СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(14.11–27.11)

2018 № 20

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(14.11–27.11)
№ 20

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

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

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2018

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

14.11.2018
В Украине запустили YouTube Music и YouTube Premium

Google объявила о запуске в Украине нового музыкального сервиса YouTube Music, а также YouTube Premium, который позволяет смотреть видео с YouTube без рекламы и получать доступ к контенту YouTube Originals. С помощью YouTube Music можно будет слушать официальные альбомы и синглы; при показе рекламы сервис будет бесплатным. Premium сервис с возможностью загрузки треков и без показа рекламы будет стоить 79 грн в месяц. Стоимость приложения YouTube Premium, который позволит смотреть видео без рекламы и загружать их, составит 99 грн в месяц. Также доступна семейная подписка YouTube Music Premium Family за 119 грн в месяц. При загрузке в течение двух недель после запуска пользоваться сервисами можно будет бесплатно в течение трех месяцев (Marketing Media Review).

***

15.11.2018
Google запустила ещё один мессенджер

Компания Google встроила мессенджер в приложение «Карты» на Android и iOS. Она надеется, что эти чаты будут использоваться людьми для общения с организациями (InternetUA).

Магазины, рестораны и прочие заведения, у которых есть бизнес-профили в картах Google, могут наладить взаимодействие с клиентами в чате. Для этого им необходимо использовать приложение Google My Business, доступное на Android и iOS.

***

16.11.2018
Facebook меняет алгоритм ленты, чтобы расправиться с кликбейтом

В посте Марк Цукерберг детально описал, как Facebook будет расправляться с проблематичным контентом. Цукерберг называет кликбейт «неоднозначным» контентом. Он не нарушает правила сети, но приводит к худшему опыту для пользователей. По словам Цукерберга, пользователи проводят больше времени с таким типом контентом. В качестве решения Facebook будет понижать такой тип контента в ленте. Находить его будут AI системы. Изменения коснутся также контента, расшариваемого в группах сети (Marketing Media Review).

По мнению Цукербрега, уменьшение охвата кликбейтных материалов является лучшим решением, чем изменение правил по постингу в сети. В связи с этим издателям следует предоставлять контент, который будет отвечать пожеланиям пользователей после прочтения заголовка. Отметим, что компания вновь оказалась в центре скандала. Расследование The New York Times обнаружило, что сотрудники сети заказывали негативные статьи об Apple и Google во время расследования скандала с Cambridge Analytica. Также ходят слухи о том, что Цукерберг запретил сотрудникам пользоваться смартфонами на базе Apple из-за критики сети Куком.

***

16.11.2018
Михаил Сапитон
Facebook запустила образовательный сайт и разрешила постить вакансии в группы

Facebook расширяет собственное HR-направление. После запуска возможности публиковать вакансии, соцсеть объявила о запуске отдельного портала Learn with Facebook.

Докладніше

***

19.11.2018
Лиза Пальчинская
Украинские соцсети: несмотря на запреты, стать популярным так никому и не удалось

После того, как в мае 2017 года указом президента был запрещен доступ к ряду российских ресурсов на территории Украины, а среди них «ВКонтакте» и «Одноклассники», значительно активизировались ранее созданные украинские социальные сети и активно стали появляться новые. Всех их объединяло амбициозное желание стать национальной площадкой для общения украинцев. Но не всем удалось выжить и воплотить в жизнь заявленные цели.

Докладніше

***

19.11.2018
«ВКонтакте» разрешила скачать данные, которые собрала о вас

Во «ВКонтакте» появилась возможность скачать архив ваших первоначальных данных, которые социальная сеть собирала и хранит на своих серверах (InternetUA).

«При этом не всегда и не все данные пользователей могут отображаться в явном виде в интерфейсах “ВКонтакте”. Поэтому сегодня мы запустили

возможность делать расширенную выгрузку копии этих данных в удобном архиве. Это позволит в любой момент получить наиболее полное и наглядное представление о том, какие данные сохраняются на серверах “ВКонтакте”», – написал управляющий директор «ВКонтакте» Андрей Рогозов.

Пока выгрузка работает в тестовом режиме. Для выгрузки нужно сделать запрос и подождать, пока соцсеть сформирует ZIP-архив. Этот процесс может занять от нескольких часов до нескольких дней.

Запрос архива нужно подтвердить с помощью одноразового кода, а уникальную ссылку для скачивания невозможно открыть из другого профиля. Вы также можете добавить дополнительный уровень защиты – и зашифровать архив с помощью персонального ключа OpenPGP.

В списке информации будет список фотографий, которым вы поставили отметку «Нравится», историю денежных переводов или круг ваших интересов, которые учитываются при таргетинге рекламных объявлений.

***

20.11.2018

В Skype улучшен набор опций для персонализации и звонков

Участникам программы предварительного тестирования Skype предложены новые версии приложений для Android, iPhone, iPad, Mac, Linux, Linux Snap, Веб и Windows. С этим обновлением им стали доступны новые и улучшенные опции для настройки звонков и интерфейса программы (InternetUA).

В настройках Skype появился новый раздел Внешний вид, в котором можно выбрать подходящую тему, цвет и режим высокой контрастности. Ранее эти опции были разнесены по разным секциям окна настроек.

Для звонков реализована опция показа окна, когда Скайп находится в фоновом режиме, а также запущена поддержка субтитров. Субтитры доступны как для голосовых, так и для видеозвонков.

Ещё раз уточним, что сейчас все эти новшества доступны только в предварительной версии Skype (8.35.76.30) и даже там развёртываются постепенно. Рядовым инсайдерам они станут доступны вероятно не раньше декабря.

***

20.11.2018

Apple удаляет из App Store приложения со стикерами для WhatsApp

Три недели назад WhatsApp позволил пользователям добавлять собственные стикеры, но эта идея показалась Apple не особо удачной. Компания стала удалять из App Store приложения, с помощью которых можно было бы добавлять стикеры в этот мессенджер (InternetUA).

В App Store стали появляться десятки одинаковых приложений со стикерами для WhatsApp. Apple отыскивает их и удаляет, а также не пропускает в App Store новый контент со схожей функциональностью.

Обоснование Apple при блокировке:

– В App Store очень много приложений, которые делают то же самое.

– Приложение требует установку другого приложения (WhatsApp) и бесполезно без него.

– У всех похожих приложений схожий дизайн.

У Google не возникло подобных претензий к разработчикам. В Play Маркете по-прежнему доступны стикеры для WhatsApp, и приложений, предлагающих их, с каждым днём становится всё больше.

***

20.11.2018

Instagram будет удалять «накрученные» лайки и подписки

Социальная сеть Instagram намерена удалять лайки, подписки и комментарии, оставленные через сторонние приложения. Об этом компания сообщила на своем сайте 19 ноября (InternetUA).

«Недавно мы увидели аккаунты, использующие сторонние приложения чтобы искусственно увеличить их аудиторию», − указали в Instagram.

В соцсети разработали средства, позволяющие вычислять такие аккаунты и удалять их активность.

Пользователи, чьи аккаунты соцсеть заподозрит в накрутке лайков, получат уведомление о действиях, которые Instagram удалил.

Кроме того, им предложат сменить пароль, поскольку сторонние приложения для накрутки зачастую требуют логин и пароль от аккаунта.

***

21.11.2018

Facebook почав показувати, скільки часу ви «сидите» у соцмережі

Facebook почав розгортати нову функцію соцмережі «Ваш час»: тепер система підраховуватиме, скільки хвилин ви витрачаєте на додаток (Espreso.tv).

Про це пише Tech Crunch.

Функція доступна в мобільному додатку мережі. Щоб користуватися нею, потрібно зайти в налаштування і вибрати вкладку Your Time on Facebook.

Ви можете встановити щоденний ліміт і отримувати нагадування, що час зробити перерву. Ви можете налаштувати функцію, перейшовши на вкладку «Додатково» Facebook -> «Налаштування і конфіденційність» -> «Ваш час на Facebook».

***

21.11.2018

Facebook запатентовал технологию определения семьи пользователя

Facebook подал патентную заявку на технологию, которая предсказывает, кто входит в состав семьи пользователя. Она определяет родственные связи на основе изображений и подписей, размещенных на Facebook, а также информации об их устройствах.

Докладніше

***

24.11.2018

Жители Кубы получили доступ к Twitter

Кубинцы получили возможность активировать аккаунты в Twitter через мобильный телефон и пользоваться соцсетью, передает газета Juventud Rebelde (InternetUA).

Ранее жители Кубы не могли подтвердить подлинность своих аккаунтов и активировать их через смс-сообщения, так как международный телефонный код страны отсутствовал в списке Twitter.

Несмотря на возможность активировать аккаунты, отмечается, что кубинцы не будут видеть вкладку «Актуальное» в соцсети, однако смогут искать новости по хэштегам.

В декабре 2017 года кубинский телекоммуникационный оператор Etecsa позволил жителям государства отправлять смс-сообщения абонентам в США. До этого оператор не поддерживал связь с американскими номерами.

***

24.11.2018

Видео в Instagram генерируют на 21 % больше взаимодействий, чем изображения

Компания Quintly проанализировала 44,432 профилей и более 8,9 млн постов с 1 января по 30 сентября 2018 года и обнаружила, что видео получают на 21 % больше взаимодействий, чем изображения. И это несмотря на тот факт, что изображения являются самым популярным типом поста. Исследование также выявило, что у 31 % всех постов в Instagram более 300 знаков в описании поста, подчеркнув недавнюю популярность длинных описаний (в основном благодаря мнению пользователей, что алгоритм отдает предпочтение длинным постам). Интересно, 35,8 % профилей используют от одного до трех эмодзи на пост, а 54,9 % профилей вообще обходятся без эмодзи (Marketing Media Review).

***

25.11.2018

Viber запустил чаты на миллиард человек

В Viber появилась возможность создавать групповые чаты с максимальным числом участников в один миллиард человек. Ни один другой мессенджер не предлагает столь массовое общение (InternetUA).

Конечно, это лишь теоретическая возможность, которая по сути предполагает отсутствие лимита на добавление новых участников в чат. В реально существующих чатах состоит гораздо меньше людей и вряд ли такой лимит когда-нибудь будет исчерпан. Миллиард человек – ограничение, которое установлено на общее количество пользователей Viber.

Присоединяться к групповым чатам можно нажатием одной кнопки по ссылке, любой пользователь может отправить сообщение, которое увидят другие участники, и всем новым участникам доступна полная история переписки, в том числе той, что велась до того, как они присоединились к общению. Администраторы чатов могут закреплять важное сообщение в верхней части чата.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

19.11.2018
Финны фотками с граблями высмеяли заявление Трампа

Трамп 17 ноября посетил штат Калифорния, где борются с крупнейшими в истории лесными пожарами. Он заявил, что основная причина пожаров – плохое управление лесными территориями (InternetUA).

«Посмотрите на другие страны, они это делают иначе. Я был с президентом Финляндии, и он мне сказал: “У нас все по-другому... мы – лесная страна”. И они проводят много времени с граблями, расчищая все и делая другие дела, и у них нет проблем», – сказал Трамп.

Но президент Финляндии сказал 18 ноября, что не обсуждал расчистку лесов во время короткой встречи с Трампом в Париже в минувшие выходные.

«Я упомянул, что Финляндия – это земля, покрытая лесами, и у нас также есть хорошая система мониторинга лесов», – сказал Ниинистьо, добавив, что он напомнил Трампу: «Мы заботимся о наших лесах».

После заявления Трампа жители Финляндии стали размещать в Twitter фотографии того, как они якобы расчищают лес.

***

19.11.2018
Супрун начала «войну» с Amazon из-за символики ДНР

И. о. министра здравоохранения Ульяна Супрун призывает присоединиться к флешмобу против всемирно известного интернет-магазина Amazon, на платформе которого продаются товары с символикой так называемой «ДНР». Об этом она сообщила в Facebook (InternetUA).

«Amazon.com – глобальная торговая онлайн-платформа продает товары с символикой самопровозглашенной террористической республики "ДНР". Предлагаю устроить флешмоб в соцсетях и на почте генерального директора Amazon Джеффа Безоса», – пишет Супрун.

Руководительница Минздрава призывает отправить Безосу сообщение о том, что его компания помогает спонсировать терроризм.

«Адрес: jeff@amazon.com. Требуйте прекратить продажу товаров, что усугубляет гибридную войну России против цивилизованного мира», – предлагает чиновница.

Она напомнила, что война, которую Россия ведет на востоке Украины, уже унесла более 10 тысяч жизней, а флаг «ДНР» – это символ терроризма, репрессий, смерти и оккупации.

«Каждый должен осознавать, что поддерживая страну агрессора и террористические организации, которые она спонсирует, он поддерживает войну и смерть», – заявила Супрун.

***

20.11.2018

Call Me Ukrainian: Зеленський запустив новий патріотичний флешмоб // Флешмоб допоможе іноземцям краще розуміти культуру України

Відомий український шоумен, продюсер, сценарист і беззмінний лідер студії «Квартал 95» Володимир Зеленський запустив черговий флешмоб під назвою «Call Me Ukrainian». Відповідне відео він опублікував у себе в Instagram (РБК – Україна).

Причиною для цього стала історія, що відбулася з актором після концерту на Кіпрі. За словами Зеленського, один з місцевих співробітників на питання «Звідки ви?», почувши відповідь «З Києва», сказав: «Так, Росія». Володимиру довелося пояснювати, що Україна – це окрема, незалежна країна, що подарувала світові багато відомих особистостей таких, як Шевченко, Сікорський.

Як сказав Зеленський, в цей момент у нього виникло відчуття, що «ми дещо не зробили».

«Тому я пропоную вам флешмоб під назвою Call Me Ukrainian. Надсилайте відео, в якому розкажіть, завдяки чому або кому ви пишаєтеся своєю країною. Будемо утворювати весь світ».

Користувачі в мережі підтримали ідею.

***

22.11.2018

У соцмережах обурилися відкриттям мережі швидкого харчування KFC у приміщенні київського будинку Профспілок

У соцмережах обурилися відкриттям мережі швидкого харчування KFC у приміщенні київського будинку Профспілок, в якому загинули люди під час Євромайдану. Коментуючи інформацію, український журналіст та блогер Юрій Романенко зазначив, що інцидент під KFC цікавий тим, що у нас народ з будь-якого приводу хоче створити музей. Знайшли археологи кілька черепків на Подолі – музей будувати. Тепер відбудовують будинок профспілок і теж очевидно треба будувати музей (Голос Українською).

За словами Романенка, виникає питання, за чий рахунок повинні функціонувати всі ці музеї в країні з економікою, що на ладан дихає. Менеджери мережі KFC виразно недалекоглядні хлопці, тому що примудрилися зробити відкриття в річницю. Могли б тиждень почекати, враховуючи негативне налаштування публіки. Але, з іншого боку, дивлячись на цю ситуацію з боку, який інвестор сюди захоче заходити, знаючи, що крім корупції, він тут зіткнеться з людьми, які з будь-якого приводу будуть тягнути шини із-за того, що для них важливо символічний простір.

Журналіст упевнений, що найкращим музеєм Революції гідності була економіка з трильйонним ВВП за номіналом, держава, відсікають загребущі руки від бюджету і армія, озброєна сучасною технікою, що здатна зламати плани будь-якого агресора за нормальну країну, в якій нормальні відносини між людьми, а не анархію, зациклену на символізмі.

***

26.11.2018

Міністерство у справах ветеранів запускає сторінки у соцмережах

Міністерство України у справах ветеранів запускає свої сторінки у соціальних мережах (InternetUA).

Про це повідомила міністр у справах ветеранів Ірина Фріз на своїй сторінці у Facebook.

«Сьогодні запускаємо наші офіційні сторінки міністерства в соцмережах Facebook і Twitter, на яких буде транслюватись наша спільна з проектним офісом зі створення міністерства прес-конференція. Початок об 11:00», – написала вона.

Фріз зауважила, що прийнято рішення не очікувати створення сайту Міністерства у справах ветеранів, адже це може тривати місяць у кращому випадку, і розпочати комунікаційну роботу в Facebook і Twitter.

***

27.11.2018

В соцмережах оприлюднили «Пам'ятку панікера» для регіонів де вводиться воєнний стан

Українці бурхливо реагують на введення воєнного стану у десяти областях України. Різноманітні ЗМІ проводять опитування, про те, як громадяни ставляться до цієї події (news.vn.ua)

Не відстають від них і користувачі соціальних мереж. Вони активно висловлюють свою позицію стосовно воєнного стану.

Коментують це і вінничани, які є користувачами мережі Фейсбук.

