СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(17.10–30.10)

2018 № 18

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(17.10–30.10)
№ 18

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

17.10.2018
Ольга Карпенко
Facebook понизит в ленте сайты с украденным контентом

Администрация социальной сети Facebook будет бороться с сайтами, которые воруют контент у других паблишеров и публикуют его без изменений или с небольшими изменениями. Об этом представители сети сообщили в комментарии TechCrunch (AIN.UA).

Этот показатель теперь влиять на ранжирование ссылок на сайты в ленте новостей, совместно с другими показателями (к примеру, кликбейтными заголовками или низкокачественной рекламой). Как сообщает издание, этот шаг продиктован результатами исследований, которые проводила сама компания, а также интервью с пользователями, которые ненавидят «копипасту» на сайтах.

Логика в том, что сайты с ворованным контентом будут меньше показываться в ленте, получат меньше реферального трафика, заработают меньше на рекламе и станут менее привлекательной моделью для тех, которые воруют чужие статьи, фото и видео.

***

19.10.2018
Мессенджер WhatsApp получил новую функцию

В скором времени в WhatsApp появится режим отпуска. Об этом стало известно сайту WEBetaInfo (InternetUA).

После активации этого режима через настройки WhatsApp вам перестанут поступать уведомления о сообщениях в чатах с отключенным звуком. Сообщения в них будут архивироваться и останутся непрочитанными, а для того, чтобы их увидеть, нужно зайти в приложение. По замыслу разработчиков, режим отпуска может использоваться в тех случаях, когда пользователь отдыхает от работы и рабочей переписки, но всё же желает оставаться на связи и может при необходимости отвечать коллегам, пусть и с задержкой.

WhatsApp также позволит связывать учётную запись с Instagram (оба сервиса принадлежат Facebook). Насколько тесной будет эта интеграция, пока неясно.

Обновлённые версии WhatsApp с этими нововведениями появятся на Android и iOS в ближайшие недели.

***

22.10.2018

В WhatsApp появится темный режим

WhatsApp получил большое обновление, в котором появилась поддержка iPhone XS Max, а также другие улучшения и подсказки о том, что будет в следующих версиях приложения. Помимо поддержки экрана iPhone XS Max, в версии 2.18.100 переработали контекстное меню действий для сообщений (Украинский телекоммуникационный портал).

Ранее длинное нажатие вызывало горизонтальное всплывающее меню, аналогичное тому, которое используется в других приложения на iOS. В новой версии добавили вертикальное меню, в котором помещается больше кнопок.

Обновление также меняет принцип работы голосовых сообщений. Теперь они воспроизводятся друг за другом, хотя ранее требовалось каждый раз включать сообщение, чтобы послушать его.

В дополнение к этим изменениям, портал WABetaInfo обнаружил скрытый код, который включает темную тему и возможность предварительного просмотра видео в уведомлениях WhatsApp.

В темном режиме входящие сообщения отображаются на сером фоне, а исходящие – на зеленом. Пока что эта тема тестируется, и к релизу она может выглядеть по-другому.

***

23.10.2018

Instagram обошел Snapchat по популярности среди подростков в США

Instagram обошел Snapchat в качестве самой популярной сети среди подростков в осеннем исследовании Piper Jaffray. 85 % опрошенных подростков пользовались Instagram хотя бы раз в месяц, 84 % – заходили в Snapchat. И хотя привлекательность Instagram растет, вовлечение с Facebook среди подростков сильно падает. Только 28 % 15-летних пользовались Facebook осенью 2018 года, два года назад их количество составляло 40 %. Исследование обнаружило, что привлекательность Instagram среди рекламодателей также растет (Marketing Media Review).

Почти 70 % подростков отметили, что предпочитают, чтобы бренды сообщали им о новых продуктах в Instagram. Второе место по вовлечению с брендом занял Snapchat, за ним последовал email.

Piper Jaffray провело 36 исследование, опросив 8600 подростков в США в возрасте 16 лет. Amazon назван любимым сайтом среди опрошенных. 47 % назвали его любимым сайтом для совершения покупок, Nike занял второе место. По данным исследования, Netflix занимает первую строчку рейтинга среди стриминговых сервисов. Подростки тратят 38 % своего времени каждый день, смотря Netflix. На YouTube приходится 33 % времени. Apple Watch названы вторыми самыми популярными смарт-часами среди подростков. Nike сохранил свое звание лучшего ритейл-бренда, однако исследование заметило

укрепление позиции Vans и перенос баланса в сторону Adidas. Lululemon также значительно укрепил свои позиции, заняв второе место после Nike среди девушек.

***

24.10.2018
Facebook изменит дизайн Messenger

Обновленная версия Facebook Messenger будет отличаться заметно упрощенным дизайном и рядом новых опций. Об этом сообщают Ведомости со ссылкой на CNBC (Portaltele).

Обновленная версия приложения для обмена мгновенными сообщениями Messenger будет запущена компанией Facebook в самое ближайшее время. Журналисты Ведомостей, ссылаясь на корреспондентов CNBC, главным отличием новой версии мессенджера станет упрощенный пользовательский интерфейс.

Так, число вкладок на главной странице приложения сократится всего до трех. Это будут «Сообщения», «Контакты» и «Группы». В число последних будут входить не только бизнес-группы, но и игры.

Ожидается, что сокращение числа вкладок и изменение их формата даст возможность пользователям общаться не только друг с другом, но и с крупными компаниями и организациями. В приложении также появится «Ночной режим». Всего Mesennger пользуется 1,3 миллиарда человек в месяц, а число отправленных сообщений достигает 10 миллиардов ежемесячно.

***

24.10.2018
Ирина Фоменко
Социальные сети на работе: демократично или рискованно

Большинство компаний считали социальные сети неуправляемыми и такими, что мешают работе, многие даже запретили использование Facebook и Twitter. Однако сегодня некоторые из крупнейших работодателей мира делают обратное: уговаривают сотрудников регистрироваться в социальных сетях, предназначенных для работы.

Докладніше

***

29.10.2018
ИИ сделает подписи на Facebook «более привлекательными»

Исследователи машинного обучения в Facebook разработали новую модель нейронной сети. Она может придумать подписи к фотографиям, которые будут более «привлекательны» для людей.

Докладніше

***

28.10.2018
Snapchat продолжает терять пользователей

Летом стало известно о том, что обновленный дизайн популярного мобильного приложения Snapchat, которое используется для обмена сообщениями с фото и видео, оттолкнул миллионы пользователей (InternetUA).

Если в первом квартале этого года активная ежедневная пользовательская база сервиса составляла 191 млн человек, то во втором квартале она уменьшилась до 188 млн пользователей.

В третьем квартале отток пользователей продолжился, в итоге пользовательская база зафиксировалась на отметке 186 млн человек, о чем стало известно из последнего финансового отчета компании.

Из позитивных моментов стоит выделить, что компания получила доход в размере 298 млн долларов в третьем квартале этого года, тогда как аналитики The Wall Street прогнозировали доход на уровне 283 млн долларов.

Возраст наиболее активной аудитории Snapchat колеблется от 13 до 34 лет.

***

29.10.2018
Facebook делает ставку на музыку

В компании Facebook готовят сразу несколько нововведений, касающихся музыки. Первый момент – это сервис-конкурент TikTok. Для него в компании создают отдельное приложение под названием Lasso, которое, как ожидается, сможет привлечь подростковую аудиторию.

Докладніше

***

29.10.2018
Задля «здорової атмосфери дебатів» Twitter планує видалити кнопку Like // Реакція користувачів на рішення соцмережі щодо даної кнопки виявилася суперечливою

Соціальна мережа Twitter має намір прибрати кнопку Like у вигляді сердечка. За словами засновника платформи Джека Дорсі, цей намір буде реалізовано «найближчим часом» (zaxid.net).

Також Дорсі заявив, що сам він ніколи не був прихильником такої функції, пише профільний ресурс Mashable.

Як повідомляється, в березні поточного року розробники соцмережі представили функцію закладок, завдяки якій користувачі можуть зберігати твіти, не натискаючи на цю кнопку.

«Потенційне видалення подібних кнопок є частиною зусиль зі створення більш здорової атмосфери для дебатів на платформі», – коментують новину журналісти.

У той же час, реакція користувачів на рішення Дорсі щодо даної кнопки виявилася суперечливою. Дехто з них висловили думку, що подібні кроки не стоять на порядку денному, і соцмережа має куди більш серйозні проблеми, ніж видалення кнопки Like.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

18.10.2018

У Києві планують запустити міську соціальну мережу

У Києві планують запустити інтернет-платформу «Спільно», за допомогою якої кияни зможуть безпосередньо спілкуватися з представниками влади, організаціями та іншими жителями столиці (OpenKyiv).

Як повідомляють розробники сервісу, користувачі «Спільно» зможуть ініціювати проекти і пропозиції, створювати петиції, голосування, які будуть прив'язані до користувача локально – його під'їзду, будинку, району, міста. Вони будуть шукати однодумців, партнерів, волонтерів, спонсорів і отримувати консультації від представників влади.

Крім того, розробники планують створити мобільний додаток. Користувачі зможуть взяти участь в опитуваннях, голосуваннях, поскаржитися про порушення своїх прав, обважування, обраховування, неякісне, несвоєчасне обслуговування в компетентні служби.

Додаток планують запустити в листопаді цього року. Весною 2019 року планується вихід спеціалізованого додатка для зручної роботи соцмережі на мобільних пристроях.

***

18.10.2018

У Кропивницькому поліція використовує соціальні мережі для покращення роботи

У Кропивницькому створили групу в Телеграмі, де можна інформувати правоохоронні органи про події в місті. Про це інформує кореспондент Трибуни.

«Ця група створена для поліції та небайдужих громадян. Замість того, щоб телефонувати на 102, можна написати повідомлення, додати фотографії, а ми вже будемо реагувати на це», – повідомила керівниця сектору зв'язків із громадськістю обласного управління Нацполіції Віталіна Бевзенко.

Щоб додатися в групу «Безпечне місто», треба завантажити додаток Telegram та додати адміністратора 050-598-70-03.

***

28.10.2018

Twitter объяснил уменьшение числа подписчиков Трампа

В компании Twitter после критики американского президента Дональда Трампа объяснили уменьшение числа подписчиков президента США удалением ненастоящих аккаунтов. Об этом пишет американская газета The Hill (InternetUA).

26 октября Трамп обвинил сервис микроблогов в том, что компания намеренно удаляет его подписчиков и в целом относится к нему предзвзято.

«Нашим приоритетом является корректное функционирование сервиса, в том числе работа по удалению поддельных аккаунтов для предотвращения вредоносного поведения. Многие популярные пользователи заметили, что число их подписчиков упало, но в результате мы в большей степени уверены в том, что подписчики являются реально существующими людьми», – заявили в компании.

***

30.10.2018

Поход Приходько в большую политику вызвал массу споров: что пишут в соцсетях

Внезапное заявление известной певицы Анастасии Приходько о том, что она уходит со сцены ради большой политики вызвало бурное обсуждение у пользователей соцсетей.

Докладніше

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

18.10.2018

Цукерберга хочуть усунути з посади голови правління

Кілька акціонерів Facebook підтримали пропозицію усунути генерального директора Марка Цукерберга з посади голови ради директорів (Espreso.tv).

Як пише Economic Times, така позиція пов’язана із тим, що Цукерберг «погано впорався з декількома серйозними скандалами», зокрема щодо втручання Росії у вибори в США та витоку даних Cambridge Analytica.

Казначеї зі штатів Іллінойс, Род-Айленд і Пенсильванія, а також ревізор міста Нью-Йорк Скотт Стрінґер долучилися до пропозиції.

Таку пропозицію винесуть на голосування на щорічній зустрічі акціонерів компанії у травні 2019 року. Окрім того, буде пропонуватись зробити роль глави компанії незалежною посадою.

Сам Цукерберг наразі володіє близько 60 % голосів, а подібну пропозицію висувають вже не вперше: така вимога пошуку незалежного глави була переможена в 2017 році, а контроль більшості голосів Цукербергом зробило рішення акціонерів фактично символічним.

***

19.10.2018

Треть пользователей совершают покупку под влиянием постов лидеров мнений

По данным исследования IZEA 36 % пользователей социальных медиа совершили покупку под влиянием лидеров мнений, а 10 % «могли совершить», но не смогли вспомнить покупку или пост. «Косметика и beaut-продукты представляют самую большую категорию всех покупок и 31,1 % участников опроса совершили покупку после того, как увидели промо продукта лидером мнений. Следующими следуют одежда и модные аксессуары, 28,8 % пользователей совершили покупку в этой сфере, далее последовали напитки и еда. В этой категории 27,6 % пользователей совершили покупку на основании онлайн-промо продукта лидерами мнений», – отмечено в исследовании (Marketing Media Review).

Другие выводы исследования:

– 74 % пользвоателей социальных медиа «знают» кто такой лидер мнений, а 1 из 7 назвали себя лидером мнений;

– 35 % миллениалов совершали покупку еды/напитков под влиянием постов от лидеров мнений;

– 46 % женщин совершали покупку beauty-продуктов из-за постов лидеров мнений;

– 48 % респондентов отметили, что Facebook влияет на их покупки;

– 38 % респондентов отмели влияние YouTube на свои покупки;

– 34 % назвали Instagram в качестве инструмента влияния на покупки.

***

18.10.2018

На Facebook подали в суд за завышение количества просмотров видео

Группа рекламодателей подала в суд Окленда коллективный иск к компании Facebook, которая могла умышленно предоставлять неверную информацию о количестве просмотров видеоконтента в социальной сети, пишет The Wall Street Journal (InternetUA).

В иске говорится о том, что впервые проблемы с алгоритмом подсчета просмотров видео были выявлены в 2015 году. Технический директор компании сообщал о них руководству социальной сети, однако мер по устранению этой проблемы принято не было.

Представители компании иск назвали безосновательным и сообщили о том, что рекламодателей предупреждали о проблемах с измерениями после их обнаружения. По словам истцов, данные были завышены в 2,5-10 раз.

***

21.10.2018

Как в Украине родители зарабатывают миллионы, снимая детей для Youtube

Топовые детские каналы на просторах украинского Youtube зарабатывает больше $100 тыс. в месяц. Разумеется, деньги попадают в кошелек родителей, которые снимают своих чад.

Докладніше

***

22.10.2018

Четыре стратегии контент-маркетинга в Instagram для «нефотогеничного» бизнеса

Как продвигаться в Instagram, – самой визуальной соцсети – если продукт «нефотогеничный»? Четыре контент-стратегии, проверенные опытом известных компаний.

Докладніше

***

23.10.2018

YouTube виділить $20 млн для блогерів, які ведуть освітні канали // Єдина умова для отримання гранту – не менше 25000 підписників

YouTube виділить $20 млн доларів для фінансування діяльності блогерів, які займаються навчанням і освітою аудиторії. Це сатло можливо завдяки власній програмі Learning Fund, передає The Verge (mind).

Повідомляється, що отримати грант зможе будь-який блогер, який займається створенням корисного контенту. Для участі в програмі потрібно мати канал з освітньої тематикою і не менше 25000 підписників.

Ті блогери, чиї кандидатури буде затверджено, укладуть договір з YouTube, де будуть обговорені умови співпраці та отримання матеріальної допомоги.

«Ми надіємося підтримати тих, хто використовує YouTube, щоб поділитися своїми знаннями зі світом і мільйонами користувачів, які приходять на нашу платформу, щоб вчитися», – зазначила CEO YouTube Сьюзан Войчицкі.

YouTube не перший раз ділиться прибутком з топовими блогерами і ютуберами-початківцями. Наприклад, на початку року відеохостинг пожертвував 5 млн доларів на створення «доброго і толерантного» контенту.

***

23.10.2018

Михаил Сапитон

Украинский Telegram-канал впервые набрал более 100000 подписчиков. Как ему это удалось

Украинский Telegram-канал о путешествиях и скидках «Ветер дует» набрал более 100000 читателей, сообщила в Facebook основательница проекта Алена Деньга. Она рассказала, что успеху канала поспособствовали несколько обстоятельств.

Докладніше

***

24.10.2018

Инфографика: лучшее время для размещения постов в сетях

Команда Unmetric проанализировала 100 американских брендов и их активности в сетях. По итогам своих наблюдений Unmetric выпустила инфографику, в которой указала дни и время для лучшего охвата поста в Facebook, Instagram и Twitter. Лучшими днями для Instagram стали воскресенье, вторник и среда, для Facebook – среда и четверг, для Twitter – вторник и среда (Marketing Media Review).

***

26.10.2018

У Twitter становится меньше пользователей, но больше денег

Компания Twitter, владеющая одноименным сервисом микроблогов, зафиксировала рост выручки и прибыли, однако столкнулась с потерей числа активных пользователей. Об этом свидетельствует опубликованная в четверг отчетность компании по итогам третьего квартала (InternetUA).

За указанный период рост общей выручки Twitter составил около $758 млн, что на 29 % больше данного показателя за аналогичный квартал прошлого

года. Это самый большой рост выручки компании, начиная с первого квартала 2016 года. Аналитики агентства Reuters прогнозировали выручку на уровне не более $702,6 млн.

Прибыль по итогам третьего квартала составила $106 млн. При этом год назад компания зафиксировала убыток в размере чуть более $21 млн.

Однако среднее число активных пользователей Twitter в месяц упало до 326 млн по сравнению с 335 млн в прошлом квартале и 330 млн – год назад. Рост числа тех, кто пользуется соцсетью ежедневно, составил за последний год 9 %, что также меньше прогнозировавшихся показателей.

Между тем, гендиректор Twitter Джек Дорси в распространенном заявлении назвал сильными результаты минувшего квартала. По его словам, компания «достигает значительного успеха» в своих попытках сделать Twitter более безопасной и удобной площадкой для ежедневного общения. Среди таких достижений Дорси назвал, в частности, прогресс в работе по своевременному определению и удалению спама и других подозрительных сообщений, а также добавление новых функций и упрощение интерфейса соцсети.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

18.10.2018
Ирина Фоменко
Ученые нашли связь между времяпровождением в сети и ожирением у детей

Новое исследование показало, что маленькие дети, которые проводят много времени в Интернете или смотрят коммерческое телевидение, чаще страдают ожирением и просят своих родителей купить им нездоровую пищу.

Докладніше

***

19.10.2018
Чем соцсети пугают крупнейших технологических лидеров мира

В последнее время социальные сети все чаще мелькают в устрашающих заголовках. Недавно крупнейшие технологические лидеры мира, Илон Маск, Джефф Безос и основатель Instagram Кевин Систром высказали свои опасения касательно соцсетей. И у каждого из них свой страх.

Докладніше

***

25.10.2018

В Instagram появился аккаунт о суровой правде любовных отношений

Анонимный блогер устал от идеальных романтических фотографий в Instagram и создал аккаунт, который назвал «Честная пара». На странице пользователь собирает снимки со счастливыми возлюбленными, однако делает к ним максимально реалистичные подписи.

Докладніше

***

26.10.2018

В Австралии предотвращение суицидов доверили чат-боту

В Австралии в 2017 году наложили на себя руки 3128 человек, и эта цифра растет год от года. Тысячи жизней можно спасти, если найти эффективный способ подсказать близким самоубийц, как вести себя в критической ситуации – и теперь сделать это может чат-бот в Twitter (InternetUA).

В США боты ассоциируются с политическими манипуляциями, а в Австралии считают, что с их помощью можно спасать жизни. Некоммерческая организация Lifeline разработала вместе с Twitter чат-бота, который помогает родственникам и друзьям человека, который собрался покончить с собой.

К #BeALifeline Direct Message Chatbot может обратиться любой пользователь Twitter. Бот подскажет, как правильно начать разговор с самоубийцей, даст ссылку на полезные материалы на сайте Lifeline и поможет найти телефон горячей линии.

Доктор Дэн Рейденберг из американской некоммерческой организации Suicide Awareness Voices of Education уверен: с помощью соцсетей можно помочь многим людям, которых посещают мысли о суициде.

Ученые уже разработали алгоритмы, которые диагностируют депрессию по постам в соцсетях. Нечто похожее можно попробовать создать для суицидников.

