, в 34 % говорять про емоції, а 10 % пишуть про свої релігійні або політичні переконання.

(вгору)

Додаток 7

2.12.2018

Чому Інтернет є відображенням нашої психіки?

Ще 20 років тому на Інтернет покладали великі надії. Люди думали, що вже через декілька років Інтернет змінить світ на краще. Зараз же ми не в захваті від мережі. Ми звинувачуємо її у всіх бідах, думаємо, що без неї було б набагато краще. Чому наше відношення до технологій так сильно змінилося (InternetUA)?

У 2011 році теоретик соціальних мереж Нейтан Юргенсон (Nathan Jurgenson) придумав термін «цифровий дуалізм» для опису помилки та різниці між реальним та віртуальним світом.

«Ми живемо в онлайн суспільстві. Технології тісно ввійшли у всі аспекти нашого життя: соціальну сферу, тіло і нашу самооцінку» – пише Нейтан у своєму блозі.

Теоретики та інші експерти згодні з тим, що віртуальні та реальні світи – це одне ціле. І саме воно не залежить від того, вважаємо ми його позитивним чи негативним – це все своєрідне вираження себе, вираження нашого психологічного стану. Це наша особистість в самій грубій та благородній формі того, що з нами відбувається.

Міхал Косинскі (Michal Kosinski), соціальний психолог та аналітик Стенфордського університету вважає, що мережа «інтернет» – це наше відображення.

«Нове всесвітнє село неперевершене – воно має всі переваги старого, але водночас підриває старі погляди на належну поведінку у суспільстві», – пише Міхал.

На думку Міхала, це нове село дозволить людям, які були відлюдниками в класичному невеличкому місті, знайти групи, де їх підтримають. Для цього їм не треба виходити з дому. Зараз ми з легкістю можемо знайти наших однодумців та приєднатися до них. Без Інтернету нам би було значно важче знайти таких людей.

«Звинувачувати інтернет у токсичності це все одно що ігнорувати історію», – вважає Косинскі.

Заплутане життя

Тим не менш, розчарування в мережі зростає з кожним днем. Соціальні мережі викликають депресію, фейкові новини впливають на вибори, а дані користувачів незаконним чином отримують інші сторонні компанії, на величезних платформах проводять психологічні експерименти. Винахідник URI, URL, HTTP, HTML, творець всесвітньої павутини Тім Бернерс-Лі (Tim Berners-Lee) називає інтернет «широкомасштабним феноменом проти людства».

Ті ж люди, які колись були впевнені в тому, що зможуть змінити світ за допомогою технологій вважають, що створили зло.

Звинувачувати молоток у руйнівній дії

Насправді, скоріш за все сам по собі Інтернет – це нейтральне явище. На нас впливає саме те що саме ми робимо в інтернеті та які сайти продивляємося. Все залежить лише від нас та від того як ми взаємодіємо всередині мережі. Ми можемо шукати в інтернеті порно, шопінг, новини, мистецтво, благодійність, фільми і т.п. Звинувачувати інтернет в недоліках суспільства те саме, що звинувачувати молоток в його характеристиках ламати речі.

Хоча Facebook та Instagram справді провокують нас на не зовсім хороші речі в житті, але ми не безсильні у цій ситуації. Ми просто слабкі й спокушаємося на всі ті яскраві речі, які існують на просторах Інтернету.

Технолог і філософ Джарон Ланьє (Jaron Lanier) не зареєстрований на таких сайтах як Facebook, Reddit, Twitter або Instagram та дотримується думки, що нам потрібно повидалятися із соцмереж. У своїй останній книзі «Десять аргументів на користь видалення акаунтів в соцмережах» Ланьє пише про те, що інтернет змушує нас відчувати себе погано, оскільки системи спроектовані таким чином, щоб маніпулювати нами, оцінюючи наші зацікавлення, передбачивши бажання, змінюючи нашу поведінку і створюючи можливості для рекламодавців.

Соціальні мережі повинні змусити нас повернутися до них знову і знову, тому технологічні компанії створили інструменти, які збирають про нас дані, а потім дають нам те, в чому ми зацікавлені. Ланьє вважає, що соціальні мережі завдають шкоди нашому здоров'ю та щастю, породжують політичні та соціальні дискусії, віднімають в нас свободу та перетворюють на негідників.

Тому він закликає усіх видалити профілі в соціальних мережах. Якщо ж ми цього не зробимо, що ж, можливо, це просто людська природа – опиратися технологічним змінам та скаржитися на них.

У своїй книзі «Інновації та їх вороги: чому люди противляться новим технологіям» Калстаус Джума (Calestous Juma) написав, що скептицизм стосовно технологічних інновацій – це невіддільна частина людської сутності:

«Спротив новим технологіям лише посилюється, коли люди розуміють, що їх переваги відчують на собі лише невеличка частина суспільства».

Таким чином, можливо, ми розчаровуємося в інтернеті тільки тому, що ми бачимо, як декілька гравців – технологічних гігантів та інфлюенсерів соцмереж отримують від технологій більше переваг, ніж решта, хоча насправді все планувалося зовсім по-іншому.

Контролювати механізм

Дивний новий світ, дуже сильно відрізняється зі світом, які знали наші предки. Інтернет характеризується деякими новими унікальними елементами. Ми обманюємо себе, ностальгуючи по тому часу, коли проводили день з розумом, вважає письменниця Лорен Ойлер (Lauren Oyler).

«Багато моїх колег задумуються над тим, «Що б ми робили, якби не просиджували в Twitter цілими днями?». Ця думка передбачає, що всередині нас ми не такі, що за цим безцільним заняттям ховається щось по справжньому важливе, своєрідний світ, в якому ми виконуємо завдання та відпочиваємо, не оновлюючи стрічку новин кожні п’ять хвилин. Насправді ж… я б витратила весь свій вільний час на перегляд старих альбомів або на балаканину з друзями телефоном. Саме так проводили час наші батьки, коли не було інтернету».

Уникати інтернету це, мабуть, те саме, що проїхатися на коні серед багатолюдного Нью-Йорку після винаходу автомобілю. Це просто незручно та непрактично.

Ми не заручники всесвітньої павутини. Ми просто повинні знайти більш природні шляхи взаємодії з інтернетом. Якщо Facebook змушує вас сумувати, запитайте себе: що я бачу в чужих життях такого, що мені хотілося б змінити у своєму житті?

«В соціальних мережах люди малюють ідеальну картину свого життя. Вони не завжди брешуть про те, що відбувається, але вони не розповідають повної історії», – стверджує Ерін Фогель (Erin Vogel), науковий співробітник Відділення психіатрії в Каліфорнійському університеті Сан-Франциско.

Проблема насправді лежить значно глибше, це явище описували ще у Біблії: ми бажаємо те, що має наш сусід і заздримо далекому нашому розумінню чужому життю.

Люди в трьох частинах

Багато робіт Зігмунда Фройда (Sigmund Freud) критикували, його модель розуму все ж вижила та стала загальноприйнятною. Він говорив про те, що людський розум розділений на три частини: ід, его та суперего. Ід – це інстинктивна та імпульсивна частина нашої сутності, якою ми наділені з дитинства. Ід знаходиться в тісному зв’язку з первинними потребами, які наповнюють вчинки людини енергією, такою як сон, їжа, секс тощо. Его стратегічне, але не моральне. Як і ід, воно хоче максимізувати задоволення, але разом з тим намагається втримати баланс між першочерговими бажаннями та вимогами суспільства. Суперего відповідає за цінності та мораль.

Інтернету властиві елементи, котрі активізують кожні із характеристик Фройда. Дійсно, у мережі існує темний бік (даркнет), де продаються наркотики, зброя та послуги сексуального характеру. Але ж даркнет – це не причина

злочинів або сексуальних домагань. Це просто віртуальне місце для речей, якими люди займаються в реальному світі.

Его в мережі теж представлено непогано. Наші постійні звички та соціальні мережі – лишній тому доказ його влади над нами.

Тепер про суперего. Воно проявляється лише тоді, коли ми намагаємося об'єднатися заради благих намірів в Інтернеті. Наприклад, компанії GoFundMe та KickStarter використовуються для фінансування, лікування, підтримки соціальних проектів тощо.

Нічого нового під сонцем

Все, що з нами відбувається – це вираження людського розуму, що завжди був здатен мріяти про жахливі або ж приємні речі. Що змінилося? Тепер у нас є інструмент, який дозволить записувати суспільну свідомість в його світлих та темних проявах.

Ми не повинні опускати руки через те, що інтернет знищить людство, яким ми його знали, тому що люди ще ніколи не були настільки чудовими. Замість цього ми повинні поставити собі питання, як жити краще за допомогою інструментів та знань, якими ми володіємо на сьогодні, як керувати собою та розвивати навички для духовного та розумового зростання та ще світлішої свідомості.

Можливо, це куди простіше, чим ми гадаємо. Варто лише віднестися до взаємодії з інтернетом як до своєрідної суспільної дії, бачити те, що кожна наша публікація або фото в соцмережах – це запис, який в майбутньому може вплинути на інших. Якщо ми будемо бачити в мережі «інтернет» наше село, наш груповий проект, суспільну платформу, ми перетворимо її в приємне та корисне проводження часу.