У мережі навіть з'явилася «пам'ятка панікера». У ній йдеться про те, що мають робити люди, які схильні сіяти паніку і нервувати.

Їм пропонують серед іншого виговоритися до 28 листопада, сховати авто, щоб не конфіскували на потреби армії, завести будильник на час введення воєнного стану.

А всім іншим, радять не втрачати здорового глузду і не панікувати.

***

27.11.2018

У соцмережах з'явилися фотожаби про воєнний стан в Україні

У них користувачі соцмереж з сарказмом розмірковують над ситуацією, що склалася (u-news).

У мережі згадали скандальні білборди з Юлією Тимошенко та написом про те, що вибори 2019 це «останній шанс для бабусі» тільки тепер щодо Петра Порошенка.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

16.11.2018

Instagram представил три новые функции для шоппинга

В преддверии праздников ритейлеры лучше смогут представить свои продукты на платформе. Пользователи смогут воспользоваться функцией «Коллекции» и сохранить выбранные продукты. Для этого нужно нажать на метку продукта в Историях или на пост в ленте и нажать на иконку «сохранить» в нижнем правом углу изображения. Зайти в коллекции можно со своего профиля и просмотреть отобранные продукты позже (Marketing Media Review).

Еще одна функция касается совершения покупок с помощью видео. Instagram вставил иконку с шоппингом в нижний левый угол брендированных видео, в которых демонстрируются продукты.

Бизнес-профили теперь включат вкладку для шоппинга, чтобы пользователи могли просмотреть продукты от компаний. Вкладка представит ленту с изображениями продуктов, на которые можно нажать и увидеть всю информацию о них.

***

16.11.2018

У Ощадбанка появился чат-бот в Telegram

Государственный банк Украины сообщил на своем сайте о том, что запустил бота @Oschadbot в Telegram. На очереди чат-бот в Messenger Facebook. В первую очередь банк предлагает воспользоваться услугами бота владельцам карточки. Пользователи смогут проверить баланс своего счета, заблокировать или активировать карточку, проверить состояние задолженности по карточному счету, продолжить срок действия карточки и другое (Marketing Media Review).

***

16.11.2018

На фоне череды скандалов сотрудники Facebook стали испытывать заметно меньше оптимизма по поводу будущего компании

Сотрудники Facebook стали испытывать куда меньше оптимизма по поводу будущего соцсети, чем годом ранее, пишет газета The Wall Street Journal со ссылкой на данные опроса, проведенного в компании. По данным издания, в недавнем исследовании приняли участие 29 тысяч сотрудников Facebook. Лишь 52 % опрошенных сообщили, что оптимистично смотрят на будущее компании, тогда как годом ранее этот показатель составил 84 %.

Докладніше

***

19.11.2018

Михаил Сапитон

Швейцарская сеть отелей запустила услугу «Instagram-сиделки»: пока вы отдыхаете – вам готовят контент

Швейцарская сеть отелей Ibis Hotels предложила клиентам в Цюрихе и Женеве услуги «Instagram-сиделок», передает USA Today со ссылкой на сайт компании.

Это возможность заказать услуги профессионального Instagram-блогера, который будет снимать, редактировать и оформлять публикации для вашей ленты во время отдыха. На сайте отеля возможность называют способом «насладиться городским путешествием без цифрового стресса». В качестве

«сиделок» выступают местные блогеры, у которых до нескольких десятков тысяч подписчиков (AIN.UA).

Запуск услуги со слоганом *Relax we post* сопроводили промороликом.

Забронировать услугу до 2 декабря может любой посетитель 17 отелей Ibis Hotels. Это бесплатная опция. Гостю придется сообщить данные для авторизации «сиделки» в Instagram-аккаунте. Один из 10 блогеров позаботится о наполнении профиля и даже будет отвечать на комментарии.

Как отмечает британский таблоид Daily Mail, отели не впервые используют Instagram для продвижения дополнительных услуг. В 2017 году мальдивский Conrad Hilton Resort предлагал заказ «Instagram-дворецких». Они подсказывали гостям наиболее интересные для съемки локации и вели по так называемой «Instagram-тропе».

***

22.11.2018
YouTube удвоил прероллы

YouTube решил удвоить количество рекламы, которые пользователи обязаны просмотреть до или в середине интересующего их видео. И хотя новые рекламные вставки увеличивают длину рекламных пауз, проигрывая два последовательных ролика, количество рекламных вставок, прерывающих видео, уменьшится. (При проигрывании двух роликов будет одна рекламная вставка). «Пользователям нравятся прероллы. И они предпочитают, чтобы их реже прерывали», – отметили в YouTube. На прошлой неделе сервис также объявил о том, что позволит зрителям смотреть голливудские фильмы бесплатно, но с рекламой (Marketing Media Review).

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

15.11.2018
Как социальные сети влияют на настроение?

Социальные сети, без всяких сомнений, оказывают большое влияние на многие сферы человеческой жизни. Например, в 2016 году было доказано влияние соцсетей на продажи, а в 2018 году Facebook вовсе объявила, что они являются прямой угрозой для демократии. Конечно же, они также напрямую влияют на самочувствие самих пользователей. Этот факт в очередной раз

доказали исследователи из Университета Пенсильвании, проведя интересный эксперимент со 143 добровольцами (InternetUA).

Люди были разделены на две группы. Первой половине было разрешено пользоваться социальными сетями как обычно, безо всяких ограничений во времени и производимых действиях. Второй группе было разрешено пользоваться только соцсетями Facebook, Instagram и Snapchat не более 10 минут в день. Придерживание правил проверялось при помощи скриншотов экрана с приложениями, расходовавшими заряд аккумулятора.

Спустя три недели добровольцы прошли опрос, который показал их степень предрасположенности к ощущению одиночества, депрессии, синдрому упущенных возможностей и других негативных чувств. По словам психолога Мелиссы Хант, люди, проводившие в социальных сетях минимум времени, ощущали меньшее чувство одиночества и депрессии.

Проведенный эксперимент в очередной раз доказал результаты прошлых исследований. Ранее психологи уже заявляли о том, что социальные сети способны усиливать чувство одиночества и депрессии. Это объяснялось тем, что пользователи социальных сетей часто сравнивают свои жизни с жизнями друзей и знакомых. При этом они забывают, что в интернет преимущественно выкладываются только позитивные фотографии, а весь негатив остается за кадром.

***

17.11.2018

Чрезмерная увлеченность социальными сетями приводит к развитию нарциссизма

Чрезмерная увлеченность социальными сетями приводит к развитию нарциссизма. Как сообщает The Open Psychology Journal, к такому выводу пришли исследователи из Университета в Суонси и Миланского университета (Aspekty.net).

В течение четырех месяцев были изучены изменения личности 74 человек в возрасте от 18 до 34 лет. Была также оценена частота посещений социальных сетей, в том числе Twitter, Facebook, Instagram и Snapchat. Выяснилось, что у фанатов социальных сетей развитие нарциссизма превышало критическую отметку.

Примечательно, что у тех, кто использовал социальные сети в основном для общения, таких отклонений не наблюдалось. Однако даже у них были задатки развития нарциссизма, что проявлялось в постепенном увеличении числа словесных сообщений.

В общей сложности Facebook использовали 60% участников исследования, Instagram – 25 %, Twitter и Snapchat – 13 %. Более двух третей испытуемых в основном использовали социальные сети для публикации фотографий. Практически все участники исследования уделяли социальным

сетям около трех часов ежедневно, не считая того времени, которое было использовано в рабочих целях.

Эксперты отмечают, что рост популярности социальных сетей приведет к еще большему усугублению ситуации.

***

21.11.2018

Юная участница телешоу покончила с собой после издевательств в сети

Британская школьница и участница музыкального телешоу Britain's Got Talent Трикси Харт (Trixie Hart) покончила с собой после онлайн-травли. Об этом сообщает The Daily Mail (InternetUA).

Подросток совершила суицид в сентябре, однако СМИ узнали о смерти певицы лишь спустя несколько месяцев. Бабушка погибшей 16-летней девочки рассказала, что над школьницей постоянно издевались в сети. Родители нередко заставали Харт в слезах, когда она сидела за компьютером. Онлайн-тролли смеялись над ее внешностью и голосом.

По словам родственников, школьница столкнулась с ужасными издевательствами, причем в травле участвовали не только подростки, но и взрослые пользователи сети. Справиться с таким серьезным напором ей не удалось.

«Люди называли ее шлюхой и говорили ей, что она уродливая. У нее был потрясающий певческий голос, и я думаю, что люди завидовали ей», – объяснила бабушка мотив троллей. Она также отметила, что у ее внучки и раньше были проблемы с психикой: несколько лет назад врачи диагностировали у нее синдром дефицита внимания и расстройство личности.

В день гибели Харт дождалась, пока ее мать уйдет на работу. Затем она приняла душ, нанесла макияж и после этого покончила с собой.

***

27.11.2018

Ученые: Фильтры Instagram и палитра фотографий может рассказать о характере человека

Ученые из Университета Сонгюнгван в Южной Корее выяснили, что выбор фильтров в инстаграме может рассказать о характере человека (InternetUA).

Целью исследования стало изучение взаимосвязи между личностью пользователя и цветовыми особенностями его фотографий. Ученые предположили, что люди с некоторыми особенностями психики будут иметь похожий стиль снимков в социальных сетях. Сотрудники университета проанализировали 25 тысяч фотографий и удовлетворенность жизнью, степень

одиночества, нарциссизм, отношение к социальным сетям их авторов – 179 добровольцев.

Выяснилось, что пользователи, которые не состоят в отношениях или чувствуют себя одинокими, меньше склонны к ярким цветам. Разнообразие палитры свойственно скорее экстравертам, чем интровертам. Они, как и люди, склонные к нарциссизму, выбирают яркие фильтры и снимки. Пол пользователя также влияет на красочность фотографий, которые он выставляет в социальных сетях: женщины выбирают снимки с более разнообразной цветовой гаммой.

Маніпулятивні технології

16.11.2018

Facebook заказывал пиар-кампании против конкурентов, чтобы отвлечь внимание от проблем безопасности

Facebook нанимал лоббистов, чтобы отвлечь внимание на своих конкурентов во время скандала об утечке данных. Об этом пишет газета New York Times (NYT) в своем расследовании.

Докладніше

***

19.11.2018

Владимир Кондрашов

Украинский хакер проник на «фабрику российских троллей»

Украинскому консультанту по кибербезопасности Егору Папышеву удалось проникнуть на «российскую фабрику троллей» и узнать некоторые подробности работы «кремлеботов» изнутри. Как оказалось, на российских ботофермах используют специальный софт для работы с социальными сетями, обучают сотрудников и готовят площадку для очередной информационной волны, «арендуя» реальные аккаунты украинцев в соцсетях.

Докладніше

***

20.11.2018

Політики інвестують в Інтернет. Як захиститися від маніпуляцій у соцмережах

Стати бототролем в соціальних мережах можна за 1000 грн, розповів керівник програм нових медіа громадської організації Інтернюз-Україна Віталій Мороз.

Докладніше

***

22.11.2018

Вице-президент Facebook признался, что нанял пиарщиков критиковать Google и Apple

Покидающий свой пост вице-президент американской корпорации Facebook по общественным коммуникациям Эллиот Шрейдж взял на себя ответственность за найм фирмы Definers Public Affairs, которая размещала критические публикации о компаниях Google и Apple (InternetUA).

«Ответственность за эти действия лежит на руководстве команды по коммуникациям. Это я», – говорится в заявлении Шрейджа, опубликованном в среду на сайте Facebook. «Я был в курсе и одобрил решение нанять Definers и подобные фирмы», – отметил он, добавив, что сожалеет о своей неудаче.

В заявлении Шрейдж признал, что Facebook просила Definers Public Affairs «заниматься работой, связанной с конкурентами», отметив, однако, что с просьбой создавать или распространять фальшивые новости корпорация к ней не обращалась.

15 ноября газета The New York Times сообщила о том, что Facebook сотрудничала с Definers Public Affairs, которая размещала критические статьи о Google и Apple на связанном с ней новостном ресурсе. По данным издания, Facebook наняла Definers Public Affairs для отслеживания посвященных корпорации публикаций в прессе, но расширила сотрудничество с фирмой в свете скандала вокруг Cambridge Analytica. Кроме того, как писало издание, Definers Public Affairs также пыталась дискредитировать лиц, выступавших против Facebook, в частности американского миллиардера Джорджа Сороса, который в январе заявил, что Google и Facebook монополизировали рынок, препятствуют инновациям и создают зависимость от сервисов, которые они предлагают.

Как утверждал источник газеты, после публикации материала The New York Times Facebook прекратила сотрудничество с Definers Public Affairs. Он также указал, что основатель социальной сети Марк Цукерберг и исполнительный директор Facebook Шерил Сэндберг не знали о задачах, которые фирма выполняла для соцсети.

Спецслужби і технології «соціального контролю»

14.11.2018

Дмитрий Демченко

В Раду внесли законопроект про защиту информационного пространства. Активисты назвали это введением цензуры

Седьмого ноября в Верховной Раде зарегистрировали законопроект №9275 «О внесении изменений в некоторые законы Украины относительно защиты информационного пространства». Ряд общественных организаций выступили против этого документа и заявили, что депутаты пытаются «в очередной раз ввести цензуру в Украине под прикрытием борьбы с российской пропагандой».

Докладніше

***

16.11.2018

Искусственный интеллект вычислит наркодилеров среди пользователей Facebook и Instagram

Весной конгрессмены раскритиковали Марка Цукерберга, указав, что FB стала платформой для наркодилеров. Теперь вычищать подозрительные объявления поручили ИИ – и алгоритм будет делать это быстрее модераторов-людей.

Докладніше

***

18.11.2018

В Китае обещают платить огромные премии нашедшим порнографию в Интернете

В Китае увеличат материальное вознаграждение за доносы о незаконном контенте, найденном как в Интернете, так и в других источниках (InternetUA).

Так, с 1 декабря максимальная сумма выплачиваемой премии составит 600 тысяч юаней (около 86 тысяч долларов). На данный момент эта сумма вдвое меньше.

Известно, что кроме порнографии, в Китае запрещены публикации, которые могут быть сочтены угрозой национальному единству или общественному устройству. Также не допускается распространение государственных секретов.

Отметим, что удвоенное вознаграждение упоминается в новых правилах, опубликованных администрацией киберпространства Китая, которая является главным органом интернет-цензуры в стране. Они обязывают онлайновые платформы к концу месяца начать сбор и хранение информации о пользователях, в том числе содержание их переписки, сетевые адреса и сведений об устройствах, используемых для доступа к интернету.

***

19.11.2018

86 компаний потребовали от Facebook улучшить систему обжалования блокировок

За последний год Facebook была вынуждена расширить свою практику модерации контента в ответ на требования защитников по правам человека, которые утверждали, что компания не защищает «уязвимых» пользователей от языка ненависти. Теперь Facebook подвергся критике из-за непоследовательной модерации контента.

Докладніше

***

21.11.2018

Twitter заблокировал пропагандиста Кремля

В Twitter удалена страница известного пророссийского пропагандиста из Великобритании Грэма Филлипса, которого в 2014 году СБУ выдворила из Украины, запретив въезд на три года (InternetUA).

Об этом сообщил он сам.

«Твитер заблокировал мой аккаунт сегодня. Теперь я обращаюсь к Твиттеру и увидим, что будет дальше», – написал он.

«Русские тролли и троглодиты, вот кто поддерживает Грэма Филлипса в Твиттере, Мелочь, а настроение поднимает», – пишут в комментариях.

При этом, на странице пропагандиста в Twitter отмечено, что «действие учетной записи приостановлено».

***

21.11.2018

Ирина Фоменко

The Guardian: Российский «тролль» подал в суд на Facebook за бан

Российская компания, чьего бухгалтера федеральные прокуроры обвинили во вмешательстве в выборы в США, подала в суд на Facebook, заявив, что у нее законный новостной канал, а учетная запись должна быть восстановлена.

Докладніше

***

24.11.2018

Почему законы о клевете не будут работать в украинском Интернете

Украинцев могут привлечь к криминальной ответственности за посты и комментарии в Интернете, содержащие клевету. НВ разбиралось, как принятие законопроекта отразится на интернет-цензуре и как это регулируют в других странах.

Докладніше

***

25.11.2018

Утечка данных. В Британии изъяли внутренние файлы Facebook по делу Cambrydge Analytica

В Британии парламент изъял внутренние файлы Facebook по делу со скандалом с Cambrydge Analytica. Об этом пишет издание The Guardian (InternetUA).

В изъятых файлах содержится информация о переписке между топ-менеджерами Facebook с генеральным директором Марком Цукербергом.