Многие из тех, кто сводит счеты с жизнью, – это молодые люди. В целом молодежь положительно относится к ботам, поэтому предотвращение суицидов таким способом может оказаться очень эффективным. К сожалению, исследований на эту тему проводится мало, отмечает Conversation.

***

27.10.2018

Знайшли користь від статусів у соцмережі

Статуси у Facebook допомають виявити ранні ознаки депресії.

Користь від дописів знайшли американські психологи Пенсільванського університету. Результати дослідження опублікували у журналі Proceedings of the National Academy of Sciences (Gazeta.Ua)

Науковці залучили до дослідження 1,2 тис. осіб. Фахівці проаналізували їхні акаунти і медичні карти. У 114 піддослідних діагностували депресію. Після цього порівняли пости у Facebook людей з діагнозом і без діагнозу.

Виявилося, що за кілька місяців до виявлення розладу люди починали використовувати слова, що описують стан самотності і ворожості. Вони частіше вживали займенник «я».

«Не можна стверджувати, що за допомогою нашого алгоритму можна чітко поставити діагноз. Але це дослідження допоможе для виявлення людей з депресією на ранній стадії», – каже керівник дослідження Йоганнес Ейхштедт.

Крім того, у лексиконі людей, які живуть депресією, частіше зустрічаються слова: самотній, жалюгідний, нещасний, я, мене.

***

29.10.2018
Ирина Фоменко
Как выявить у себя зависимость от смартфона

Еженедельно Apple отправляет пользователям iPhone стимулирующий отчет о «цифровом оздоровлении», в котором говорится, сколько часов они потратили на смартфоны. Как утверждают в Apple, отчет направлен на уменьшение зависимости от технологий.

Докладніше

***

29.10.2018
Двое парней прошлись по улицам Ровно в одних трусах ради лайков в социальных сетях

В Ровно двое парней почти голышом разгуливали по центру города при температуре +10 (СТРАНА.ua).

Свою осеннюю прогулку экстремалы транслировали в прямом эфире в социальной сети. Прохожие ошарашенно останавливались, некоторые жали отчаянным прохожим руку.

Оказалось, что любителям путешествий в нижнем белье – 20 и 21 год. Ребята решили раздеться ради лайков. Они придумали себе челлендж накануне и обнародовали в соцсетях пост с обещанием: если он наберет три тысячи лайков – выйдут раздетыми на прогулку по городу.

После шествия голышом они вошли во вкус и заявили, что следующий шаг – прыжок в трусах с парашютом.

Маніпулятивні технології

19.10.2018

Мужчину приговорили к тюрьме за посты «ВКонтакте» // Пользователь социальной сети проведет за решеткой длительное время

Как стало известно «Властям», на днях Александрийский горрайонный суд Кировоградской области приговорил к четырем с половиной годам тюремного заключения местного жителя Игоря Ткаченко, который на протяжении прошлого года вел в соцсети «ВКонтакте» группу сепаратистской направленности «Елисаветград-Кировоград-Новороссия, в которой призывал к вооруженному свержению конституционного строя (InternetUA).

Что интересно, Ткаченко в 2015 году уже был осужден за аналогичное преступление, однако «блогерскую» деятельность не оставил, и продолжал призывать к преступному перевороту.

В этот раз суд оказался менее лоялен к сепаратисту, полностью исключив возможность его интернет-активности в тюремной камере.

***

19.10.2018

Российские интернет-тролли пытались повлиять на американцев с помощью Brexit

Опубликованный социальной сетью Twitter архив контента «российских фейковых аккаунтов» показал, что в день голосования по вопросу Brexit в Великобритании «интернет-троллями» велась кампания по продвижению идеи выхода страны из Европейского Союза (ЕС) – к такому выводу пришли аналитики из Atlantic Council, пишет The Times.

Докладніше

***

21.10.2018

Исследование: большинство американцев не может отличить бота от живого человека

Большинство американцев не может отличить ботов в социальных сетях от реальных людей. Об этом стало известно из исследования некоммерческой организации Pew Research Center. Только 47 % уверены, что смогут отличить механическое сообщение от настоящего. При этом 31 % из них относится к ботам негативно (InternetUA).

Исследование Pew – это новый взгляд на то, что среднестатистический человек думает об автоматизированных учетных записях, которые массово

появляются в социальных платформах. После опроса более 4,5 тыс. взрослых в США Pew обнаружил, что большинство людей на самом деле не знают о ботах. Однако, поскольку результаты опроса зависят только от интервью, есть вероятность, что респонденты завышают или занижают свои знания.

При этом 80 % опрошенных, независимо от политических взглядов, возраста и пола, говорят, что учетные записи используются в «плохих целях». Также ученые обнаружили, что чем больше человек знает об устройстве ботов, тем меньше поддерживает их массовое введение. При этом респонденты считают, что большинство ботов используется для продвижения политических кандидатов.

Исследователи также предложили решение, которое может помочь пользователям идентифицировать бота в будущем. Выходом может быть алгоритм Sloan, который предлагают академики MIT. Он будет анализировать его взаимодействия с другими учетными записями. Идея заключается в том, что если учетная запись очень активна, но получает мало ответов, значит, это робот.

***

20.10.2018

В США обнаружили новую лазейку для российских троллей

Россия использовала американские стартапы, чтобы вмешиваться в американские выборы. Об этом пишет агентство Bloomberg со ссылкой на данные активности учетных записей в Twitter.

Докладніше

***

21.10.2018

NY Times: наследный принц Саудовской Аравии собрал «армию троллей»

Наследный принц Саудовской Аравии Мухаммед ибн Салман и его ближайшие советники создали в Эр-Рияде организацию, на которую работают «сотни» троллей. Об этом пишет газета The New York Times (InternetUA).

По данным издания, сотрудники организации распространяют в сети информацию по запросу властей. Отмечается, что они работают с твиттером, а также публикуют данные в чатах WhatsApp и Telegram. В газете рассказали, что сотрудники данной организации получают около $3 тыс. в месяц.

По информации NY Times, саудовские власти начали устраивать кампании в соцсетях против критиков саудовского правительства со времен «арабской весны» 2010 года. Саудовские тролли в первую очередь уделяли внимание войне в Йемене и теме прав женщин в Саудовской Аравии. Подчеркивается, что если администрации социальных сетей находят поддельные аккаунты, то их создатели сразу же открывают новые.

Также в газете добавили, что эта организация занималась сетевой критикой оппозиционного саудовского журналиста Джамаля Хашкуджи, смерть которого саудиты признали 21 октября.

***

21.10.2018

Ирина Фоменко

Опубликованы темники российских оперативных дезинформаторов для Facebook

Покойный сенатор Джон Маккейн был «старым чудаком». Спикер палаты представителей Пол Д. Райан – «никем». И расследование возможного сговора между кампанией президента Трампа и Россией – это «охота на ведьм» во главе с «марионеткой», пишет The Wall Street Journal.

Докладніше

***

28.10.2018

Иранские интернет-тролли используют «методички» Кремля для раздора в соцсетях

Администрация Facebook заблокировала сеть, в которую входили 82 группы, в сообщества и пользователи, выдававшие себя за граждан США и Великобритании. Эти интернет-тролли занимались публикацией мемов, статей и прочего контента политической тематики, касающейся межнациональных отношений, выборов в Конгресс и прочего.

Докладніше

Спецслужби і технології «соціального контролю»

17.10.2018

Facebook будет блокировать дезинформацию во время выборов в США

Facebook будет блокировать ложную информацию о правилах голосования, сообщения о стычках и длинных очередях на предстоящих промежуточных выборах в США, передает Reuters со ссылкой на представителей компании (InternetUA).

Как сообщается, Facebook намерен проводить такую информационную политику на всем протяжении выборной кампании – остаток октября и весь ноябрь.

Отмечается, что это повысит расходы компании, а также может повлечь обвинения в цензуре. В то же время избирательная кампания – «чувствительная

сфера» для Facebook, поскольку после президентских выборов в США в 2016 году соцсеть раскритиковали за публикуемые пользователями дезинформацию и fake-news. Reuters отмечает, что многие посчитали это причиной победы действующего президента Дональда Трампа.

***

17.10.2018

Глава Google впервые признал создание поисковика с цензурой

Гендиректор Google Сундар Пичаи впервые публично прокомментировал слухи о разработке специальной версии поисковой системы для пользователей в Китае. Об этом сообщает TechCrunch (InternetUA).

По его словам, китайская версия поисковика будет содержать встроенную систему цензурирования, однако она сможет ответить на «более чем 99 процентов пользовательских запросов». Гендиректор Google отметил, что в правлении пока нет четкого понимания, будет ли проект запущен в ближайшее время.

Google намерен конкурировать с популярной китайской поисковой системой Baidu. На претензии в ограничении свободы слова Пичаи объяснил, что компания намерена «предоставлять информацию всем», но не может нарушать законы страны, в которой собирается работать.

О проекте Google под кодовым названием Dragonfly стало известно в конце июля 2018 года. Тогда в СМИ просочилась информация о разработке отдельной версии поисковика для Китая, который должен скрывать сайты из государственного черного списка, включая ресурсы, содержащие информацию о демократии, религии и правах человека.

***

17.10.2018

Twitter рассекретил тысячи аккаунтов российских троллей

Соцсеть Twitter обнародовала архив из более чем 10 миллионов твитов и других материалов, которые могут быть результатом работы спецслужб России и Ирана. Об этом сообщает Reuters (InternetUA).

Доступной стала информация о 4 тысячах аккаунтов, связанных с российским Агентством интернет-исследований, которое ранее американские власти обвинили во вмешательстве в выборы. Его возглавляет бизнесмен Евгений Пригожин, считающийся близким другом Владимира Путина.

В сервисе микроблогов пояснили, что раскрытие этих сведений призвано помочь всем тем, кто занимается исследованиями в области социальных сетей.

***

18.10.2018

В ФСБ заявили о необходимости контролировать киберпространство

Первый заместитель главы ФСБ России Сергей Смирнов заявил, что для гарантий должного уровня безопасности, спецслужбам необходимо установить контроль за киберпространством, передает «Красная звезда» (InternetUA).

«Для нас, профессионалов, давно очевидно, что киберпространство должно находиться под контролем компетентных органов. Без этого гарантировать должное обеспечение информационной безопасности и успешно противостоять современным террористическим угрозам невозможно», – сказал Смирнов.

По его словам, в ходе 33-го заседания Совета Региональной антитеррористической структуры ШОС было разработано решение, которое дает возможность для «эффективного сотрудничества компетентных органов (стран ШОС) в мониторинге глобального информационного пространства на предмет таких угроз».

***

19.10.2018

В Facebook создан спецотдел по борьбе с вмешательством в выборы // Компания планирует привлечь к работе в новом отделе более двадцати тысяч сотрудников

Крупнейшая социальная сеть Facebook сформировала в своей структуре новое подразделение – специальный отдел по борьбе с вмешательством в выборы; целью нового отдела будет борьба с распространением ложной информации.

Докладніше

***

22.10.2018

Ирина Фоменко

«War Room» от Facebook оказался дешевой маркетинговой уловкой

Журналисты The Fortune считают, что «War Room» Facebook является маркетинговой уловкой: конференц-зал напоминает центры кибербезопасности, которые банки и другие компании создают для «замыливания глаз» посетителям.

Докладніше

***

18.10.2018

За мемы в соцсетях россиянка была вынуждена переехать в Украину

Фигурантка уголовного дела об экстремизме за мемы в соцсетях Мария Мотузная уехала из России в Украину. По мнению Мотузной, основной

причиной ее преследования является общественная деятельность, так как она неоднократно публиковала в соцсетях анонсы оппозиционных митингов (InternetUA).

Фигурантка уголовного дела об экстремизме за мемы в соцсетях Мария Мотузная уехала из России в Украину. Летом 2018 года следователи из Барнаула нашли в архиве страницы Мотузной в «ВКонтакте» за 2015 год несколько мемов с изображением Христа. Против девушки завели уголовные дела по статьям об экстремизме и оскорблении чувств верующих.

По мнению Мотузной, настоящая причина ее преследования – общественная деятельность: она неоднократно публиковала в соцсетях анонсы оппозиционных митингов, в частности – акций Алексея Навального.

9 октября суд в Барнауле вернул дело Мотузной в прокуратуру. Мотузная вину не признала. В суде она рассказала, что оперативники обманом заставили её дать признательные показания. Защита отмечала, что стороне обвинения так и не удалось установить, что Мотузная хотела своими действиями нанести ущерб конституционному строю.

***

22.10.2018
В России вознамерились ограничить Google

Группа депутатов Госдумы внесла на рассмотрение нижней палаты парламента законопроект, призванный ограничить иностранное участие в капитале новостных агрегаторов 20 процентами. Полный текст документа доступен в думской базе данных (InternetUA).

Авторы инициативы – Андрей Луговой (ЛДПР), Антон Горелкин («Единая Россия»), Борис Пайкин (ЛДПР) и Михаил Старшинов. В пояснительной записке они указывают, что более чем 20 процентами новостного агрегатора не должны владеть иностранные государства, международные организации (или организации под их контролем), иностранные юридические лица, иностранные граждане, а также лица без гражданства или с двойным гражданством. Владельца новостного агрегатора также стоит оградить от российских юрлиц, если доля иностранного участия в их капитале превышает 20 процентов.

«Внедряемые проектом ограничения предлагаются в целях предотвращения угрозы общественному порядку в России и создания, тем самым, благоприятных условий для развития гражданского общества», – утверждают парламентарии.

***

25.10.2018
Facebook и Twitter оценили влияние Китая на выборы в США

Facebook и Twitter не нашли признаков вмешательства КНР в выборы в конгресс США. Об этом сообщает Bloomberg (InternetUA).

По данным агентства, компании не нашли доказательств того, что Китай ведет кампанию по дезинформации перед предстоящими выборами в США.

Как отмечается, Facebook и Twitter опровергли заявления президента США Дональда Трампа о том, что КНР пытается повлиять на выборы в конгресс США.

Проблема захисту даних. DDOS та вірусні атаки

17.10.2018
Британцы готовятся к разрушительной кибератаке

Это только вопрос времени, когда Великобритания столкнется с масштабной разрушительной кибератакой, способной привести к страшным последствиям, в том числе к человеческим жертвам. К такому выводу пришли специалисты Национального центра кибербезопасности Великобритании (NCSC) в своем втором годовом отчете, опубликованном 16 октября (InternetUA).

NCSC был учрежден Центром правительственной связи Великобритании в 2016 году и с тех пор столкнулся с 1167 инцидентами безопасности. 557 из них имели место в течение последнего года – в среднем 10 атак еженедельно. Большинство атак осуществлялись правительствами иностранных государств или финансируемыми ими киберпреступными группировками. Эти группировки остаются наиболее острой и непосредственной угрозой безопасности Великобритании, отметил глава NCSC Сиаран Мартин (Ciaran Martin).

За два года своего существования NCSC столкнулся с множеством разнообразных кибератак, однако наиболее значительной является атака шифровальщика WannaCry. Тем не менее, по словам Мартина, впереди Великобританию ждет еще более серьезная угроза.

«Я не сомневаюсь, что в ближайшие годы нам, и как Центру, и как нации, предстоит пройти испытание крупным инцидентом безопасности, который мы называем атакой Категории 1», – отметил Мартин.

Согласно формулировке NCSC, атака Категории 1 или «экстренная ситуация национального масштаба в киберпространстве» представляет собой кибератаку, вызывающую постоянный сбой в работе основных служб Великобритании или влияющую на национальную безопасность. Атака Категории 1 может привести к серьезным экономическим или социальным последствиям и даже к гибели людей.

***

17.10.2018

Хакери, пов'язані з РФ, готували кібернапад на компанії України та Польщі

Хакери провадили дії проти трьох компаній, що працюють в енергетиці та транспортній галузі в Україні та Польщі і, можливо, планували новий руйнівний кібернапад.

Докладніше

***

17.10.2018

У Києві викрили зловмисників, які продавали персональні дані в Telegram

Продаж здійснювався у закритому Telegram-каналі. Серед послуг, які надавали зловмисники, перевірка особи по інформаційним базам українських банків, надання інформації про рух коштів за рахунками та вся кредитна історія.

Докладніше

***

17.10.2018

Twitter засыпал пользователей странными сообщениями

Пользователи Twitter получили множество оповещений с кажущимся бессмысленным набором букв и цифр. Глава сервиса Джек Дорси сообщил, что ему известно об этой проблеме, и скоро она будет устранена (InternetUA).

Чуть позже Дорси рассказал, что проблемы уже нет, однако компания до сих пор не выяснила, чем она была вызвана. После нажатия на уведомление открывалось приложение Twitter с вкладкой, куда попадают все уведомления.

Набор символов напоминает некий хэш, вроде того, который используется для транзакций с криптовалютой или для шифровки информации.

***

17.10.2018

Acronis открывает в Болгарии центр разработок в сфере киберзащиты, блокчейна, ИИ

Для разработки передовых технологий компания Acronis развивает сеть научно-исследовательских центров, расположенных в странах Азии, Европы и Америки. Глобальное присутствие позволяет непрерывно совершенствовать технологии в сфере киберзащиты, искусственного интеллекта и блокчейна.

Докладніше

***

17.10.2018

Похищены данные и кредитные карты 30 тыс. сотрудников Пентагона

Представители Пентагона сообщили о взломе записей о поездках в Министерстве обороны, в результате которого были скомпрометированы личные данные и информация о кредитных картах военного и гражданского персонала (Компьютерное Обозрение).

По данным Associated Press, которая ссылается на официальное лицо, знакомое с вопросом, утечка могла затронуть до 30 тыс. человек, но это число может увеличиться по мере продолжения расследования.

Взлом, предположительно, мог произойти несколько месяцев назад, но был обнаружен только недавно. Источник сообщил, что расследование пока не обнаружило утечки какой-либо секретной информации.

Представитель Пентагона, подполковник Джозеф Бучино (Joseph Buccino), сообщил, что они продолжают собирать информацию о размере и масштабах взлома и о том, кто его совершил. Пока известно, что был взломан сервис одного коммерческого поставщика, который предоставлял услуги небольшому проценту от общего количества сотрудников Министерства обороны.

***

17.10.2018

Пользователи продолжают слушать нелегальную музыку

По данным Международной федерации звукозаписывающей индустрии (IFPI), 38 % потребителей музыкального контента по-прежнему получают его незаконными путями вроде торрент-треккеров.

Докладніше

***

17.10.2018

Владимир Кондрашов

Документы Энергоатома были доступны российским террористам

В открытом доступе опять оказались документы НАЭК «Энергоатом». На этот раз – касающиеся работы Южно-Украинской АЭС. Утечку данных обнаружил эксперт по кибербезопасности, ведущий разработчик компании «IT Лаборатория» Александр Галущенко.

Докладніше

***

17.10.2018

IBM будет использовать ИИ для решения проблем кибербезопасности

Порой для разработки средств защиты стандартных методов уже недостаточно, но обезопасить киберпространство решилась крупная компания IBM, применив для этого искусственный интеллект.

Докладніше

***

18.10.2018

Как Интернет следит за детьми

Джастин Льюис, британец, отец двух малышей в возрасте 4 и 6 лет, решил уточнить – какие сведения собирают сайты в интернете по запросам, поступающим от детей, не достигших 13 лет? Его потрясло, что посещение всего лишь пяти страниц вызвало удивительный каскад из 1871 запросов фоновых данных.

Докладніше

***

18.10.2018

В даркнете продаются данные миллионов избирателей США

Специалисты из Anomali Labs и Intel 471 обнаружили на одном из популярных киберпреступных форумов около 35 млн записей, содержащих сведения об избирателях, в том числе персонально идентифицируемую информацию и историю голосований.

Докладніше

***

18.10.2018

Ирина Фоменко

Apple запускает новый веб-сайт с персональными данными пользователей

Сайт конфиденциальности тестировали в мае в Европейском союзе, как раз во время принятия Общего регламента по защите данных (GDPR).