(вгору)

Додаток 8

28.11.2018

Міноборони закликає співгромадян не вестися на фейки та довіряти інформації з офіційних джерел

Шановні українці! Міністерство оборони України звертає Вашу увагу, що Російська Федерація у традиційній для себе манері продовжує підвищувати градус ненависті до всього українського, у зв'язку з чим помітно збільшилася кількість російських фейків та вкидів в інформаційному просторі на військову тематику, зокрема, у соціальних мережах та стрічках новин деяких засобів масової інформації (Урядовий портал).

Мета цих фейкових повідомлень, виготовлених спецслужбами Російської Федерації та контрольованою ними «фабрикою тролів», цілком зрозуміла – посіяти панічні настрої серед українців у зв'язку із оголошенням воєнного стану у визначених областях нашої держави.

Зокрема, у деяких ЗМІ та стрічках соцмереж з'являються неіснуючі та відверто абсурдні за своїм змістом нібито «накази, директиви та

розпорядження» від керівництва Міністерства оборони України. Однією з цих нісенітниць є нібито «наказ Міністра оборони України» щодо компенсації нестачі автомобільного транспорту у Збройних Силах за рахунок авто на іноземній реєстрації, власники яких не розмитнили свій автотранспорт.

Міністерство оборони України офіційно повідомляє, що усі ці нібито «офіційні документи» та «накази», які начебто мають підписи військового керівництва Міноборони та Збройних Сил України, не існують та є черговими фейками.

Також Російська Федерація вдається до інших провокаційних інформаційних дій в окремих районах вздовж державного кордону України. Як повідомлялося, 27 листопада жителям Путивльського району Сумської області, що територіально межує з державним кордоном з Російською Федерацією, від імені Міністерства оборони України надходили SMS-повідомлення з пропозицією прибути до найближчої військової частини. Подібні SMS зафіксовано й в інших областях.

Міністерство оборони України повідомляє, що не має жодного відношення до розсилання подібних повідомлень та й ніколи Збройні Сили України не вдавалися до подібних заходів інформування громадян. Натомість є чимало прикладів розсилки спам-повідомлень російсько-окупаційними військами та незаконними збройними формуваннями, що підтримуються Росією на території Донецької та Луганської областей. Тому ця тактика окупанта-агресора вже відома.

Даний російський інформаційний вплив на громадян України є не що інше, як черговий прояв «гібридної» агресії Росії проти нашої держави.

Міноборони України закликає співгромадян не вестися на провокації спецслужб Російської Федерації, перевіряти новини та довіряти лише інформації з офіційних джерел.

(вгору)

Додаток 9

29.11.2018

Фейки та паніка в українському інтернет-просторі: хто в цьому винен

У Сумській області розсилали підробні повідомлення про мобілізацію (InternetUA). Про це – у сюжеті Радіо НВ.

Повідомлення подібного змісту отримали й мешканці Харківської області. Меседжі з пропозицією з’явитися до військової частини розсилали на мобільні телефони начебто від імені Міністерства оборони України, повідомила прес-служба Військової служби правопорядку Збройних сил.

В Україні почне діяти режим воєнного стану. На що це вплине і як житиме країна

Там зазначили, що повідомлення фейкові, а саму ситуацію назвали черговою російською провокацією. Начальник управління комунікацій та преси

Міністерства оборони Олексій Чорнобай закликав громадян не довіряти інформації з неперевірених джерел.

Офіційне першоджерело інформації

Ситуація за останні три доби показала, наскільки українці легко піддаються паніці, заявила співвласник видання Букви, медіаексперт Катерина Рошук.

Люди поширюють інформацію, користуються сайтами із сумнівною репутацією, не перевіривши офіційних джерел. Передові ЗМІ поки що справляються з висвітлення подій в країні, вважає Рошук.

«Нещодавно було дослідження, де перевірялися онлайн-ЗМІ на предмет достовірності, коректності публікацій. Зокрема, там був наступний пункт: якщо ЗМІ посилається на публікації у Facebook неверифікованого акаунту, без синьої галочки, значить ЗМІ чинить неправильно», – розповіла Рошук.

Гнучка політика ЗМІ

Як зазначила головний редактор сайту NV.ua Юлія МакГаффі, громадяни не довіряють ЗМІ, а тому шукають інформацію в інтернеті і нормально сприймають фейки.

«Це може бути наслідком того, що період, коли ЗМІ контролювала партія, був дуже довгим. А от період гласності та перебудови – короткий. На українському ринку дуже легко зайти в певний засіб масової інформації за певну суму і розмістити там інформацію», – зазначила МакГаффі.

Інформаційна війна та ресурси

Україна почала програвати інформаційну війну ще до початку революції, заявив голова комітету з електронної комерції Інтернет-асоціації України Олександр Ольшанський. У Росії більше фінансових ресурсів, які можна вкладати в інформаційну війну. Українським медіа та відомствам залишається тільки казати правду, вважає Ольшанський.

«З плином часу будувати віртуальну реальність стає все дорожчим. На жаль, українські ЗМІ і блогерське середовище в певний момент піддалися на провокацію», – сказав Ольшанський.

У кіберполіції України також попередили про можливе розповсюдження недостовірної інформації в мережі.

(вгору)

Додаток 10

5.12.2018

Как украинцам не стать жертвой информационных диверсий

Что такое «сливные бачки» в Интернете? Как информация оттуда попадает в качественные СМИ? И как украинцам не стать жертвой информационных диверсий и распространителей паники во время войны с Россией (InternetUA)?

Интернет-издание «Тексты» построили глубокую нейросеть и научили ее распознавать манипуляционные новости в информационном потоке. С

помощью этого инструмента «Тексты» подготовили рейтинг так называемых «сливных бачков», или сайтов, которые публикуют манипулятивные новости.

По мнению авторов проекта, такие издания являются благоприятной средой для российской пропаганды в украинском информационном пространстве. Об этом в эфире Радио Донбасс.Реалии рассказал главный редактор интернет-издания «Тексты» Роман Кульчинский.

– Роман, что это за глубокая «нейросеть»? Как вы ее построили?

– Грубо говоря, это искусственный интеллект. Алгоритм, который мы научили определять манипулятивные новости. Когда мы его начинали, примерно прошлой зимой, столкнулись с проблемой, что никто не знает, что такое «фейковые» новости, нет определения. Чистые «фейки», как, например, «распятый мальчик», бывают очень редко. Но есть другие типы, как правило, это манипуляция: есть реальное событие, но делаются неправильные выводы или несколько искажаются.

Чтобы создать методологию, мы собрали редакторов украинских СМИ, которые ежедневно работают с новостями, и определили несколько типов манипуляций. Попросили всех желающих журналистов проклассифицировать по определенной методологии семь тысяч новостей. Это учебная база, на которой мы учили алгоритмы определять тип текста. Алгоритм научился определять два типа, мы прогнали весь массив загруженных новостей из наших более 100 сайтов и создали такой рейтинг.

– За какой период были загружены эти новости?

– Мы качали нон-стопом с конца прошлой зимы и до октября.

– Что это за сайты?

– Мы сначала хотели исследовать российскую пропаганду и вручную составляли список сайтов, где замечали ее или антиукраинскую пропаганду. Таких сайтов собрали около 150 и далее их исследовали. За год исследования часть закрылась, часть изменила название. В финальное опубликованное исследование приняли тех, чей уровень манипуляции был более 25 %, в результате в нашем рейтинге оказались около 100 сайтов, около 20 из них администрируемых и выдаются на временно оккупированных территориях, другие – чисто украинские сайты.

– Посещаемость этих сайтов действительно безумная, как оказалось. Насколько высок процент украинцев заходит на эти сайты? И как вы различаете так называемые нормальные сайты и так называемые «сливных бачков»?

– Человек, который заходит в «УКРНЕТ», не интересуется СМИ, журналистикой, он кликает на какие-то ссылки, ему трудно разобраться, он попал на нормальный сайт или нет.

А между прочим есть простые индикаторы. Первое – если вы читаете что-то очень страшное, о чем вам хочется сразу сообщать еще кому-то, что-то делать, то в большинстве случаев это информационная манипуляция.

Второе – посмотрите, как этот сайт сделан, какая верстка, как он выглядит. Там есть контактные данные, фамилия редакторов, если нет – это, как правило, «сливной бачок».

Что такое «сливные бачки»? В украинских реалиях есть целый пласт сайтов, которые печатают что-то в виде новостей. «Сливные бачки» не проверяют информацию. А ради того, чтобы на них заходили, могут и придумать новость. Эти сайты существуют только для того, чтобы зарабатывать деньги. Они зарабатывают на заказных материалах, но основной их бизнес – публикация какого-то компромата, часто выдуманного, часто истинного – здесь невозможно разобраться. Затем они предлагают человеку, о котором эта публикация, снять ее за деньги. Этот бизнес процветает.

– Вы сказали, что есть несколько факторов, которые отличают «сливной бачок» от качественного. Есть, например, сайт «Украина.ру», он довольно популярен в Украине, там и хорошая верстка, и известные журналисты. Его посещаемость – 2,2 миллиона украинцев в месяц. Это не «сливной бачок», а манипулятивное СМИ?

– Да. Часть сайтов, попавших в наше исследование, администрируемых из России или через оккупированные территории и алгоритм обозначил их с высокой степенью манипулятивности. Они используют очень эмоциональные слова, приемы, эмоционально накручивают людей.

– Какой объем проблемы? Как много украинцев читают информацию из «сливных бачков» или таких специальных манипулятивных СМИ?