Глава парламентского Комитета по вопросам культуры, медиа и спорта Дамиан Коллинз, заявил, что это – «беспрецедентный шаг».

«Нам не удалось получить ответа от Facebook по поводу скандала с Cambrydge Analytica, и мы считаем, что документы содержат информацию с очень большим общественным интересом», – заявил он.

Изъятые файлы помогут выяснить, какое компания приняла решение об использовании данных перед скандалом с Cambridge Analytica, в том числе и то, что именно о проблеме знали Цукерберг и топ-менеджеры.

***

26.11.2018

Facebook на тиждень заблокував сторінку Омеляна

Міністра інфраструктури Володимира Омеляна заблокували у соцмережі Facebook на сім днів (InternetUA).

Про це повідомила прес-секретар міністра Марина Томко у Facebook.

Останній пост Омеляна у Facebook опублікований з написом англійською «Росія атакує Україну».

***

26.11.2018

В РФ ввели жесткую цензуру в популярных соцсетях

Соцсети Facebook и Instagram начали скрывать от российских пользователей сообщения по решению суда. Об этом сообщили российские СМИ (InternetUA).

Накануне соцсети заблокировали посты по решению московского суда. Речь идет о владельце БТА-банка Кенесе Ракишеве, которого обвиняли в отношениях с несовершеннолетними, доведении до самоубийства и сокрытии преступлений. Теперь посты в РФ недоступны, однако в других странах они по-прежнему открываются.

Отметим, что случившееся является первым случаем блокирования постов в соцсетях согласно действующему с апреля 2018 года закону. Согласно

ему, соцсети должны блокировать информацию по решению суда, иначе им будет грозить штраф до 50 миллионов рублей.

***

26.11.2018

В России возбудили дело против Google

Управление Роскомнадзора возбудило административное дело в отношении корпорации Google. Об этом представители ведомства написали на официальной странице во «ВКонтакте» (InternetUA).

По данным регулятора, компания не подключена к федеральной государственной информационной системе, что требуется в рамках российского законодательства, чтобы исключать ссылки на ресурсы с противоправной информацией из поисковой выдачи.

«Данный факт образует состав административного правонарушения, предусмотренного частью 1 статьи 13.40 КоАП РФ», — сообщили представители Роскомнадзора. Они также отметили, что размер штрафа для Google может составить от 500 тысяч до 700 тысяч рублей. Рассмотрение дела в суде состоится в декабре 2018 года.

***

26.11.2018

Прокуратура, СБУ та поліція просять закарпатців не піддаватись на сепаратистські провокації у соцмережах

Від 25 листопада в одній із соціальних мереж ширяться різного роду заклики «поставити на перевалах блок-пости і відкрити кордон з ЄС» чи «перенести державний кордон України за лінію оборони Арпада». Через заклики, що поширюються з фейкових акаунтів, робиться, таким чином, спроба втягнути завжди мирних і толерантних закарпатців у інформаційну війну (ПРОЗАХІД).

За вказаним фактом Управлінням СБ України в Закарпатській області зареєстроване кримінальне провадження за ч.2 ст.110 КК України (посягання на територіальну цілісність і недоторканність України).

Прокуратура Закарпатської області здійснює процесуальний контроль за ходом досудового розслідування.

Наголошуємо, що заклики до сепаратизму, зміни меж державного кордону чи до вчинення інших злочинів проти основ національної безпеки можуть привести на лаву підсудних.

Правоохоронці, і органи прокуратури, зокрема, жорстко і принципово реагуватимуть на всі такі заклики.

Проблема захисту даних. DDOS та вірусні атаки

14.11.2018
Ирина Фоменко
Ваш старый смартфон представляет угрозу

Старый смартфон, спрятанный в ящике или шкафу, хоть и не кажется угрозой национальной безопасности, однако администрация Трампа считает его таковым.

Докладніше

***

15.11.2018
Дмитрий Демченко
В МХП хотят отслеживать эмоции сотрудников с помощью видеонаблюдения. Это законно?

14 октября появилась информация о том, что агрохолдинг «Мироновский хлебопродукт» ввел систему мониторинга эмоций сотрудников, которая работает с помощью камер видео наблюдения. Об этом заявил глава правления компании Юрий Косюк на форуме «Дирижеры изменений». Редактор AIN.UA рассказывает о ситуации и приводит мнение юристов о том, законно ли это.

Докладніше

***

15.11.2018
Мощнейший вирус-вымогатель вернулся и захватил компьютеры по всему миру

Мощный вымогатель WannaCry, атаковавший в 2017 году компьютеры по всему миру, стал самым распространенным вирусом-вымогателем. Об этом сообщили эксперты «Лаборатории Касперского» в своем отчете (InternetUA).

По подсчетам аналитиков, в последние месяцы WannaCry занимает первое место по количеству атак на компьютеры клиентов компании. Доля нападений с помощью этого вируса составляет почти 29 процентов от общего числа.

Второе место после WannaCry по распространенности занимают новые версии трояна GandCrab. Эта программа-вымогатель атаковала чуть более 12 процентов компьютеров.

Также в число вирусов-«лидеров» специалисты внесли известные шифровальщики Crysis, Shade, PolyRansom и Cryakl. Последний занимает третью строчку вирусного рейтинга – с его помощью совершено почти девять процентов нападений.

Последним громким нападением компьютерного вируса WannaCry стала атака на авиастроительную компанию Boeing. Обновленная версия вредного ПО затронула некоторые системы организации.

***

15.11.2018

Уязвимость в Android позволяет следить за местонахождением пользователей

Исследователи компании Nightwatch Cybersecurity раскрыли подробности об уязвимости в Android, позволяющей следить за местонахождением пользователей. С помощью уязвимости (CVE-2018-9581) злоумышленник вблизи Wi-Fi маршрутизатора может отслеживать передвижение пользователей в зоне действия сигнала беспроводной сети.

Докладніше

***

16.11.2018

В браузере Firefox появилась новая функция

Mozilla пополнила функционал браузера Firefox Quantum новой системой уведомлений, которая будет предупреждать пользователей в случае посещения скомпрометированных сайтов. Об этом сообщается в блоге компании (InternetUA).

Всплывающее уведомление будет включать краткие сведения о характере и масштабе утечки данных, а также ссылку на сервис Firefox Monitor, где представлена более полная информация об инциденте. Новый функционал будет доступен в течение ближайших нескольких недель.

С помощью Firefox Monitor пользователи смогут проверить наличие своего электронного адреса среди утекших данных, используя базу данных сервиса Have I Been Pwned?. На каждом сайте уведомление будет выводиться только один раз, при желании пользователи смогут отключить функцию в настройках Firefox. Стоит отметить, что предупреждения будут отображаться только в тех случаях, если утечка данных произошла в последние 12 месяцев.

***

16.11.2018

Microsoft обвинили в тайном сборе персональных данных пользователей

Согласно результатам исследования, проведенного специалистами компании Privacy Company по заказу Министерства безопасности и правосудия Нидерландов (Ministerie van Justitie en Veiligheid; JenV), через встроенный в Office механизм компания собирает большие объемы данных об

индивидуальном использовании Word, Excel, PowerPoint и Outlook без надлежащего уведомления.

Докладніше

***

16.11.2018

Большинство банкоматов признаны уязвимыми для хакеров

Злоумышленники могут похитить данные клиентов в течение 15 минут после проникновения в сервисную зону любого банкомата. Об этом сообщается в исследовании компании Positive Technologies (InternetUA).

Отмечается, что 85 процентов банкоматов уязвимы к атакам, направленным на хищение денег. При этом преступники могут не только использовать считывающие устройства (скиммеры), но и перехватить информацию во время передачи данных между банкоматом и процессинговым центром или между операционной системой банкомата и картридером.

Кроме того, компания выявила, что большинство банкоматов работает на устаревшем программном обеспечении, а многие банки предпочитают не покупать обновления.

***

16.11.2018

Ирина Фоменко

Смарт-часы, которые отслеживают местоположение ребенка, могут взломать преступники

Популярные смарт-часы, отслеживающие геолокацию детей, настолько легко взломать, что их должны снять с продажи. Об этом сообщает The Telegraph.

Докладніше

***

18.11.2018

Instagram случайно обнародовала пароли пользователей

Некоторые пользователи соцсети Instagram, которые скачивали свои данные, стали жертвами ошибки сервиса, из-за которой их пароли показывались в адресной строке браузера. Когда пользователи Instagram хотели загрузить свои данные, они вводили пароль от своего аккаунта, который затем показывался в адресной строке, хранился на устройствах и серверах Facebook (InternetUA).

По словам представителя Instagram, проблема касается только небольшого количества жителей США. Все пользователи, которых затронула проблема, получили письмо с просьбой изменить пароль и очистить историю

их браузера, чтобы никто не смог увидеть пароль. Саму ошибку в компании исправили.

Instagram добавила возможность загрузки личных данных в апреле 2018 года, чтобы соответствовать правилам GDPR. По запросу пользователей, в течение 48 часов, Instagram отправляет письмо с полной копией всего, что они делали в Instagram и какие данные собирала компания.

***

18.11.2018

В Google Play найдены новые вредоносные приложения

Eset предупредила о новых вредоносных приложениях в Google Play (InternetUA).

Антивирусная компания Eset предупредила о новых вредоносных приложениях, появившихся в Google Play. Эти программы выдавали себя за популярные криптовалютные сервисы NEO, Tether и MetaMask и использовались для кражи пользовательских учетных данных.

Одна из схем заключается в подделке кошельков. Настоящие криптовалютные кошельки генерируют для пользователя приватный ключ и публичный адрес для перевода средств. Нелегитимные версии вместо этого показывали пользователю публичный адрес кошелька атакующих. Криптовалюту, переведенную на такой адрес, невозможно вернуть без приватного ключа, доступ к которому есть только у злоумышленников.

Авторы вредоносного приложения, замаскированного под MetaMask, действуют по классической схеме фишинга. После установки и запуска пользователю предлагалось ввести приватный ключ и пароль от своего криптовалютного кошелька – эти данные затем оказывались в распоряжении злоумышленников.

В Eset отмечают, что поддельные приложения созданы с помощью широкодоступного конструктора мобильных приложений, который позволяет «собирать» подобные программы без специальных знаний и навыков.

Компания Google получила от экспертов Eset предупреждения о вирусных программах и уже удалила их из магазина Google Play.

***

19.11.2018

Хакеры взломали самый известный почтовый сервис с шифрованием

Группа хакеров утверждает, что они взломали почтовый сервис ProtonMail и украли «значительные» объемы данных. Они пока не опубликовали данные о взломе, однако выдвинули свои требования к компании по выкупу украденной информации.

Докладніше

***

19.11.2018

Умные камеры положат конец приватности

К 2022 году половина семей в США обзаведется умными камерами наблюдения. Люди сознательно начнут жертвовать своей приватностью, а распознавание лиц станет стандартом во всех сферах – от торговли до медицины.

Докладніше

***

19.11.2018

Новый банковский троян для Android развлекает своих жертв игрой

Специалисты компании «Доктор Веб» обнаружили в каталоге Google Play банковского трояна Android.Banker.2876, распространявшегося под видом официальных приложений нескольких европейских кредитных организаций (Bankia, Banco Bilbao Vizcaya Argentaria (BBVA) и Santander, французских Credit Agricole и Groupe Banque Populaire, а также немецкой Postbank).

Докладніше

***

20.11.2018

Дмитрий Демченко

Google и Минобразования представили бесплатный онлайн-курс по безопасности в Интернете

Google совместно с Министерством образования и науки создали бесплатный онлайн-курс «По сетевому этикету и безопасности». Об этом сообщается на сайте Кабмина (AIN.UA).

Курс, в первую очередь, предназначен для школьников, но пройти его могут все желающие. Он состоит из пяти модулей с текстовыми материалами, видеороликами и короткими тестами:

– Обучение правилам безопасности и конфиденциальности в интернете;

– Безопасность пользования мобильными устройствами;

– Правила безопасного поиска информации;

– Самозащита от фишинга и мошенничества;

– Забота о своей репутации в сети.

«Современные дети сталкиваются с рядом вызовов, которых не было в нашем детстве. Школа должна адекватно на эти вызовы реагировать. Развитие цифровой компетентности у детей, умение грамотно использовать современные технологии – важная часть того, чем должен учить школа в 21 веке. И мы благодарны нашим партнерам, что они готовы сотрудничать с нами и

разрабатывают материалы для учеников и учителей», – отметила Министр образования и науки Украины Лилия Гриневич.

***

20.11.2018

Кіберполіція затримала банду, яка викрала 5 мільйонів гривень з банківських терміналів

У Кривому Розі затримано злочинну групу, викриту у махінаціях з банківськими терміналами самообслуговування. Про це повідомили в департаменті кіберполіції Національної поліції України.

Докладніше

***

21.11.2018

Facebook прослушивает пользователей смартфонов

При записи видео была замечена активность мессенджера. При этом он был отключён. Видимо, приложение работает в фоновом режиме и собирает данные (InternetUA).

Пользователь iOS 12.1 заметил баг Facebook Messenger, который указывает на то, что приложение прослушивает владельцев смартфонов. Об этом он рассказал на Reddit.

Во время записи видео приложение пыталось прервать процесс, на экране высвечивался непонятный код. При этом мессенджер был выключен. Пользователь допустил, что приложение продолжает работать в штатном режиме и записывать разговоры через микрофон или собирать данные с помощью камеры.

***

21.11.2018

Зафиксирована первая в истории ботнет-атака на смарт-телевизоры

В компании DoubleVerify (DV), занимающейся аналитикой и программным обеспечением для измерений в сфере цифровых медиа, сообщили о выявлении новой сети ботов, нацеленной специально на подключаемые телевизоры (Connected TV), или же смарт-телевизоры.

Докладніше

***

21.11.2018

Новый троян удаляет антивирусы и скрытно добывает криптовалюту

«Доктор Веб» предупреждает о появлении новой вредоносной программы, способной инфицировать устройства под управлением операционных систем на ядре Linux (InternetUA).

Зловред-майнер получил название Linux.BtcMine.174. Он представляет собой большой сценарий, написанный на языке командной оболочки sh и содержащий более 1000 строк кода.

В процессе работы вредоносная программа использует несколько различных компонентов. В частности, в случае успешного проникновения в систему жертвы загружается одна из версий трояна Linux.BackDoor.Gates.9. Бэкдоры этого семейства позволяют выполнять поступающие от злоумышленников команды и проводить DDoS-атаки.

Кроме того, зловред может использовать набор эксплойтов для повышения уровня своих привилегий. Наконец, подгружается руткит-модуль, который способен выполнять такие функции, как кража вводимых пользователем паролей команды su, сокрытие файлов в файловой системе, сетевых соединений и запускаемых процессов.

Linux.BtcMine.174 способен завершать процессы антивирусов, а также с помощью пакетных менеджеров удалять файлы и директории соответствующих защитных продуктов.

Наконец, вредоносная программа осуществляет скрытую добычу криптовалюты Monero (XMR), что приводит к излишнему расходованию аппаратных ресурсов компьютера и увеличению счетов за электроэнергию.

***

21.11.2018

Банковские троянцы охотятся на любителей онлайн-шопинга

Клиенты интернет-магазинов имеют повышенные шансы стать жертвой вредоносного банковского ПО, особенно в преддверии «черной пятницы» и стартующего вслед за ней предпраздничного сезона. В зоне риска находятся покупатели из европейских стран, в частности Италии, Германии и Франции, а также Северной Америки и ряда экономически активных азиатских государств (Компьютерное Обозрение).

Чаще всего банковские троянцы следят за вводимыми данными на сайтах интернет-магазинов, продающих одежду, обувь, украшения, игрушки, подарки и прочие популярные товары (своего рода онлайн-универмаги) – на их долю приходится 50 % всех попыток сбора конфиденциальной информации в секторе электронной коммерции. Другими излюбленными категориями злоумышленников являются онлайн-магазины электроники (12%) и сайты, предлагающие развлечения, – интернет-кинотеатры, игры и т.п. (тоже 12 %).

За девять месяцев 2018 г. защитные решения «Лаборатории Касперского» заблокировали более девяти миллионов попыток кражи учетных данных и финансовой информации пользователей популярных онлайн-магазинов. Для достижения своей цели банковские троянцы перехватывают информацию,

когда пользователь вводит ее на странице интернет-магазина или платежного сервиса. Кроме того, они могут модифицировать контент страницы или перенаправить жертву на фишинговый сайт.

В основном кражей конфиденциальных данных с площадок электронной коммерции занимаются 14 семейств банковских троянцев. Среди них такие распространенные экземпляры, как Betabot, Panda, Gozi, Zeus, Chthonic, TinyNuke, Gootkit2, IcedID и SpyEye.