Докладніше

***

19.10.2018

В конце года 62 % всех сайтов в интернете лишатся обновлений безопасности

По данным W3Techs, на сегодняшний день около 78,9 % всех сайтов в интернете работают на PHP. Однако 31 декабря нынешнего года официально прекращается выпуск обновлений безопасности для PHP 5.6.x, что ознаменует полное прекращение поддержки всех версий устаревшей ветки PHP 5.x.

Докладніше

***

19.10.2018

Sony будет использовать блокчейн для защиты цифровых авторских прав

Компания Sony объявила, что она будет использовать технологию блокчейн для защиты цифровых авторских прав. Проект начнется с образовательных материалов под управлением Sony Global Education, которые предназначены для бизнеса (InternetUA).

В Sony также рассказали, что решение экспериментировать с новой технологией пришло к ним после похожих действий со стороны других компаний – например, Kodak, которая запускает собственную криптовалюту. В пресс-релизе отмечается, что блокчейн идеально подходит для защиты прав в интернете, так как Sony в основном работает с цифровыми активами.

В первую очередь Sony будет отслеживать цифровые транзакции в записях, которые особенно трудно подделать – в этом случае блокчейн будут использовать сами авторы контента. Сейчас же они при желании могут заниматься этим вручную, что отнимает много времени и усилий.

В будущем блокчейн позволит Sony отслеживать свой контент от процесса создания. Это означает, что пользователи смогут увидеть и проверить, кто создал контент, кто владеет на него правами и когда он был создан. В настоящее время Sony Global Education будет единственной платформой для экспериментов, но компания планирует, что и другой контент, например, музыка и фильмы, позднее будет защищен таким же образом.

Блокчейн внес немало новшеств в сферу защиты авторских прав, и этот проект – не первый из них. Однако прежде они были рассчитаны на защиту отдельных аспектов авторского права, а не всей индустрии. Sony утверждает, что если эксперимент удастся, то она применит блокчейн для защиты всех работ компании.

***

19.10.2018

Уязвимость на сайте Tumblr позволяла похитить данные пользователей

17 октября администрация блог-платформы Tumblr сообщила об уязвимости в web-интерфейсе для десктопных компьютеров, позволяющей похищать конфиденциальную информацию. По словам представителей Tumblr,

в ходе расследования свидетельств эксплуатации уязвимости в преступных целях выявлено не было (InternetUA).

Проблема затрагивала код, отвечающий за кнопку «Рекомендуемые блоги» на сайте Tumblr. Кнопка видна только авторизованным пользователям и, как следует из названия, предоставляет список блогов, которые могут быть им интересны. С помощью ПО для отладки можно было просматривать определенную информацию из блогов, указанных в списке рекомендуемых.

В частности, злоумышленники могли видеть электронные адреса, подсоленные хешированные пароли, вводимые пользователем данные о местоположении (позднее эта функция была деактивирована), использовавшиеся ранее электронные адреса, IP-адрес, с которого пользователь в последний раз заходил на сайт, и название связанного с учетной записью блога.

Специалисты Tumblr не смогли с точностью установить затронутые уязвимостью учетные записи, однако отметили, что проблема встречалась довольно редко. Блог-платформе стало известно об уязвимости от исследователя безопасности (его имя Tumblr не называет), сообщившего о ней в рамках программы выплаты вознаграждений. Уязвимость была исправлена несколько недель назад в течение 12 часов с момента получения сообщения от исследователя.

***

19.10.2018

10 типів даних, які збирає про вас браузер // Цю інформацію ви видаєте навіть тоді, коли заходите на безпечні сайти

Існують різні типи даних, збору яких не можуть перешкодити навіть VPN-сервіси.

Докладніше

***

21.10.2018

В Стэнфорде создают лабораторию для борьбы с негативными последствиями технологий

Исследовательский центр возглавит Алекс Стеймос. Он покинул Facebook из-за несогласия с тем, как компания реагирует на скандал с российским вмешательством в американские выборы. Расследование киберпреступлений – одно из главных направлений работы лаборатории.

Докладніше

***

22.10.2018

Владимир Кондрашов

Украинские государственные сайты почему-то оставляют лазейки для хакеров

Украинские хактивисты снова обнаружили на ряде сайтов государственных организаций XSS и SQL-уязвимости. Некоторые ресурсы взломали хакеры из восточных стран, а на одном из них вообще не был установлен пароль для доступа в административную панель (InternetUA).

Информацию об этом на своей странице в Facebook опубликовал спикер Украинского киберальянса, известный в сети под ником Sean Townsend, передает InternetUA.

Согласно опубликованной информации, проблемы с безопасностью обнаружены на сайтах Физико-механического института им Г. В. Карпенко НАН Украины, Управления агропромышленного развития Черкасской ОГА, Малой академии наук, Департамента социальной защиты Закарпатской ОГА и Корецкой РГА (Ровенская область).

Сайты Малой академии наук и Департамента социальной защиты Закарпатской ОГА уже взломали хакеры из Ближнего Востока.

На сайте Корецкой РГА активисты обнаружили незапароленный вход в административную панель.

Напомним, украинские хактивисты в рамках флешмоба #fuckresponsibledisclousure выявляют и публикуют в открытом доступе сведения об уязвимостях украинских государственных Интернет-ресурсов. Публичная огласка уязвимостей, по словам участников флешмоба, позволяет добиваться результата: государственные органы реагируют на подобную информацию намного оперативней, устраняя бреши и проблемы на своих ресурсах. За время существования флешмоба были закрыты десятки уязвимостей на ресурсах Энергоатома, Госфинмониторинга, Национальной полиции, Херсонского облсовета, Донецкой ОВЦА и многих других.

***

22.10.2018

Атаки криптомайнеров на iPhone увеличились в пять раз

Check Point в отчете Global Threat Index за сентябрь отмечает, что количество атак майнеров криптовалюты на устройства Apple iPhone увеличилось почти на 400 %. Атаки проводятся при помощи вредоносного ПО Coinhive, которое занимает верхнюю строчку в рейтинге Global Threat Index с декабря 2017г (Компьютерное Обозрение).

Майнер Coinhive остается самым распространенным вредоносным ПО – им атакованы 19 % организаций по всему миру. Специалисты Check Point также обнаружили значительное увеличение числа атак Coinhive на ПК, планшеты и смартфоны с установленным браузером Safari, который обычно используется в устройствах Apple. Майнер Cryptoloot поднялся на третью строчку в рейтинге угроз Global Threat Index. Это второе по охвату вредоносное ПО для скрытой

добычи криптовалют. Главное конкурентное отличие Cryptoloot от Coinhive – более низкие комиссионные для владельцев сайтов.

В сентябре Dorkbot, троян, основная цель которого – похитить конфиденциальную информацию и запустить DDoS-атаку, сохранил второе место в рейтинге самых активных угроз. С ним столкнулись 7 % организаций.

Исследователи Check Point также проанализировали наиболее эксплуатируемые уязвимости. Первое место сохранила уязвимость CVE-2017-7269, затронувшая 48 % организаций по всему миру. На втором месте – проблема CVE-2017-5638 с глобальным охватом в 43%, на третьем, с небольшим отставанием, – возможность инъекции кода из-за неверной конфигурации PHPMyAdmin на веб-сервере (Web servers PHPMyAdmin Misconfiguration Code Injection). Эта уязвимость выявлена у 42 % компаний.

***

22.10.2018

Неизвестные похитили данные 75 тыс. жителей США через портал медстрахования

Киберпреступники взломали систему регистрации на портале медицинского страхования HealthCare.gov и похитили персональные данные порядка 75 тыс. человек (InternetUA).

Речь идет о системе Federally Facilitated Exchanges (FFE), находящейся в ведении Центров Medicare & Medicaid Services (CMS). Страховые агенты и брокеры в области медицинского страхования используют ее для регистрации своих клиентов в страховых планах Obamacare на официальном портале HealthCare.gov.

Как сообщается в пресс-релизе CMS, аномальная активность в системе FFE была обнаружена 13 октября, после чего сразу же было инициировано расследование. 16 октября был подтвержден факт взлома.

Связанные с аномальной активностью учетные записи агентов и брокеров были деактивированы. В качестве дополнительной меры предосторожности для брокеров и агентов была отключена прямая регистрация клиентов. Граждане США по-прежнему могут самостоятельно оформлять страховку Obamacare через HealthCare.gov. Функция регистрации клиентов для агентов и брокеров будет включена в течение семи дней.

CMS сообщили об инциденте в ФБР и в ближайшее время разошлют соответствующие уведомления всем затронутым утечкой пользователям.

Obamacare – Закон о защите пациентов и доступном здравоохранении. Представляет собой федеральный закон США, подписанный президентом Бараком Обамой 23 марта 2010 года. Законодательная основа реформы здравоохранения, ставшей одним из самых крупномасштабных проектов в истории США с середины 1960-х годов.

***

23.10.2018

Япония потребовала от Facebook улучшить защиту данных

Правительство Японии в лице комиссии по защите личной информации начало эту неделю с обращения к компании Facebook с требованием лучше защищать личные данные пользователей одноименной социальной сети. Требование прозвучало после неоднократно зафиксированных в текущем году ситуаций, когда были затронуты права десятков миллионов пользователей Facebook (InternetUA).

Так, в этом месяце стало известно, что злоумышленники похитили данные 29 миллионов учетных записей пользователей. А в апреле личные данные почти 87 миллионов пользователей были неправомерно получены британской фирмой Cambridge Analytica.

Японская комиссия участвовала в расследовании инцидента с Cambridge Analytica совместно с властями Великобритании и других стран. Ей удалось установить, что инцидент, вероятно, затронул до 100000 японских пользователей. Итогом работы комиссии стало обращение к Facebook.

Крупнейшую в мире социальную сети просят в полном объеме сообщать пользователям о проблемах, связанных с безопасностью, усилить надзор за поставщиками приложений и информировать регулирующие органы о любых изменениях в мерах безопасности.

Уточним, что обращение не предусматривает наказаний и не имеет юридической силы.

***

23.10.2018

Миллионы людей пользуются функцией «Не отслеживать» в браузере. Но она не работает

Миллионы людей пользуются настройками конфиденциальности в своем браузере – в частности, кнопкой «Не отслеживать», которая передает сайту требование не собирать данные о пользователе.

Докладніше

***

24.10.2018

Bloomberg: додатки продовжують шпигувати навіть після їхнього видалення

Деякі провайдери послуг кажуть, що такі інструменти стеження призначені для визначення реакції користувачів на оновлення додатків та інші зміни.

Докладніше

***

23.10.2018

Небезпечний NFC: виявили спосіб як можна викрасти дані із смартфонів

Виявили спосіб як можна викрасти дані із смартфонів за допомогою NFC

Модуль NFC, який зараз є практично на всіх смартфонах під управлінням Android, може стати засобом для їх віддаленого «злому». За допомогою цього виду бездротового зв'язку можна отримати логіни та паролі до облікових записів (24 Канал).

Про це в рамках конференції Hack.lu розповів дослідник в галузі інформаційної безпеки компанії Checkmarx Педро Умбеліно.

Виявлений науковцем метод дозволяє передавати по бездротовому з'єднанню логіни і паролі облікових записів з одного смартфона на інший за умови його знаходження в зоні досяжності технології Near-field communication.

За словами Умбеліно, дослідницьким шляхом він з'ясував, що дальність спрацьовування NFC-модуля в певних сценаріях використання може перевищувати заявлені виробниками смартфонів 7-10 сантиметрів. Це означає, що зломщик може ініціювати отримання даних навіть на пристроях з відключеними модулями Wi-Fi, Bluetooth або GSM, перебуваючи на значній відстані (до декількох десятків метрів) від своєї жертви, і при дотриманні ряду умовностей залишатися абсолютно непоміченим.

Втім, щоб метод Умбеліно спрацював, зловмисникові необхідно спочатку встановити на смартфон жертви шкідливий компонент, який перетворить його в передавач. Саме він завдяки так званій амплітудній маніпуляції, що отримала назву on-off keying, буде здійснювати передачу даних зі швидкістю 10-12 біт / с.

Для досягнення оптимального сигналу необхідно, щоб відстань між передавачем і приймачем не перевищувало 10 метрів. В іншому випадку в процесі передачі можуть виникати помилки, які, на радість зломщиків і на жаль їх жертв, підлягають коригуванню постфактум.

Основну складність в процедурі злому, за власною заявою Умбеліно, представляє встановлення зловмисного компонента на пристрій жертви.

Однак, констатує дослідник, враховуючи велику кількість способів підробки програмного забезпечення, спровокувати людину завантажити файл не є нездійсненною умовою, яка окупиться сторицею при зараженні мережі корпоративних пристроїв.

***

23.10.2018

Гендиректор Youtube закликає авторів контенту бойкотувати нове законодавство ЄС про авторське право // Сьюзан Войчіцкі вважає, що зокрема стаття 13 перекриє доступ невеликих авторів контенту до платформ Youtube, Facebook, Twitter та Google

Генеральний директор Youtube Сьюзан Войчіцкі попереджає виробників відеоконтенту про загрозу суперечливого законодавства про авторське право в ЄС і закликає їх «негайно вжити заходів» та протестувати проти нових правил публікації відео та дописів у соціальних мережах.

Докладніше

***

23.10.2018

У Швейцарії затримали двох росіян за плани хакерської атаки на WADA

Громадяни РФ планували здійснити хакерську атаку на лабораторію Всесвітнього антидопінгового агентства у Лозанні. Раніше розвідслужба Швейцарії застерігала від атак РФ на міжнародні установи в країні (DW).

Двох громадян РФ затримали 23 жовтня за підозрою в плануванні здійснення хакерської атаки на лабораторію Всесвітнього антидопінгового агентства (WADA) у Лозанні, інформує агенція SID. Міністерство юстиції Швейцарії дало дозвіл на подальше розслідування справи. Двоє ймовірних хакерів, на додачу до лабораторії WADA, планували хакерські атаки на ряд інших установ.

Як ми повідомляли раніше, місяць тому виконавчий комітет WADA поновив у правах Російське антидопінгове агентство (РУСАДА), котре було позбавлене акредитації з листопада 2015 року, коли з'явилася інформація про вживання допінгу російськими легкоатлетами. Утім, поновлення супроводжувалось жорсткими умовами і вказанням чітких термінів, у які WADA має отримати доступ до лабораторних даних і зразків проб у московській лабораторії.

***

23.10.2018

SIM-карта Tor-only для полной анонимности в сети

Один из британских провайдеров начал бета-тестирование SIM-карты, которая блокирует весь мобильный трафик, кроме трафика через Tor. Сервис может пригодиться абонентам, которые остро нуждаются в соблюдении полной конфиденциальности, ради которой готовы поступаться скоростью доступа.

Докладніше

***

23.10.2018

США начали первую кибероперацию против российских хакеров

В США началась спецоперация в киберпространстве против, вероятно, сотрудников российских спецслужб (InternetUA).

Как отметили в Министерстве юстиции, Россия с помощью «информационной войны» пытается повлиять на выборы.

«Кампания, которая включает ряд миссий, проведенных за последние несколько дней, является первой подобного рода операцией за рубежом, призванной защитить американские выборы, в частности ноябрьские промежуточные выборы (в Конгресс, – ред.)», – сказано в сообщении.

Американские специалисты в области информационных технологий отследили в киберпространстве несколько подозрительных пользователей из России и выяснили подробности их деятельности.

«Киберкомандование направляло прямые сообщения агентам, которые стоят за кампаниями воздействия. Высокопоставленные официальные лица, работающие в сфере обороны, заявили, что они не угрожали непосредственно этим лицам», – отмечается в материале.

В настоящее время неизвестно, с помощью каких каналов связи проводилась операция.

***

23.10.2018

Шахраї крадуть особисті дані з ProZorro для отримання мікрокредитів

Співзасновник українського стартапу DroneUA Валерій Яковенко розповів, що опинився серед постраждалих, від імені яких нібито були взяті кредити у фінансовій компанії Moneyveo.

Докладніше

***

23.10.2018

Власти Китая объявили войну анонимности на блокчейн-платформах

Управление по вопросам киберпространства КНР подготовило законопроект, который обяжет пользователей блокчейн-сервисов раскрывать свои реальные имена и номера персональных ID.

Докладніше

***

24.10.2018

Ирина Фоменко

Как выжить в кибератаке

«Есть несколько возможностей ограничить уровень разрушений от кибератак», – заявил адмирал Майкл Роджерс. – «Нужно знать цель злоумышленника, и какой вектор он пытается использовать для ее достижения. Не зацикливайтесь на одном».

Докладніше

***

24.10.2018

Signal ставит под угрозу безопасность конфиденциальных данных

Хотя разработчики Signal позиционируют мессенджер как средство для безопасной коммуникации, приложение не обеспечивает должную защиту при обновлении с расширения для Chrome на декстопную версию, экспортируя сообщения пользователей в виде незашифрованных файлов (InternetUA).

В процессе апгрейда пользователю требуется указать локацию, куда будут сохраняться данные сообщений (текст и вложения), для автоматического импорта информации в новую версию. Однако, по словам эксперта по безопасности Мэтта Суиша (Matt Suiche), обратившего внимание на проблему, приложение сохраняет данные в незашифрованном виде.

Главная директория содержит отдельные папки для каждого контакта в Signal, которые названы по имени контакта и номеру телефона. В папках также хранятся файлы JSON, содержащие диалоги. Таким образом, просто открыв директорию, можно получить доступ к ценной информации. Более того, данные сохраняются на диске даже после завершения процесса апгрейда. Пользователям потребуется вручную удалить папки для снижения риска утечки конфиденциальной информации.

Весной нынешнего года в различных версиях мессенджера были обнаружены сразу несколько уязвимостей, предоставляющих возможность обойти аутентификацию или внедрить код.

***

25.10.2018

Владимир Кондрашов

Украинские хакеры украли банковские данные с помощью приложения для знакомств

Украинские полицейские ищут распространителя вредоносного программного обеспечения, позволяющего несанкционированно вмешиваться в работу мобильных Android-устройств для последующего списания денежных средств с банковских счетов и электронных кошельков пораженных смартфонов.

Докладніше

***

26.10.2018

Ирина Фоменко

Миллионы пассажиров пострадали из-за хакерской атаки на авиакомпанию

В Cathay Pacific Airways Ltd сообщили, что хакеры получили личную информацию 9,4 млн клиентов. Это крупнейшее в мире хищение данных авиакомпании.

Докладніше

***

27.10.2018

Китай уличили в систематическом перехвате интернет-трафика

Китайская государственная телекоммуникационная компания China Telecom на регулярной основе осуществляет перехват и перенаправление в Китай интернет-трафика, направляемого или проходящего через США и Канаду в рамках масштабной операции по кибершпионажу и краже интеллектуальной собственности, следует из доклада специалистов Военно-морского колледжа США и Тель-Авивского университета (InternetUA).

С помощью разработанной ими системы мониторинга BGP анонсов специалисты выявили многочисленные случаи перехвата интернет-трафика, проведенного China Telecom в последние несколько лет. К примеру, в 2016 году компания перенаправила трафик правительственных сетей в Канаде и Южной Корее на свои точки присутствия (Point of presence, POP) в Торонто. Далее трафик был перенаправлен на POP China Telecom на Западном побережье США, а оттуда в Китай и Южную Корею. В 2017 году компания перехватила трафик между Японией и Скандинавией, проходящий через территорию США и отправила его на почтовый сервер, принадлежащий крупной тайваньской финансовой организации.

После копирования трафика для его дальнейшей расшифровки и изучения China Telecom «возвращает» трафик в сети лишь с небольшой задержкой, отмечается в докладе. Подобные инциденты довольно сложно обнаружить, поскольку China Telecom владеет многочисленными точками присутствия в Северной Америке и Европе, располагающимися в непосредственной близости от целевых сетей, в результате задержки в потоке трафика практически незаметны, несмотря на то, что он проходит по более длинному маршруту.

В свою очередь, Китай запрещает иностранным операторам связи и провайдерам размещать POP на своей территории, таким образом защищая внутренний и транзитный трафик от перехвата.