– Это сложный вопрос. Точные данные могут знать только Google, но он их не предоставляет. По данным SimilarWeb – организации, которая исследует трафик по своим критериям и на нее ссылаются все рекламодатели – около 50 миллионов визитов в месяц происходит на эти сайты, которые мы исследовали.

Но это не 50 миллионов людей, а именно визитов. Визиты могут считаться по-разному. Например, если вы два раза в день с одного компьютера зашли на сайт, у вас в статистике будет два визита – но это не два человека.

Для сравнения, на «Украинскую правду», которая считается качественным изданием, около 15 миллионов визитов в месяц, по данным SimilarWeb.

Интернет очень сегментирован. Кроме «Украинской правды», есть еще «Новое время», «Лига», «Общественное Радио», Радио Свобода и тому подобное – мы не считали суммарную аудиторию качественных ресурсов. Но мы хотели обратить внимание на то, что очень многие люди читают абсолютно вымышленные новости. А это очень благоприятная среда для российской пропаганды, потому что можно заплатить и запустить что угодно.

– Есть ли какое-то противоядие к подходу «прочитал в интернете»? Если спросить, на каком сайте человек прочитал новость, были ссылки на какие-то источники, на все это не обращается внимания. Это украинская проблема или мировая?

– Мне кажется, это мировая проблема, и мало кто в мире знает, что с этим делать. Есть различные решения, различные методы. Например, наиболее радикально сейчас действует Франция. У них приняли закон, который позволяет за два дня заставить сайт снять информацию, если она не соответствует действительности. Но это в период избирательной кампании. В

Испании очень интересный опыт, там этим занимается не медиарегулятор, не суд, а агентство кибербезопасности, это уже силовой орган.

Читателю с этим бороться очень сложно. Что могут сделать правительственные структуры или гражданское общество? Блокировать такие сайты, смотреть, как финансируется этот сайт. Но это все законодательные инициативы. В наш сложный предвыборный период будет не до этого, тем более, что все политсилы хотят воспользоваться заказными материалами.

Во Франции журналисты работают над тем, чтобы ввести сертификат качества.

– Что это значит?

– Если какое-то издание не манипулирует, не врет, дает информацию взвешенно, на нем будет размещен сертификат, и с этим соглашается все медиасообщество.

В таком направлении надо двигаться украинским медиа: создать общие стандарты для всех и четко говорить, что те, кто придерживается этих стандартов – журналисты, а все остальные – это пираты, флибустьеры, которые зарабатывают деньги на информации.

– Вы проследили интересный путь от неизвестного аккаунта на Facebook к «СМИ сообщают». Много сообщений из этих так называемых «сливных бачков» или каких аккаунтов в социальных сетях могут появиться на тех же авторитетных СМИ, «Украинская правда», «Обозреватель», которые ценят свою репутацию. Как это происходит?

– Я люблю «Обозреватель», но я с ним очень осторожен, они работают как раз на грани.

Любые заказчики понимают, что аудитория и авторитет «сливных бачков» не такая, как в крупных известных СМИ. Поэтому придумываются способы, как перейти в нормальные СМИ. Например, «сливной бачок» пишет какую-то информацию, затем «лидер мнения» с Facebook, грубо говоря, человек, у которого более 5000 подписчиков, пишет об этом у себя на странице. И уже легализует эту ложь, которую может напечатать известное СМИ со ссылкой на этого человека. Это системная проблема, встречающаяся регулярно.

Поэтому нужно договориться со СМИ, мы не ставим информацию с Facebook, мысли с Facebook в ленту новостей. И это очень существенно ограничит возможность манипуляций, которые попадают в приличных СМИ.

Хочу добавить, что эти лидеры мнений, как правило, делают это за деньги. Также есть целый класс политологов, абсолютно респектабельных, которых мы видим на телеэфирах, которые тоже делают это не бесплатно. Им платят не медиа, а кто-то другой, чтобы они выражали определенные тезисы.

(вгору)

Додаток 11

7.12.2018

Фейковые новости и как с ними жить

Битва с дезинформацией превращается в соревнование между платформами распространения новостей и тем, кто этими платформами злоупотребляет (InternetUA).

Публике эпитет «фейковые новости» стал известен благодаря тому, что президент США Дональд Трамп клеймит им любую неприятную для него публикацию, но в основе своей это строгий аналитический термин, которым обозначается преднамеренная дезинформация, представленная в виде рядового новостного репортажа. Именно теме «фейковых новостей» посвящена новая колонка Джозефа Ная, бывшего председателя Национального совета разведслужб США, а ныне – профессора Гарвардского Университета.

Джозеф Най напоминает, что проблема, ставшая сегодня такой актуальной, совсем не нова – еще в 1925 году популярный журнал Harper's Magazine опубликовал статью «Fake news and the public: How the press combats rumor, the market rigger, and the propagandist», посвященную угрозе «фейковых новостей». Однако сегодня, пишет эксперт, две трети взрослых американцев получают значительную часть новостной информации из социальных сетей, которые опираются на бизнес-модель, уязвимую для внешних манипуляций и с автоматизированной системой защиты, которую легко обходят группы, заинтересованные в получении прибыли или в совершении информационных диверсий.

Най отмечает, что коммерческие, общественные, правительственные и (естественно) криминальные группы и организации по всему миру вполне преуспели в инженерном анализе алгоритмов, с помощью которых технические платформы выявляют информационные злоупотребления. «Отдадим должное России, – пишет Най, – ее правительство в числе первых осознало, как превратить социальные сети в оружие и использовать ведущие американские компании против самой Америки».

Из-за того, что читетель перегружен огромным объемом доступной ему информации, людям часто сложно сориентироваться в том, на чем действительно стоит сосредоточить внимание. Внимание, а не информация, – вот тот приз, за который идет борьба. Технологии анализа больших объемов данных и развитие искусственного интеллекта позволяют осуществлять настолько точный таргетинг аудитории, чтобы информация, получаемая людьми, ограничивалась «фильтрующим пузырем» единомышленников.

Автор указывает, что «бесплатность» услуг, предлагаемых социальными сетями, обусловлена моделью окупаемости, в которой информация и внимание пользователей фактически являются товаром, который продается рекламодателям. Именно на это направлены алгоритмы вовлечения и удерживания пользователей, позволяющие предложить им больше рекламы и получить больше доходов от ее размещения.

Най пишет, что волеченность пользователей стимулируют сильные эмоции, – такие как, например, негодование, – а скандальные и недостоверные новости привлекают больше внимания, чем достоверные. Согласно результатам исследований, у таких лживых сообщений на 70 % больше шансов быть

ретвитнутой в Твиттере. Изучение информационного освещения демонстраций в Германии в начале этого года показало, что алгоритм YouTube систематически направлял пользователей именно к экстремистскому контенту, потому что тот вызывал наибольшее количество «кликов» и, соответственно, доходов. Проверка же фактов силами обычных СМИ зачастую не поспевает за немедленной реакцией аудитории, отмечает автор, а временами может даже оказаться контрпродуктивной, так как возвращает внимание читеталя к опровергаемой лжи.

Далее эксперт обращает внимание на то, что используемая социальными медиа модель самоокупаемости может стать оружием как государств, так и негосударственных субъектов. Facebook, например, серьезно критуют за то, что он допускает бесцеремонное использование частной информации его пользователей. Марк Цукерберг признал, что в 2016 году Facebook «не был готов к скоординированным информационным операциям, с которыми мы регулярно сталкиваемся». Однако он настаивает, что компания «многому научилась с тех пор и разработала сложные системы, объединяющие технологии и людей, чтобы препятствовать вмешательству в выборы через наши сервисы».

Эти системы, по словам Цекерберга, включают автоматические программы по поиску и удалению фейковых учетных записей; выявление страниц Facebook, которые распространяют дезинформацию более скрытно, чем это было обычным раньше; публикацию отчетов о количестве выявленных и удаленных фальшивых аккаунтов; проверку гражданства тех, кто размещает политическую рекламу; наем 10 тысяч новых сотрудников для усиления информационной безопасности; улучшение координации с правоохранительными службами и другими компаниями для выявления и пресечения подозрительной деятельности. Тем не менее, замечает Най, проблему по-прежнему нельзя считать решенной.

Най уверен, что информационная «гонка вооружений», в которую вступили социальные медиа и государственные и негосударственные субъекты, которые инвестируют в способы обхода защитных систем, будет продолжаться. Чисто технологические решения, такие как искусственный интеллект, не являются в ней решающим фактором. Фейковые новости распространяются глубже и быстрее, чем настоящие, и это связано с их фундаментальным свойством привлекать большее внимание. Ложную информацию в Twitter ретвитят гораздо больше людей и намного быстрее, чем достоверную информацию, а ее повторение, даже при условии проверки фактов, увеличивает вероятность, что человек примет ее за чистую монету.

Автор считает важным, что целью вбросов часто является не распространение дезинформации, а ухудшение качества информационной среды как таковой. В ходе подготовки к американским президентским выборам в 2016 года российское «Агенство интернет-исследований» из Санкт-Петербурга потратило больше года на создание в социальных сетях десятков аккаунтов, замаскированных под местные американские новостные агенства.

Иногда их публикации благоприятствовали кандидату, но зачастую они работали лишь для того, чтобы создать впечатление хаоса, дискредитировать демократические институты и снизить явку избирателей.