***

22.11.2018

Facebook заплатит до $40 тысяч за взлом аккаунтов

Компания Facebook будет платить до 40000 долларов за обнаружение критических уязвимостей на сайтах и в приложениях компании, которые могут привести к захвату чужого аккаунта (InternetUA).

Об этом сообщила пресс-служба программы Facebook Bug Bounty.

«Сегодня, чтобы побудить исследователей безопасности работать над поиском проблем с высоким уровнем воздействия, мы увеличиваем среднюю выплату за ошибки, связанные с захватом аккаунта», – говорится в сообщении.

Отмечается, что к рассмотрению принимаются уязвимости, которые могут привести к полной компрометации чужой учетной записи. В частности, это касается и утечек токенов доступа, и перехвата действующих сессий пользователей.

Так, 40000 долларов будут платить за обнаружение уязвимости, которые не требуют никакого взаимодействия с пользователем. В случае, если какое-то минимальное взаимодействие все же нужно, награда составит 25000 долларов.

«Увеличивая вознаграждение за уязвимость в овладении учетной записи, и уменьшая технические накладные расходы, необходимые для получения бонуса, мы надеемся поощрять еще большее количество высококачественных материалов от наших существующих и новых исследователей, чтобы помочь привлечь более 2 миллиардов пользователей», – резюмировали в компании.

***

22.11.2018

Европейские интернет-провайдеры массово блокируют The Pirate Bay // Украинские провайдеры пока колеблются

Греческие интернет-провайдеры заблокируют доступ к 38 пиратским доменам, включая The Pirate Bay. По просьбе местной группы по борьбе с пиратством, Ассоциации защиты аудиовизуальных произведений (EPOE), и решению комиссии IPPC при Министерстве культуры и спорта Греции провайдеры интернет-услуг заблокируют доступ к The Pirate Bay, 1337x, YTS и другим сайтам, нарушающим права интеллектуальной собственности.

Докладніше

***

23.11.2018
Ирина Фоменко
Мир не осознает угрозы от Интернета вещей

Опрос, проведенный компанией по кибербезопасности Trend Micro, показал, что 86 % ИТ-специалистов и экспертов в области безопасности во всем мире считают, что их организациям необходимо повысить уровень осведомленности об угрозах IoT. Об этом сообщает IoTTechNews (InternetUA).

Причина – в отсутствии знаний, растущем уровне угроз и проблемах безопасности, связанных с подключенными устройствами, которые ставят организации в компрометирующее положение.

Trend Micro опросил 1150 лидеров ИТ, которые выявили отсутствие кибербезопасности во многих организациях по всему миру, развертывающих проекты IoT для внедрения инноваций и цифровых трансформаций.

Более 50 % опрошенных, ответственных за принятие решений в области ИТ и безопасности, заявили, что они определяют приоритетность нескольких ключевых возможностей в своих решениях.

Управление уязвимостями и мониторинг аномального поведения являются главными требованиями для снижения риска компрометации устройств IoT. Trend Micro предлагает комплексный подход к защите сети для таких организаций, гарантируя необходимый уровень безопасности.

Согласно другому исследованию, проведенному Dynatrace в августе, хоть потребители по-прежнему заинтересованы в устройствах IoT, две трети из них признают, что они уже столкнулись с проблемами производительности и потенциальным риском.

Наиболее очевидным примером этой проблемы являются автономные автомобили, причем 85 % обеспокоены тем, что эти транспортные средства могут выйти из строя, а 72 % уверены, что программные сбои в них могут привести к серьезным травмам и летальным исходам. 84 % заявили, что не будут ездить на автономных авто из-за страха программного сбоя.

***

26.11.2018
Ирина Фоменко
Эксперты показали, как можно усложнить пароли против взлома

Несмотря на все предупреждения, некоторые люди все еще ставят пароли наподобие «123456» или «пароль», пишет The Star Online. «Они совершенно небезопасны, их легко угадать и взломать», – заявил директор Института имени Хассо Платтнера в Университете Потсдама в Германии Кристоф Мейнель.

Докладніше

***

26.11.2018

Северокорейские хакеры атакуют банки в Латинской Америке

Специалисты Trend Micro подготовили отчет о деятельности северокорейской хак-группы Lazarus. Исследователи предупреждают, что с середины сентября текущего года группировка заражает бэкдорами финансовые учреждения в странах Латинской Америки.

Докладніше

***

27.11.2018

Соцсеть из Германии получила штраф за нарушение GDPR

Взлом, в результате которого были похищены 808 тыс. электронных адресов и более 1,8 млн имен пользователей, обернулся немецкой соцсети штрафом в размере 23 тыс. евро за нарушение недавно принятого Общего регламента по защите данных (GDPR) (InternetUA).

В июле нынешнего года платформа nuddels.de стала жертвой кибератаки. Неизвестные похитили данные с серверов соцсети и опубликовали их в открытом виде на Pastebin и Mega. По словам сотрудников компании, инцидент затронул всех пользователей, имевших учетную запись в сервисе или зарегистрированных в чате по состоянию на 20 июля 2018 года.

Как оказалось позднее, соцсеть хранила конфиденциальные данные пользователей, в том числе пароли, без какой-либо защиты. В связи с этим, власти обязали сайт nuddels.de заплатить штраф за нарушение требований GDPR. Данный случай является первым в Германии, когда компанию привлекли к ответственности за нарушение GDPR, вступившего в силу в Евросоюзе в мае нынешнего года.

В зависимости от ущерба и количества пострадавших, GDPR предусматривает наказание в виде штрафа до 20 млн евро или 4% от годовой выручки компании. Соцсеть nuddels.de выполнила практически все требования регламента, за исключением одного – пункта «а» статьи 32, требующего шифровать персональные данные пользователей.

***

27.11.2018

Мошенники научились захватывать банковские счета с помощью Google Maps

Мошенники научились использовать Google Maps для собственного обогащения, выдавая с их помощью себя за сотрудников службы поддержки банковских организаций.

Докладніше

***

27.11.2018
Ирина Фоменко
Что делать, чтобы спецслужбы не смогли вас отследить через Google

Отключение функции «История местоположений» на смартфоне Android не помешает Google узнать, куда и когда вы ходили, пишет The Star Online (InternetUA).

Информацию о вашем местоположении по-прежнему будут собирать, поскольку Google обнародовал условия договора использования Android «мелким шрифтом». Так, отключение функции гарантирует только, что ваши данные не будут добавлены в ежемесячную историю местоположений. Тем не менее, некоторые данные геолокации будут сохранены, например, при использовании Google Карты.

Впрочем, есть один способ полностью отключить сбор данных на вашем устройстве Android.

- Откройте меню конфиденциальности в своей учетной записи Google и выберите «Отслеживание действий».
- Отключите функцию «История приложений и веб-поиска».

Только если выполнить вышеизложенные пункты, Google больше не будет собирать данные о вашем местоположении.

Эти шаги можно предпринять непосредственно на вашем смартфоне в приложении Google или через интернет-браузер после входа в свою учетную запись.

Также в меню конфиденциальности пользователи могут выбрать «Мои действия», чтобы узнать, какие данные создаются при использовании служб Google, и какая информация удаляется.

ДОДАТКИ

Додаток 1

16.11.2018
Михаил Сапитон
Facebook запустила образовательный сайт и разрешила постить вакансии в группы

Facebook расширяет собственное HR-направление. После запуска возможности публиковать вакансии, соцсеть объявила о запуске отдельного портала Learn with Facebook (AIN.UA).

Это образовательная платформа, пользователи которой могут получить знания для продвижения по карьерной лестнице или поиска новой вакансии. Курсы отличаются по направлениям: есть советы по составлению качественного резюме, обучающие материалы по маркетингу, технике интервьюирования, программированию.

В Facebook говорят, что содержимое портала ориентировано на новичков. Для более детального ознакомления, они могут переправить учащихся на курсы от зарегистрированных партнеров. На данный момент Learn with Facebook работает во Франции, Германии и США, но в ближайшее время запланировано расширение географии проекта.

Также, Facebook обновила функциональность основной соцсети. Вакансии теперь можно публиковать не только на страницах своего бизнеса, но в и группах. По данным компании, в группах сегодня состоят более 200 млн пользователей.

Инструмент Mentroship, который позволяет выбирать квалифицированных пользователей в качестве инструкторов или учителей в группах, тоже получил новые возможности. Теперь он позволит юзерам публиковать более детальную информацию для поиска нужного партнера. Помимо этого, инструмент научился присылать еженедельные уведомления о прогрессе.

(вгору)

Додаток 2

19.11.2018

Лиза Пальчинская

Украинские соцсети: несмотря на запреты, стать популярным так никому и не удалось

После того, как в мае 2017 года указом президента был запрещен доступ к ряду российских ресурсов на территории Украины, а среди них «ВКонтакте» и «Одноклассники», значительно активизировались ранее созданные украинские социальные сети и активно стали появляться новые. Всех их объединяло амбициозное желание стать национальной площадкой для общения украинцев. Но не всем удалось выжить и воплотить в жизнь заявленные цели (AIN.UA).

Ранее AIN.UA писал про особенности и идеи семи из них. Рассмотрим, что с этими социальными сетями происходит сейчас.

1. «Українці»

Эта социальная сеть была одной из первых украинских, и она до сих пор работает, даже несмотря на архаичность своего набора функций. Однако, она значительно сказывается на посещаемости и активности сайта. Например, в период с августа по октябрь 2018 года эту платформу посетили немногим больше 10 000 человек. Из них 80,66 % – пользователи из Украины.

2. Yachudo

Такой социальной сети не существует с июля 2017, поскольку именно тогда перестал существовать ее домен. Он был изменен на новый, и, если вы перейдете по старой ссылке социальной сети, новый сайт предложит вам найти ресторан поблизости.

3. FamalyUa

Эта платформа должна была стать «самой прогрессивной и удобной в использовании», поскольку задумывалась, как уникальная социальная сеть, объединяющая в себе все лучшее, что есть у остальных. Но, увы, таковой стать ей не удалось. Судя по отзывам пользователей, проблемы со входом на сайт начались еще весной 2017 года. Сейчас социальная сеть FamalyUa не работает, а при переходе на ее сайт вы будете переправлены на различные страницы с подозрительными линками.

4. СІЧ.УКР

Официально эта социальная сеть начала работать 22 января 2017 года и позиционировала себя как площадка для объединения украинцев со всего мира. Но, судя по всему, эта цель оказалась слишком масштабной, сейчас этой сети больше не существует.

5. «НаМайдані»

Эта социальная сеть, созданная в 2014 году, пользуется наибольшим спросом. За три выбранных месяца ее посетили 128548 пользователей. Ежемесячно заходят более десяти тысяч уникальных посетителей.

6. CIMBOR

Эта сеть задумывалась как платформа для жителей Украины, Словакии, Венгрии, Польши и Румынии, но на нее вовсе не заходят жители последних четырех стран. Так, 87,5 % посетителей приходят из Украины, меньше 3 % – из Франции, Чехии и России.

7. Ukrainians

Первая версия этой социальной сети была представлена в начале июня 2017 года. Но по причине отказа ее сооснователя и разработчика канадской компании StartupSoft от дальнейших инвестиций в развитие этого проекта, в начале сентября 2017 Ukrainians прекратила работу.

(вгору)

Додаток 3

21.11.2018

Facebook запатентовал технологию определения семьи пользователя

Facebook подал патентную заявку на технологию, которая предсказывает, кто входит в состав семьи пользователя. Она определяет родственные связи на основе изображений и подписей, размещенных на Facebook, а также информации об их устройствах (InternetUA).

Заявку под названием «прогнозирование демографических данных семей на основе графических данных» подали 10 мая 2017 года, однако о ней стало известно только в ноябре 2018 года.

В тексте патента говорится о том, что компания заинтересована в изучении технологии, которая призвана помочь Facebook более эффективно таргетировать рекламу. «Мы часто публикуем патенты на технологии, которые никогда не реализуем, они не должны восприниматься как указание на будущие планы», – отметили в социальной сети.

Facebook подал заявку до скандалов в области безопасности и конфиденциальности в этом году – Cambridge Analytica, но публикация патента приходит в то время, когда гигант социальных сетей борется с растущим недоверием общественности.

Система, которую Facebook описывает в своей патентной заявке, будет использовать модели распознавания лиц и текста, чтобы в будущем лучше понимать с кем вы живете и с кем чаще всего взаимодействуете. Технология ищет подсказки на фотографиях вашего профиля в Facebook и Instagram, а также на фотографиях ваших друзей.

Алгоритм будет оценивать информацию из комментариев к фотографиям, подписям или тегам (#семья, #мама, #дети) – все, что указывает, являются ли пользователи чьими-то родственниками. Согласно патентной заявке, модели прогнозирования Facebook будут также анализировать «историю обмена сообщениями, прошлую историю тегов, и просмотры веб-страниц».

Социальная сеть привела пример использования алгоритма: сначала робот анализировал изображение с двумя женщинами, где подписью был указан тег «#my_boss_at_home», и другое изображение молодой девушки с пометкой «мой ангел». «Facebook предсказал, что в семье было три человека, в том числе пользователь мужского пола, и две женщины, которые, вероятно, являются женой и дочерью пользователя мужского пола».

Информация предназначена для того, чтобы помочь Facebook доставлять целевую рекламу более эффективно. «Существующие решения доставки контента в семьи не являются эффективными. Без таких знаний рекламные публикации плохо адаптированы для пользователя и, скорее всего, игнорируются им», – добавили в Facebook.

(вгору)

Додаток 4

16.11.2018

На фоне череды скандалов сотрудники Facebook стали испытывать заметно меньше оптимизма по поводу будущего компании

Сотрудники Facebook стали испытывать куда меньше оптимизма по поводу будущего соцсети, чем годом ранее, пишет газета The Wall Street Journal со ссылкой на данные опроса, проведенного в компании (InternetUA).

По данным издания, в недавнем исследовании приняли участие 29 тысяч сотрудников Facebook. Лишь 52 % опрошенных сообщили, что оптимистично смотрят на будущее компании, тогда как годом ранее этот показатель составил 84 %. Кроме того, 53 % респондентов заявили, что Facebook делает мир лучше

– год назад этого мнения придерживались 72 % опрошенных. Наконец, 70 % сообщили, что испытывают гордость, работая в Facebook – этот показатель снизился за год на 17 %.

Сообщается, что основатель и глава Facebook Марк Цукерберг обратил внимание на итоги исследования в ходе недавнего общения с сотрудниками компании. По словам источников WSJ, он и другие топ-менеджеры намерены предпринять шаги для решения наметившихся проблем с настроем персонала.

Издание отмечает, что зафиксированное снижение оптимизма сотрудников компании примечательно тем, что ранее Facebook удавалось преодолевать сложные периоды без таких осложнений. В частности, компания сравнительно успешно пережила обвинения в слабой реакции на фейковые новости, которые распространялись в ходе президентской кампании в США.

Однако, по словам собеседников в Facebook, нынешний период ощущается иначе. Отчасти это объясняется необычной турбулентностью в верхушке соцсети, которая пытается реагировать на внутренние и внешние вызовы. Напомним, в этом году Facebook оказалась в центре скандала с утечкой данных пользователей через одно из приложений, а недавно компания стала жертвой хакерской атаки.

Моральный дух сотрудников Facebook подрывает и заметное падение акций компании, поскольку для многих опционы на акции составляют значительную часть вознаграждения.

«Это был сложный период, но каждый день мы видим, как люди объединяются, чтобы извлечь уроки прошлого года и построить более сильную компанию», – отметила представитель Facebook.

WSJ напоминает, что за последние четыре месяца акции Facebook упали в цене на 35 %. При этом в конце сентября численность сотрудников компании составляла 33,6 тыс. человек, на 45 % больше, чем годом ранее.

(вгору)

Додаток 5

16.11.2018

Facebook заказывал пиар-кампании против конкурентов, чтобы отвлечь внимание от проблем безопасности

Facebook нанимал лоббистов, чтобы отвлечь внимание на своих конкурентов во время скандала об утечке данных. Об этом пишет газета New York Times (NYT) в своем расследовании (InternetUA).

Газета пишет, что Facebook пыталась отвлечь внимание после того, как стало известно о ее сотрудничестве с компанией Cambridge Analytica.

В марте выяснилось, что с соглашения руководства соцсети Cambridge Analytica использовала данные пользователей фейсбука. По информации СМИ, всего британская аналитическая фирма, работавшая на предвыборный штаб Дональда Трампа, получила доступ к нескольким десяткам миллионов аккаунтов. В мае Cambridge Analytica подала документы о банкротстве.