***

28.10.2018

9 из 10 приложений для Android сливают ваши данные Google

9 из 10 приложений для устройств под управлением Android собирают информацию о своих пользователях и передают ее Google или аффилированным предприятиям. К такому выводу пришли исследователи в области информационной безопасности Оксфордского университета. Они изучили ассортимент Google Play, и выяснили, что ретрансляцией пользовательских данных занимаются даже те программы, которые прямо не заявляют об этом. Впоследствии эти сведения продаются на сторону за немалые деньги (InternetUA).

По словам авторов исследования, приложения осуществляют сбор информации с помощью специальных трекеров. Они позволяют накапливать самый широкий спектр данных, который включает в себя сведения об устройстве, его уникальный идентификатор, частоте постановки на зарядку, перемещения владельца, его возрасте, поле, истории веб-браузера, установленных приложениях и так далее. На основе полученной информации формируются персонализированные профили, которые передаются Google, а та продает их по назначению.

Зачем Google собирает информацию о вас

Как правило, профили пользователей пользуются спросом у рекламодателей, которые используют их в формировании рекламной выдачи, и у банковских организаций, составляющих на их основе кредитный скоринг своих клиентов. Чем больше информации содержит профиль, тем ценнее он для рекламодателя или банка, поскольку в перспективе может обернуться максимальной конверсией.

Очевидно, что тайный сбор информации о пользователях, – это серьезная проблема для всей отрасли. Но хуже всего, что сама Google не заинтересована в ее разрешении, рискуя навсегда лишить себя постоянного источника дохода. Компания спустя рукава контролирует ПО, которое попадает в фирменный каталог приложений, поскольку понимает, что масштабная чистка не принесет денег. А разовые удаления приложений с вынесением предупреждения разработчикам – это не более чем театр безопасности с четко спланированным сценарием.

***

29.10.2018

В Google Play обнаружено несколько десятков вредоносных банковских приложений

Компания ESET сообщает об обнаружении в официальном магазине Google Play ряда троянских приложений, нацеленных на похищение банковских данных пользователей.

Докладніше

***

29.10.2018

Майя Яровая

В Днепре киберполиция задержала хакера, продававшего вирусы через собственные закрытые сайты

Киберполиция разоблачила хакера, который распространял созданные компьютерные вирусы через собственные закрытые хакерские ресурсы. Количество авторизованных пользователей этих ресурсов превышала 2500. Правоохранители устанавливают количество пострадавших (пока известно про около 50 жертв) и точное количество покупателей (AIN.UA).

Как удалось установить следствию, 35-летний житель Днепра разрабатывал вредоносное программное обеспечение, а для его распространения создал закрыт хакерских форум и сайт. Для регистрации на сайтах нужно было подать заявку и пройти некое «собеседование» с хакером, после чего пользователь получал доступ к ресурсу и возможность покупать вирусы.

Вредоносное ПО преимущественно использовалось с целью получения доступа к компьютерным системам с возможностью удаленного управления. После инфицирования компьютера хакер мог копировать всю файловую систему, логины и пароли в браузере, осуществлять запись работы рабочего стола. Для сокрытия следов своей деятельности, после завершения работы вируса, пораженный компьютер принудительно перезагружался с одновременным запуском форматирования жестких дисков компьютера.

***

29.10.2018

Данные сотрудников украинской «дочки» Сбербанка России утекли в сеть

Имена и адреса электронной почты примерно 420 тыс. сотрудников Сбербанка России попали в сеть. Причину утечки в банке не раскрывают, возможный вариант – «злонамеренные действия одного из сотрудников».

Докладніше

***

29.10.2018

Владимир Кондрашов

Информационный «стриптиз» государственных сайтов продолжается

Флешмоб Украинского кибералъянса #fuckresponsibledisclousure, начатый около года назад, несмотря официальное окончание, похоже, заканчиваться и не собирается. Причина тому – отношение органов власти к собственной кибербезопасности.

Докладніше

***

29.10.2018
Ирина Фоменко
Google Play больше не хочет быть рассадником вредоносного софта

Google предпринимает новые меры для защиты конфиденциальности и предотвращения злоупотребления приложениями на смартфонах Android. Об этом сообщает The Star Online (InternetUA).

Технологический гигант планирует ужесточить ограничения на запрос сторонних приложений к журналам вызовов и текстовым сообщениям на смартфонах Android.

Так, приложения из Play Маркета теперь могут получить разрешение только на чтение этих данных, если пользователь установил его как приложение по умолчанию для совершения телефонных звонков или написания текстовых сообщений.

Раньше любое приложение могло получить доступ к данным, если пользователь предоставил ему разрешение.

Тем не менее, пользователи часто соглашаются на запросы на получение разрешений от приложений, не зная, действительно ли на самом деле им это необходимо для работы.

ДОДАТКИ

Додаток 1

24.10.2018
Ирина Фоменко
Социальные сети на работе: демократично или рискованно

Большинство компаний считали социальные сети неуправляемыми и такими, что мешают работе, многие даже запретили использование Facebook и Twitter. Однако сегодня некоторые из крупнейших работодателей мира делают обратное: уговаривают сотрудников регистрироваться в социальных сетях, предназначенных для работы. Об этом сообщает The Telegraph (InternetUA).

Среди первых был Yammer, клон Facebook для компаний и команд, запущенный в 2008 году и купленный Microsoft в 2012. Позже был Slack, причудливое приложение для офисного чата. Microsoft выпустил Teams, которым пользуются уже 200 000 компаний. Даже Google Plus останется в качестве офисного продукта. После долгого застоя корпоративные социальные сети, похоже, набирают обороты.

Но, пожалуй, самым интересным игроком является сам Facebook. Приложение Workplace запустили в 2011 году в качестве внутреннего инструмента, но оно стало публичным два года назад. На первый взгляд

Workplace почти идентичен Facebook: пользователи могут общаться, создавать группы, отвечать на сообщения и транслировать видео в прямом эфире. Но приложение финансируется за счет подписки, а не рекламы, и данные, которые Workplace генерирует, доступны только для компаний, использующих его.

Доступность руководителей

Глава проекта Жюльен Кодорниу объяснил, что значит «эффект Workplace»: когда ранее изолированные рабочие получают новый канал связи, превращающий «компании в сообщества».

«Когда вы даете каждому право голоса и соединяете всех, вершатся великие дела», – заявил Кодорниу. – «Идея заключается в том, что, поощряя неформальное общение между различными департаментами на более равной основе, вы помогаете появлению и реализации новых идей».

По словам Вики Хафф Эккерт из PWC, такие системы в будущем будут более востребованы, так как все больше людей работают дистанционно. «Миллениалы теперь занимают руководящие должности, и они хотят общаться со своими сотрудниками, используя технологию, с которой они выросли. Разговоры, ранее ведшиеся по телефону, на встречах и в кулуарах, теперь все чаще происходят в Интернете», – прокомментировала Эккерт.

Как считает исполнительный директор Service Rocket Роб Кастанеда, раньше социальные медиа были только для «белых воротничков» (офисный персонал), тогда как с появлением Workplace ситуация поменялась – теперь к этому можно приобщить и «синих воротничков» (технические работники), например, экипаж авиакомпаний или фабричных рабочих, которые часто культурно отделены от коллег из головного офиса. Эккерт же убеждена, что такие приложения будут «сглаживать» офисные иерархии.

Решение на каждый день

Получить неоспоримые доказательства полезности таких социальных медиа довольно сложно, однако многие лидеры бизнеса заявили, что сотрудники становились более счастливыми, а рабочий процесс – улучшался. По словам Джен Бакстер из GlaxoSmithKline, Workplace помог ученым-интровертам сотрудничать комфортным для них образом.

Тем не менее, существуют и определенные угрозы. Slack критиковали как отвлекающую, захватывающую псевдо-видео-игру, которая мешает концентрации сотрудников, обязывая их быстро отвечать на все сообщения. Хоть Workplace и немного лучше в этом плане, многие эксперты отметили, что приложение вызывает привыкание, как, например, печально известные социальные сети.

Другая потенциальная проблема заключается в том, какую коммуникацию могут оказывать такие службы. «Дизайн программного обеспечения совершенно по-разному влияет на поведение людей. Разговорный или неформальный характер этих платформ мешает восприятию серьезного контента», – заявил руководитель Wiretap Грег Моран.

Моран привел в пример Uber, где уволили главного исполнительного директора и еще 20 человек в прошлом году после того, как бывший сотрудник

подробно рассказал о сексуальных домогательствах в корпоративном чате, а также Google, чей внутренний мессенджер использовали для дискуссии над «заметкой о запрете разнообразия».

Новая форма контроля?

Появляется вопрос о контроле. Немногие будут возражать против использования инструментов Wiretap для прекращения сексуальных домогательств, утечки данных или анализа счастья сотрудников. Но их также могут использовать для увольнения рабочих, которые отрицательно отзываются о начальстве.

Для социолога Джейми Вудкока, полгода работавшего под прикрытием в британском call-центре, это всего лишь одни из способов для работодателей контролировать сотрудников. По его мнению, офисные социальные сети являются своего рода захватом личной территории работников.

«Риски конфиденциальности не отличаются от мониторинга использования Интернета, электронной почты и так далее. Представьте: работодатель узнает через ИИ, что сотрудник недоволен чем-то, и увольняет его. А потом уже бывший работник предъявляет иск о неправомерном увольнении, а суд заинтересован в алгоритме. Нам предстоит узнать о том, насколько точны эти инструменты и можно ли их использовать для принятия решений», – заявил юрист по вопросам конфиденциальности Альберт Гидари.

На сегодняшний день социальные сети на работе – это в основном инструмент для общения, но в будущем данные, которые они генерируют, могут использоваться для улучшения деловой практики, анализа отношений команд или даже оценки эффективности отдельных сотрудников.

(вгору)

Додаток 2

29.10.2018

ИИ сделает подписи на Facebook «более привлекательными»

Исследователи машинного обучения в Facebook разработали новую модель нейронной сети. Она может придумать подписи к фотографиям, которые будут более «привлекательны» для людей. При этом ИИ сможет делать это с помощью разного тона и выражений, притворяясь более «романтичным» или «прагматичным» пользователем (InternetUA).

Исследователи из подразделения Facebook AI нашли способ обучить модели машинного обучения описывать не только фактические предметы на фотографиях, но и подписывать их. Ученым кажется, что при этом стилистика комментариев будет более интересна для других пользователей и станет учитывать «отношения между пользователями внутри социальной сети», а также «стилистику изложения мыслей человека».

Традиционные задачи ИИ, который уже используется в социальной сети, намного проще – автоматическое описание предметов, которые расположены на фотографии.

Личность пользователя при этом может варьироваться между «романтичным, высокомерным, тревожным». Например, изображение сэндвича может быть подписано как «это прекрасный бутерброд» или более иронично – «я могу приготовить хорошо только такую еду». Работа ИИ представляет собой соединение из нескольких современных методов, таких как определение содержания изображения и генерация новых предложений.

«В будущем мы планируем встраивать черты личности в работу ИИ. Также наша задача – обучение «извлечению следующего высказывания». Для этого мы используем базу данных, содержащую диалог, состоящий из 1,7 млрд пар высказываний. Это и станет учебником для робота, который будет учиться писать мысли правильно и в разной стилистике», – отмечается в анонсе.

(вгору)

Додаток 3

29.10.2018
Facebook делает ставку на музыку

В компании Facebook готовят сразу несколько нововведений, касающихся музыки. Первый момент – это сервис-конкурент TikTok. Для него в компании создают отдельное приложение под названием Lasso, которое, как ожидается, сможет привлечь подростковую аудиторию. Как ожидается, в приложении пользователи смогут танцевать под музыку и «петь» под фонограмму. Записанные ролики можно будет отправлять друзьям (InternetUA).

Сообщается, что разработкой занимается подразделение Facebook, которое в том числе развивает сервис Watch. А непосредственно проектом Lasso руководит продуктовый дизайнер Брэди Восс (Brady Voss). Раньше он трудился над ТВ-приложением Facebook и сервисом для звонков Hello, который закрыли в июле 2018 года.

Кроме того, теперь в «Истории» Facebook можно добавлять музыкальные треки в виде стикеров. Для добавления нужно нажать на значок наклейки и выбрать песню. Также всем пользователям открыт доступ к функции Lip Sync Live. Она даёт возможность снимать собственные клипы и петь. Как обещают разработчики, понемногу к песням будут добавляться тексты.

Кроме того, в ближайшие недели Facebook внедрит возможность добавлять песни в новый раздел музыки в профиле пользователя. Песню можно будет закрепить в верхней части профиля, а посетители страницы смогут прослушивать эти треки, смотреть сопроводительное видео с фотографиями исполнителей и обложками альбомов, добавлять песню себе и так далее.

Отметим, что всё это рассчитано на молодых людей. В компании уже пытались добиться внимания молодёжи с помощью отдельных приложений вроде Poke, Slingshot, Bolt, Flash и других вариаций Snapchat. Однако ни одна из них не прожила долго. Нынешняя инициатива также взята со Snapchat. Посмотрим, чем это закончится в данном случае.

(вгору)

Додаток 4

30.10.2018

Поход Приходько в большую политику вызвал массу споров: что пишут в соцсетях

Внезапное заявление известной певицы Анастасии Приходько о том, что она уходит со сцены ради большой политики вызвало бурное обсуждение у пользователей соцсетей. Поводом стал не само решение, а выбор политической силы. Приходько присоединилась к партии «Батькивщина» Юлии Тимошенко (Факты).

Стоит отметить, что ее неожиданный выбор привел к громким обсуждениям и даже ссорам между известными в Украине блогерами и активистами.

Некоторые пользователи поспешили напомнить, что в 2015 году Приходько начала сотрудничать с Олегом Ляшко, однако очень быстро их совместная работа прекратилась. Тогда певица пообещала «творить добрые дела вне политики».

В то же время блогеры припомнили Приходько другие ее слова. В мае этого года в интервью изданию Цензор, отвечая на вопрос «к какой из политических сил артистка никогда бы не пошла», Приходько ответила: «Оппозиционный блок». «БЮТ», скорее всего. Я, наверное, боюсь людей, которые очень долго уже у власти. Наверное, не пойду к людям, которые уже по 20 лет сидят в парламенте. Надо идти к молодым».

«П – последовательность», – написали об этом некоторые блогеры.

Брат Анастасии, известный волонтер Назар Приходько также высказался о ситуации: «Тимошенко – никогда не была моим кандидатом в президенты, никогда не была политиком, за которым я был готов идти. Не мое, короче говоря. Поэтому я не меньше других удивлен и растерян от решения Насти. Впрочем, это ее выбор, выбор взрослого человека с достаточно солидным бэкграундом. Не нам ее судить или осуждать».

(вгору)

Додаток 5

21.10.2018

Как в Украине родители зарабатывают миллионы, снимая детей для Youtube

Топовые детские каналы на просторах украинского Youtube зарабатывает больше $100 тыс. в месяц. Разумеется, деньги попадают в кошелек родителей, которые снимают своих чад (InternetUA).

Как налажена работа детских каналов, почему эти видеоблоги так популярны и можно ли это назвать эксплуатацией детей пишет MC Today.

По данным ресурса Socialblade, детский контент – самый востребованный в украинском YouTube. Трехлетние видеоблогеры дарят миллионам мам минуты спокойствия, а взамен получают недетскую прибыль.

На самом популярном в Украине канале Kids Diana Show сейчас 10 миллионов подписчиков и больше 100 тысяч долларов дохода в месяц, пишет издание. Маленькая Диана стала блогером еще в младенчестве, а спустя несколько лет уже обеспечила семью недвижимостью в США.

Одесские брат и сестра Miss Katy и Mister Max еще не пошли в школу, но уже позволили маме с папой эмигрировать из Украины в Великобританию. У них около 20 млн подписчиков на двоих и сотни тысяч долларов дохода в месяц.

Как правило, родители детей-блогеров категорически избегают журналистов, но мама пятилетнего Влада из Vlad TV Show с 1,2 млн подписчиков оказалась исключением.

«Сейчас канал является единственным источником дохода для нашей семьи, – делится Оксана. – На жизнь и наши непритязательные запросы хватает. До появления канала мой муж работал программистом, а я – в торговле».

Идея создать канал пришла в голову родителям Влада три года назад, когда мальчику еще не было трех.

«Пришло время задуматься о выходе на работу после декрета. Возвращаться в торговлю не было желания, поэтому я искала новые идеи», – делится мать видеоблогера.

Определиться помог случай. Оксана заметила, как Влад уверенно выбирает иконку YouTube на планшете и с удовольствием смотрит ролики.

«Я немного удивилась, когда посмотрела видео вместе с ним – дети открывали игрушки, играли в развлекательных центрах, – говорит Оксана. – Некоторые видео были абсолютно ерундовыми, но при этом набирали миллионы просмотров».

Муж рассказал Оксане, что блогеры на YouTube неплохо зарабатывают, и через несколько дней Влад уже гулял в парке «под прицелом» родительской камеры. Семье повезло: всего через месяц один из роликов «выстрелил».

«После того как первое видео попало в “похожие”, подписчики начали добавляться активнее. Появился первый доход, первые бесплатные игрушки для рекламы», – вспоминает Оксана.

Сейчас канал Vlad TV Show занимает девятое место по популярности в Украине, по данным Retailers, и приносит от 3 до 50 тыс. долларов дохода в месяц, если верить Socialblade.

«Для детских каналов все же стоит ориентироваться на нижнюю границу доходной вилки и даже меньше», – комментирует Оксана.

Заработок YouTube-канала зависит от количества просмотров рекламы во время просмотра роликов и от наличия нативной рекламы (когда блогеры лично рекомендуют товары).

«В среднем нам поступает 10 коммерческих запросов в месяц, но мы рекламируем только то, чем сами потом пользуемся», – говорит мама Влада.

Рекламы в детских видеоблогах много. В основном это игрушки и сладости – то, что маленькие зрители смогут попросить у родителей после просмотра. Контент довольно однообразный и состоит из походов в развлекательные центры, распаковок и постановочных роликов на темы вроде противостояния брата и сестры.

«Это настоящий наркотик, – делится мама пятилетней Софии на родительском форуме. – Не знаю, как моя дочка это нашла, я давала ей смотреть только мультики. Теперь ищем способ заблокировать канал Miss Katy, потому что София все время хочет смотреть ее ролики, а потом клянчит такие же игрушки и спрашивает, почему мы не живем в таком доме, как Katy».

Психолог Виталина Устенко советует родителям избегать подобных видеоблогов, потому что они не развивают в детях ничего, кроме желания потреблять. «Во влогах мы не видим развития отношений между людьми (или их аллегорией, как в сказках и мультфильмах), не видим настоящих конфликтных ситуаций, которые формируют представления о добре, зле, красоте, дружбе и прочих важных вещах», – комментирует психолог.

В описании детских каналов обычно заявлено что-то о счастливом детстве. Причем обращение к подписчикам часто оформлено от лица трехлетнего блогера, что выглядит довольно абсурдно. Но даже если дети, демонстрируемые на каналах, и правда счастливы, то маленькие зрители от просмотра испытают только фрустрацию, ведь для такого же счастья им не хватает бесконечного количества игрушек и бесконечных развлечений. Трудно объяснить ребенку, что веселые игры маленьких блогеров – это на самом деле работа, и не всегда приятная.

«Для производства ролика иногда нам хватает пары часов, а бывает, что и трех дней мало, – рассказывает Оксана, мама Влада. – Пока что я со всем справляюсь сама, с некоторыми деталями помогает муж. Было время, когда я чувствовала себя белкой в колесе из-за непрерывного цикла работы, но сейчас мы перестали гнаться за другими, замедлили темп и работаем себе в удовольствие».

В удовольствие работают не все маленькие блогеры. На канале Kids Diana Show новое видео выходит каждые несколько дней, чуть реже обновляется блог брата Дианы – Kids Roma Show. Такие же темпы в семье Miss Katy и Mister Max – производство контента происходит беспрерывно.

По словам бренд-менеджера AIR Network Дмитрия Редько, для некоторых каналов видео монтируют специально нанятые специалисты. Оно и понятно, иначе родители просто не справились бы со своим реалити-шоу. Но герои роликов всегда одни и те же – дети. «Пока Влад был маленьким, он всегда снимался с удовольствием, – вспоминает Оксана. – Каждый день было что-то интересное: новая игрушка, новое место, новое приключение. Сейчас у него появились свои предпочтения, он может устать после садика. Стараемся учитывать его мнение и снимать тогда, когда он этого хочет. Наш график

съемок это позволяет». Видео на канале Vlad TV Show появляется примерно раз в неделю.