Най напоминает, что когда в 1996 году Конгресс принимал Communications Decency Act, зарождавшиеся сетевые социальные сервисы рассматривались как нейтральные поставщики телекоммуникационных услуг, которые лишь давали возможность пользователям взаимодействовать друг с другом. Но это представление, пишет автор, определенно устарело. Только испытав на себе политическое давление ведущие сеьевые платформы всерьез занялись защитой своих сервисов и взялись бороться с безусловными фейками, включая распространяемые через фабрики ботов.

Однако введение ограничений на свободу слова, которую гарантирует Первая поправка к Конституции США, создает трузноразрешимые на практике проблемы, пишет эксперт. Хотя Первая поправка не распространяется на машины (включая системы искусственного интеллекта) и иностранных субъектов, а деятельность частных компаний не попадает под Первую поправку в принципе, ее действие вполне распространяется на американские маргинальные группы и отдельных лиц, которые могут выступать в качестве посредников для осуществления влияния извне.

В любом случае, замечает Най, ущерб, нанесенный внешними игроками, вполне может оказаться меньше того ущерба, который американцы наносят сами себе. Проблема фейковых новостей и искажение информации реальных источников новостей трудноразрешима, поскольку предполагает согласование нового уровня компромисса между фундаментальными для демократии ценностями. Социальные медиа настороженно относятся к попыткам ограничить их свободу и стремятся избежать введения регулирования их деятельности со стороны законодателей, которые все сильнее критикуют их как за то, что они делают, так и за то, чего они не делают.

В заключение Джозеф Най пишет, что, согласно опыту европейских выборов, журналистские расследования и превентивные меры могут хотя бы частично дать избирателям «прививку» против кампаний по дезинформации. Но битва с фейковыми новостями, скорее всего, еще долго будет оставаться полем игры в кошки-мышки между источниками информации и платформами, которые они используют. Эта борьба, пишет автор, будет постоянным источником «фонового шума» во время выборов по всему миру. «Ценой защиты наших демократий будет постоянная бдительность», – заключает он.

(вгору)

Додаток 12

9.12.2018

Пророссийские Twitter-аккаунты причастны к разжиганию протестов во Франции

Сотни связанных с Россией аккаунтов в социальных сетях, в частности, в Twitter, причастны к разжиганию уличных протестов «желтых жилетов», которые потрясли Францию (InternetUA). Об этом сообщает издание The Times.

Так, сеть аккаунтов распространяла сообщения о беспорядках и насилии во Франции. При этом распространялась дезинформация с акцентом на жестокости французской полиции.

Согласно данным журналистов, с момента начала протестов в прошлом месяце группа из не менее 200 учетных записей публиковала примерно 1600 твитов и ретвитов в день. Большая часть аккаунтов были фейковыми и велись от имени жителей западных стран.

Согласно анализу, проведенному компанией New Knowledge, которая занимается кибербезопасностью, публикации в указанных сотнях аккаунтов были направлены на усиление протестов. В частности, в этих аккаунтах распространялась фейковая информация, проиллюстрированная фотографиями раненых протестующих, которые были сделаны в ходе других акций, не имеющих отношения к событиям во Франции.

Как сообщает агентство Bloomberg, более 600 прокремлевских Twitter-аккаунтов в последнее время начали использовать хэштег #giletsjaunes в поддержку «Желтых жилетов». Указанные аккаунты ранее освещали новости из США и Великобритании, но в последние недели переключились именно на освещение массовых протестов во Франции.

Агентство ссылается на данные Альянса за обеспечение демократии – организации, которая отслеживает деятельность указанных аккаунтов.

Основной тематикой недавних твитов стало то, что французская полиция якобы находится на грани мятежа и готова поддержать протестующих. Указанные заявления не подтверждаются фактами. Сама же информационная кампания напоминает другие, которые ранее запускал Кремль.

Большая часть ссылок в указанных Twitter-аккаунтах ведет на сообщения пропагандистских российских СМИ: таких как Russia Today, Sputnik и немецкое агентство Ruptly (принадлежит RT). Все указанные медиа очень пристально следят за протестами «Желтых жилетов». Представители RT даже объявили, что 12 их журналистов якобы пострадали, освещая события во Франции.

(вгору)

Додаток 13

28.11.2018

Facebook видаляє пости про агресію РФ і напад у Керченській протоці

Facebook видалив низку дописів українських користувачів, що розповідали про ескалацію в Керченській протоці (Espreso.tv).

Про це повідомила «Радіо Свобода».

Як пояснила адміністрація соцмережі, пости українців в день розгляду Верховною Радою питання щодо запровадження воєнного стану в Україні, 26 листопада, видалили через нібито «порушення стандартів спільноти».

«Фейсбук закрив два моїх пости. Я думала, може, ті, де не стримувалася і писала певні негарні слова під час учорашнього засідання ВР, але ж ні. Ці пости стосуються російської агресії проти України. Звісно, я надіслала їх на повторну перевірку», – сказала заступниця гендиректора «Укрінформу» Марина Сингаївська.

Крім того пости з хештегами волонтера Анастасії Тимофієвої видалили через 3 години.

«Я додала два хештеги #RussiaAttacksUkraine #StopRussianAggression. І що ви думаєте? Facebook вирішив видалити мій пост через 3 години. Таке враження, ніби мої два речення дуже сильно травмували репутацію "моєї улюбленої соцмережі". Або ж вони були більш шкідливі, аніж пости ботів і схожих веб-категорій», – розповіла волонтер.

«Інфовійна триває», – сказала керівник програм Центру досліджень визвольного руху Ярина Ясиневич, допис якої про російську агресію також заблокували у Facebook.

У Facebook заблокували також і дві новини. У першій йшлося про напад та захоплення Росією українських суден у нейтральних водах Керченської протоки, де цитувались слова міністра закордонних справ Павла Клімкіна, що це «абсолютно новий рівень провокацій та агресії» і є бажанням Росії «захопити Азовське море».

Інша новина передавала заяву Головного управління розвідки Міністерства оборони України про те, що Росія підтягнула до кордону з Україною 500 своїх бойових літаків тактичної авіації та до 340 вертольотів армійської авіації.

«Я повідомив, що є дивне блокування, яке не має нормальної логіки. І в принципі Facebook достатньо швидко відреагував. Виглядає так, що пости були марковані чомусь як спам. Причин може бути дві. Одна – технічний збій, але мені видалось достатньо дивним те, що три різні публікації, які стосувались Росії, були одночасно заблоковані, і в мене є певні підозри, але підтвердити їх наразі неможливо, бо Facebook не завжди детально пояснює причини блокування», – зазначив медіаюрист Ігор Розкладай.

Міністерство інформаційної політики України вже підготувало скаргу до адміністрації соцмережі. У МІП вважають, що вищезгадане блокування є наслідком «шкідливого використання мережі зацікавленими особами, або наявності системної помилки в алгоритмах оцінки контенту».

(вгору)

Додаток 14

29.11.2018

ФБР и Google ликвидировали мошенническую схему на миллионы долларов

ФБР, Google и компания по борьбе с ботами White Ops ликвидировали новую рекордную мошенническую схему «3ve» (произносится «Eve» – «канун», «предшествие»). Злоумышленники пытались заработать на фейковых кликах.

«3ve» являла собой рассылку ложной рекламы, которая охватила почти 2 млн устройств и задействовала почти 5000 поддельных веб-сайтов. Теперь схему ликвидировали, а 8 лицам выдвинули обвинений: трое были арестованы, еще пять остались на свободе (InternetUA).

Схема представляла собой «очень сложный, постоянно меняющийся лабиринт», говорят эксперты. Все начиналось как небольшая бот-сеть, впервые обнаруженная в 2016 году. Впоследствии она росла. Для заражения пользовательских компьютеров использовались вредоносные пакеты Boaxxe и Kovter. Они попадали на устройство через письма с «ловушкой» или скрытую загрузку.

Злоумышленники создали поддельные сайты и с их помощью собирали с рекламных агентств деньги за клики на рекламу. Потом вредоносные программы «заставляли» устройства пользователей переходить на эти сайты и кликать по рекламе. Таким образом, собирались деньги с рекламщиков.

Схема «3ve» действовала в огромных масштабах: на своем пике она контролировала более миллиона IP-адресов как обычных пользователей, так и корпоративных. Наибольшее количество пострадавших зафиксировано в Северной Америке и Европе. Для сравнения это больше, чем количество широкополосных подписчиков в Ирландии, заявили в Google, подводя итог операции на этой неделе.

Google объединила для операции 16 организаций, среди которых Департамент внутренней безопасности США и Центр ФБР по работе с жалобами на интернет-преступность. Они наблюдали за злоумышленниками несколько месяцев, а потом смогли обрушить схему всего за 18 часов.

(вгору)

Додаток 15

30.11.2018

Феминистку навсегда удалили из соцсети за одну фразу о мужчинах

Знаменитая писательница Меган Мерфи (Meghan Murphy), известная своими феминистическими настроениями, рассказала, что ее аккаунт в социальной сети Twitter был навсегда удален администрацией. Такое решение сотрудники социальной сети приняли после того, как на странице Меган появился пост с фразой «мужчины – это не женщины». Слова писательницы восприняли как проявление ненависти. Все подробности Мерфи подробно описала в авторской колонке для ресурса Quillette (InternetUA).