Еще одной проблемой для Facebook стала информация о том, что аккаунты, связанные с Россией, используют сеть с целью дискредитации демократов в ходе президентской кампании.

Из-за скандала, как пишет NYT, в Facebook приняли решение нанять несколько лоббистских фирм, в том числе чтобы дискредитировать своих критиков. Одним из способов стала попытка связать оппонентов с миллиардером Джорджем Соросом, который несколько раз публично критиковал Facebook. Также часть критики соцсеть попыталась выставить как антисемитскую.

Еще Facebook попыталась отвлечь внимание от скандалов и поддержала инициативу, которая вводит ответственность для ИТ-компаний за рекламу секс-торговли. Против законопроекта выступал, например Google, так как считал, что его будет слишком сложно выполнять. Кроме того, нанятые компанией лоббисты опубликовали несколько статей на консервативных сайтах с критикой Google и Apple. Apple до этого воспользовалась скандалом с Facebook и Cambridge Analytica и публично заявила, что не торгует данными пользователей. Это вызвало ярость у главы Facebook Марка Цукерберга, отмечает NYT.

Официально же компания Цукерберга выбрала более спокойный тон, пишет газета, и регулярно говорила, что работает над тем, чтобы исправить допущенные ошибки.

(вгору)

Додаток 6

19.11.2018
Владимир Кондрашов
Украинский хакер проник на «фабрику российских троллей»

Украинскому консультанту по кибербезопасности Егору Папышеву удалось проникнуть на «российскую фабрику троллей» и узнать некоторые подробности работы «кремлеботов» изнутри. Как оказалось, на российских ботофермах используют специальный софт для работы с социальными сетями, обучают сотрудников и готовят площадку для очередной информационной волны, «арендуя» реальные аккаунты украинцев в соцсетях.

Об этом Егор Папышев написал на своей странице в Facebook, передает InternetUA (InternetUA).

Внимание украинского хактивиста несколькими днями ранее привлекла публикация его товарища, в которой тот обсуждал рекламу в Facebook с предложением для украинцев заработать на своём аккаунте. Некое «рекламное агентство» запустило в соцсети рекламу с предложением заработка именно украинским пользователям – они предлагали собственнику аккаунта установить программу, через которую удаленно могли бы управлять профилем. Ключевые условия «рекламного агентства»: профиль обязательно должен быть «реальным». За возможность управлять чужим профилем в социальной сети,

«рекламщики» предлагают оплату каждые два дня на карту банка либо на счета запрещенных в Украине платежных систем.

Как пишет Егор Папышев, он решил пойти дальше и посмотреть на работу «рекламного агентства» изнутри.

Масштабы происходящего, по его словам, «впечатляют неискушенного в “накрутках” и прочих приемах зрителя»:

– Используя недостатки в системе коммуникации владельцев ботофермы, мне удалось проникнуть и посмотреть на неё изнутри. У ботоводов детально налажены процессы работы и учета, отчетности, настроена инфраструктура и специализированный софт, – написал Папышев. – Они управляют своим ресурсом, постоянно актуализируют его и оперативно переключают на выполнение разных задач. Они занимаются обучением своих сотрудников. Они могут регистрировать сотни аккаунтов, создавать посты, лайкать, репостить, жаловаться на другие аккаунты, писать в сообщества, менять информацию в своих профилях, и всё это – массово, всего в пару кликов.

Папышев подчеркивает: ботофермы – это бизнес, который сегодня может «продвигать» одну персону, а завтра сделать «массовый вброс» фейковых новостей с перекрестными репостами и лайками, чтобы ударить по репутации другой.

– В условиях приближающихся выборов я бы хотел напомнить вам, друзья, что происходит масса информационных операций и различных манипуляций, буквально поставленных на поток. Информационная война в разгаре, одно из направлений атаки – социальные сети. С сожалением отмечу, что большая часть аудитории соцсетей – это люди, которые достаточно легко поддаются на провокации, «вбросы» и по-прежнему верят фейковым новостям, – напоминает Папышев.

– Просматривая скриншоты, на которых я попытался раскрыть контекст, пожалуйста, подумайте о том, насколько критично следует относиться к различным инфоповодам, касающимся политики и репутации каких-либо известных персоналий. Как показал ряд недавних кейсов, развернуть серьезную информационную операцию ничего не стоит, в сравнении с «выхлопом», который получают заинтересованные лица, – резюмирует консультант по кибербезопасности.

(вгору)

Додаток 7

20.11.2018

Політики інвестують в Інтернет. Як захиститися від маніпуляцій у соцмережах

Існує кілька типів так званих маніпулятивних тролів

Стати бототролем в соціальних мережах можна за 1000 грн, розповів керівник програм нових медіа громадської організації Інтернюз-Україна Віталій Мороз (Новое время).

Електорат у соцмережах

За словами експерта, напередодні українських виборів у 2019 році такий спосіб впливу на громадську думку лише посилюватиметься. Політики інвестують великі гроші в інтернет, адже розуміють, що там є активний електорат, який може впливати на своє оточення. Проте ці потенційні виборці погано реагують на політичну рекламу, адже мають власну думку.

Найбільш поширеною маніпуляцією є вплив через умовних лідерів думок

Тому партії вигадують способи, як вплинути на них, говорить медіаексперт. Мороз додає, що сьогодні вакансії троля у соцмережах, наприклад, Facebook, Twitter, Instagram можна без проблем знайти у відкритому доступі на сайтах з пошуку роботи.

«Створювалися фейкові акаунти, які могли викрадати фотографії реальних людей і змінювати ім'я. Часто користувачі помічали фейкові акаунти і про це говорили. В інтернеті уже з'явилися оголошення, зокрема, на OLX, на яких пропонують дати доступ до свого акаунту на Facebook за 1000 грн в місяць», – сказав Мороз.

Типи маніпуляторів

Як розповів медіаексперт, існує кілька типів так званих маніпулятивних тролів. Перший, тобто класичний, це люди, які коментують і створюють контент на користь певних політиків чи партій. Робота в інтеренеті для них – це заробіток.

Це справжні публічні люди, які отримують гроші за свої пости, в яких не прямо, проте рекламують певну особу чи політичний рух. Вони також коментують пости та різні дописи. На все є відповідна ціна, яка залежить від рівня публічності самої особи.

Другий тип – це напівавтоматизовані системи, а саме боти. Люди здають в оредну свій акаунт в соцмережі за відповідну суму. Це може бути від 500 до 1000 грн на місяць та вище. Натомість програма аналізує дані ваших друзів – таргетує, надсилає їм рекламу, що матиме найбільший вплив персонально на цю людину.

Третій тип – прості користувачі, у яких купують доступ до акаунту й через них відбувається певна політична активність. Актуальними також залишаються фейкові сторінки, додав Віталій Мороз.

Вплив через лідерів думок

Соціальні мережі стали фактично засобами масової інформації, принаймні, за своїм змістом, говорить політтехнолог та політичний консультант Павло Кругляковський. За його словами, ці платформи в майбутньому можуть стати основними каналами, звідки ЗМІ братимуть інформацію. Адже вже зараз редактори та журналісти часто знаходять інформаційні приводи саме там.

Маніпуляції громадською думкою в інтернеті є дуже небезпечними. На думку Кругляковського, напередодні виборів найбільш поширеною маніпуляцією є саме вплив через умовних лідерів думок. Тобто, перший вид тролів за класифікацією медіаексперта Віталія Мороза.

«Користувачі соціальних мереж не дуже дисципліновані як виборці. Там сидять лідери думок. Це канал комунікації, ексклюзивної інформації. А потім її вже підхоплюють ЗМІ», – зазначив Кругляковський.

Технологічно впливати через соцмережі простіше, адже вони не регулюються законодавством й ніяких вимог до тексту чи відео немає.

Що рекомендують для захисту акаунтів

Передусім, щоб захистити себе у соцмережах, потрібно обов'язково перевіряти, яким додаткам ви надали доступ до управління своїми персональними даними, розповів експерт із онлайн-комунікацій, керуючий партнер агенції цифрових комунікацій PlusOne DA та редактор онлайн-видання Watcher.com.ua Максим Саваневський.

За його словами, багато додатків, що збирали великі дані, наприклад, у Facebook вже не пропускаються через систему авторизації соцмережі, проте вони все ще є, а дані користувача в них можуть зберігатись невизначений час.

«Треба використовувати двофакторну авторизацію, прив'язувати номер телефону. А у налаштуваннях applications можна переглянути список додатків, яким ви дали доступ до вашого акаунту у Facebook», – сказав Саванецький.

У висновках делегації Національного демократичного інституту та Європарламенту, які проводили оцінку передвиборчого середовища в Україні з 12 до 17 листопада 2018 року, йдеться про те, що ймовірність втручання Росії у вибори – один із ключових викликів президентської виборчої кампанії України в 2019 році.

У березні 2018 року стало відомо, що компанія Cambridge Analytica через свій додаток в Facebook збирала дані користувачів. Передбачається, що ці дані могли бути використані під час виборчої кампанії в США в 2016 році та референдуму про вихід Великобританії з Євросоюзу.

(вгору)

Додаток 8

14.11.2018

Дмитрий Демченко

В Раду внесли законопроект про защиту информационного пространства. Активисты назвали это введением цензуры

Седьмого ноября в Верховной Раде зарегистрировали законопроект №9275 «О внесении изменений в некоторые законы Украины относительно защиты информационного пространства». Ряд общественных организаций выступили против этого документа и заявили, что депутаты пытаются «в очередной раз ввести цензуру в Украине под прикрытием борьбы с российской пропагандой» (AIN.UA).

Законопроект №9275 содержит изменение двух норм существующего законодательства.

Во-первых, его авторы предлагают расценивать как терроризм «предоставление информационной поддержки» террористическим

організаціям или любым другим незаконным вооруженным формированиям – и закрепить это положение в соответствующем законе.

Во-вторых, авторы документа хотят предоставить Верховной Раде исключительное право предлагать СНБО СМИ, к которым должны применяться санкции.

Против этого законопроекта выступили несколько украинских общественных организаций: коалиция «За свободный Интернет», Национальный союз журналистов Украины, Академия украинской прессы, «Детектор медіа» и другие. Они считают, что законопроект №9275 «создает очередную возможность власти произвольно и незаконно вмешиваться в свободу слова и деятельность СМИ (в том числе, интернет-изданий), что особенно угрожающей в условиях приближения выборов».

Указанный законопроект не содержит процедуры и четких критериев оценки, какие медиа могут подлежать санкциям. Предлагаемое определение «информационной поддержки» терроризма допускает произвольное толкование, при котором любое упоминание незаконных формирований в СМИ может считаться их популяризацией и приравниваться к террористической деятельности. Таким образом, народные депутаты получат практически неограниченное право вмешиваться в деятельность СМИ, основываясь лишь на собственной политической воли.

Общественные организации подчеркивают, что депутаты должны разработать другие механизмы, отвечающие международным стандартам защиты прав человека. В частности – привлекать суды или независимые органы для решений об ограничении контента в интернете: «При этом, решение должно быть конкретным, направленным на достижение четкой цели и основываться на оценке эффективности ограничений и рисков чрезмерного блокировки».

(вгору)

Додаток 9

16.11.2018

Искусственный интеллект вычислит наркодилеров среди пользователей Facebook и Instagram

Весной конгрессмены раскритиковали Марка Цукерберга, указав, что FB стала платформой для наркодилеров. Теперь вычищать подозрительные объявления поручили ИИ – и алгоритм будет делать это быстрее модераторов-людей (InternetUA).

Facebook и Instagram начинают применять ИИ для выявления наркодилеров, которые работают со своими клиентами через соцсети. Технология «проактивного обнаружения» позволяет удалять фотографии, на которых изображены наркотики, еще до того, как на них пожалуются пользователи, пишет Telegraph.

«Наша технология распознает изображения, на которых есть не только сами запрещенные вещества, но и информация о намерении их продать, цены, номера телефонов и ссылки на аккаунты дилеров», – рассказал глава департамента по связям с общественностью Facebook Кевин Мартин.

Технологию также будут развивать и использовать другие IT-компании, среди которых Google и Twitter.

ИИ заменит модераторов, в обязанности которых входил просмотр страниц, хэштегов и групп на предмет возможной связи с наркобизнесом.

К альянсу, который называют Tech Together to Fight the Opioid Crisis, присоединятся исследователи Алабамского университета. Они будут отслеживать новые тактики продаж, которые применяют дилеры, а также новые сленговые названия наркотиков.

Представитель Google Сьюзен Молинери говорит, что ежедневно в поисковике регистрируется 50000 запросов, связанных с опиоидами. Многие пользователи ищут, как справиться с зависимостью родственников или друзей. Таким людям будут предлагать доступные на территории США программы психологической и физической реабилитации, пример Partnership for Drug-Free Kids.

Видеохостинг YouTube также будет размещать таргетированную рекламу бесплатных центров реабилитации для пользователей, которых алгоритмы посчитали потенциальными клиентами наркодилеров.

Facebook обещает регулярно публиковать отчеты о масштабах и эффективности проделанной работы по борьбе с нежелательным, запрещенным и незаконным контентом. Так, технологический гигант начал блокировать ссылки на сайты, если там содержатся чертежи для печати оружия на 3D-принтере.

(вгору)

Додаток 10

19.11.2018

86 компаний потребовали от Facebook улучшить систему обжалования блокировок

Авторы текста считают, что социальная сеть необоснованно блокирует большое количество публикаций (InternetUA).

За последний год Facebook была вынуждена расширить свою практику модерации контента в ответ на требования защитников по правам человека, которые утверждали, что компания не защищает «уязвимых» пользователей от языка ненависти. Теперь Facebook подвергся критике из-за непоследовательной модерации контента.

Открытое письмо Марку Цукербергу, подписанное 86 организациями, требует от Facebook обеспечить четкий и быстрый механизм, который позволяет пользователям обжаловать случаи удаления контента и деактивации учетных записей. В тексте также есть призыв ко всем социальным сетям.

Авторы требуют улучшить прозрачность и отзывчивость модераторов на обжалованные сообщения и призывы к удалению контента.

В апреле этого года Facebook запустил жалобы на сообщения, которые удаляются по мотивам ненависти или призывам к насилию. Пресс-релиз социальной сети утверждает, что один из рецензентов рассмотрит все апелляции в течение 24 часов и уведомит пользователей об ответе. У Facebook было 4500 модераторов контента в мае 2017 года, а через год их количество удвоилось.

Существует несколько громких примеров удаления контента Facebook и деактивации учетных записей, которые позже признали ошибочными. Например, аккаунт рэпера Lil B приостановили на 30 дней за комментарии о белых людях, которые, по утверждению Facebook, нарушили политику толерантности. После этого пользователи по всей стране заявили, что их учетные записи часто ошибочно отключаются временно или навсегда, а их контент помечается и удаляется за нарушения стандартов сообщества.

Открытое письмо Марку Цукербергу также требует, чтобы все апелляции на удаление и деактивацию контента были рассмотрены модератором-человеком. Однако компания, наоборот, планирует доверить это роботам.

В мае этого года Facebook опубликовал свой первый отчет о соблюдении стандартов сообщества. Согласно нему, компания получила 3,4 миллиона жалоб в первом квартале 2018 года. В докладе также утверждается, что только 14 % контента – это жалобы пользователей, 86 % же публикаций нашли сами модераторы.

(вгору)

Додаток 11

21.11.2018
Ирина Фоменко
The Guardian: Российский «тролль» подал в суд на Facebook за бан

Российская компания, чьего бухгалтера федеральные прокуроры обвинили во вмешательстве в выборы в США, подала в суд на Facebook, заявив, что у нее законный новостной канал, а учетная запись должна быть восстановлена. Об этом сообщает The Guardian (InternetUA).

Федеральное агентство новостей LLC, известное как ФАН, и его единственный акционер Евгений Зубарев, подали иск в федеральный суд в северном районе штата Калифорния, требуя возмещения убытков и судебного запрета для Facebook на бан аккаунта.

Facebook удалил учетную запись ФАН в апреле во время «чистки страниц», связанных с находящимся в Санкт-Петербурге Агентством интернет-исследований, которое в прошлом году Роберт Мюллер обвинил в распространении в социальных сетях ложной информации с целью вмешаться в выборы 2016 года.

ФАН и Зубарев заявили, что их аккаунт Facebook ошибочно удалил во время «чистки», в результате которой заблокировано более 270 учетных записей и страниц на русском языке. «ФАН – независимое, достоверное и законное информационное агентство, которое публикует актуальные и интересные отчеты», – прокомментировали в компании.