«От обилия развлечений и игрушек у детей спустя какое-то время наступает информационное перенасыщение, окружающий мир превращается в шум, – говорит психолог Виталина. – Атрофируется мотивация достигать чего-либо (поскольку и так всё есть), перестаёт вырабатываться гормон удовольствия (потому что постоянно происходит гиперстимуляция), не формируется уважительное отношение к труду и понимание того, как живет и из чего состоит общество».

Участие детей в видеоблогах может быть и полезным для их развития, если не перегибать палку.

«Детям нужно чувствовать, что задачи, которые перед ними стоят – это серьезные, сложные задачи, а не детские игры. Это поддерживает их интерес», – комментирует педагог Кристина Москаленко. «Но тут нужно знать меру и понимать, когда производство контента идет на пользу ребенку, а когда ребенок идет на пользу этому производству и становится средством в руках родителей. Если мы говорим только о заработке, то такая деятельность как минимум незаконна», – добавляет Кристина.

«Нет норм труда для детей до 14-ти лет, поскольку детский труд запрещен в принципе, – объясняет юрист Juscutum Семен Астапов. – Если ребенок задействован в съемках не более 24 часов в неделю и не в ночное время, если это не вредит его интересам, здоровью и нормальному развитию – я думаю, это не будет считаться эксплуатацией».

(вгору)

Додаток 6

22.10.2018

Четыре стратегии контент-маркетинга в Instagram для «нефотогеничного» бизнеса

Как продвигаться в Instagram, – самой визуальной соцсети – если продукт «нефотогеничный»? Четыре контент-стратегии, проверенные опытом известных компаний (AIN.UA).

Соцсети – must have для продвижения бизнеса. Facebook, Instagram и другие площадки – это естественная среда обитания платежеспособной аудитории. И бизнесу важно регулярно попадаться на глаза клиентам, удовлетворяя их потребности в информации.

Но соцсети – это в первую очередь визуальный контент. Продавцы «фотогеничных» товаров (одежды, техники, продуктов питания и т. д.) могут публиковать по 10 фото ежедневно, показывая товар с разных ракурсов. Но предприниматели, продающие услуги или инфопродукт, результаты которых запечатлеть просто невозможно, хватаются за голову: «Что публиковать в соцсетях, чтобы привлечь внимание клиентов?»

Если вас тоже волнует этот вопрос, вооружитесь одной из четырех проверенных стратегий развития «нефотогеничного» бизнеса в Instagram.

Стратегия № 1. Ставка на эмоции

Чтобы конкурировать на рынке соцмедиа, бизнесу важно создавать цепляющие образы, которые вызывают нужные эмоции у целевой аудитории (ЦА) и повышают лояльность к бренду. Покажите, что компания «на одной волне» с клиентами, что у вас одинаковые ценности, восприятие мира.

Подумайте, что важно для ЦА:

- Какие у этих людей ценности?
- Какие проблемы, вопросы, боли, желания?
- Чего хотят: учиться, развлекаться, общаться, делиться мнением и опытом?
- Какой уникальный эмоциональный опыт люди могут получить от использования вашего продукта?

Instagram-страница бренда Mastercard – яркий пример того, как можно создать эмоциональную связь с аудиторией за счет визуального контента. Аккаунт Mastercard – это клуб по интересам. Он на 70 % состоит из фотографий и роликов с различных мероприятий компании: гольф, бейсбол, семейные пикники, тренинги для детей, концерты и т. д. Mastercard разделяет ценности клиентов и всячески это демонстрирует.

Еще пример эмоциональной контент-стратегии – компания FedEx, которая показывает, что доставка посылок – увлекательное путешествие. В профиле полно креативных фотографий грузовиков и самолетов, которые доставляют клиентам их мечты. Это выглядит чертовски мило.

Стратегия № 2. Бекстейдж и рабочие процессы компании

Людям всегда было интересно заглянуть за кулисы. Тайное влечет.

Поэтому покажите процесс создания продукта, рабочий день команды, производства. Вещи, которые вам кажутся обычными, могут поразить или, как минимум, заинтересовать потенциального клиента.

Показывайте лица сотрудников – это очеловечивает бизнес. Позвольте заглянуть в рабочие процессы – это докажет, что вы честны, открыты и уверены в качестве продукта.

Такой стратегии придерживается компания IBM, чей Instagram похож на научно-фантастический сериал о сверхтехнологиях.

Здесь можно заглянуть в серверную и дата-центр IBM, посмотреть на самый мощный суперкомпьютер, понаблюдать за работой программистов. Страница IBM − это сплошное закулисье и рай для техномана.

Стратегия № 3. Жизнь корпоративного персонажа

С эмоциями пока туго, а закулисье показывать категорически нельзя? На помощь придет корпоративный персонаж.

Если вы продаете услуги или обучение, тренинги, курсы, то есть продукт не имеет материальной оболочки, проработайте визуализацию. Создайте корпоративного персонажа, который будет общаться с ЦА, представлять ваш бизнес, транслировать ценности.

Так сделал сервис рассылок MailChimp. Обезьянка-почтальон по имени Фредди – центральная фигура страницы компании.

Второй вариант – создать не просто героя, а яркий и узнаваемый стиль визуального контента. Это блог о продвижении в Instagram, в котором абсолютно все картинки выполнены в стиле комиксов.

Стратегия № 4. Личный бренд

Instagram – площадка для людей, и они хотят наблюдать за личностями, а не за бизнес-страницами. Поэтому фотографии и видео с интересным человеком – то, что нужно «невизуальному» бизнесу.

Личный бренд – сильное конкурентное преимущество. Через личность собственника и полезный контент вы показываете экспертность и создаете доверительные отношения с ЦА.

Страница Кира Уланова, маркетинг-ревизора и основателя digital-холдинга Marketing Gamers − пример построения личного бренда в Instagram. За 3 года Кир провел 1687 маркетинг-ревизий и помог заработать своим клиентам более $5000000 прибыли с помощью автоворонок продаж.

У себя на странице Кир делится рекомендациями по маркетингу и развитию бизнеса, событиями из личной жизни, наблюдениями и мыслями.

Важно помнить, что в развитии личного бренда нужно ставить интересы и пользу для клиента во главу угла.

Кстати, Кир запустил медиапроект «Marketing Ревизор», где проводит ревизии опыта успешных предпринимателей, а также бизнес-проекты, которые уперлись в финансовый потолок. Находит места, где бизнес проседает, а затем показывает, что конкретно нужно сделать, чтобы достичь желаемых результатов. А у себя в Instagram Кир публикует самые интересные моменты этих маркетинг-ревизий.

Подведем итог. Использовать Instagram для продвижения бизнеса нужно, независимо от того, продаете вы роскошные свадебные платья, которые можно фотографировать по сто раз, или же оказываете услуги психолога, ремонтируете сантехнику или занимаетесь производством кирпичей. Просто используйте одну из 4-х контент-стратегий, описанных выше, и ваш «невизуальный» бизнес станет заметным и привлекательным для аудитории.

(вгору)

Додаток 7

23.10.2018

Михаил Сапитон

Украинский Telegram-канал впервые набрал более 100000 подписчиков. Как ему это удалось

Украинский Telegram-канал о путешествиях и скидках «Ветер дует» набрал более 100000 читателей, сообщила в Facebook основательница проекта Алена Деньга (AIN.UA).

В комментарии AIN.UA она рассказала, что успеху канала поспособствовали несколько обстоятельств:

«Я до сих пор считаю, что одним из самых важных факторов успеха было то, что канал появился 2,5 года назад, когда Telegram мало кто пользовался. Условно, я успела запрыгнуть в поезд под названием “Каналы”, когда он еще стоял на перроне. Это помогло получить упоминания в СМИ, которые включали канал в подборки.

Второй фактор – безвиз. В день, когда украинцы получили возможность путешествовать только по биометрическому паспорту, аудитория канала увеличилась вдвое. Его порекомендовала Женя Гаврилко у себя в Instagram. У нее десятки тысяч подписчиков — но мы не знакомы, Женя просто читает канал и решила поделиться. Также я написала пост, который хорошо разлетелся – около 1500 лайков и 500 репостов. Это был второй поезд, в который я успела запрыгнуть.

Далее была рутина, работа над каналом, эксперименты с рекламой, публичные лекции, постоянные посты в личных аккаунтах соцсетей, пара публичных интервью, поддержка друзей. Все это так или иначе помогало продвижению канала. Также я заметила, что люди сами часто рекомендуют канал, рассказывают о том, что купили дешевые билеты и отправились в путешествие. Это самое крутое!»

В январе 2018 года на «Ветер дует» были подписаны около 24500 человек. Наибольший скачок количества подписчиков в «Ветер дует» пришелся на период с мая по июнь, когда аудитория проекта выросла на 16 000 человек.

На момент написания материала, количество читателей достигло 100207. Это лучший результат в украинском сегменте Telegram. По данным сервиса Tgstat, на втором месте по популярности находится канал Lowcost UA (84400), на третьем – канал издания «Ракета» (62600). Также «Ветер дует» лидирует по показателю охвата постов – каждая публикация, в среднем, набирает более 42000 просмотров.

По словам Алены Деньги, она не ставит конкретных задач по привлечению аудитории:

«Мне была интересна эта круглая цифра – 100000. Просто хотелось и все. Планов по количеству подписчиков нет, поскольку для меня более показательны вовлеченность людей, читаемость материалов и отклик».

Сейчас команда проекта «Ветер дует» состоит из нескольких человек – они занимаются развитием одноименного сайта. Telegram-канал основательница ведет самостоятельно. По ее словам, делегировать такие полномочия непросто:

«Пока каналом занимаюсь я единолично. Была неуспешная попытка делегировать эту задачу. Причина в том, что канал “Ветер дует” – это уже более сложный механизм из публикаций, понимания трендов путешествий, рекламы и ручного контента. Должна быть высокая степень понимания не только инструментов Telegram, но и тематики. А еще ответственности. Я была бы рада найти человека, которому можно доверить часть работы».

У «Ветер дует» открыты данные о стоимости рекламных материалов. Публикация на канале стоит от 1650 до 4000 грн в зависимости от условий, времени, тематики и продолжительности размещения. Сообщается, что обычно места раскуплены на 1,5-2 недели вперед.

В мировом рейтинге популярности лидерство удерживают иранские каналы – аудитория крупнейшего из них превышает 13,5 млн подписчиков.

(вгору)

Додаток 8

18.10.2018

Ирина Фоменко

Ученые нашли связь между времяпровождением в сети и ожирением у детей

Новое исследование показало, что маленькие дети, которые проводят много времени в Интернете или смотрят коммерческое телевидение, чаще страдают ожирением и просят своих родителей купить им нездоровую пищу. Об этом сообщает The Guardian (InternetUA).

Согласно исследованиям Cancer Research UK, дети, которые пользуются Интернетом более получаса в день, почти в два раза чаще просят родителей купить шоколад, чипсы и сладкие напитки, чем те, кто сидит в сети меньше.

Дети старшей школы, которые проводят более трех часов в день в Интернете, чаще тратят свои карманные деньги на вредные продукты, чем те, кто находится в сети менее 30 минут.

Любители Интернета на 79 % чаще имеют избыточный вес или ожирение, а те, кто проводит в сети от получаса до трех часов, почти в 53 % случаев страдают избыточным весом.

Доклад исследовательского центра CRUK и ученых из Ливерпульского университета основан на опросе почти 2 500 детей в возрасте от 7 до 11 лет и их родителей относительно зрительских привычек и приема пищи.

«Родители хорошо знакомы с выпрашиванием детьми сладостей и газированных напитков в супермаркете. Наши исследования показывают, что такое поведение может быть связано с количеством времени, которое дети проводят перед экраном, и, как следствие, увеличением числа привлекательных рекламных объявлений этих продуктов», – заявила ведущий исследователь Ливерпульского университета Эмма Бойланд.

В целом, дети, как правило, бывают онлайн в течение 16 часов в неделю и тратят 22 часа еженедельно на просмотр телевизора. Дети, проводящие время за коммерческим ТВ, чаще просят родителей купить рекламируемую еду.

«Дети видят до 9 объявлений нежелательных продуктов питания в течение одного 30-минутного эпизода своих любимых телешоу, поэтому неудивительно, что это заставляет их приставать, покупать и есть больше нездоровой пищи», – прокомментировала Кэролайн Черни из Obesity Health Alliance.

Недавно министры опубликовали планы по борьбе с ожирением среди детей, запретив акцию «купи один, второй в подарок» в отношении сладостей и рекламу нездоровой пищи до 9 вечера.

(вгору)

Додаток 9

19.10.2018

Чем соцсети пугают крупнейших технологических лидеров мира

В последнее время социальные сети все чаще мелькают в устрашающих заголовках. То Facebook сталкивается с очередной волной фейковых новостей, то вдруг выясняется, что Google Plus повинен в утечке пользовательских данных. Да и ученые постоянно твердят, что соцсети вгоняют пользователей в депрессию (IGate).

Казалось бы, люди, находящиеся на гребне волны технологического прогресса, должны более оптимистично смотреть на интернет-технологии. Но и они относятся к социальным сетям с опаской. Недавно крупнейшие технологические лидеры мира, Илон Маск, Джефф Безос и основатель Instagram Кевин Систром высказали свои опасения касательно соцсетей. И у каждого из них свой страх.

Илон Маск боится зависти и депрессии

В прошлом месяце Илон Маск пришел на интервью к телеведущему Джо Рогану. Там он много говорил о своих компаниях Tesla и SpaceX, а также покурил марихуану в прямом эфире, чем особенно порадовал армию своих фанатов. Но также Маск сделал пару интересных замечаний о том, как социальные сети могут наносить ущерб психическому здоровью пользователей.

«Одна из проблем социальных сетей заключается в том, что люди стараются показывать свою жизнь лучшей, чем она есть на самом деле. Люди размещают фотографии моментов, когда они были особенно счастливы, редактируют эти фотографии, чтоб казаться лучше. Даже если они ничего не изменяют, то просто выбирают фото, сделанные с лучшим освещением и под лучшим углом», – сказал Маск.

Это кажется вполне очевидным. В конце концов, никто не станет размещать в соцсети откровенно неудачное фото. Но в результате такой избирательности создается виртуальная картина жизни, которая выглядит в разы лучше реального положения дел. Как следствие – несправедливые сравнения и зависть других пользователей.

Когда человек просматривает ленту и видит там исключительно красивых и счастливых людей, он сравнивает себя с ними и решает, что его жизнь намного хуже. «На самом деле люди, которых вы принимаете за счастливчиков, могут быть очень несчастными», – говорит Маск.

Джефф Безос опасается информационных пузырей

Джефф Безос, глава Amazon и Blue Origin, обеспокоен тем, что социальные сети могут образовывать информационные пузыри вокруг

пользователей. По его словам, интернет в его современном виде – это своеобразная «машина по производству предвзятого подтверждения».

Когда пользователь что-либо лайкает в соцсети, он формирует область своих интересов. После этого алгоритм начинает выдавать ему только те материалы, которые могут ему понравиться. Таким образом, раз за разом пользователь получает подтверждение своей точки зрения и попросту не замечает существования альтернативных мнений.

Человеческий мозг по своей биологической природе ненавидит противоречия. Из-за этого он пытается повсюду находить подтверждение привычной точке зрения. Но теперь еще и «умные» алгоритмы социальных сетей усугубляют этот эффект, избирательно отсеивая часть информации.

Безос считает, что людьми, которые не видит общей картины, становится легко манипулировать. Он переживает, что благодаря эффекту информационного пузыря соцсети могут стать инструментом в руках нечестных политиков и диктаторских режимов.

Кевин Систром переживает за приватность

В конце сентября основатель Instagram Кевин Систром объявил о своем уходе из Facebook. И на той же конференции он выступил с критикой компании. По его словам, Facebook не дает пользователям достаточного контроля над показом информации. Компания сама определяет, какую информацию должны видеть пользователи.

Систром с этим не согласен. Он считает, что у пользователей должно быть больше инструментов для тонкой настройки. К примеру, люди должны иметь возможность закрывать комментарии под своими фото, выборочно блокировать определенные слова или группы. Но проблема в том, что благодаря таким настройкам пользователи могут меньше времени проводить в соцсети. И это, кажется, не вполне устраивает Марка Цукерберга.

(вгору)

Додаток 10

25.10.2018

В Instagram появился аккаунт о суровой правде любовных отношений

Анонимный блогер устал от идеальных романтических фотографий в Instagram и создал аккаунт, который назвал «Честная пара» (InternetUA).

На странице пользователь собирает снимки со счастливыми возлюбленными, однако делает к ним максимально реалистичные подписи. Получается жестокая правда жизни, в которой Роза мечтает расстаться с Джеком, а ваша вторая половинка уже задумывается о новом партнере.

Психологи и социологи всего мира не устают говорить о том, насколько далеки идеальные образы пользователей в социальных сетях от реальной жизни. Хотя многие блогеры с удовольствием разоблачают секреты

безупречных фото, в Instagram все еще достаточно юзеров, которые своими снимками вызывают у подписчиков комплекс неполноценности.

Развеять мифы о прекрасной жизни людей из инстаграма решил анонимный пользователь, который в 2017 году создал аккаунт Honest Couple, или «Честная пара». Чтобы понять, насколько название сообщества соответствует его контенту, нужно просто взглянуть на любую из публикаций.

Идея создать страницу «о жестокой правде жизни» пришла к нему после просмотра фотографий других пользователей. Менее чем за год у аккаунта появилось свыше 37 тыс. подписчиков, а все благодаря особому подходу автора к постам.

«Люди в интернете хотят показать другим свою якобы идеальную жизнь, но очевидно, что это ложь. В какой-то степени это даже вредно. Почему люди не могут быть честными? Этот обман заставляет многих людей чувствовать себя неполноценными из-за того, что в жизни они не так счастливы, как эти обманщики». При этом не последнюю роль в формировании контента «Честной пары» играет личное отношение администратора к интернет-признаниям в любви.

«Я действительно устал от людей, которые пишут в социальных сетях, как сильно они любят своих близких, а затем расстаются через неделю».

(вгору)

Додаток 11

29.10.2018
Ирина Фоменко
Как выявить у себя зависимость от смартфона

Еженедельно Apple отправляет пользователям iPhone стимулирующий отчет о «цифровом оздоровлении», в котором говорится, сколько часов они потратили на смартфоны. Об этом сообщает The Telegraph (InternetUA).

Как утверждают в Apple, отчет направлен на уменьшение зависимости от технологий. Фиксируется каждое уведомление, звонок и сообщение, а также точное количество минут, потраченных на различные приложения.

Главный минус доклада о «цифровом оздоровлении» – на iPhone нет предупреждающего уведомления, например, что 18 часов в Twitter – слишком много, или что разблокировка телефона каждые три минуты разрушает жизнь.

Стоит отметить, что в отчете данные сравниваются исключительно с предыдущими показателями, а не с информацией других пользователей: «вы потратили на этой неделе на 26 % меньше времени на смартфон, чем на прошлой».

Согласно исследованию, опубликованному в сентябре Оттавским университетом, у детей, использующих смартфоны более двух часов в день, более плохая память, языковые навыки и внимание. У взрослых зависимость от гаджетов вызывает депрессию и беспокойство.

Тем не менее, некоторые эксперты убеждены, что длительное времяпровождение за смартфоном может принести больше пользы, чем вреда. Так, в докладе Лондонской школы экономики Parenting for a Digital Future утверждается, что смартфоны могут помочь объединить семьи, например, через мессенджеры для родителей и детей.

«Мы обнаружили, что родительская озабоченность по поводу ограничения использования смартфонов была намного выше, чем обеспокоенность по поводу контента, с которым их дети сталкиваются», – объясняет соавтор отчета Алисия Блум-Росс. – «Я бы посоветовала родителям задуматься: они учатся? Это помогает им проявлять интерес к внешнему миру?».