Меган Мерфи уверена, что ее Twitter-аккаунт администрация социальной сети заблокировали по идеологическим соображениям. Писательница считает, что удаление ее страницы основано на том, что фраза «мужчины – это не женщины» могли задеть чувства транссексуалов.

Этот подход возмущает Мерфи. По словам писательницы-феминистки, такие люди не нуждаются в защите, поэтому удаление ее Twitter-аккаунт – абсолютно несправедливое. «Сегодня это считается ересью, родственной террористическим словам, которые стараются отрицать человечность», – подчеркнула женщина. И добавила, что по итогу этого инцидента она лишилась аккаунта в Twitter, который вела довольно длительное время, большое фан-сообщество и контракт на книгу.

Меган Мерфи считает, что современное общество пытается выглядеть чересчур терпимым. Писательница является ярой сторонницей транс-эксклюзивного радикального феминизма, одна из главных идей которого заключается в следующем: мужчина, ставший женщиной не по рождению, не может состоять в феминистическом сообществе. Участницы такого движения полностью уверены в том, что операции по смене пола были придуманы «мужчинами для мужчин», чтобы усилить патриархат.

(вгору)

Додаток 16

4.12.2018
Марк Цукерберг потерял контроль над Facebook

Член парламента ЕС: Вряд ли можно сомневаться, что монополия над личными данными миллионов людей и новостным потоком создает явную угрозу демократии (InternetUA).

Редакция публикует сокращенный перевод колонки Гая Верхофстадта, бывшего премьер-министра Бельгии, президента Альянса либералов и демократов Европы в Европейском парламенте. Она была опубликована на сайте Project-syndicate.org.

Вряд ли можно сомневаться, что монополия над персональными данными миллионов людей и новостным онлайн-потоком создает явную угрозу демократии. Руководство Фейсбука вновь показывает, что на него нельзя положиться.

Брюссель – когда Марк Цукерберг, генеральный директор и сооснователь Facebook, появился перед Европейским Парламентом в мае, я высказал ему мнение, что он потерял контроль над своей компанией. Но, к моему разочарованию, я не получил прямого ответа ни на один из моих вопросов.

И я не один. Политики со всего мира устали от постоянных попыток Фейсбука уйти от ответственности в погоне за прибылью. Миф о «саморегуляции», который активно продвигали высокооплачиваемые лоббисты, развенчан раз и навсегда. Прошли месяцы после того, как Цукерберг выступил перед Конгрессом США и Европейским парламентом, а самые

неотложные вопросы насчет бизнес-практик Фейсбука так и остались нерешенными.

Действительно ли таргетированное распространение пропаганды через Фейсбук может поставить под угрозу демократические выборы? Руководители соцсети утверждают, что они улучшили защиту конфиденциальности. Но учитывая, что они не смогли обеспечить полноценный внутренний аудит ситуации с Cambridge Analytica по требованию Европейского парламента, то существует риск, что грядущие выборы в Европейский парламент в мае станут объектом для множества иностранных манипуляций (как и выборы Трампа – Ред.).

Несмотря на то, что Фейсбук и многие другие гиганты диджитал-сферы, подписали «кодекс поведения» Европейской Комиссии по вопросам разжигания ненависти и распространении ложной информации, все равно многое нужно еще сделать.

Кодекс поведения слишком слаб и не включает временные рамки, в которых компании должны выполнить свои обязательства. Куда больше ресурсов нужно, чтобы обеспечить выполнение новых Общих правил защиты данных Европейского союза, поэтому эти компании могут не бояться наказаний за неправомерное использование персональных данных в качестве простых бизнес-инструментов.

Европе также не хватает профессиональных следственных и судебных органов, которые способны привлечь высокотехнологичные компании к ответственности. В США Роберт Мюллер, специальный советник по расследованию вмешательства России в выборы 2016 года, вынес десятки обвинительных заключений, добился вынесения ряда приговоров и всячески демонстрировал потребность в уполномоченных прокурорах в делах, которые касаются социальных сетей. Европе нужно наверстать упущенное, сначала назначив специального прокурора для расследования атак недавних выборов, а также через активную борьбу с преступлениями, которые совершаются из-за неправомерного использования данных.

Кроме того, ЕС остро нуждается в развитии эффективного механизма для отслеживания и анализа российских дезинформационных кампаний во всех государствах-членах и на всех языках. Только в таком случае прокуроры и другие правоохранительные органы получат все, что нужно для сбора показаний и обеспечения эффективного противодействия подобным атакам.

В долгосрочной перспективе, однако, есть только один верный способ для устранения угрозы для западной демократии, которую представляют Фейсбук и аналогичные платформы. И это регулирование. Саморегуляция банков не смогла предотвратить финансовый кризис 2008 года, а саморегуляция в диджитал-секторе также не смогла возложить на Фейсбук должный уровень ответственности.

Регулирования техгигантов должно начаться с обновления правил конкуренции, которые касаются монополий на контроль над персональными данными. Также нужны новые нормы, чтобы прозрачность и транспарентность

в алгоритмах, которые обрабатывают информацию, была обеспечена каждым действующим лицом, частным или государственным. Но, в конце концов, мы не должны исключать распад Фейсбука и некоторых других крупных техкомпаний.

В итоге все, что я говорил Цукербергу в мае, по-прежнему актуально: не похоже, что у него остались рычаги контроля над своим детищем. Но даже если остались, нам всем следует задуматься о «более открытом» мире, о котором он говорит.

Просто представьте, что десятки тысяч низкооплачиваемых сотрудников Facebook в Индии или где-нибудь еще тщательно проверяют каждое наше слово, чтобы решить, что является разжиганием ненависти или фейковыми новостями, а что нет.

Как недавно установил журнал The New York Times, Facebook так отчаянно защищает свою бизнес-модель, что запустил теневую PR-кампанию, чтобы распространять ложные антисемитские лозунги якобы от одного из ведущих критиков, финансиста и филантропа Джорджа Сороса. Такое возмутительное поведение позволяет предположить, что Фейсбуку есть, что скрывать. И, как ни странно, парламентский комитет Великобритании изъял внутренние электронные письма компании, которые подтверждают, что руководство Фейсбука знало о злонамеренной активности россиян на их платформе уже с 2014 года.

Вряд ли можно сомневаться, что монополия над персональными данными миллионов людей и новостным онлайн-потоком создает явную угрозу демократии. Руководство Фейсбука вновь показывает, что на него нельзя положиться. И нет никакой причины, почему мы, обычные люди, должны придавать значение обещаниям о чистом и легальном использовании наших данных. Саморегуляция триумфально провалилась. Настало время реальных действий.

(вгору)

Додаток 17

3.12.2018

Опубликована переписка убитого саудовского журналиста в WhatsApp

Саудовский журналист Джамаль Хашкуджи обсуждал в личной переписке планы по созданию протестного движения против властей страны, из-за чего его могли убить. Об этом сообщает телеканал CNN (InternetUA).

Активист из Монреаля Омар Абдулазиз предоставил изданию доступ к сообщениям, фотографиям, аудио- и видеозаписям, которыми он обменивался с Хашкуджи в WhatsApp. Как следует из переписки, журналист был сильно обеспокоен происходящим в стране. «Чем больше жертв он получает, тем больше хочет. Я не удивлюсь, если он станет преследовать даже тех, кто его

поддерживает», – писал Хашкуджи о действиях принца Мухаммада бин Салмана в мае.

Мужчины начали планировать организацию молодежного онлайн-движения, которое привлечет Саудовскую Аравию и наследного принца к ответственности. Проект носил название «Кибер-пчелы» и предполагал создание портала в сети и короткометражных фильмов, где будут показаны нарушения прав человека в стране. Кроме того, активисты собирались разослать участникам движения иностранные сим-карты, чтобы их не могли отследить при написании оппозиционных постов в Twitter. Хашкуджи удалось найти источники финансирования, первоначальный взнос составил 30 тысяч долларов.

В августе Хашкуджи заподозрил, что саудовские власти получили доступ к их переписке. Спустя два месяца его убили.

Абдулазиз подал в суд на компанию из Израиля, которая разработала программное обеспечение, использованное для получения доступа к его мобильному. «Взлом моего телефона сыграл решающую роль в том, что случилось с Джамалем. Чувство вины меня убивает», – сказал Абдулазиз.

(вгору)

Додаток 18

3.12.2018

Ирина Фоменко

Крупнейшие производители продвинутых автомобилей «сливают» данные о своих клиентах властям

Китайское правительство использует «подключенные автомобили» (автомобиль с сетевыми возможностями – Ред.) для слежки за гражданами. Об этом сообщает IoTTechNews (InternetUA).

Согласно отчету Associated Press, в список попали более 200 автопроизводителей, которые предоставляют данные китайским властям – включая Tesla, Volkswagen, BMW, Daimler, Ford, General Motors, Nissan и Mitsubishi.

Автопроизводители утверждают, что они не нарушают национальные законы. Чиновники не отрицают сбор данных, но считают, что для аналитических целей необходимо улучшить общественную безопасность и планирование инфраструктуры.

По мнению некоторых экспертов, сбор данных выходит за рамки стандартных требований. Другие крупные рынки, в том числе США, Европа и Япония, не собирают информацию о гражданах таким образом.

Shanghai Electric Vehicle Public Data Collecting, Monitoring and Research Center имеет дисплей, показывающий точки, которые передвигаются вдоль улиц Шанхая в режиме реального времени. На каждую точку можно нажать, чтобы получить подробную информацию о транспортном средстве вплоть до оставшегося заряда батареи.