В иске утверждается, что Facebook фактически действовал на поводу у правительства, нарушив право на свободу слова. Также ссылаются на Закон о гражданских правах 1964 года: соцсеть обвиняют в дискриминации в связи с русским происхождением.

Ренато Мариотти, бывший федеральный прокурор, назвал эти аргументы слабыми и предполагает, что истцам будет сложно найти поддержку в судах. «Можно с уверенностью сказать, что этот иск не будет успешным. Это больше похоже на PR-ход», – заявил Мариотти.

В прошлом месяце ФАН признало, что ранее занимало одно и то же офисное здание вместе с Агентством интернет-исследований, а также то, что в агентстве работает Елена Алексеевна Хусяйнова на должности бухгалтера, которую обвиняют во вмешательстве в промежуточные выборы 2018. По словам истцов, роль Хусяйновой в компании ограничивается бухгалтерией, она не является офицером и не имеет никакого влияния в отношении редакционного контента.

Истцы также заявили, что они не участвовали в «Проекте Лахта» – поддерживаемой Кремлем информационной кампании, которая, как утверждают прокуроры США, была начата в 2014 году и финансировалась Евгением Пригожиным, олигархом, близким к президенту России Владимиру Путину.

В феврале этого года Пригожин, известный как «шеф-повар Путина» из-за кейтеринговой компании и связей с Кремлем, был обвинен вместе с Агентством интернет-исследований, которое он контролирует. Хусяйнова была также главным бухгалтером «Проекта Лахта». Мюллер не рассматривает дело Хусяйновой, поскольку его внимание сосредоточено на президентских выборах 2016 года, а обвинения против нее связаны с промежуточными выборами в 2018 году.

(вгору)

Додаток 12

24.11.2018

Почему законы о клевете не будут работать в украинском Интернете

Украинцев могут привлечь к криминальной ответственности за посты и комментарии в Интернете, содержащие клевету. НВ разбиралось, как принятие законопроекта отразится на интернет-цензуре и как это регулируют в других странах (InternetUA).

На днях, на сайте Верховной Рады Украины появился проект закона, в котором предлагают внести изменения по поводу ответственности граждан за

клевету. Три депутата от Блока Петра Порошенко – Николай Паламарчук, Артур Палатный и Олег Великин – собираются ужесточить наказания за умышленное распространение заведомо ложных данных, в том числе в интернете.

Как известно, до сих пор в Украине действует лишь гражданская и административная ответственность за клевету, но теперь политики планируют добавить это правонарушение к разряду криминальных.

Согласно пояснительной записке законопроекта, причиной таких жестких мер является недавний случай с убийством правозащитницы Екатерины Гандзюк, в котором некоторые СМИ обвиняли самого Николая Паламарчука и его бывшего помощника Игоря Павловского.

Сам Паламарчук, который также является первым заместителем главы правоохранительного комитета, теперь предлагает за публикацию заведомо ложной информации в СМИ или в интернете наказывать штрафом от 500 до 1,5 тыс. необлагаемых минимумов, исправительными работами до одного года или ограничением свободы до двух лет.

Если же клевета связана с совершением тяжкого или особо тяжкого преступления, – автору грозит от двух до пяти лет ограничения свободы или до трех лет лишения свободы.

Почему это важно?

Несмотря на то, что законопроект касается информации, которая «порочит честь и достоинство другого человека или подрывает его деловую репутацию», некоторые эксперты обеспокоены цензурированием украинского онлайн-пространства.

В зависимости от того, насколько действенным будет этот закон, интернет-платформы и онлайн-медиа могут привлекаться к ответственности за простую критику чиновников.

До Роскомнадзора, конечно, еще далеко, но новый закон может стать подспорьем для ограничений свободы слова в сети. Как рассказала юрист общественной организации «Лаборатория цифровой безопасности» Вита Володовская интернет-изданию Ain.ua, такой закон может привлекать к ответственности даже за комментарии или посты в Facebook.

«Опасность возвращения клеветы в Уголовный кодекс состоит в том, что даже угроза быть привлеченным к ответственности может быть существенным ограничительным фактором для журналистов и медиа, ведь за любое расследование о злоупотреблениях или коррупции против них уже могут инициировать уголовное производство. Это ведет к самоцензуре, тем более, с уровнем доверия к украинским судам», – прокомментировала Володовская для Ain.ua.

По сути: привлечение к криминальной ответственности за клевету может вызвать цепную реакцию в становлении интернет-цензуры в условиях выборочного действия украинских законов.

Что с этим в других странах?

В пояснительной записке инициаторы поправок к закону привели примеры международного опыта борьбы с публичной клеветой. В частности, политики указали, как карают за клевету в Польше, Италии, Швеции, Германии, Франции, США.

По их данным, наиболее серьезные наказания существуют в США, где некоторые штаты предусматривают за клевету штраф до $250 тыс. или до 10 лет лишения свободы.

Депутаты от БПП вспомнили еще ряд стран, законы которых предусматривают криминальную ответственность за клевету и написали, что такие действия в Украине несут «существенную общественную опасность».

«Вследствие безнаказанности за откровенную клевету, в обществе укрепляется стойкое ощущение того, что можно что-либо и когда-либо сказать о человеке и не нести за это никакой ответственности», – написали Паламарчук, Палатный и Великин.

По сути: Подобные законы существуют и в других странах, наравне с наличием действующего цифрового права, которое фактически отсутствует в Украине.

Примут ли закон?

Напомним, что это не первый скандальный законопроект, который грозил становлением цензуры в сети. Летом 2018-го был отозван закон #6688, согласно которому интернет-провайдеры должны были устанавливать оборудование для фильтрации трафика, персонифицировать абонентов и получали право досудебной блокировки сайтов.

Чтобы узнать, не повторит ли новый законопроект о клевете эту же участь, НВ пообщалось с руководителем программ новых медиа общественной организации «Интерньюз-Украина» Виталием Морозом.

Виталий подтверждает, что законы о клевете или диффамации приняты во многих европейских странах и они призваны защищать честь и достоинство истцов. Но, что касается Украины, по его словам, важно помнить, в каких целях собираются использовать этот закон и когда именно его хотят принять.

«Украинские реалии не позволяют надеяться, что этот закон будет служить в первую очередь в благих целях», – говорит Виталий.

Эксперт напоминает о том, что комментарии и посты в соцсетях являются проблемным местом для действующего украинского законодательства, поскольку сейчас онлайн-медиа в нашей стране практически не регулируются.

«Даже вердикты судов за нарушение статей 109 и 110 Криминального кодекса Украины (действия с целью захвата власти и посягательство на государственную целостность - ред.) против модераторов групп в социальных сетях должны были бы иметь отдельные законодательные нормы, прописанные конкретно по поводу онлайн-пространства. Сегодня же суды трактуют онлайн-пространство как публичное пространство на основе законов, которые были приняты для офлайн-среды».

Виталий Мороз также говорит о неоднозначности возможного закона о дезинформации и распространении фейков, учитывая гибридную войну в

Украине. Дескать, некоторые страны, включая недавний опыт Германии и Малайзии, подписывают законы, которые обязывают онлайн-платформы бороться с фейками, но это, опять же, встречается шквалом критики и дискуссий о цензуре.

«Сейчас в Украине изучают французский опыт, который базируется на судебных решениях и отдельных судьях. Но там не идет речь о криминальной ответственности», – объясняет Виталий.

Что касается конкретно предложенных депутатами БПП поправок к криминальной ответственности за публичную клевету, эксперт уверен – накануне выборов такие неоднозначные законопроекты вряд ли найдут поддержку.

По сути: Учитывая проблемы в украинском законодательстве с онлайн-публикациями и грядущие президентские выборы в стране, подобные законопроекты можно рассматривать как манипуляции отдельных политических сил.

(вгору)

Додаток 13

14.11.2018
Ирина Фоменко
Ваш старый смартфон представляет угрозу

Старый смартфон, спрятанный в ящике или шкафу, хоть и не кажется угрозой национальной безопасности, однако администрация Трампа считает его таковым, пишет The Star Online (InternetUA).

Недобросовестные китайские производители могли перерабатывать старые телефоны в «контрафактные товары, которые входят в цепочку поставок военной и гражданской электроники Соединенных Штатов». Чтобы этого не произошло, Министерство торговли США предлагает строго ограничить экспорт используемой электроники.

Идея не нова. За последнее десятилетие подобные предложения неоднократно терпели неудачу в Конгрессе. Но антикитайская политика правительства вселила надежду в сторонников экспортных ограничений.

На долю США приходилось менее 15 % используемых электронных гаджетов, выброшенных во всем мире в 2017 году. Эксперты утверждают, что запрет даст только ложное чувство безопасности, а взамен потребует значительных экономических и экологических потерь.

В конце 1990-х годов журналисты и общественные организации начали фиксировать ущерб, вызванный рециркуляцией низкотехнологичной электроники на юге Китая. Рынки подержанных устройств сделали электронные «отходы» оффшорами. В Китае продавцы электроники зарабатывают до 80 % своих доходов, продавая устройства и детали.

В Хуацянбэйе, Шэньчжэнь, тысячи компаний продают и покупают подержанные устройства и запчасти. Нужны 1000 материнских плат iPhone 6?

Поставщики могут организовать их, используя огромную, неформальную сеть перерабатывающих компаний Китая. Многие из б/у деталей установлены в новых устройствах. Наиболее распространенными направлениями являются более дешевые потребительские товары, предназначенные для развивающихся стран.

Смартфоны для африканских и индийских рынков часто имеют восстановленные дисплеи или другие, бывшие в употреблении, детали (соответственно, устройства «живут» меньше и стоят дешевле). Производители редко информируют потребителей об этом, что побуждает многих критиков обвинять китайских поставщиков в подделке.

Впрочем, для американских военных это не новость. В 2012 году Комитет по вооруженным силам Сената США опубликовал отчет, в котором раскрыто не менее 1800 дел, где в военной технике оказалось около 1 млн фальшивых деталей, и большинство из них получены из Китая. Такие запчасти создают серьезные риски для национальной безопасности.

В последние годы военные предприняли шаги по ограничению торговли. Вскоре после доклада комитета Конгресс принял законодательство, требующее расширенных инспекций, отчетности и штрафов за закупку контрафактных деталей. На долю Азии, а не Европы или Северной Америки, приходится наибольший объем производства электронных отходов – около 40 % от общей суммы. Крупнейшим источником был Китай, с 1 млрд пользователей смартфонов.

Кто выиграет от ограничений на экспорт подержанной электроники из США? Конечно, не военные, которые все равно должны избегать подделок, поступающих из Китая. Вместо этого экспортный контроль США обеспечит ложное чувство безопасности для организаций, закупающих детали в Китае, одновременно устанавливая экологические издержки для обеих стран.

Повторное использование гаджета – будь то смартфон или полупроводник – всегда является более экологичным вариантом, чем переработка в сырье. Кроме того, это более выгодно, а также снижает затраты для потребителей.

(вгору)

Додаток 14

15.11.2018

Дмитрий Демченко

В МХП хотят отслеживать эмоции сотрудников с помощью видеонаблюдения. Это законно?

14 октября появилась информация о том, что агрохолдинг «Мироновский хлебопродукт» ввел систему мониторинга эмоций сотрудников, которая работает с помощью камер видео наблюдения. Об этом заявил глава правления компании Юрий Косюк на форуме «Дирижеры изменений». Редактор AIN.UA

рассказывает о ситуации и приводит мнение юристов о том, законно ли это (AIN.UA).

Глава правления МХП отметил, что руководство мониторит эмоции сотрудников, чтобы вычислять счастливых и несчастных людей. С последними работают психологи и HR-специалисты холдинга, чтобы исправить ситуацию или, в ином случае, заменить их.

«Есть у нас парень, который очень стремительно набрал вес. И HR-специалист наблюдал последние полгода, как он толстеет. Когда психологи начали работать с этим человеком, оказалось, что единственной радостью в жизни он считал возможность вкусно поесть. Мы поняли, что человек не может занимать высокую позицию, поскольку он занимает чье-то место и сдерживает рост молодых активных мотивированных людей».

Что заявили представители МХП

Директор департамента управления персоналом и комуникаций МХП Ксения Прожогина на своей странице в Facebook подчеркнула, что издания, написавшие о заявлении Косюка, неправильно интерпретировали его слова. Она отметила, что сейчас такая система только тестируется: в процессе участвует более 70 сотрудников, и все они выразили готовность экспериментировать.

«Они подписывают письменное уведомление. Также, когда сотрудник принимается на работу, мы с ним подписываем соглашение об обработке не только персональных данных, но и биометрических. А съемка камерой — это персональные биоданные», – комментирует Прожогина изданию Лига.net.

Она также отмечает, что за время тестирования ни один человек не был уволен – лишь трех компания перевела на другие проекты. История же о сотруднике, которому задали вопросы из-за его телосложения, «вообще не имеет отношения к проекту». При этом представитель МХП добавляет, что если помощь от HR-специалистов помогать не будет, компания будет стараться, чтобы сотрудник ушел сам. Кроме этого, Лига.net сообщает, что до конца 2019 года МХП планирует перевести под наблюдение весь административный персонал компании – около 6000 человек.

Что говорят юристы

Дима Гадомский, адвокат, партнер Axon Partners

Украинский кодекс законов о труде 1971 года, мягко говоря, не особо современный – слежку за сотрудниками он не регулирует никак. Документ лишь в общих чертах предусматривает, что компания должна ознакомить сотрудника под расписку об условиях труда. А вот гражданское законодательство прямо запрещает съемку человека без его согласия (кроме публичных мероприятий, вроде митингов или конференций).

Поэтому я бы советовал предупреждать сотрудников о том, что компания за ними наблюдает. В трудовом договоре или же во внутренних правилах.

Вообще это абсолютно нормально, когда компания следит за сотрудниками – но только если это имеет бизнес-цель, и при этом не нарушается право сотрудника на личную жизнь.

К примеру, американский Electronic Communications Privacy Act (1986 год) позволяет работодателю читать рабочую переписку и мониторить телефонные переговоры сотрудников (это бизнес-цель). Но как только сотрудник обсуждает личные вопросы по телефону, компания обязана прекратить запись разговора (это его личная жизнь). Другой вопрос, что работодатель может запретить сотрудникам использовать рабочие средства связи для личных вопросов.

Я не вижу особых проблем с системами для определения эмоций сотрудников. Главное, чтобы компания не принимала решения об увольнении или об уменьшении зарплаты только на основании каких-то поведенческих паттернов. Украинский кодекс законов о труде хоть и ретроградный, все же предусматривает четкий перечень оснований, к примеру, для увольнения. И неудовлетворительные эмоции в этот перечень и близко не входят.

У меня иногда ощущение, что в Украине работники имеют больше прав, чем работодатели. При этом на работодателе лежат все бизнес-риски, а сотрудник, наоборот, хочет находиться в состоянии условной «стабильности».

Применимо к истории вокруг МХП мне очень нравится мысль футбольного тренера сэра Алекса Фергюсона. Он говорит, что самый лучший игрок может отравить обстановку в команде и от такого игрока нужно срочно избавляться. Так что действия МХП мне вполне понятны.

В трудовых спорах суд почти всегда занимает сторону сотрудника. Поэтому если компания хочет полагаться в своих решениях на результаты компьютерного моделирования поведения и хочет выглядеть красиво в суде, то нужно иметь письменное согласие сотрудника на такие эксперименты. Это может быть трудовой договор, или подпись сотрудника под правилами внутреннего распорядка.

Кристина Немчинова, сооснователь юридической фирмы Brightman

Гражданский кодекс Украины устанавливает, что проведение фото-, кино-, теле- и видеосъемки физического лица возможно только с его согласия. Получение такого согласия необязательно в двух случаях. Первый – это проведение съемки открыто на улице, сборах, конференциях, митингах и других мероприятиях публичного характера. Второй – в случаях, установленных законом (следственные действия, судебный процесс и так далее). Закон «О защите персональных данных» и закон «Об информации» также обязывают получать согласие человека на проведение съемки.

Видеонаблюдение в офисе правомерно только когда оно соблюдает требованиям законодательства. Для этого такой пункт должен содержаться в Правилах внутреннего трудового распорядка и Положении о защите персональных данных компании и в специальном указе. Кроме этого, в помещении, где ведется съемка, работодатель обязан установить оповещение – например, табличку с предупреждением.

Кодекс законов о труде Украины устанавливает, что работодатель обязан сообщить работнику об условиях труда, ознакомить его с правилами внутреннего распорядка и коллективным договором. При этом такое

разъяснение проводится под роспись. Соответственно, работодатель может устанавливать контроль над действиями сотрудника на рабочем месте только с его согласия. При этом работодатель не имеет права отказать в принятии на работу, если кандидат не дал такое согласие.