В Великобритании руководящие принципы, установленные Национальным институтом по вопросам здравоохранения и медицинской помощи (NICE), предполагают, что у детей любого возраста должно быть не более двух часов в неделю на смартфоны. В США же считают, что такого времени не должно быть вообще.

По словам преподавателя клинической психологии в Университете Суррея Боба Паттона, пользователей должны настораживать мысли о смартфонной зависимости. Отчеты Apple могут стать предупреждением для тех, кто постоянно использует телефон без всякой причины.

«Длительное использование гаджетов может иметь серьезные последствия. Нужно помнить, что наличие технологий еще не означает, что мы должны использовать их постоянно», – объясняет Паттон.

Отсутствие «вдумчивого» использования технологий, особенно среди подростков, является одним из самых тревожных аспектов смартфонной зависимости. Недавнее исследование показало, что подростки сидят до 12 часов в Интернете ежедневно, не тратя на контент более нескольких секунд.

«Разница в том, используете ли вы смартфон вдумчиво или бессознательно», – прокомментировал психолог и директор по исследованиям в Оксфордском институте Интернета Эндрю Пшибылски.

(вгору)

Додаток 12

19.10.2018

Российские интернет-тролли пытались повлиять на американцев с помощью Brexit

Опубликованный социальной сетью Twitter архив контента «российских фейковых аккаунтов» показал, что в день голосования по вопросу Brexit в Великобритании «интернет-троллями» велась кампания по продвижению идеи выхода страны из Европейского Союза (ЕС) – к такому выводу пришли аналитики из Atlantic Council, пишет The Times (InternetUA).

Таким образом «интернет-тролли», которых связывают с Россией, продвигали кампанию по дезинформации с помощью хэштега

#ReasonsToLeaveEU (#ПричиныПокинутьЕС). Как заявили в аналитическом центре, его использовали 1,1 тыс. раз в день референдума по Brexit в 2016 году. При этом эксперт Atlantic Council Бен Ниммо отмечает «скоординированность действий» фейковых аккаунтов, направленную на то, чтобы вывести данный хэштег в тренды социальной сети.

17 октября социальная сеть Twitter опубликовала архив, включающий более девяти миллионов сообщений, опубликованных с 3 841 фейковых аккаунта в период с 2013 по 2018 год. Фейковые аккаунты связывают с российским «Агентством интернет-исследований». Помимо этого, соцсеть опубликовала около миллиона сообщений, принадлежащих 770 фейковым аккаунтам, которых связывают с Ираном.

Как пишет Times, «российская кампания по дезинформации» включала «исламофобские» посты после террористических атак в Великобритании.

В Atlantic Council объясняют, что российская кампания по дезинформации по основным британским событиям была направления на «поляризацию» жителей США. Например, аккаунты, выдававшие себя за правых после терактов на Лондонском мосту и стадионе «Манчестер-арена» «демонизировали мусульман», а продвигающие идеи Brexit – атаковали глобалистов, пишет газета.

Как отмечает The Guardian со ссылкой на исследовательскую лабораторию в области цифровой судебной экспертизы в Вашингтоне (DFRLab), обе кампании – и российская, и иранская – были направлены на американцев, однако их «оппортунистический» характер показал, что и другие попали под удар. В вашингтонской аналитической лаборатории отметили, что «российские интернет-тролли» использовали техники подлинной онлайн-активности, что впоследствии затруднило способность отличить их от настоящих аккаунтов.

Однако кампания по дезинформации не ограничивалась твиттером, пишет The Guardian. Ранее газета провела расследование, которое показало, что российские фейковые аккаунты были процитированы в около 100 новостях британских СМИ «неизвестными авторами», которые использовали их в качестве примера общественного мнения или юмора, говорится в материале.

(вгору)

Додаток 13

20.10.2018

В США обнаружили новую лазейку для российских троллей

Россия использовала американские стартапы, чтобы вмешиваться в американские выборы. Об этом пишет агентство Bloomberg со ссылкой на данные активности учетных записей в Twitter (InternetUA).

Социальная сеть выложила архив публикаций более 3,8 тысячи аккаунтов, которые, по мнению компании, являются ботами российского Агентства интернет-исследований, которое в США считают замешанным во

вмешательстве в выборы. Основная часть контента в этом архиве – гиперссылки, перенаправляющие пользователей на другие платформы. Они уже либо удалены, либо уже не существовали.

Выяснилось, что сотни этих ботов использовали для автоматизации распространения информации и расширения аудитории такие американские стартапы, как IFTTT., RoundTeam. и Dlvr.it.

В частности, компанией IFTTT из Сан-Франциско активно использовали в конце 2017-го – начале 2018 года. Он помогает людям подключаться к различным приложениям и автоматически публиковать контент на нескольких сервисах. Как считает старший научный сотрудник Digital Forensic Research Lab Бен Ниммо, она стала популярна у русских ботов из-за возможности скрыть происхождение информации. Он подчеркнул, что иранские боты пользовались той же услугой.

По данным Crunchbase, компания IFTTT поддерживает таких инвесторов, как Salesforce Ventures, IBM Ventures и Andreessen Horowitz. Стартап RoundTeam автоматизирует задачи поиска и совместного использования твитов. Компания Dlvr.it автоматически публикует контент на разных страницах социальных сетей и используется в основном издателями.

19 октября стало известно, что Минюст готовит обвинение в адрес Елены Хусьяновой, которая якобы пыталась повлиять на будущие выборы в Конгресс США. Женщина работала главным бухгалтером проекта «Лахта», который СМИ связывают с именем бизнесмена Евгения Пригожина (его считают причастным к вмешательству в американские выборы).

Вашингтон многократно обвинял Москву в попытке повлиять на президентские выборы. По данным спецслужб США, российская разведка использовала две хакерские группировки – Fancy Bear и Cozy Bear – для взлома серверов Демократической партии, а также влияла на мнение общественности с помощью ботов российского Агентства интернет-исследований. Москва отвергает обвинения в причастности ко взломам.

(вгору)

Додаток 14

21.10.2018

Ирина Фоменко

Опубликованы темники российских оперативных дезинформаторов для Facebook

Покойный сенатор Джон Маккейн был «старым чудаком». Спикер палаты представителей Пол Д. Райан – «никем». И расследование возможного сговора между кампанией президента Трампа и Россией – это «охота на ведьм» во главе с «марионеткой», пишет The Wall Street Journal (InternetUA).

У русских дезинформационных оперативников была стратегия, как выдавать себя за политически активных американцев, поскольку они тайно пытались манипулировать избирателями онлайн – подстрекательскими

высказываниями, ложными замечаниями и призывом к политической предвзятости. Ту же тактику, отточенную в ходе президентских выборов 2016 года, используют в преддверии промежуточных выборов 2018.

Таковы выводы из подробного 38-страничного обвинительного заключения Министерства юстиции, опубликованного 19 октября. Официально обвиняют 44-летнюю жительницу Петербурга Елену Хусяйнову, которая якобы играла ключевую роль в операциях, направленных на обман избирателей.

Обвинительное заключение опубликовали в политически важный момент. Примерно за две недели до промежуточных выборов примеры российских сообщений в социальных сетях подчеркивают тщательное изучение Кремлем американской политики и возможности использовать существующие подразделения для развязывания конфликта. Вопросы, упомянутые в этих сообщениях, широко обсуждаются, что позволяет российским оперативникам вмешиваться.

По словам республиканца Скотта Дженнингса, россияне, по-видимому, определили ключевые термины и фразы из американской политики, благодаря которым их публикации вписывались в социальные медиа. «Они выяснили, что использование определенных ключевых слов создаст впечатление, что учетная запись реальна. Некоторые из публикаций выглядят очень правдиво», – заявил Дженнингс.

Для каждого сегмента политического спектра – и для каждого крупного чиновника – у российских оперативников, казалось, был план. Согласно обвинительному заключению, россияне в декабре 2017 года опубликовали твит, призывающий читателей пожертвовать деньги оппозиции: сенатору Клэр МакКаскилл и Тэмми Болдуин. Так, россияне настраивали либеральных и консервативных избирателей против выборов 6 ноября и расследования Роберта С. Мюллера III о политическом вмешательстве России в 2016 году.

Они рекомендовали не ссылаться на статьи Breitbart News Network при отправке сообщений либеральным группам и избегать «публикаций в Washington Post или Buzzfeed» в материалах для консерваторов. Они также сообщили, что в сообществах лесбиянки, гомосексуалисты, бисексуалы и транссексуалы хорошо реагируют на крупные, красочные фотографии и большой текст, а публикации получают наибольшее количество трафика ночью, потому что именно тогда пользователи ЛГБТ «активны» в Интернете. Люди других рас в этих же сообществах реагируют на «#whiteprivilege».

Во время выборов в 2016 году на страницах Facebook и Instagram для 140 млн американцев появились фотографии, публикации и другой контент Агентства интернет-исследований, что стало причиной изменений в платформе социального гиганта. Facebook пришлось нанять тысячи сотрудников для мониторинга контента. Ранее Twitter уведомил людей о российской дезинформации: компания опубликовала имена профилей, привязанных к Агентству, и миллионы их твитов.

Тем не менее, в обвинительном акте подчеркивается, что угроза российского вмешательства все еще существует: например, в августе 2017 года

дезинформаторы стремились исказить ситуацию с Маккейном – когда он критиковал план Трампа о вводе границы между США и Мексики – называя его «чудаковатым стариком, которому уже давно пора в дом престарелых». Российские дезинформаторы использовали еще одну новость августа 2017 года: одна и та же группа Facebook цитировала новостной сайт в своих атаках на Мюллера, называя его «марионеткой» и «политизированной фигурой».

В рамках усилий Агентства интернет-исследований в поддержании беспорядков в Интернете, многочисленные учетные записи в Facebook и Twitter часто принимали противоположные стороны одной проблемы. Например, в 2017 году профиль Secured Borders в Facebook поставил под сомнение расследование Мюллера, назвав его «политически мотивированным». Примерно в феврале 2018 года аккаунт @JemiSHaaaZzz в Твиттере занял противоположную позицию, отвечая на сообщение о более раннем обвинительном заключении Министерства юстиции касательно 13 российских граждан, имеющих связи с Агентством.

В обвинительном заключении также говорится о том, что российские оперативники ввязывались в недавние политические споры, такие как митинг Unite the Right в Шарлоттсвилле в прошлом году и культурную битву за профессиональных футболистов, стоящих на коленях во время национального гимна. Они создали тысячи поддельных профилей в Facebook и Twitter, в некоторых случаях используя общие имена, например, Bertha Malone, а в других – скрываясь за анонимными аккаунтами пользователей, в том числе @imdeplorable201.

В мае 2018 года учетная запись Twitter, связанная с российской кампанией, даже пыталась извлечь выгоду из политически противоречивого вопроса о сетевом нейтралитете, побуждая избирателей «аннулировать» сенатора Теда Круса после его голосования против более жестких положений о телекоммуникационной отрасли.

(вгору)

Додаток 15

28.10.2018

Иранские интернет-тролли используют «методички» Кремля для раздора в соцсетях

Администрация Facebook заблокировала сеть, в которую входили 82 группы, в сообщества и пользователи, выдававшие себя за граждан США и Великобритании. Эти интернет-тролли занимались публикацией мемов, статей и прочего контента политической тематики, касающейся межнациональных отношений, выборов в Конгресс и прочего. В Facebook утверждают, что эта сеть происходила из Ирана, пишет Wired (InternetUA).

При этом в отличие от предыдущей пропагандистской сети из Ирана, заблокированной прошлым летом, ее тематика была сфокусирована не на повестке иранского правительства, а на британской и американской политике.

Как отмечает издание, такой подход очень напоминает интернет-кампанию перед выборами 2016 года в США, в проведении которой обвинили Россию. На момент блокировки у сети было уже более миллиона подписчиков.

«Их целью было создать раздор. Они сеяли несогласие и концентрировались на темах, разделяющих общество», – приводит Wired слова главы отдела кибербезопасности Facebook Натаниэля Глейхера. Глейхер также заявил, что публиковавшиеся сетью материалы были схожи с материалами, использовавшимися в предыдущих подобных акциях.

В августе, Facebook, Twitter и Google заблокировали широкую сеть фальшивых аккаунтов в соцсетях и сайтов, связанных с иранской гостелерадиокомпанией «Голос Исламской республики Иран». Эти аккаунты, выдавая себя за реальных людей, журналистов и СМИ, активно пропагандировали политику Тегерана. Недавно заблокированные сообщества, как сообщает издание, взяли на вооружение иной подход: они притворились сообществами американских либералов и публиковали противоречивые материалы об американской политике, с целью вызвать раздор в обществе. При этом, как информирует Wired, у Facebook пока нет данных о связи сети с иранским правительством.

«Это выглядело, как иранская медиа-кампания, взявшая на вооружение методы проведённых ранее российских кампаний», – заявил Бен Ниммо из вашингтонской лаборатории цифровой криминалистики. Как пишет издание, сотрудники лаборатории также отметили, что позаимствованная у русских стратегия оказалась очень успешной, пусть иногда и имела место быть искусственная накрутка просмотров.

Это не единственная связь между российскими и иранскими медиа-кампаниями, отмечает Wired. В августе, директор лаборатории цифровой криминалистики Джонатан Олбрайт обнаружил, что Facebook-страница «Расширение для музыки», рекламировавшая расширение Chrome, связанное с российским агентством интернет-исследований, имеет в разделе «похожие» иранскую страничку «Британские левые», заблокированную этим летом.

Как отметил Олбрайт, это не могло прозойти случайно, поскольку у двух страничек «нет ничего общего». Facebook пока никак не комментировал данную ситуацию для Wired. Как резюмирует издание, остаётся неясным, был ли это сбой системы, или же это свидетельство более глубокой связи между российскими и иранскими кампаниями в соцсетях.

(вгору)

Додаток 16

19.10.2018

В Facebook создан спецотдел по борьбе с вмешательством в выборы // Компания планирует привлечь к работе в новом отделе более двадцати тысяч сотрудников

Крупнейшая социальная сеть Facebook сформировала в своей структуре новое подразделение – специальный отдел по борьбе с вмешательством в выборы; целью нового отдела будет борьба с распространением ложной информации, сообщает AFP (Зеркало недели. Украина).

Поскольку Facebook устал от обвинений в том, что слишком мало делал для пресечения распространения фейковой информации со стороны России и других стран в период выборов в США в 2016 году, на этот раз в компании создали так называемую «War Room» (военную комнату) – подразделение, которое будет бороться с дезинформацией и попытками повлиять на выборы через социальную сеть.

Главный офис отдела расположился в Калифорнии; в нем собраны эксперты по аналитике и программированию. В дальнейшем к работе отдела хотят привлечь до двадцати тысяч сотрудников.

«Наша задача – выявить... любого, кто пытается манипулировать общественными дебатами», – сказал Натаниэль Глейхер, бывший директор по политике кибербезопасности Белого дома, который теперь возглавляет политику кибербезопасности Facebook.

Так, отдел уже добился кое-какого успеха: согласно данным специалистов, при отслеживании президентских выборов в Бразилии в день голосования было зафиксировано распространение ложного сообщения о якобы изменении даты выборов из-за протестов. Эти сообщения успели удалить до того, как они стали вирусными.

В дальнейшем отдел будет следить за подозрительными аккаунтами во время выборов в США и Бразилии. 28 октября в Бразилии состоится второй тур выборов президента, а на 6 ноября в США назначены промежуточные выборы в Конгресс.

(вгору)

Додаток 17

22.10.2018
Ирина Фоменко
«War Room» от Facebook оказался дешевой маркетинговой уловкой

В ответ на растущую критику со стороны потребителей, граждан и законодателей, Facebook хочет изменить то, как люди воспринимают борьбу социального гиганта с дезинформацией и сопутствующей угрозой выборам, представленной веб-сайтами и приложениями. Об этом сообщает The Fortune (InternetUA).

Facebook пригласил журналистов из ряда изданий (включая The Fortune) посетить конференц-зал в кампусе компании Menlo Park, в котором группа из 20-ти и более сотрудников отвечает за защиту демократии. Стены и столы загромождают видеоэкраны и мониторы компьютеров, за ними работники Facebook ведут борьбу с политически мотивированными кампаниями влияния.

По словам исполнительного директора Facebook Самида Чакрабартиа, присутствие всех в одной комнате, «лицом к лицу», позволяет сотрудникам общаться и принимать быстрые решения. Тем не менее, своих «коллег» Facebook не приглашает, например, Twitter и Reddit, поскольку, как утверждает глава политики кибербезопасности Facebook Натаниэль Глейхер, таким группам лучше сотрудничать «практически, а не физически».

Журналисты The Fortune считают, что «War Room» Facebook является маркетинговой уловкой: конференц-зал напоминает центры кибербезопасности, которые банки и другие компании создают для «замыливания глаз» посетителям. «Это в основном для шоу», – заявил главный сотрудник по информационной безопасности в американском банке Джейсон Уитти.

Следует отметить, что компания пытается решить многие проблемы. «War Room» действительно служит важной цели: сделать закулисные битвы компании более осязаемыми для своих сотрудников, регуляторов и общественности.

Недавно редакционная коллегия Times сообщила, что Facebook полагается на новостных репортеров как на армию неофициальных, неоплачиваемых, сторонних модераторов контента, помогающую избавиться от спамеров, троллей и пропагандистов. «Такие компании, как Facebook, имеют все инструменты и несут полную ответственность за поиск той же информации, что и журналисты, – и все же, очевидно, они этого не делают», – писали в Times.

(вгору)

Додаток 18

17.10.2018

Хакери, пов’язані з РФ, готували кібернапад на компанії України та Польщі

Хакери провадили дії проти трьох компаній, що працюють в енергетиці та транспортній галузі в Україні та Польщі і, можливо, планували новий руйнівний кібернапад. Про це заявила компанія з безпеки програмного забезпечення, повідомляє Reuters (InternetUA).

Словацька фірма ESET заявила, що хакери діяли з 2015 до середини 2018 років і вказала, що дії вчиняла та сама група, яку Британія звинуватила у зв’язках з російською військовою розвідкою.

Компанія ESET раніше брала участь в розслідуванні кібернападів на Україну.

Група, яка раніше проводила напади на енергетичну галузь в Україні з використанням вірусу BlackEnergy, тепер розробила нову зловмисну програму GreyEnergy.

«Важливо те, що вони все ще активні, – сказав в коментарі Reuters дослідник ESET Роберт Ліповські. – Це означає, що діє дуже небезпечний і наполегливий «фактор загрози».

Росія заявляла, що доказів на підкріплення звинувачень проти ГРУ немає.

На початку було розіслано електронну пошту зі шкідливими Інтернет-посиланнями, або документами, або було проведено зараження серверів приєднаних до Інтернету. Це дозволило GreyEnergy скласти схему мереж своїх жертв і зібрати конфіденційну інформацію, таку як паролі, йдеться в заяві ESET.

Потім, команда намагалась отримати доступ до критично важливих елементів систем, включаючи комп'ютери, які контролюють промисловий процес. «Я розумію, що це була стадія розвідки і шпигунства, яка може призвести до кіберсаботажу», – заявив Ліповські.

Кіберполіція України підтвердила напади на дві українські компанії, однак, не навела деталей. Польські посадовці не відповіли на запити про коментар.

Бен Рід, менеджер компанії FireEye з питань шпигунства заявив, що група Sandworm, ймовірно, є відповідальною.

«Діяльність подібна до дій групи, яку ми відслідковуємо як Sandworm», – заявив він. «Діяльність, яку, як ми вважаємо, проводить Sandworm, була визначена міністерством юстиції США як ГРУ», – наголосив Рід.

(вгору)

Додаток 19

17.10.2018

У Києві викрили зловмисників, які продавали персональні дані в Telegram

Продаж здійснювався у закритому Telegram-каналі. Серед послуг, які надавали зловмисники, перевірка особи по інформаційним базам українських банків, надання інформації про рух коштів за рахунками та вся кредитна історія. Наразі вирішується питання щодо оголошення підозри усім учасникам злочинної групи (InternetUA).