Такие данные будут использовать полицейские: чтобы избежать длительных и опасных преследований, сотрудники правоохранительных органов могут захватить преступника, когда автомобиль разряжен, хотя не стоит исключать возможности дистанционного отключения транспортного средства.

То, что для Китая норма и часть повседневной жизни, – интернет-цензура, технология распознавания лиц – для Запада неприемлемо. На сегодняшний день многие теперь задаются вопросом, будут ли автопроизводители продавать полученные данные третьим сторонам.

(вгору)

Додаток 19

4.12.2018
Владимир Кондрашов
Депутаты опять пытаются ввести цензуру в Интернете

В Верховной Раде Украины появился очередной законопроект, который под соусом борьбы за информационную безопасность продвигает цензуру всемирной паутины для украинцев. Общественные организации уже бьют тревогу (InternetUA).

Определить информационную безопасность

Речь идет о законопроекте «О внесении изменений в законы Украины об информационной безопасности» авторства народных депутатов Игоря Котвицкого и Андрея Тетерука. Документ был зарегистрирован в раде 26 ноября и уже предоставлен на рассмотрение во все профильные парламентские комитеты.

Согласно пояснительной записке к законопроекту, он был разработан с целью усовершенствования норм Законов Украины «О национальной безопасности Украины» и «Об информации» касательно введения понятия информационной безопасности и определения содержания обеспечения информационной безопасности.

Информационную безопасность законопроектом предлагается рассматривать как «состояние защищенности жизненно важных интересов человека и гражданина, общества и государства, при котором предотвращается нанесение ущерба из-за неполноты, несвоевременности и недостоверности распространяемой информации, нарушения целостности и доступности информации, несанкционированного оборота информации с ограниченным доступом, а также из-за негативного информационно-психологического воздействия и умышленного причинения негативных последствий применения информационных технологий».

Сам законопроект занимает всего полторы страницы, но менее важным от этого явно не становится.

«Северный ветер» законопроекта

– Благодаря вот таким вот небольшим законопроектам власть вводит нужные ей определения, и в последний момент окажется, что для введения цензуры в сети достаточно собрать эти инициативы в «мозаику» и в нужном месте поставить запятую, чтобы использовать их против граждан, – считает телеком-эксперт, вице-президент УСПП, лидер ГС «Национальная ассамблея Украины» Иван Петухов. По его словам, вместе с законопроектами №9306 («О клевете») и №9275 (о якобы борьбе с российской пропагандой) данный законопроект является очередной попыткой ввести практику досудебной блокировки информационных ресурсов и цензуры неугодных властям СМИ.

Более того, в Украине уже есть действующий закон, который определяет понятие «информационная безопасность». Закон Украины «Об основных принципах развития информационного общества в Украине на 2007-2015 годы», который, кстати, до сих пор не отменен, определяет термин «информационная безопасность» как «состояние защищенности жизненно важных интересов человека, общества и государства, при котором предотвращается нанесения вреда через: неполноту, несвоевременность и недостоверность информации; негативное информационное влияние; негативные последствия применения информационных технологий; несанкционированное распространение, использование и нарушение целостности, конфиденциальности и доступности информации».

По словам эксперта, «ветер» законопроекта № 9340 явно «дует с севера»:

– Не знаю, откуда точно дует этот ветер – из Северной Кореи или из Российской Федерации – следы можно найти и там, и там.

Иван Михайлович отмечает, что использованный в законопроекте термин «негативное информационно-психологическое воздействие» (НИПВ) – отсылает к работам ученых из России, которые готовили аналогичные законопроекты так называемому «великому пу» для «защиты соотечественников». Кроме того, этот и ряд других определений в законопроекте № 9340 выписаны настолько нечетко (термин «негативное информационно-психологическое воздействие» вообще должен быть предварительно исследован), что предполагают множество трактовок и, следовательно, развязывают властям руки в деле цензуры:

– Введение НИПВ в определение термина «информационная безопасность» словами «информационно-психологическое воздействие» без понимания того, что это такое, даст возможность свободно трактовать ситуацию с воздействием на сознание, перенося удар не на технологии деструктивных идеологий и иные негативные информационно-психологические воздействия, а на СМИ, Интернет, социальные сети и т.д. Законопроект уже не первый за достаточно короткое время наталкивает на мысль о подготовке властями внедрения авторитарных механизмов влияния на общество. Разница между этим и другими подобными проектами лишь в том, что раньше подобные законопроекты подавали БПП, а теперь отметился «Народный фронт».

(вгору)

Додаток 20

29.11.2018

Восемь приложений из Google Play с миллиардами загрузок оказались вредоносными

Как минимум восемь приложений из Google Play, имеющих в общей сложности более двух миллиардов загрузок, оказались задействованы в демонстрации мошеннических рекламных объявлений. Об этом пишет BuzzFeed News со ссылкой на исследователей в области компьютерной безопасности фирмы Kochava. Семь из них принадлежат популярной китайской компании Cheetah Mobile, а одно – стартапу Kika Tech, базирующемуся в Кремниевой долине (InternetUA).

По словам экспертов, узнавших о деструктивной деятельности размещенных в Google Play приложений, те занимались отслеживанием действий пользователей инфицированных устройств. Это было частью кампании по продвижению приложений сторонних разработчиков, за каждую установку которых Cheetah Mobile и Kika Tech получали от 0,5 до 3 долларов. А чтобы доказать факт установки, программы, задействованные в схеме, незаконно фиксировали нажатия пользователей на экран.

Приложения, которые уличили в мошеннической схеме

– Clean Master;
– CM File Manager;
– CM Launcher 3D;
– Security Master;
– Battery Doctor;
– CM Locker;
– Cheetah Keyboard.

Последнее приложение из списка, помимо отслеживания действий пользователей на устройстве, фиксировало нажатия на клавиатуру, отправляя полученные данные на сервера разработчиков. Впоследствии эта информация могла использоваться для формирования релевантных рекламных объявлений и повышения заработка создателей. А, учитывая колоссальную аудиторию пользователей приложений Cheetah и Kika, вероятный доход их создателей от реализации мошеннических схем, может исчисляться миллиардами долларов.

Google со своей стороны пообещала, что расследует ситуацию и вынесет свой вердикт. Тем не менее, к настоящему моменту компания удалила только два приложения, сохранив за остальными право размещения в Google Play за отсутствием должного количества доказательств незаконной деятельности. Чем это закончится в конечном итоге, остается только догадываться.

(вгору)

Додаток 21

30.11.2018

Одна из важных функций Android может оказаться вне закона

Функция трекинга, лежащая в основе многих продуктов Google и ОС Android в том числе, противоречит европейскому законодательству о персональных данных. На это обратила внимание группа пользователей из Норвегии, которая подала жалобу в местное ведомство защиты прав потребителей. По их мнению, отслеживая перемещения пользователей при помощи фирменных сервисов, поисковый гигант нарушает их конфиденциальность и право на свободу передвижений (InternetUA).

«[У пользователей Android] отсутствует реальная возможность отключить функцию «История местоположений», – следует из содержания жалобы. – Пользователи могут только приостановить ее, если заведут учетную запись Google. Но и тогда они получат абстрактные предупреждения о том, что ограничение [функции по отслеживанию их местоположения] приведет к нарушению работы других функций ОС Android».

Google следит за вами

Но, принуждая пользователей играть по своим правилам, Google действует вразрез с сразу с массой нормативно-правовых актов. Фактически, поисковый гигант не оставляет им выбора, указывая на единственно верный вариант настроек геолокационных данных. Таким образом компания не только противоречит GDPR (Европейскому регламенту по защите данных), но и закону о защите прав потребителей, поскольку, по сути, навязывает им дополнительные услуги по предоставлению доступа к другим своим сервисам.

Если действия Google получат негативную оценку в Норвегии, у компании могут быть серьезные проблемы и на территории остальной Европы. Например, недавно поисковый гигант уже ответил перед законом за навязывание своих приложений производителям смартфонов, заплатив за нарушение законодательства 5 миллиардов долларов. Кроме того, то событие повлекло за собой пересмотр модели распространения фирменного ПО Google, которое стало платным для всех вендоров без исключения.

(вгору)

Додаток 22

4.12.2018

Михаил Сапитон

Масштабная утечка в Quora – хакеры похитили данные 100 млн аккаутов

Сервис для обмена знаниями Quora рассказал о масштабной утечке, которая произошла 30 ноября. Хакеры украли данные около 100 млн пользователей. В число похищенных сведений могли входить юзернеймы, email-адреса, IP-адреса, зашифрованные версии паролей, настройки, персонализированные сведения (AIN.UA).

При импорте профиля из другой социальной сети, злоумышленники могли получить информацию о списке контактов, интересах и демографической сводке. Токены для доступа к соцсетям уже перевели в нерабочее состояние. Наконец, в список скомпрометированной информации могла попасть публичная активность на сайте: запросы, голоса на ответах, сообщения, черновики. Сообщается, что анонимные вопросы не находятся под угрозой.

Пострадавшим разослали email-сообщения. Их также автоматически разлогинили из сервиса, а пароли – обнулили. В письме сообщается, что компания проводит внутреннее расследование, уведомила правоохранительные органы и работает над улучшением ИБ-систем.

Что делать, если у вас профиль на Quora?