Ситуация с видеонаблюдением в МХП весьма резонанса. Если компания установила видеонаблюдение в офисе в соответствии с вышеуказанными требованиями, такая видеосъемка будет считаться законной. Но проведение видеосъемки для выявления эмоций сотрудников (даже с их письменного согласия) фактически представляет собой мониторинг за поведением граждан и анализ их поведения.

Выявление каких-то «неправильных» эмоций на рабочем месте не может стать причиной увольнения сотрудника. Их четкий перечень закреплен в статье 40 КзоТ, и эмоциональное состояние работника в него не входит. По сути такой мониторинг не имеет никакого отношения к выполнению лицом своих профессиональных обязанностей.

Можно предположить, что анализ эмоционального состояния работника, его настроения и того, насколько он счастлив – это вмешательство в личную и семейную жизнь, что нарушает статью 32 Конституции. Неприкосновенность частной и семейной жизни лица закреплена также на международном уровне, например, в статье 8 Конвенции о защите прав человека и основных свобод.

(вгору)

Додаток 15

15.11.2018

Уязвимость в Android позволяет следить за местонахождением пользователей

Исследователи компании Nightwatch Cybersecurity раскрыли подробности об уязвимости в Android, позволяющей следить за местонахождением пользователей. С помощью уязвимости (CVE-2018-9581) злоумышленник вблизи Wi-Fi маршрутизатора может отслеживать передвижение пользователей в зоне действия сигнала беспроводной сети (InternetUA).

Проблема связана с утечкой информации через межпроцессное взаимодействие. Как правило, на Android-устройствах приложения отделяются операционной системой как друг от друга, так и от самой ОС. Тем не менее, в случае необходимости они могут обмениваться информацией между собой с помощью специальных механизмов.

Один из таких механизмов предполагает использование объекта обмена сообщениями Intent. С помощью Intent приложение или сама ОС может отправлять сообщения, распространяющиеся на всю систему, которые могут «слушать» другие приложения. При отсутствии надлежащих ограничений доступа к этому механизму вредоносные приложения могут воспользоваться им для перехвата информации, доступа к которой у них быть не должно.

Как пояснили в Nightwatch Cybersecurity, существуют специальные функции, позволяющие ограничивать доступ к сообщениям Intent, однако разработчики приложений часто ими пренебрегают. В результате возникает распространенная уязвимость, позволяющая вредоносному приложению следить и перехватывать сообщения, предназначенные для других приложений на одном с ним устройстве.

В случае с CVE-2018-9581 вина лежит на разработчиках самой ОС. По словам исследователей, Android регулярно транслирует информацию о подключении Wi-Fi с помощью двух объектов Intent. В частности, ОС сообщает всем приложениям данные об индикаторе мощности принимаемого сигнала (RSSI), который не всегда совпадает с транслируемым сигналом.

Чем ближе мобильное устройство к маршрутизатору, тем сильнее сигнал. Поскольку данные о RSSI транслируются на всю систему, вредоносное приложение может использовать их для определения местоположения пользователя относительно маршрутизатора. Таким образом, с помощью уязвимости начальник, например, может следить за сотрудниками в офисе и знать, как часто и как надолго они отходят от своего рабочего места. Кроме того, данные о текущем расположении жителей в доме будет на руку грабителям.

Уязвимость затрагивает все версии Android, однако неизвестно, планирует ли Google выпускать патч. Сведений о реальных атаках с ее использованием пока нет.

Межпроцессное взаимодействие – обмен данными между потоками одного или разных процессов. Реализуется посредством механизмов, предоставляемых ядром ОС или процессом, использующим механизмы ОС и реализующим новые возможности для взаимодействия.

(вгору)

Додаток 16

16.11.2018

Microsoft обвинили в тайном сборе персональных данных пользователей

Microsoft скрыто собирает персональные данные пользователей корпоративной версии пакета Office ProPlus, тем самым нарушая требования Общего регламента по защите данных (GDPR). Согласно результатам исследования, проведенного специалистами компании Privacy Company по заказу Министерства безопасности и правосудия Нидерландов (Ministerie van Justitie en Veiligheid; JenV), через встроенный в Office механизм компания собирает большие объемы данных об индивидуальном использовании Word, Excel, PowerPoint и Outlook без надлежащего уведомления (InternetUA).

При этом, отмечается в очете, Microsoft не предоставляет возможность контролировать объем собираемых данных, отключить телеметрию или узнать, какую именно информацию собирает компания, поскольку она отправляется в

зашифрованном виде. Как и в случае с Windows 10, Microsoft встроила отдельный модуль, который регулярно отправляет данные телеметрии на сервер в США. По словам исследователей, Microsoft собирает не только данные диагностики (стандартная практика среди разработчиков), но и содержимое используемых приложений, например, темы электронных писем или предложения из документов, в которых применялись инструменты для перевода и проверки правописания компании.

Согласно требованиям GDPR, данные пользователей в Евросоюзе должны храниться на серверах, расположенных в ЕС, однако, как выяснили специалисты, данные телеметрии нидерландских пользователей отправлялись на серверы в США, что предоставляет американским властям возможность получить доступ к информации. Нидерландские власти обеспокоены тем фактом, что собранная через систему телеметрии конфиденциальная информация, связанная с правительством, также может оказаться на этих серверах. По последним данным, пакет Office установлен на более чем 300 тыс. правительственных компьютеров.

Исследователи отметили более широкий масштаб сбора данных системой телеметрии в Office по сравнению с Windows 10. Если «десятка» собирает до 1,2 тыс. типов событий, к которым имеют доступ всего 10 команд инженеров, то в случае с Office речь идет о порядка 25 тыс. событий и 30 командах.

Специалисты передали Microsoft результаты исследования, по их словам, компания уже добавила опцию, позволяющую регулировать сбор данных или отключить телеметрию. Кроме того, техногигант пообещал предоставить документацию о сборе данных в Office, а также возможность устанавливать уровень телеметрии и просматривать собранную информацию.

(вгору)

Додаток 17

16.11.2018

Ирина Фоменко

Смарт-часы, которые отслеживают местоположение ребенка, могут взломать преступники

Популярные смарт-часы, отслеживающие геолокацию детей, настолько легко взломать, что их должны снять с продажи. Об этом сообщает The Telegraph (InternetUA).

MiSafes Kid’s Watcher Plus – это GPS-устройство для мониторинга местоположения ребенка и звонков, которое используют тысячи родителей в Великобритании.

Исследователи обнаружили серьезные недостатки безопасности в продукте, в том числе использование незашифрованных данных. Так, хакеры могут загружать программное обеспечение для отслеживания местоположения ребенка, слушать его разговоры и звонить ему, притворяясь родителями.

«Мы были в шоке от того, насколько легко можно взломать эти смарт-часы», – заявил эксперт по кибербезопасности Pen Test Partners Кен Мунро. – «У меня есть доступ к профильным данным детей: к фото, имени, дате рождения, полу, весу и росту».

Смарт-часы MiSafes, впервые вышедшие на рынок в 2015 с ценой в 9 фунтов стерлингов, имеют функцию GPS, которая обновляется в реальном времени и отслеживает предыдущие местоположения. Часы также позволяют осуществлять звонки.

Pen Test Partners доказали, что кто-то может поменять номер вызывающего абонента и связаться с ребенком под именем «Мама» или «Папа».

«Такие товары продаются якобы для безопасности ребенка, поэтому родители будут потрясены, узнав, что они сами подвергли детей риску из-за неудовлетворительного уровня надежности», – прокомментировал сотрудник Pen Test Partners Алекс Нил. – «Смарт-устройства могут оказаться полезными в повседневной жизни, но безопасность должна быть всегда в приоритете. Если ее нельзя гарантировать, то продукта не должно быть на рынке».

(вгору)

Додаток 18

19.11.2018

Хакеры взломали самый известный почтовый сервис с шифрованием

Группа хакеров утверждает, что они взломали почтовый сервис ProtonMail и украли «значительные» объемы данных. Они пока не опубликовали данные о взломе, однако выдвинули свои требования к компании по выкупу украденной информации (InternetUA).

Пока неизвестно идет ли речь о хакере-одиночке или команде киберпреступников, однако в их заявлении говорится о том, что им удалось украсть «значительные» объемы данных компании, которые проходили через почтовый сервис. Пользователь, опубликовавший текст с этой информацией, также обвинил ProtonMail в отправке расшифрованных данных пользователей на американские серверы.

«Мы предлагаем вернуть данные ProtonMail за небольшую плату. Если они откажутся, то мы будем публиковать или продавать данные пользователей по всему миру», – отмечено в тексте.

Также в тексте есть несколько претензий к системе безопасности сервиса. «Открытый исходный код ProtonMail может быть свободно проверен на Github, и каждый может увидеть, что они не настроили обязательную функцию SRI; это позволяет фальсифицировать и собирать данные пользователей в любое время». Хакер добавил, что сбор данных при этом будет незаметен серверу, потому что без включения SRI все пользователи должны проверить код сайта во время выполнения задач.

Они также обвинили сервис в том, что ProtonMail отправляет расшифрованные пользовательские данные на американские серверы. Хакеры предположили, что это может быть связано со швейцарским договором о взаимной правовой помощи MLAT. «Это было удивительно отметить, хотя напрямую и не касается факта взлома», – отмечается в тексте.

ProtonMail опровергает взлом и говорит о том, что у них нет никаких доказательств того, что хакеры имеют доступ к информации о пользователях. При этом в сервисе подтвердили, что они знают об ограниченном количестве взломанных учетных записей, которые были скомпрометированы после ввода учетных данных из-за фишинговых атак. В сервисе уверены, что это не системная проблема.

«Преступники пытаются вымогать деньги у ProtonMail, утверждая, что мы нарушаем конфиденциальность данных, однако у них нет никаких доказательств. Внутреннее расследование выявило два сообщения от преступников, которые снова повторили обвинения, однако у нас нет признаков нарушения», – добавили в компании. Они обещали всерьез рассмотреть их в случае, если получат достоверную информацию о взломе.

(вгору)

Додаток 19

19.11.2018

Умные камеры положат конец приватности

К 2022 году половина семей в США обзаведется умными камерами наблюдения. Люди сознательно начнут жертвовать своей приватностью, а распознавание лиц станет стандартом во всех сферах – от торговли до медицины (InternetUA).

Ключевые тренды в сфере технологий и медиа представил в свежем отчете сооснователь консалтинговой компании Activate Майкл Вулф. Его прогнозами о будущем рынка потребительских технологий делится Wall Street Journal. В 2022 году американцы будут потреблять больше контента, чем когда-либо прежде, а развлечения – видеоигры, музыка и подкасты – будут пользоваться все большим спросом.

По прогнозу Вулфа, через четыре года на рынке домашних устройств будут доминировать не умные колонки, а камеры наблюдения.

Системы слежения появятся в домах, офисах, автомобилях и гаражах. Большинство будет оснащено функцией распознавания лиц и образов.

Вулф уверен, что из-за распространения видеокамер распознавание лиц станет новым стандартом идентификации. Американцы будут совершать покупки в автоматизированных магазинах, таких как Amazon Go, которые обходятся без кассиров как раз благодаря камерам. Домашние системы позволят людям проходить медицинскую диагностику, не покидая жилье.

Камеры с поддержкой искусственного интеллекта станут настолько популярными и модными, что ими заинтересуются даже те, кого прежде беспокоили вопросы приватности.

По оценкам Вулфа, к 2022 году умными системами слежения обзаведется 50 % семей в США.

Поворотный момент также наступит в области электронной коммерции. В 2019 году выручка онлайн-магазинов впервые превысит показатели офлайн-точек.

Где потратить

Сейчас именно для прослушивания музыки большинство американцев заводит умные колонки. По данным маркетинговой компании Nielsen, динамиками с поддержкой голосовых помощников уже обзавелись 24 % домохозяйств в США. Многие используют устройства для получения оперативной информации о погоде или пробках, а также ищут данные в интернете.

По оценке Вулфа, музыкальная индустрия вырастет с $20,6 млрд в 2018 до $24,5 млрд в 2022 году. Количество слушателей подкастов в США достигнет 132 млн человек в месяц. Однако выручка от рекламы будет расти умеренно: с $402 млн в этом году она поднимется до $887 млн в 2022.

Стремительный рост ожидает и другие сферы. Например, ставки на спорт. У пользователей появится доступ к большему объему данных, а также к интерактивным интерфейсам и букмекерским системам в режиме реального времени.

Вулф прогнозирует расцвет на рынке видеоигр. Бум мобильных игр и возрождение игровых приставок по всему миру приведет к рекордной выручке в $150 млрд уже в следующем году.

(вгору)

Додаток 20

19.11.2018

Новый банковский троян для Android развлекает своих жертв игрой

Специалисты компании «Доктор Веб» обнаружили в каталоге Google Play банковского трояна Android.Banker.2876, распространявшегося под видом официальных приложений нескольких европейских кредитных организаций (Bankia, Banco Bilbao Vizcaya Argentaria (BBVA) и Santander, французских Credit Agricole и Groupe Banque Populaire, а также немецкой Postbank). В общей сложности было найдено шесть модификаций угрозы и все они уже удалены из официального каталога приложений (InternetUA).

Вредонос действовал классическим для банковской малвари образом. После запуска пользователем он запрашивал доступ к управлению телефонными звонками и совершению вызовов, а также к отправке и получению SMS-сообщений. При этом на устройствах с ОС Android ниже версии 6.0 эти разрешения предоставляются автоматически во время установки.

Затем банкер собирал и передавал в облачную базу данных Firebase конфиденциальную информацию:

– текущее время;
– IMEI-идентификатор;
– MEID-идентификатор (идентификатор для CDMA-устройств);
– deviceToken – токен Firebase для зараженного устройства;
– код страны SIM-карты;
– код оператора связи;
– название оператора связи;
– номер телефона;
– IP-адрес;
– MAC-адрес Wi-Fi-адаптера;
– наименование модели, производителя и бренда устройства.

Если данные удалось успешно отправить в БД, троян информировал своих операторов о том, что был зарегистрирован новый пользователь (посредством сервиса Firebase Cloud Messaging). Для этого он передавал сообщение типа «New user» с текстом «New user added with device id <id устройства>», где id устройства – идентификатор зараженного смартфона или планшета.

Затем троян показывал пользователю окно с сообщением, в котором потенциальной жертве, якобы для продолжения работы с программой, предлагалось указать номер телефона. При этом каждая из модификаций банкера предназначена для конкретной аудитории. Например, если троян имитирует приложение испанского банка, то его интерфейс и демонстрируемый текст будут на испанском языке.

Введенный жертвой номер также передавался в облачную базу данных, а пользователь видел второе сообщение. В нем говорится о необходимости подождать подтверждения «регистрации». Здесь же отображается кнопка «Submit», при нажатии на которую совершенно неожиданно для жертвы вирусописателей запускается встроенная в приложение игра.

Если ранее малвари удалось загрузить в облако информацию о мобильном устройстве, она скрывает свой значок с главного экрана и в дальнейшем запускается в скрытом режиме автоматически при включении зараженного смартфона или планшета.

Троян перехватывал все входящие SMS-сообщения и сохранял их содержимое в локальную базу данных. Кроме того, текст сообщений загружался в базу Firebase и дублировался в SMS, отправляемых малварью на мобильный номер киберпреступников.

В результате злоумышленники были способны получать одноразовые пароли подтверждения банковских операций и другую конфиденциальную информацию, которая может быть использована для проведения фишинговых атак. Помимо этого, собираемые трояном номера телефонов могли помочь вирусописателям в организации различных мошеннических кампаний.

(вгору)

Додаток 21

20.11.2018

Кіберполіція затримала банду, яка викрала 5 мільйонів гривень з банківських терміналів

У Кривому Розі затримано злочинну групу, викриту у махінаціях з банківськими терміналами самообслуговування.

Про це повідомили в департаменті кіберполіції Національної поліції України.

«Встановлено близько 400 банківських операцій, проведених зловмисниками на території 11 регіонів України. Їх діями завдано збитків на більш як 5 мільйонів гривень. Усі 6 учасників цієї міжрегіональної злочинної групи, на чолі з організатором, затримані в порядку статті 208 КПК України», – йдеться у повідомленні (InternetUA).

Працівники Департаменту кіберполіції Національної поліції України спільно зі співробітниками Служби безпеки України в Харківській області, слідчими поліції Харківщини та військовою прокуратурою, встановили групу зловмисників, які шляхом обману валідатора банківських терміналів для самообслуговування, викрадали гроші з державних та приватних українських банків.