Працівники Київського управління Департаменту кіберполіції Національної поліції України викрили діяльність трьох киян, які організували схему збуту інформації з обмеженим доступом та персональних даних громадян, за допомогою всесвітньої мережі Інтернет.

Працівники кіберполіції встановили: до складу групи входило троє осіб. Вони пропонували свої послуги із встановлення даних громадян та надання відносно них персональної інформації. Пропозиції щодо своїх послуг зловмисники розміщували на закритому Telegram-каналі, через який також відбувалося і отримання замовлень від клієнтів.

Інформацію стосовно громадян зловмисники отримували з баз даних однієї із кредитних спілок та бази Державної фіскальної служби України (ДФС). При цьому доступ до цих баз надавали співробітники цих організацій, які входили до складу злочинної групи.

Оплата послуг клієнтом відбувалася через довірену особу. В подальшому гроші потрапляли на підконтрольні учасникам групи банківські рахунки.

Поліцейські зафіксували декілька випадків, коли учасники злочинної групи у такий спосіб продали інформацію щодо громадян. Ця інформація містила паспортні дані, номери мобільних телефонів, банківські рахунки громадян, відомості щодо родичів, близьких осіб та майна, що перебуває у власності.

Працівники кіберполіції провели декілька санкціонованих обшуків за місцем проживання зловмисників. Відтак, поліцейські вилучили комп'ютерну техніку, мобільні телефони, сім картки та банківські картки, які зловмисники використовували у своїй злочинній діяльності. Також, під час обшуків було вилучено декілька флеш-накопичувачів з витягами персональних даних відносно громадян України. Наразі вилучену техніку направлено на комп'ютерно-технічну експертизу.

Кримінальне провадження розпочато за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України. У подальшому буде вирішено питання щодо оголошення підозри учасникам злочинної групи.

(вгору)

Додаток 20

17.10.2018

Acronis открывает в Болгарии центр разработок в сфере киберзащиты, блокчейна, ИИ

Для разработки передовых технологий компания Acronis развивает сеть научно-исследовательских центров, расположенных в странах Азии, Европы и Америки. Глобальное присутствие позволяет непрерывно совершенствовать технологии в сфере киберзащиты, искусственного интеллекта и блокчейна (Компьютерное Обозрение).

Новый европейский офис и научно-исследовательского центр открылся в Софии (Болгария). Этот стратегически важный пункт не только поможет быть ближе к европейским заказчикам, но и дает возможность привлекать технических специалистов из Европы.

В начале года руководство Acronis приняло решение в течение следующих трех лет инвестировать 50 млн долл. в создание 300 новых рабочих мест для специалистов в сфере высоких технологий в своем новом офисе в Софии, который в первую очередь нацелен на технологии киберзащиты, поддержку работы центров обработки данных и разработку соответствующих продуктов и услуг.

Как и остальные Центры киберзащиты компании Acronis, расположенные по всему миру, болгарский офис будет осуществлять мониторинг различных сред защиты данных и получать жизненно важную информацию о новейших угрозах.

Команда, работающая в Софии, в настоящий момент состоит из 30 инженеров, но уже до конца года она вырастет до 50 сотрудников. В рамках запуска центра разработок Acronis в Болгарии развернуто сотрудничество с местными университетами и общественными организациями, а также планируются совместные проекты в сфере образования. Компания уже работает с Софийским университетом и расширяет партнерство с научными и образовательными организациями.

(вгору)

Додаток 21

17.10.2018
Пользователи продолжают слушать нелегальную музыку

По данным Международной федерации звукозаписывающей индустрии (IFPI), 38 % потребителей музыкального контента по-прежнему получают его незаконными путями вроде торрент-треккеров (InternetUA).

Зачастую музыка копируется прямо в процессе потокового вещания.

В отчёте указывается, что потоковыми трансляциями пользуются 86 % слушателей, при этом 50 % предпочитают именно такой способ при отсутствии других. Смартфонами для этого пользуются 75 % слушателей.

Четверо из десяти пользователей получают контент из нелегальных источников. Копирование потокового вещания юридически не является нарушением. Формально это может быть сделано для прослушивания музыки для локального устройства, что выводит пиратов из-под удара. В IFPI отметили, что потоковое вещание не решает проблему пиратства в целом, хотя редкие тактически победы и присутствуют.

В 35 % пользователей, по данным IFPI, не хотят платить за подписку, поскольку всё, что им надо, есть бесплатно. А попытки требовать от поисковых систем удалять ссылки на нелегальный контент зачастую не приносят результата.

Google «бомбардируют» требованиями удалить ссылки, но есть поисковики вроде DuckDuckGo, которые игнорируют подобные воззвания.

В федерации остаётся надеяться, что ситуация изменится к лучшему, однако учитывая развитие децентрализованных систем, это вызывает сомнения. По сути, главной проблемой для многих являются завышенные цены на контент, что и побуждает многих людей искать бесплатные или хотя бы более дешёвые альтернативы.

(вгору)

Додаток 22

17.10.2018
Владимир Кондрашов
Документы Энергоатома были доступны российским террористам

В открытом доступе опять оказались документы НАЭК «Энергоатом». На этот раз – касающиеся работы Южно-Украинской АЭС (InternetUA).

Утечку данных обнаружил эксперт по кибербезопасности, ведущий разработчик компании «IT Лаборатория» Александр Галущенко.

Эксперт на своей странице в Facebook опубликовал скриншоты некоторых из обнаруженных им документов и попросил представителей Энергоатома связаться с ним.

Среди опубликованных документов – «Рабочая программа вихретокового контроля теплообменных труб парогенераторов энергоблока №2 ОП ЮУ АЭС в период ППР-2018» с подписью главного инженера ОП ЮУ АЭС Николая Феофентова, «Картограмма контроля ТОП 2ПГ2 в период ППР2018» и Акт по результатам контроля коррозионного состояния внутренних поверхностей парогенераторов и другие документы.

Как сообщил Александр Галущенко нашему журналисту, представители Энергоатома вышли с ним на связь около 12.40 дня. На данный момент утечка закрыта, но не силами НАЭК – связь оборвалась.

Документы «светили в сеть» с 10 до 11 утра.

В пресс-службе НАЭК «Энергоатом» нашему журналисту отказались предоставить комментарий относительно сложившейся ситуации.

Это уже не первая утечка документации НАЭК «Энергоатом». Напомним, в декабре прошлого года хактивист, известный в сети под ником Дмитрий Орлов в рамках акции #fuckresponsibledisclosure, инициированной Украинским киберальянсом, сообщил об утечке данных Запорожской АЭС. Он обнаружил в открытом доступе внутреннюю документацию ЗАЭС, среди которой такие документы, как Акт технического состояния объекта ядерной безопасности, служебные записки, Анализ герметичности оболочек ТВЭЛ ТВС и прочее. 19 марта этого года полиция открыла уголовное производство по факту несанкционированного вмешательства в работу компьютерных сетей ОП «Запорожская АЭС» ГП НАЭК «Энергоатом». Тогда причастными к утечке данных в местном отделении СБУ назвали трех сотрудников отдела ядерной безопасности Запорожской АЭС, среди которых и его руководитель. По информации нашего издания, расследование продолжается.

Отметим, что до привлечения правоохранителей к ситуации, в Энергоатоме пытались полностью отрицать факт утечки данных Запорожской АЭС и заявляли о её «несерьезности».

(вгору)

Додаток 23

17.10.2018

IBM будет использовать ИИ для решения проблем кибербезопасности

В последнее время хакеры и другие киберпреступники изобретают все новые и новые средства для похищения данных или нанесения вреда

компаниям и частным лицам. И порой для разработки средств защиты стандартных методов уже недостаточно, но обезопасить киберпространство решилась крупная компания IBM, применив для этого искусственный интеллект (Украинский телекоммуникационный портал).

Согласно анализу, проведенному IBM, только в рамках самой компании используется в среднем 80 решений в сфере кибербезопасности от 40 различных поставщиков, что делает систему при всей своей глобальности довольно уязвимой. Для решения этого вопроса компания разработала платформу IBM Security Connect. Как заявила пресс-служба компании, «IBM Security Connect – это первая облачная платформа безопасности, основанная на открытых технологиях, управляемая ИИ».

Участники платформы смогут свободно использовать ИИ для своих целей. У них будет даже доступ к суперкомпьютеру IBM Watson. Искусственный интеллект платформы включает в себя нейронные сети и глубокое машинное обучение.

«Поскольку платформа является открытой, ее участники легко смогут создавать уникальные решения и небольшие сервисы для внедрения в свои проекты. При этом за безопасностью даже очень маленьких сервисов будет следить огромная система».

По словам руководителя проекта IBM Security Connect Джейсона Корбина, уже на старте программы к ней присоединилось 16 компаний, которые взяли на себя обязательство открывать потоки данных или разработки приложений.

«IBM Security Connect построен таким образом, что если приложение интегрировано с платформой, оно может интегрироваться со всеми другими приложениями, доступными на ней».

Одной из основных технологий, которая лежит в основе платформы, является проект STIX-Shifter (Structured Threat Information eXpression) – протокол, используемый для безопасного обмена информацией об угрозах. Он обеспечивает согласованность передачи данных во всех продуктах IBM Security Connect для глубокой аналитики. В сочетании с огромными массивами данных, которые предоставляют один общий API, программа может использовать информацию из любого источника. Ну и что касается интеграции в систему искусственного инителлекта. По словам господина Корбина, абсолютно не важно, по какой системе устроена нейронная сеть. Все они будут совместимы между собой.

«Одной из проблем, связанных с ИИ, является то, что организации могут быть изолированы в рамках своей платформы. Мы хотим сделать ИИ более открытыми. Мы берем ваш ИИ, независимо от того, где он был построен, как он был построен и где он работает, и мы позволяем ему контактировать с другими ИИ, включая Watson. Таким образом функциональность каждого отдельного ИИ возрастает в несколько раз».

(вгору)

Додаток 24

18.10.2018
Как Интернет следит за детьми

Отец двоих малышей выяснил, как поисковики собирают личные данные пользователей (InternetUA).

Джастин Льюис, британец, отец двух малышей в возрасте 4 и 6 лет, решил уточнить – какие сведения собирают сайты в интернете по запросам, поступающим от детей, не достигших 13 лет? Его потрясло, что посещение всего лишь пяти страниц вызвало удивительный каскад из 1871 запросов фоновых данных.

Платформы управления данными

Конфиденциальность интернет-пользователей подрывается, прежде всего, так называемыми платформами управления данными (DMPs), которые объединяют все детали и всю информацию, которые мы оставляем после каждого посещения Интернета. Это похоже на наши справочные карточки в библиотеке: DMPs готов представить полные профили о каждом из нас – что угодно, от прозвищ домашних животных до почтовых кодов. Интернет-гиганты, такие как Google, разработали своё собственное программное обеспечение для миграции данных пользователя. Это позволяет эффективно идентифицировать вас на любом устройстве, которое вы используете, в любом месте, и «преследовать» вас с целевой рекламой, настроенной настолько точно, что от этого становится жутко. Особенно страшно, когда атакам со стороны Интернета подвергаются дети.

Предмет исследования

Что ваш мальчик или девочка вытворяют в сети? Возможно, они слишком маленькие, и поэтому, крайне редко, вы позволяете им запускать YouTube на своем iPad или посмотреть на мобильном телефоне «Свинку Пеппу» – совсем недолго, всего пару минут, пока вы выгружаете покупки, запускаете посудомоечную или стиральную машину. Или, может быть, они немного старше. Не совсем подростки, но уже в том возрасте, когда увлечены строительством в онлайн-игре Minecraft. Или, возможно, им 13 лет, и они только что открыли свой первый аккаунт в Instagram и делятся фотографиями с друзьями. Где же подвох?

Все эти сайты утверждают, что развлекают, а не эксплуатируют детей. В конце концов, сбор любой информации, которая может считаться идентифицирующей личность ребенка в возрасте до 13 лет (до 16 в некоторых странах), в настоящее время является незаконным – это нарушение нового закона ЕС о защите данных детей, который вступил в силу в мае 2018 года. Большинство популярных сайтов теоретически устанавливают возрастные ограничения. Google, которому принадлежит YouTube, пишет, что «для входа на YouTube у вас должен быть аккаунт Google, соответствующий минимальным возрастным требованиям» – для Великобритании это возраст 13 лет. Но при этом пользователю не нужно регистрироваться. И когда ваши дети

настраиваются на Peppa Pig, Minecraft, Instagram или Twitch, сколько же на самом деле информации о них собирается?

«Чтобы узнать это, я решил провести простой эксперимент, чтобы как родителю двух мальчиков, четырёх и шести лет, получить чёткое представление о том, что делают основные технические платформы во время стандартных цифровых путешествий юных пользователей интернета – от малышей до подростков, – пишет Джастин Льюис на страницах The Telegraph. – Так я оказался в зале заседаний в центре Лондона вместе с Диланом Коллинзом и Джошуа Велем, генеральным директором и техническим директором SuperAwesome – британской компании, которая производит цифровые технологии «kid safe» (защита детей).

Запрос на Свинку Пеппу

Веле познакомил Льюиса с «Чарльзом» – частью программного обеспечения, которое способно отслеживать поток данных между устройствами в интернете, прежде чем перейти на YouTube на смартфоне. «Чарльз» показал запрос, сделанный его устройством, последующее подключение к YouTube и передачу видеоданных обратно. При этом выяснилось, что данные были переданы таким образом, чтобы Google могла точно идентифицировать пользователя ещё до того, как он вошёл в YouTube. Задействован при этом был, прежде всего, IP-адрес – уникальный идентификационный код любого устройства в интернете. Данные о том, как вы получаете доступ к интернету – какой браузер, какая операционная система и так далее – часто могут быть настолько детальными, что легко идентифицирует вас.

В эксперименте Льюиса, пока отправлялся запрос на Свинку Пеппу, множество других запросов втихую делались в фоновом режиме.

«Я вижу, что разные идентификаторы были отправлены, – говорит Веле, указывая на цифры, отображаемые “Чарльзом”. – Я вижу DSID – это метод Google для кросс-таргетинга на устройстве, который идентифицирует меня вне зависимости от того, захожу ли я со своего компьютера или использую свой телефон или что-то ещё. Этот метод способен соотнести все эти данные».

Пока Веле излагал всё это, запросы данных были сделаны более чем в 20 других доменах за пределами YouTube, что стало сигналом для поставщиков услуг онлайн-рекламы. Затем Веле последовательно посетил Minecraft, Instagram и Twitch; всего трое мужчин просмотрели пять сайтов за 54 минуты. Но эти пять просмотров вызвали удивительный каскад из 1871 (!) фоновых запросов – более 34 в минуту – на рекламные серверы, DMPs и так далее.

Защитить несовершеннолетних

Cookies, маяки, пинги, трекеры: существует целый лексикон, чтобы описать способы интернет-компаний сбора данных о пользователях и использовать их, чтобы заработать деньги. В сети созданы профили не только взрослых, но и детей, хотя наблюдения за тем, как они перемещаются с сайта на сайт, являются незаконными. Впрочем, большинство из специалистов по безопасности считают, что принятый не так давно в ЕС закон о защите данных несовершеннолетних не имеет смысла, поскольку не исполняется.

Макс Шремс, успешный адвокат, говорит, что существует целая «культура неисполнения». Речь идёт о штрафах, которые выписывают интернет-гигантам за интернет-слежку за детьми. «Индустрия поняла, что может делать всё, что хочет», – говорит Шремс. Адвокат подал жалобы на действия таких компаний в Австрии, Франции, Бельгии и Германии. Цель жалоб состоит в том, чтобы составить иск против интернет-компаний за незаконный сбор данных и оштрафовать их. В настоящее время, говорит Шремс, «наказание за нарушение правил парковки более строгие, чем в случае нарушения вашего основного права – на неприкосновенность частной жизни».

Родителей, «отпускающих» своих детей в Интернет, должна насторожить активность рекламщиков: бюджеты на цифровую рекламу, ориентированную на детей, растут на 25 % в год, и, по прогнозам, в следующем году составят почти £1 млрд. И даже если будет создан особый, специальный Интернет для детей, где сведения о них не станут собирать ради получения прибыли, то почему эти дети, вырастая, должны терпеть эксплуатацию приватных сведений? Конечно, это часть обмена информацией, ставшей основополагающим моментом для роста интернета – так называемые, личные данные для бесплатных услуг.

«Этот обмен данными соткал всю ткань интернета, – говорит Коллинз. – Но это была сделка с дьяволом, и теперь мы пожинаем её плоды».

(вгору)

Додаток 25

18.10.2018

В даркнете продаются данные миллионов избирателей США

Всего за несколько недель до промежуточных выборов в Конгресс США данные избирателей из 19 штатов оказались выставленными на продажу в даркнете (InternetUA).

Специалисты из Anomali Labs и Intel 471 обнаружили на одном из популярных киберпреступных форумов около 35 млн записей, содержащих сведения об избирателях, в том числе персонально идентифицируемую информацию и историю голосований. Обнаруженные исследователями БД являются первым выявленным случаем утечки данных избирателей, зарегистрированных для участия в выборах в Конгресс 2018 года, назначенных на 6 ноября.

Записи содержат полные имена, телефонные номера, сведения о местожительстве, историю голосований и другие данные. Исследователи проанализировали образцы данных и подтвердили их подлинность. По их словам, персональная информация избирателей в сочетании с данными из других утечек может использоваться злоумышленниками для вмешательства в избирательный процесс или осуществления крупномасштабной кражи личностей.

Поскольку продавцы обещают еженедельное пополнение своего товара и имеют хорошую репутацию на киберпреступных форумах, исследователи предположили, что у них может быть постоянный доступ к базам данных избирателей или контакты с государственными чиновниками в каждом штате.

Название подпольного форума специалисты Anomali Labs и Intel 471 не приводят. Стоимость БД варьируется в зависимости от штата и составляет от $150 до $12500. По мнению исследователей, на стоимость может влиять количество данных в той или иной базе.

Спустя всего несколько часов после выставления товара на продажу один из авторитетных киберпреступников организовал кампанию по сбору средств на покупку всех БД. Киберпреступник пообещал, что после покупки сделает БД доступными бесплатно для всех зарегистрированных участников форума, а самыми первыми доступ получат те, кто пожертвовал средства.

(вгору)

Додаток 26

18.10.2018

Ирина Фоменко

Apple запускает новый веб-сайт с персональными данными пользователей

Apple запускает новый поисковой портал, где пользователи смогут найти свои данные, которыми владеет компания. Об этом сообщает CNBC (InternetUA).

Сайт конфиденциальности тестировали в мае в Европейском союзе, как раз во время принятия Общего регламента по защите данных (GDPR). Собранная информация может включать в себя такие данные, как записи в календаре, фотографии, напоминания, документы, закладки веб-сайтов, покупки в App Store или историю ремонта устройств.

На сегодняшний день Apple стремится быть компанией, зарабатывающей на продаже аппаратных средств, а не на целевой рекламе, основанной на данных своих клиентов.

«По правде говоря, мы могли бы заработать огромное количество средств, если бы наш клиент был нашим продуктом. Но мы решили не делать этого», – заявлял в марте Тим Кук.

Главный исполнительный директор Facebook Марк Цукерберг отметил, что Кук «говорил бойко и много», и, по его мнению, бизнес-модель Facebook – это «единственная рациональная модель, которая может способствовать созданию этого сервиса».

В дополнение к поисковому порталу Apple запустила несколько улучшенных инициатив по обеспечению конфиденциальности с помощью своего веб-сайта и новой операционной системы iOS 12 для iPhone и iPad.

Компания рекламирует свою технологию Intelligent Tracking Prevention, чтобы приостановить сбор данных для таргетированной рекламы.

В Apple также внесли изменения, которые стандартизируют определенные настройки для предотвращения так называемых «цифровых отпечатков устройств» или «цифровых отпечатков браузеров» – способом, которым индивидуальное устройство человека может быть идентифицировано с использованием его уникальных настроек и предпочтений, таких как специальные шрифты, даже если клиент заблокировал другие формы отслеживания данных.

Как заявили в компании, планируется внедрить сквозное шифрование для видеочата Group FaceTime, где количество участников в конференции может достигать до 32 человек. Шифрование также защитит новую функцию Screentime.