Во-первых, пароль на Quora необходимо обновить. Во-вторых, специалисты Quora рекомендуют не использовать один и тот же пароль повторно на нескольких сайтах, поэтому если старый пароль сервиса использовался на других сайтах – обновите пароли и там.

По состоянию на 2015 год глава Quora Адам Динджело заявлял, что у сервиса около 200 млн активных пользователей ежемесячно.

(вгору)

Додаток 23

4.12.2018

Группа киберпреступников Sednit снова атакует пользователей

ESET продолжает исследовать вредоносное программное обеспечение Zebrocy группы киберпреступников Sednit. Целями атак Zebrocy становятся посольства и министерства иностранных дел, расположенные в Центральной Азии, а также в странах Центральной и Восточной Европы. Для распространения этой угрозы, как и ранее, группа Sednit использует фишинговые электронные письма (Компьютерное Обозрение).

Занимаясь преступной активностью по меньшей мере с 2004 года, кибершпионы Sednit осуществляют сложные атаки, направленные на похищение конфиденциальной информации. В частности, группа причастна к атакам на глобальную телевизионную сеть TV5Monde, Всемирное антидопинговое агентство (WADA), а также другие организации.

Для этого кибершпионы Sednit применяют разнообразный набор инструментов. Одним из таких является вредоносное программное обеспечение Zebrocy, которое киберпреступники активно используют в течение последних двух лет.

В августе операторы Sednit развернули два новых компоненты Zebrocy, а активность угрозы возросла. Это вредоносное программное обеспечение состоит из загрузчиков MSIL и Delphi, дроппер Delphi и бэкдоров. Пока загрузчики и Дроппер проводят разведку, бэкдоры активно следят за целью. Новые компоненты используют необычный способ перехвата собранной

информации с помощью протоколов, связанных с почтовыми службами, такими как SMTP и POP3.

Еще раньше специалисты ESET обнаружили сходство между Zebrocy и другими вредоносными программами группы Sednit. Также исследователи ESET зафиксировали факт загрузки угрозой Zebrocy флагманского бэкдора Sednit – XAgent. Однако обнаруженные ошибки при анализе бинарных файлов компонентов Zebrocy указывают на разный уровень опыта в разработке этого набора инструментов. Хотя Sednit управляет этим вредоносным программным обеспечением, специалисты ESET уверены, что разрабатываются они не этой группой, а другой менее опытной командой.

При этом компоненты Zebrocy являются важным дополнением к набору инструментов Sednit. В частности, исследователи ESET заметили рост использования вредоносного программного обеспечения Zebrocy по сравнению с другими инструментами Sednit.

(вгору)

Додаток 24

5.12.2018

Eset: наиболее активными в Украине остаются инфицированные сайты, рекламное ПО и майнеры

Eset представляет основные тенденции распространения компьютерных угроз в ноябре 2018 г. Согласно данным, полученным с помощью системы быстрого оповещения Eset LiveGrid, наиболее активным в Украине остается программное обеспечение, которое перенаправляет жертву на инфицированные сайты, рекламное программное обеспечение и угрозы для скрытой добычи криптовалюты (Компьютерное Обозрение).

Лидером украинского рейтинга вредоносных программ в ноябре стала угроза SMB/Exploit.DoublePulsar (9,15 %), которая предотвращает использованию уязвимых систем вредоносным программным обеспечением Win32/Exploit.CVE-2017-0147.A и Win32/Filecoder.WannaCryptor.

Вторую позицию заняла угроза HTML/ScrInject (5,35 %). Она перенаправляла пользователей на ресурсы с вредоносным программным обеспечением, а его код, как правило, был встроен в HTML-страницы. Подобный функционал имеет угроза HTML/Refresh (1,8 %), которая также вошла в рейтинг.

Замыкает тройку самых активных программ угроза Win32/MediaGet (4,7 %). Вредоносная программа после попадания на компьютер жертвы могла устанавливать расширения браузера, добавлять файлы для запуска во время загрузки системы и проникать в другие процессы устройства. Киберпреступники часто использовали угрозу для загрузки вредоносных приложений, например, рекламного программного обеспечения.

Кроме этого, активным оставалось и программное обеспечение, предназначенное для показа рекламных сообщений. Например,

распространенная угроза Win32/Adware.FileTour (4,12 %) после попадания на компьютер жертвы вместе с бесплатными программами показывала рекламные баннеры и всплывающие рекламные сообщения в браузерах. В топ-10 также попало такое рекламное программное обеспечение, как JS/Adware.Agent.AA (3,85 %) и Win32/Adware.HiRu (1,5 %).

Одну из последних позиций заняла угроза JS/CoinMiner (4,04 %). Эта троянская программа использует аппаратные ресурсы зараженного компьютера для скрытого добычи криптовалюты. Еще одной популярной угрозой с подобным функционалом является Win64/CoinMiner (1,31 %), которая была распространена в Украине в течение ноября.

(вгору)

Додаток 25

10.12.2018
Хакеры взломали сайт Linux.org

Сайт коммьюнити разработчиков Linux вывели из строя из-за нового кодекса поведения Contributor Covenant за авторством трансгендера Коралайн Ада Эмке (Coraline Ada Ehmke) (InternetUA).

Масштабный дефейс

Злоумышленники вывели из строя официальный сайт Linux.org, подменив его содержимое. Посетители ресурса вместо привычного контента видели на экране неприличные изображения и различные нецензурные надписи, а также высказывания против ряда разработчиков и скриншоты других сайтов. Инфраструктура Linux.org не пострадала: хакеры ограничились перенаправлением трафика на другой сервер путем подмены данных в DNS.

Отметим, что Linux.org – это сайт коммьюнити пользователей и разработчиков Linux. Официальный портал операционной системы носит имя Linux.com, и целью хакеров он не был.

Как сообщил администратор ресурса Linux.org, у преступников был доступ к аккаунту владельца домена у регистратора Network Solutions. Через сервис Whois они получили все данные о владельце, в том числе и адрес его электронной почты в сервисе Yahoo. Последний был скомпрометирован еще в 2013 году, и тогда хакеры завладели паролями и другими сведениями о 3 млрд учетных записях.

Причина взлома

Истинная причина взлома пока устанавливается, но представители Linux.org связывают его с недавними изменениями на сайте и в структуре его руководства. В 2017 г. руководство ресурса полностью сменилось, и был удален весь ранее размещенный контент.

Хакеры, стоявшие за взломом портала, прямо на главной странице Linux.org высказали свой протест относительно принятой осенью 2018 г. разработчиками ядра Linux новой редакции кодекса поведения Code of Conduct. Это своего рода инструкция по решению возникающих между разработчиками

проблем и конфликтных ситуаций, и изначально он представлял собой лишь краткий список рекомендаций. Новая версия документа базируется на более серьезном кодексе Contributor Covenant, применяемом, в том числе, разработчики GitLab, Ruby, Kubernetes и ряда других проектов с открытым исходным кодом.

В число авторов Contributor Covenant входит и трансгендерный разработчик и юрист Коралайн Ада Эмке (Coraline Ada Ehmke). Взломавшие Linux.org хакеры разместили на главной странице сайта его персональные данные, включая домашний адрес и номер социального страхования. Преступники назвали девелопера «врагом номер один».

Кто виноват

Как сообщает издание Vice Motherboard, ответственность за взлом взял на себя хакер под псевдонимом kitlol5. В своем микроблоге в Twitter он выложил скриншот, подтверждающий наличие у него доступа к настройкам домена Linux.org и вместе с ним и таких сайтов, как Linuxonline.com, Linuxonline.net, Linuxonline.org и Linuxhq.com. Действовал ли он один или в группе хакеров, остается неизвестным.

По состоянию на 10 декабря 2018 г. работа портала Linux.org полностью восстановлена. Добавим также, что не только сайты, посвященные Linux, но и сама ОС Linux не может похвастаться совершенной системой защиты. К примеру, в мае 2018 г. стало известно об уязвимости CVE 2018-8718 в ядре Linux версии от 3.4 и до 4.15, позволяющей локальному пользователю повышать свои права на ПК и запускать любой код, включая вредоносный.

Последняя на сегодняшний день стабильная версия ядра Linux с индексом 4.19 вышла 8 декабря 2018 г. О наличии или отсутствии в ней этой уязвимости не сообщается.

(вгору)

Додаток 26

11.12.2018
Ирина Фоменко
Ваш смартфон шпионит за вами и продает полученную информацию

Миллион точек на карте обозначают автомагистрали, переулки и велосипедные дорожки, каждая из которых совпадает с маршрутами пользователей мобильных телефонов, пишет The New York Times (InternetUA).

Один путь показывает, как человек ездил с мэром Нью-Йорка днем и вернулся на Лонг-Айленд ночью. Другой – что пользователь вышел из дома в северной части штата Нью-Йорк в 7 часов утра и отправился в среднюю школу, оставаясь там до позднего вечера каждый день. И только один человек совершает такую поездку: Лиза Магрин, 46-летняя учительница математики. И ее смартфон всегда с ней.

Приложение на устройстве собирало информацию о ее местонахождении каждые две секунды, которая затем продавалась без ее ведома. The New York

Times проверили базу данных более миллиона телефонов в районе Нью-Йорка и обнаружили, что этот человек – Лиза Магрин.

Приложение отслеживало, когда она ходила на встречу с Weight Watchers, посещала дерматолога, гуляла с собакой и как долго она находилась в доме своего бывшего парня. Эта информация встревожила ее.