За даним фактом поліція розпочала кримінальне провадження за ч.3 ст.190 (шахрайство) КК України. Документування діяльності злочинної групи відбувалося протягом останніх шести місяців.

Правоохоронці, спільно зі службою безпеки АТ КБ «Приватбанк», встановили учасників злочинної групи та схему, за якою ті втручались в роботу систем і комп'ютерних мереж банків. Зловмисники досконало знали принцип роботи терміналів та знайшли спосіб втручання в систему роботи банку.

За схемою, термінал приймав спеціально підготовлені зловмисниками купюри, фіксуючи зарахування на рахунку клієнта. На наступному етапі проходження купюри, система терміналу видавала помилку та повертала купюру власнику. Таким чином зловмисники з одного банкомату могли зарахувати на підконтрольні рахунки від 5 до 170 тисяч гривень. При цьому, використовуючи засоби конспірації, зловмисники постійно змінювали місце скоєння злочину, переміщуючись протягом доби по обласним центрам усієї держави.

Правоохоронці затримали в порядку статті 208 КПК України двох організаторів злочинної групи та ще чотирьох виконавців. Усі вони – громадяни України віком від 23 до 33 років. Затримання відбувалося, коли зловмисники вкотре намагалися зарахувати кошти на підконтрольні рахунки в одному із терміналів міста Кривий Ріг (Дніпропетровщина). У них вилучено спеціально видозмінену купюру для вчинення злочину.

Крім того, поліцейські встановили, що організатор злочинної групи створив офіс для виготовлення фальшивих грошей. Устаткування для

виготовлення валюти розміщувалося в одній із квартир на Київщині, де поліцейські провели обшук. Для створення фальшивих купюр зловмисники встановили спеціальне програмне забезпечення, придбали спеціальний папір, виготовили кліше, а також створили сайт для продажу виготовлених грошей.

Загалом, поліцейські провели 8 одночасних обшуків на території Київської, Харківської та Дніпропетровської областей. За їх результатами вилучено комп'ютерну техніку, устаткування для виготовлення грошових коштів, спеціальний папір, кліше та флеш-накопичувачі. Також вилучено засоби зв'язку та картки різних банків, які зловмисники використовували у своїй злочинній діяльності. Вилучене направлено на експертизу.

Затриманим загрожує до 8 років ув'язнення.

(вгору)

Додаток 22

21.11.2018

Зафиксирована первая в истории ботнет-атака на смарт-телевизоры

В компании DoubleVerify (DV), занимающейся аналитикой и программным обеспечением для измерений в сфере цифровых медиа, сообщили о выявлении новой сети ботов, нацеленной специально на подключаемые телевизоры (Connected TV), или же смарт-телевизоры (InternetUA).

По сообщению Broadband TV News, в DV выявили данную сеть ботов (ботнет) после того, как заметили 40 %-ный всплеск трафика от таких устройств, и уже назвали её первой целенаправленной ботнет-атакой, которая была обнаружена экспертами в среде Connected TV. Мошенническая схема была раскрыта экспертами специальной лаборатории компании, занимающейся поиском мошенников – DV Fraud Lab, которые, используя набор машинных алгоритмов и ручных процессов, постоянно анализируют тенденции в данной сфере.

Для генерирования ложной информации, ботнет использует полученные обманным путём URL-адреса издателей, отправляя на рекламные сервера фальшивые сигналы об откликах, которые якобы происходят с Connected TV устройства. Также в DV изучили список OTT-устройств, оказавшихся наиболее тесно вовлечёнными в мошенническую схему. Было выявлено, что примерно треть откликов выглядели так, будто они приходят от игровых консолей, а ещё две третьих – от смарт-телевизоров.

«Нас нисколько не удивило данное открытие – учитывая то, что мошенники обычно имеют привычку появляться везде, где есть деньги, – говорит генеральный директор DoubleVerify Вэйн Гаттинелла. – Учитывая то, что, по последним данным примерно 50 % всех пользователей Интернета смотрят видео в сети с подписных платформ или через ТВ-приложения по меньшей мере раз в неделю, объёмы рекламы в среде Connected TV растут, что влечёт за собой и рост мошенничества в данной сфере».

После выявления данной схемы, в компании DV незамедлительно приняли меры для защиты своих клиентов – а это всемирно известные бренды – от потенциальных атак мошенников, расширив качество охвата медиа-транзакций (до и после конкурса). Данный тип мошеннических схем похож на схемы, которые эксперты DV ранее уже выявляли в среде настольных компьютеров и мобильных приложений. И вот теперь подобные атаки начались и в растущем секторе Connected TV.

«Мы постоянно проводим независимые проверки как среды, так и оборудования, что позволяет нам проверять подлинность сигналов, выявляя несоответствия, которые указывают на факт фальсификации, – заявил руководитель лаборатории по борьбе с мошенничеством компании DoubleVerify Рой Розенфельд. – Компания DV и в дальнейшем будет оставаться на передовой борьбы с мошенничеством, давая рекламодателям ясность и уверенность касательно их цифровых инвестиций».

(вгору)

Додаток 23

22.11.2018

Европейские интернет-провайдеры массово блокируют The Pirate Bay // Украинские провайдеры пока колеблются

Греческие интернет-провайдеры заблокируют доступ к 38 пиратским доменам, включая The Pirate Bay. По просьбе местной группы по борьбе с пиратством, Ассоциации защиты аудиовизуальных произведений (EPOE), и решению комиссии IPPC при Министерстве культуры и спорта Греции провайдеры интернет-услуг заблокируют доступ к The Pirate Bay, 1337x, YTS и другим сайтам, нарушающим права интеллектуальной собственности (Телекритика).

Об этом сообщает украинская антипиратская инициатива «Чистое небо».

Чуть раньше The Pirate Bay заблокировали интернет-провайдеры Румынии. Несколько голливудских студий, включая Twentieth Century Fox, Disney, Sony, Paramount, Universal и Columbia, подали в Румынии судебный иск на знаменитый торрент и получили решение, требующее от местных интернет-провайдеров ограничить доступ к сайту.

Блокирование ресурса превращается в международную акцию против The Pirate Bay. Ресурс уже заблокирован примерно в двух десятках стран, в основном в Европе.

Игорь Михайлов, заместитель главы Украинской антипиратской ассоциации (УАПА), которая защищает в Украине права голливудских мейджоров, говорит, что УАПА не подавала в суд на The Pirate Bay: «Наши доверенности от голливудских студий не дают нам права подавать судебные иски, кроме уголовных производств, а takedown notices мы направляем провайдерам, предоставляющим услуги хостинга пиратским сайтам». В 2015 УАПА направляла такое письмо украинскому хостинг-провайдеру, который

приютил торрент thepiratebay.to. С тех пор The Pirate Bay в Украине не хостится.

Pirate Bay уже недоступен во многих сетях по всему миру. Similarweb оценивает снижение более чем на 32 % в октябре 2018 года. Точные причины этого не знает и сам ресурс, их связывают с определенным поведением магистральных интернет-узлов. Дмитрий Ганзенко, заместитель директора сети «Ланет», говорит, что провайдер не блокировал доступ к The Pirate Bay, но на текущий момент сайт не работает.

В других сетях пиратский торрент доступен. Директор «Паутина.NET» Александр Арутюнян: «У нас открывается. Но от желания провайдера мало что зависит в нашем государстве. Парадокс в том, что если провайдер заблокирует по собственному желанию любой сайт, то он нарушит закон про телекоммуникации. Выходит, мы не имеем права блокировать просто так, нам нужен законодательный механизм. Безусловно, нам как провайдеру, который продает контент вместе со своими партнерами (телеканалы, VOD-сервисы), невыгодно существование пиратских сайтов, но, увы, мы вынуждены работать согласно законодательству нашей страны».

Чтобы заблокировать доступ к этому пиратскому ресурсу, украинским интернет-провайдерам нужно решение суда или органов государственной власти, как это уже делалось ранее с сайтами, доступ к которым ограничивался решением СНБО.

В «Укртелекоме» сообщили «Чистому небу», что как только поступит официальное обращение от силовых структур в установленном порядке, провайдер начнет процесс блокировки. «Исходя из опыта компании, процесс блокировки может занимать от нескольких часов до недели».

«Правда, я сомневаюсь, что СНБО признает деятельность The Pirate Bay угрожающей государственному суверенитету, – считает Дмитрий Ганзенко. – Блокирование незаконных сайтов украинскими провайдерами, бесспорно, имеет право на жизнь, но грамотной процедуры его внедрения на сегодня де-факто не существует».

Вадим Сидоренко, генеральный директор группы компаний «Триолан», считает, что возможно достичь единой договоренности между провайдерами и заблокировать глобального нарушителя интеллектуальной собственности. Но тут важно учесть восприятие клиентов интернет-провайдера. «Если мнение клиентов по поводу отключения пиратских сервисов разделится – часть будет считать, что пиратский контент – это плохо, а часть – хорошо, то, отключив пиратские сервисы, потерю части аудитории провайдер может компенсировать за счет тех, кто против пиратства». Соответственно, инициатива более чем реальная», – говорит Вадим. Конечно, есть некоторые юридические нюансы: теоретически могут быть иски к провайдерам с вопросом об отключении, но это можно решить. «Но, если все не поддерживают инициативу, тогда нужно решение закона, например, суда. На сегодняшний день в Украине практически все считают, что пиратство – это хорошо, это не преступность. Маловероятно,

что народ будет поддерживать политику провайдера, который захочет отключить какого-то пирата».

О блокировке The Pirate Bay говорили и на недавнем Международном саммите в Варшаве. В частности, управляющий директор голландской антипиратской группы Brein Тим Куик потребовал большей ответственности со стороны ISPs, интернет-провайдеров. Он заметил, что прецеденты для блокировки The Pirate Bay уже создаются и число посредников, помогающих блокировать пиратов, из государственной и частной сфер растет.

(вгору)

Додаток 24

26.11.2018
Ирина Фоменко
Эксперты показали, как можно усложнить пароли против взлома

Несмотря на все предупреждения, некоторые люди все еще ставят пароли наподобие «123456» или «пароль», пишет The Star Online. «Они совершенно небезопасны, их легко угадать и взломать», – заявил директор Института имени Хассо Платтнера в Университете Потсдама в Германии Кристоф Мейнель (InternetUA).

Существует два основных правила для создания безопасного пароля. Во-первых, чем он длиннее и разнообразнее, тем лучше. «Количество попыток, необходимых для взлома пароля, увеличивается в 95 раз с каждой дополнительной буквой верхнего и нижнего регистра, специальным символом и цифрой», – прокомментировал Мейнель.

Для взлома пароля из пяти символов необходимо около 7 млрд попыток. С рекомендуемой длинной в восемь символов – более шести квадриллионов попыток, при условии, что пароль не содержится ни в одном словаре. По словам Мейнеля, пароль должен включать специальные символы и бессмысленные комбинации букв верхнего регистра, нижнего регистра и цифр.

Во-вторых, один и тот же пароль нельзя использовать для нескольких учетных записей. Каждый онлайн-сервис должен иметь индивидуальный пароль, иначе злоумышленники сразу получат доступ ко всем вашим аккаунтам.

«Только треть провайдеров использует безопасный метод обфускации для хранения паролей. Остальные хранятся с использованием устаревшего алгоритма или в виде простого текста, поэтому доступны бесплатно в Интернете после атаки», – поделился Кристоф.

Как запомнить сложный пароль

Согласно рекомендации Федерального управления по информационной безопасности Германии (BSI), один из способов – придумать предложение и использовать первую букву каждого слова для формирования пароля, используя заглавные буквы для существительных.

Например, из фразы «I get up in the morning and brush my teeth for three minutes» (Я встаю утром и чищу зубы в течение трех минут – Ред.) получается такой пароль – «IguitM&bmTf3M». BSI советует не использовать известные цитаты или строки из песен.

Пароли нельзя записывать, а лучший способ запомнить их – использовать программу менеджера паролей. Они могут не только хранить их в безопасной зашифрованной форме, но также генерировать и более надежные. Самое важное в использовании одной из этих программ – запомнить главный пароль для разблокировки.

Чтобы еще больше повысить уровень защиты учетной записи, используйте двухфакторную аутентификацию: при входе в систему необходим PIN-код, SMS-код или сгенерированный приложением ключ, поэтому злоумышленникам отказывают в доступе, даже если у них есть ваш пароль.

(вгору)

Додаток 25

26.11.2018

Северокорейские хакеры атакуют банки в Латинской Америке

Специалисты Trend Micro подготовили отчет о деятельности северокорейской хак-группы Lazarus. Исследователи предупреждают, что с середины сентября текущего года группировка заражает бэкдорами финансовые учреждения в странах Латинской Америки (InternetUA).

По словам экспертов, данные атаки перекликаются с деятельностью Lazarus в 2017 году, когда группа атаковала азиатские страны. Сейчас злоумышленники так же используют в атаках файл FileTokenBroker.dll и тот же модульный бэкдор, который уже был замечен аналитиками ранее.

Малварь группы состоит из трех компонентов, каждый из которых отвечает за выполнение различных целей: AuditCred.dll/ROptimizer.dll играет роль загрузчика, который запускается как служба, Msadoz.dll – это сама зашифрованная бэкдор-малварь, а Auditcred.dll.mui/rOptimizer.dll.mui представляет собой конфигурационный файл вредоноса.

Проникнув в систему, преступники с помощью своего бэкдора получают возможность выполнять самые разные вредоносные задачи. Они могут: собирать различные данные о системе и похищать файлы, загружать дополнительную малварь, запускать или останавливать процессы, внедрять вредоносный код в запущенные процессы, удалять файлы, задействовать обратный шелл, прокси и так далее.

Эксперты Trend Micro предупреждают, что эта вредоносная кампания Lazarus сложна и опасна, равно как и другие кампании группы. Исследователи подчеркивают, что обнаруженная ими малварь намерено борется как с обнаружением, так и с удалением из системы (например, лоадер и файл конфигурации расположены в %windows%\system32, тогда как сам бэкдор скрывается в другой директории, %Program Files%\Common Files\System\ado).

Хакерская группировка Lazarus (она же Hidden Cobra, APT38 и BlueNoroff) получила широкую известность после кибератаки на Sony Pictures Entertainment в 2014 году. После этого специалисты по информационной безопасности детально изучили и связали эту группу с Северной Кореей и целым рядом инцидентов. Так, в 2016 году хакеры едва не совершили «кибероГрабление века»: злоумышленники успешно похитили 81 млн долларов у Центробанка Бангладеш и только чудом не сумели украсть почти миллиард.

Кроме того, группу связывают с эпидемией Wannacry, атаками на банки в Польше и Мексике, фишинговыми атаками на подрядчиков Министерства обороны США, кампаниями против онлайновых казино в странах Латинской Америки. В текущем году Lazarus также атаковала криптовалютную биржу Bithumb и еще один неназванный криптообменник в Азии.

(вгору)

Додаток 26

27.11.2018

Мошенники научились захватывать банковские счета с помощью Google Maps

Мошенники научились использовать Google Maps для собственного обогащения, выдавая с их помощью себя за сотрудников службы поддержки банковских организаций, узнал Business Insider. Эксплуатируемая схема оказалась настолько простой и эффективной, что потенциальные жертвы сами связываются с мошенниками, позволяя тем избежать «холодных» звонков и повышая тем самым вероятность заполучить учетные данные для доступа к банковскому счету (InternetUA).

Описываемая мошенническая схема получила наибольшее распространение в Индии, однако с переменным успехом используется и в других странах, в том числе в России. Она состоит в том, что абсолютно любой пользователь может назваться собственником того или иного предприятия, включая банковские организации, и изменить контактный телефон, который приводится в Google Maps, на свой. А поскольку поисковый гигант уделяет недостаточно внимания контролю за достоверностью сведений, возможность отредактировать информацию есть практически у любого.

Как обезопасить себя от банковских мошенников

В первую очередь схема с подлогом телефонных номеров рассчитана на наименее осведомленных пользователей, которые ищут контактные данные своего банка в Google. Как показала практика, таких людей гораздо больше, чем тех, кто связывается со службой поддержки банка через чат в приложении или сразу заходят на официальный сайт в поисках телефонного номера или адреса электронной почты.

Как только жертва набирает номер, ей отвечает заранее подготовленный член преступной группировки, который тоном банковского служащего запрашивает персональные данные позвонившего, якобы идентифицируя его в

соответствии с имеющимися сведениями. Затем под предлогом дополнительной проверки мошенник просит продиктовать номер карты и CVV-код, используемый для подтверждения транзакций в интернете. После этого в считанные минуты мошенники списывают все сбережения жертвы, оставляя счет пустым.

(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.