«Это как раз тот случай, когда вы не хотите, чтобы люди узнали ваши интимные подробности», – прокомментировала Магрин.

Как и большинство потребителей, Магрин знала, что приложения могут отслеживать геолокацию пользователей. Но поскольку смартфоны стали повсеместными, а технологии – более точными, индустрия слежки за повседневными привычками людей распространилась и стала более навязчивой.

Согласно данным The New York Times, не менее 75 компаний получают анонимные точные данные о местонахождении из приложений, пользователи которых позволяют службам определения геолокации получать местные новости, погоду и другую информацию. Некоторые предприятия утверждают, что отслеживают до 200 миллионов мобильных устройств в Соединенных Штатах – около половины тех, которые использовались в прошлом году.

База данных, проверенная The New York Times, показывает удивительные подробности маршрутов людей с точностью до нескольких ярдов, а в некоторых случаях обновляется более 14 000 раз в день.

Эти компании продают, используют или анализируют данные для угоды рекламодателям, ретейлам и даже хедж-фондам, ищущих информацию о поведении потребителей. Рынок объема продаж рекламы, ориентированной на геолокацию, в этом году оценивается в 21 млрд долларов.

IBM вошла в индустрию, купив приложение Weather Channel. Социальная сеть Foursquare переделана в локационную маркетинговую компанию. Инвесторами подобных стартапов стали Goldman Sachs и соучредитель PayPal Питер Тиль.

Интерес для компаний представляет модель поведения потребителя, а не его личность. Информация, которую собирают приложения, связана не с чьим-либо именем или номером телефона, а с уникальным идентификатором. Но те, кто имеет доступ к необработанным данным, включая сотрудников или клиентов, могут по-прежнему идентифицировать человека без его согласия. Например, они могли определить личность пользователя, проверив, где он живет: отслеживать геолокацию по ночам, а потом через публичную информацию идентифицировать его.

Многие компании, связанные с определением местоположения, утверждают, что, когда пользователи активируют службы геолокации, то сбор данных с их стороны является честным. Но, как выяснили в The New York Times, объяснения, которые люди видят, когда их просят дать разрешение, часто бывают неполными или вводящими в заблуждение. Приложение может сообщить пользователям, что предоставление доступа к их местоположению

поможет им получить информацию о трафике, но не упомянуть, что данные будут переданы и проданы.

«Информация о геолокации может раскрыть некоторые из самых интимных деталей жизни человека – посещали ли вы психиатра или встречи анонимных алкоголиков. Неправильно оставлять потребителей неосведомленными, как продают и передают их данные», – прокомментировал сенатор Рон Виден.

Мобильные устройства наблюдения

Индустрия отслеживания геолокации через смартфоны была основана как способ кастомизации приложений и целевой рекламы для близлежащих предприятий, но превратилась в машину для сбора и анализа данных.

Ретейлы обращаются к компаниям, чтобы рассказать о своих клиентах и конкурентах. В прошлом году на веб-семинаре руководитель GroundTruth Элина Гринштейн определила путь гипотетического потребителя от дома до работы, чтобы показать потенциальным клиентам, как отслеживание может выявить предпочтения человека. Например, кто-то может искать в Интернете полезные рецепты, но GroundTruth видит, что человек часто ест в ресторанах быстрого питания.

«Мы стремимся понять, какой человек, исходя из того, где он был и куда идет, чтобы повлиять на его дальнейшие действия», – заявила Гринштейн.

Финансовые фирмы могут использовать эту информацию для принятия инвестиционных решений до того, как компания отчитается о доходах, например, проверив, работают ли люди больше на производстве или ходят в ретейлы.

Медицинские учреждения относятся к числу наиболее привлекательных, но проблемных областей для отслеживания. Предприятие Tell All Digital, клиент компании, специализирующейся на определении местоположения, рекламирует адвокатов по травмам в отделениях неотложной помощи.

Тюрьмы, школы, военная база и атомная электростанция - даже места преступления – появились в базе данных The New York Times. Один человек, возможно, детектив, прибыл на место ночного убийства в Манхэттене, а затем провел время в близлежащей больнице, неоднократно возвращаясь в местный полицейский участок.

Две фирмы, занимающиеся отслеживанием геолокации, Fysical и SafeGraph, обозначили на карте людей, присутствовавших на инаугурации президента 2017 года. На карте Fysical ярко-красная точка около Капитолия указала на общее местонахождение президента Трампа и окружающих его людей. Генеральный директор Fysical заявил, что данные, которые использовала фирма, были анонимными.

Более 1000 популярных приложений содержат код обмена информацией о позиционировании от таких компаний. Установлено, что в системе Android от Google имеется около 1200 приложений с таким кодом, по сравнению с около 200 на Apple iOS.

Самой преуспевающей в этом плане компанией оказалась Reveal Mobile, у которой был код для определения местоположения в более чем 500 приложениях, в том числе во многих новостных. В Reveal заявили, что предприятие помогает разработчикам приложений зарабатывать на рекламе, а потребители таким образом получают бесплатные услуги.

The New York Times протестировали 20 приложений, большинство из которых были помечены исследователями и инсайдерами отрасли как те, что потенциально обмениваются данными. 17 из них отправили точную широту и долготу пользователей примерно 70 предприятиям. Данные о местоположении из WeatherBug на iOS получили 40 компаний.

WeatherBug, принадлежащий GroundTruth, запрашивает у пользователей разрешение на сбор информации о их местонахождении и сообщает им, что эта информация будет использоваться для персонализации рекламы.

The New York Times также идентифицировали более 25 других компаний, которые сообщили в маркетинговых материалах или интервью о продаже данных о местоположении. По словам исследователя компьютерной безопасности и конфиденциальности Сержа Эгельмана, распространение этой информации поднимает вопросы о том, насколько безопасно она обрабатывается и является ли уязвимой для взлома.

«На самом деле нет никаких последствий для компаний, которые не защищают данные, кроме негативных отзывов в прессе», – прокомментировал Серж.

Вопрос осведомленности

Как утверждают в компаниях, использующих данные о местоположении, люди соглашаются делиться своей информацией в обмен на индивидуальные услуги, вознаграждения и скидки. «Вы получаете эти услуги бесплатно, потому что рекламодатели помогают монетизировать и оплачивать их», – заявил исполнительный директор Kiip Брайан Вонг.

Легко делиться информацией, не осознавая этого. Из 17 приложений только три на iOS и одно на Android сообщили пользователям во время получения разрешения, что информация может использоваться для рекламы. GasBuddy, идентифицирующее близлежащие заправки, указало, что данные могут также использоваться для «анализа тенденций в отрасли».

Более типичным было спортивное приложение theScore: когда пользователю предлагается предоставить доступ к своему местоположению, в разрешении указывается, что данные помогут «рекомендовать местные команды и игроков, которые имеют к вам отношение». Приложение передавало точные координаты 16 рекламным и локационным компаниям.

Представитель TheScore заявил, что стиль разрешения был задуман только как «быстрое введение в некоторые ключевые функции продукта» а полное использование данных описано в политике конфиденциальности приложения.

Приложение Weather Channel, принадлежащее IBM, сообщает пользователям, что информация о местоположении позволит им получать персонализированные местные сводки погоды.

Даже инсайдеры отрасли признают, что многие люди либо не читают политику конфиденциальности, либо не понимают смысл текста. В политиках конфиденциальности приложений, которые направляют информацию о местоположении, указывается, что данные используются для анализа рынка или просто передаются в коммерческих целях.

Sense360, например, засекречивает данные в пределах 1 000 футов вокруг приблизительного местоположения устройства. Factual собирает данные от дома потребителя, но в базе данных нет адресов.

Некоторые компании удаляют данные о местоположении после использования их для показа рекламы, другие – передают компаниям, занимающимся агрегацией данных, а третьи – хранят информацию годами.

«Идентифицировать личность человека через данные о геолокации потребовало бы огромного количества ресурсов», – заявил представитель Cuebiq Билл Дадди.

Не существует федерального закона, ограничивающего сбор или использование таких данных. Тем не менее, приложения, которые запрашивают доступ к местоположениям пользователей, не сообщают о том, как будут использоваться данные.

Зарабатывая на данных

Приложения составляют основу новой экономики данных о местоположении. Разработчики приложений могут зарабатывать деньги, напрямую продавая свои данные или передавая их для рекламы. Компании, связанные с данными геолокации, платят от 0,50 центов до 2 центов за пользователя в месяц.

Целевая реклама – наиболее распространенное использование информации. Google и Facebook, которые доминируют на рынке мобильной рекламы, также лидируют в рекламе, основывающейся на местоположении. Оба гиганта собирают данные из своих приложений, но не продают их, а персонализируют услуги благодаря им.

Меньшие компании конкурируют за остальную часть рынка, в том числе путем продажи данных и анализа финансовым учреждениям. По данным исследовательской компании Opimas, этот сегмент отрасли невелик, но растет, и ожидается, что к 2020 году он достигнет 250 миллионов долларов в год.

Apple и Google заинтересованы в том, чтобы разработчики были довольны, но оба предприняли шаги по ограничению сбора данных о местоположении. В самой последней версии Android приложения в фоновом режиме могут собирать данные о геолокации «несколько раз в час», а не на постоянной основе. Apple требует, чтобы приложения оповещали пользователей о сборе данных через всплывающие сообщения.

(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.