Как и в случае с запуском поискового портала ЕС в мае, веб-сайт является одним из способов, с помощью которого Apple пытается продолжить активный подход к регулированию конфиденциальности.

(вгору)

Додаток 27

19.10.2018

В конце года 62 % всех сайтов в интернете лишатся обновлений безопасности

По данным W3Techs, на сегодняшний день около 78,9 % всех сайтов в интернете работают на PHP. Однако 31 декабря нынешнего года официально прекращается выпуск обновлений безопасности для PHP 5.6.x, что ознаменует полное прекращение поддержки всех версий устаревшей ветки PHP 5.x (InternetUA).

В начале 2019 года из-за прекращения поддержки около 62 % сайтов, до сих пор работающих на версиях PHP 5.x, перестанут получать обновления безопасности, а значит, сотни миллионов ресурсов окажутся под серьезной угрозой. Если после Нового года киберпреступники обнаружат в PHP уязвимость, огромное число сайтов и их пользователей подвергнутся большому риску.

По словам директора по разработкам компании Paragon Initiative Enterprise Скотта Арцишевски (Scott Arciszewski), возможность эксплуатации уязвимостей в неподдерживаемых версиях представляет «огромную проблему для экосистемы PHP».

«Многие не могут вот так просто взять и отказаться от PHP 5 в 2019 году. Это решение (команды PHP – ред.) является необдуманным», – сообщил Арцишевски в интервью изданию ZDNet.

По мнению эксперта, серьезные, широко эксплуатируемые уязвимости в PHP 5.6 наверняка затронут и более новые версии. «PHP 7.2 будет регулярно получать бесплатные патчи от команды PHP; PHP 5.6 получит патч, только если вы платите за продолжающуюся поддержку производителю вашей ОС», – отметил Арцишевски.

Сообществу PHP уже давно было известно о планируемом прекращении поддержки. Когда весной 2017 года 5.6 стала самой популярной версией PHP, разработчики решили повременить с прекращением поддержки и продлить ее до конца 2018 года.

Тем не менее, поголовного перехода на ветку 7.x не произошло. Только системы управления контентом (CMS) постепенно стали модифицировать минимальные требования и предупреждать пользователей о необходимости перехода на более современную хостинговую среду. Из трех крупнейших CMS (WordPress, Joomla и Drupal) только Drupal указала PHP 7 в минимальных обязательных требованиях, хотя ветка PHP 7.0.x устарела еще 3 декабря 2017 года. В минимальных требованиях Joomla до сих пор указана версия PHP 5.3, а WordPress – PHP 5.2.

(вгору)

Додаток 28

19.10.2018

10 типів даних, які збирає про вас браузер // Цю інформацію ви видаєте навіть тоді, коли заходите на безпечні сайти

Існують різні типи даних, збору яких не можуть перешкодити навіть VPN-сервіси (InternetUA).

Які дані може збирати браузер

1. Начинка пристрою і програмне забезпечення

Браузер знає, які плагіни на нього встановлені і яка у вас операційна система. Що стосується заліза, то програма збирає дані про центральний процесор, відеокарту і акумулятор.

2. Інформація про з'єднання

У браузера є деякі дані про ваше підключення до інтернету. Сюди входять IP-адреса і швидкість завантаження файлів.

3. Місцезнаходження

Той чи інший сайт може досить точно визначити вашу геолокацію, навіть якщо ви не надали йому доступ до GPS-координат. Для цього використовується Geolocation API від Google.

З цим можна боротися за допомогою проксі-серверів. Існує маса безкоштовних варіантів.

4. Історія переглядів

Найбільш очевидний варіант даних, які збирає браузер, – історія відвідувань. Звичайно, її можна очистити, але навіть так повної гарантії безпеки немає. Наприклад, в середині цього року стало відомо, що Google в будь-якому випадку зберігає певну інформацію про перегляди з Chrome.

5. Руху миші

Браузер може розповісти навіть те, як ви перенесли курсор миші. Щоб подивитися, як це працює, можете скористатися сайтом ClickClickClick.

6. Орієнтація пристрою

Майже всі сучасні смартфони оснащені гіроскопом. Він використовується в фітнес-додатках та інших подібних сервісах.

Ваш браузер бачить, чи є в пристрої гіроскоп і компас, яка орієнтація встановлена в даний момент – горизонтальна або вертикальна. Також в списку присутні і деякі інші технічні подробиці.

7. Використовувані соціальні мережі

Інформація про те, в які соціальні мережі ви увійшли, теж зберігається. Браузер уміє зіставляти ці дані з іншими, щоб рекламодавці знали максимум про ваших інтересах.

8. Шрифти і мову

Додаток знає, які шрифти встановлені на комп'ютері. Те ж стосується мови, яка використовується в операційній системі.

9. Дані про зображення

Коли ви завантажуєте в Мережу фотографію або ще якусь картинку, браузер сканує метадані файлу. Вони можуть включати розташування, дозвіл зображення, технічні подробиці файлу і навіть модель камери, на яку був зроблений знімок.

10. Технічна інформація

Браузер збирає і масу інших, більш специфічних даних. Це може бути інформація про наявність або відсутність сенсорного екрану, розмір дисплея і багато іншого.

(вгору)

Додаток 29

21.10.2018

В Стэнфорде создают лабораторию для борьбы с негативными последствиями технологий

Исследовательский центр возглавит Алекс Стеймос. Он покинул Facebook из-за несогласия с тем, как компания реагирует на скандал с российским вмешательством в американские выборы. Расследование киберпреступлений – одно из главных направлений работы лаборатории (InternetUA).

Лучшим умам Кремниевой долины и Вашингтона нужно объединиться, чтобы разрешить проблему киберугроз, уверен Алекс Стеймос. Он выступил в Стэнфорде с лекцией «Битва за душу интернета», которая уже выложена на YouTube.

Стеймос работал главным сотрудником по вопросам информационной безопасности в Facebook, но после своего увольнения в августе исчез из поля зрения, отмечает Washington Post. Теперь выяснилось, что он как приглашенный преподаватель будет работать в Stanford Internet Observatory – лаборатории, которая займется проблемами негативного влияния технологий на общество.

«Кремниевая долина основана оптимистами. Но они никогда, никогда не говорят об обратной стороне медали. А правда в том, что мир – это достаточно мрачное место… и если вы разработаете технологию, то она обязательно будет использована со злым умыслом. И нам неплохо было бы это признать», – отмечает преподаватель Стэнфорда.

Как эксперт по безопасности, Стеймос занимался в Facebook проблемой вмешательства Кремля в американские выборы. Стеймос уверен, что демократическим странам нужно выработать план действий в случае нападения в стиле «взлом и утечка».

«Это фундаментальная проблема открытого общества, – говорит эксперт. – Вы не можете предотвратить такие взломы и утечки, но нужно уметь их остановить».

Киберугрозы – одно из направлений для исследования в Stanford Internet Observatory. Там также планируют объединить усилия компаний, которые сейчас поодиночке представляют легкую мишень для преступников. Эксперт по безопасности Кевин Мандиа уверен, что за любой крупной кибератакой стоят геополитические интересы.

(вгору)

Додаток 30

23.10.2018

Миллионы людей пользуются функцией «Не отслеживать» в браузере. Но она не работает

Миллионы людей пользуются настройками конфиденциальности в своем браузере – в частности, кнопкой «Не отслеживать», которая передает сайту требование не собирать данные о пользователе. Согласно исследованию Forrester Research, четверть взрослых американцев используют эту функцию. Однако она практически не работает (InternetUA).

Функцию «Не отслеживать» впервые представили десять лет назад. Она должна была стать мерой по защите прав потребителей в сети, чтобы помочь им освободиться от навязчивой рекламы и сбора данных. Однако исследователям удалось выяснить, что только несколько сайтов придерживаются запретов, среди них – Pinterest и Medium. Pinterest не использует данные за пределами сайта для таргетинга и не отслеживает местоположение, а Medium не отправляет информацию третьим лицам.

Компании Yahoo и Twitter при введении функции заявили, что будут придерживаться договоренностей с пользователем, однако позже отказались от этого. Самые популярные сайты в интернете, от Google и Facebook до Pornhub и xHamster, никогда не придерживались функции «Не отслеживать». Facebook же продолжает собирать данные даже при включенном «Не отслеживать», но отмечает, что «предоставляет пользователям несколько способов контролировать, как компания использует данные для рекламы».

При этом браузер Chrome от Google периодически предлагает отключить функцию, причем Google и так не придерживается ее. В компании отмечают, что пользователи могут контролировать свои данные самостоятельно и отказаться от персонализированной рекламы в настройках аккаунта. Там же можно регулировать интересы, на которые ориентируется робот при показе рекламы.

«Это во многих отношениях неудачный эксперимент, – отметил Джонатан Майер, доцент компьютерных наук в Принстонском университете. – Возникает вопрос, пора ли объявить о неудаче, двигаться дальше и вывести эту функцию из веб-браузеров».

(вгору)

Додаток 31

24.10.2018

Bloomberg: додатки продовжують шпигувати навіть після їхнього видалення

Деякі провайдери послуг кажуть, що такі інструменти стеження призначені для визначення реакції користувачів на оновлення додатків та інші зміни (Techtoday).

Навіть якщо ви видалили додаток зі свого смартфона, це не означає, що він припинив шпигувати за вами. Нові системи трекерів дозволяють розробникам продовжувати відстежувати користувачів та подавати їм таргетовану рекламу. Це стосується власників як iOS, так і Android.

Серед компаній, які пропонують деінсталяційні трекери, є Adjust, AppsFlyer, MoEngage, Localytics та CleverTap. Серед їхніх клієнтів – мобільні оператори та інтернет-компанії, такі як T-Mobile US, Spotify Technology, Yelp, Bloomberg Businessweek.

Деякі провайдери послуг кажуть, що такі інструменти стеження призначені для визначення реакції користувачів на оновлення додатків та інші зміни. Директор Localytics Джад МакКолган каже, що він не знає, щоб цю технологію використовували для показу таргетованої реклами колишнім користувачам додатків. Віце-президент MoEngage Ерен Маедж каже, що в інтересах розробників додатків не використовувати трекери для стеження за користувачами, які видалили їхню розробку.

Деінсталяційні трекери використовують один із головних елементів операційних систем Apple та Google – пуш-повідомлення. Розробники програм завжди мали можливість використовувати так звані «тихі пуш-повідомлення» для регулярного стеження за своїми додатками без турбування користувача. Подібні пуш-повідомлення використовуються для оновлення вхідних повідомлень, стрічки новин тощо, поки додаток працює у фоновому режимі.

Якщо додаток не відгукується на пуш-повідомлення розробника, його помічають як видалений. Деінсталяційні трекери додають цю інформацію в уже

наявний файл з унікальним рекламним ідентифікатором для даного користувача.

Деінсталяційні трекери можуть бути і корисним інструментом. Їх можна використовувати для виправлення багів та вдосконалення додатків без необхідності запускати опитування чи використовувати інші набридливі інструменти.

(вгору)

Додаток 32

23.10.2018

Гендиректор Youtube закликає авторів контенту бойкотувати нове законодавство ЄС про авторське право // Сьюзан Войчіцкі вважає, що зокрема стаття 13 перекриє доступ невеликих авторів контенту до платформ Youtube, Facebook, Twitter та Google

Генеральний директор Youtube Сьюзан Войчіцкі попереджає виробників відеоконтенту про загрозу суперечливого законодавства про авторське право в ЄС і закликає їх «негайно вжити заходів» та протестувати проти нових правил публікації відео та дописів у соціальних мережах. Про це повідомляє CNBC (mind).

«Це законодавство становить загрозу для вашого існування та вашої здатності ділитись своїм голосом із світом», – підкреслила вона.

Войчіцкі говорила про статтю 13 нової директиви ЄС про авторське право, яка була прийнята на початку вересня. Вона змушує технологічні платформи відповідати за контент, захищений авторським правом. По суті, це значить, що гігантські платформи, які покладаються на контент, створений користувачами, включно з Youtube, Facebook, Twitter та Google, є відповідальними за те, щоб користувачі не ділились матеріалами, захищеними авторськими правами. Наразі платформи не є фінансово відповідальними за порушення, хоча вони і змушені видаляти такий контент на вимогу.

Критики стверджують, що стаття 13 не дозволить користувачам ділитись навіть мемами в мережах.

Прихильники законодавства вважають, що воно є необхідним для захисту справедливої оплати для творців контенту. Крім того, на їх думку, великі технічні платформи надто довго «обходили» відповідальність за порушення авторських прав.

Генеральний директор Youtube написала у своєму блозі, що прийняття відповідальності за весь контент на платформі зробить розміщення контенту від невеликих творців контенту надто ризикованим.

Очікується, що остаточна версія нового законодавства ЄС буде публікована наступного року.

«… стаття 13 несе загрозу для тисяч робочих місць, європейських авторів контенту, підприємств і усіх інших. Ця пропозиція може змусити платформи, такі як Youtube, дозволяти лише контент від невеликої кількості великих

компаній. Було б надто ризиковано для платформ розміщувати контент від більш дрібних авторів контенту, тому що тепер платформи нестимуть відповідальність за цей контент», – написала вона та додала, що оскільки процес може бути завершено до кінця року, важливо говорити про це зараз.

(вгору)

Додаток 33

23.10.2018
SIM-карта Tor-only для полной анонимности в сети

Один из британских провайдеров начал бета-тестирование SIM-карты, которая блокирует весь мобильный трафик, кроме трафика через Tor. Сервис может пригодиться абонентам, которые остро нуждаются в соблюдении полной конфиденциальности, ради которой готовы поступаться скоростью доступа (Portaltele).

Поборники анонимности в сети уже давно освоили браузер Tor для обхода блокировок или просто, чтобы не оставлять следов при просмотре сайтов. Действительно, зачем раскрывать свои данные, если можно сохранить их в тайне. Проблема в том, что решение предназначено для активности в браузере, но некоторые приложения все равно собирают информацию о пользователе.

Один из британских провайдеров интернет-услуг увидел в этом привлекательную коммерческую нишу и создал SIM-карту, которая блокирует любой трафик, направленный не через Tor. В отличие от существующих решений, например, десктопного приложения Tor Browser Bundle или Orbot для Android, SIM-карта гарантировано обеспечит полную анонимность.

«Ключевой момент состоит в том, что она самоотключающаяся: если у вас нет Tor, тогда ничто не может попасть в интернет», – Гарет Ллевелин, основатель Brass Horn Communications

Некоммерческий провайдер Brass Horn ранее начал предлагать услугу Tor-only, которая обеспечивает анонимность на провайдерском уровне. Это был ответ на недавние изменения в британском законодательстве, закреплявшие нормы о массовом надзоре за клиентами. Новая SIM-карта позволяет воплотить эту же идею для мобильных устройств.

Это требует некоторой настройки: пользователям необходимо создать новое имя точки доступа на своем смартфоне, чтобы он мог подключаться к новой сети. При этом на самом устройстве должно быть установлено и запущено приложение Orbot. В настоящее время сервис работает только в Великобритании (Гарет Ллевелин предоставил изданию Motherboard одну из таких SIM-карт для подтверждения работоспособности сервиса).

По мнению Натана Фрейтаса из The Guardian Project (Orbot), использование SIM-карты Tor-only подходит определенной категории пользователей, которые хотят замаскировать свой трафик. Это может создать неудобства при использовании некоторых приложений, которые считают

подозрительными пользователей, работающих через Tor, например, Twitter. Но решение вполне жизнеспособно: «Если Facebook может продавать SIM-карты, которые подключаются только к их утвержденным сайтам с нулевым рейтингом, то почему бы не использовать альтернативу, ориентированную на обеспечение конфиденциальности через Tor?… К сожалению, это обеспечит только уверенность в анонимности данных через мобильное подключение, но не через WiFi».

(вгору)

Додаток 34

23.10.2018

Шахраї крадуть особисті дані з ProZorro для отримання мікрокредитів

Співзасновник українського стартапу DroneUA Валерій Яковенко розповів, що опинився серед постраждалих, від імені яких нібито були взяті кредити у фінансовій компанії Moneyveo (InternetUA).

«Я став жертвою шахраїв. І таких, як я, за даними СБУ, понад 1000 осіб. Ба більше, так втрапити може кожен. Інтернет-сайт Moneyveo.UA видав кредит третім особам, які оформили договір на моє ім’я. Про це я дізнався випадково, відкривши схожий на рекламний лист місячної давності», – повідомляє «Фінансовий клуб».

За його словами, інформація, на підставі якої були видані фіктивні кредити, була отримана на ресурсі Prozorro.

«Договір відкритий за документами, розміщеними на сайті Prozorro. Таких, як я, багато. Більшість потерпілих – підприємці, які працюють на платформі державних закупівель, керівники фірм і відповідальні особи, які зобов’язані розміщувати скани своїх паспортів у відкритому доступі», – зазначив Яковенко, додавши, що тепер він повинен повернути Moneyveo 9300 грн.

Яковенко припустив, який вигляд має шахрайська схема: «Хтось у відкритому доступі бере персональні дані українців. Далі з цими документами оформляється заявка на отримання кредиту онлайн і важливий момент – як одержувач вказується кредитна карта абсолютно лівої людини. Звірення відповідності імені в документах і власника на карті не виконується. Сума береться невелика – кілька тисяч гривень, але вже через кілька місяців вона збільшується в 2-3 рази, за рахунок драконівських відсотків кешевого кредиту. Сума зростає з кожним місяцем і в певний момент починає бути абсурдною».

Яковенко вже написав заяву в поліцію.

У компанії Moneyveo закликали всіх, на кого були оформлені кредити без їхнього відома, повідомити їм свої дані та контакти.

(вгору)

Додаток 35

23.10.2018

Власти Китая объявили войну анонимности на блокчейн-платформах

Управление по вопросам киберпространства КНР подготовило законопроект, который обяжет пользователей блокчейн-сервисов раскрывать свои реальные имена и номера персональных ID. Провайдерам услуг придется делиться пользовательскими данными с Компартией, а заодно внедрять цензуру (InternetUA).

Криптовалютным компаниям в Китае приходится открывать офисы за рубежом, чтобы сохранить свой бизнес, а трейдеры ищут хитрые способы обойти строгие запреты на операции с криптовалютой, введенные в КНР. Правительство также запрещает проводить ICO и организовывать тематические конференции. Технология распределенного реестра при этом живет параллельной жизнью – правительство открыто ее поддерживает, а местные компании лидируют по количеству патентов. Однако развивать блокчейн-проектам разрешают только под государственным контролем.

Как сообщает South China Morning Post, Управление по вопросам киберпространства КНР подготовило законопроект о регулировании работы компаний, которые предоставляют услуги на блокчейне. Согласно новым правилам, пользователям придется раскрывать свое имя и номер ID при регистрации на сайте или в приложении.

Провайдеров блокчейн-услуг в Китае обяжут хранить пользовательские данные и предоставлять их правительству по первому требованию. Компании также будут самостоятельно цензурировать контент, который публикуется на их площадках.

Предполагается, что правительство решило ужесточить регулирование после публикации анонимного открытого письма на блокчейн-платформе. В нем неизвестные активисты сообщают о случаях сексуальных домогательств в одном из известных китайских вузов.

Авторы письма утверждают, что руководство университета намеренно скрыло детали дела от общественности. Текст прилагается к транзакции на Ethereum, поэтому удалить или переписать его уже нельзя. При этом прочитать публикацию может каждый. Ранее активисты выложили те же материалы на платформах WeChat и Weibo, но цензоры их удалили.

Законопроект оставят на общественном рассмотрении до 2 ноября. Дату его вступления в силу регулятор пока не называет. В случае принятия закона все провайдеры блокчейн-услуг будут проходить регистрацию в Управлении по вопросам киберпространства в течение 10 дней после начала работы.

Если они планируют предоставлять сервисы в сфере образования, медиа или фармацевтики, то им придется получить специальную лицензию перед регистрацией.

В ноябре китайские ИТ-гиганты Tencent и Huawei представят новую блокчейн-платформу FISCO BCOS для бизнеса. Эксперты сравнивают систему

с Hyperledger Fabric на базе Ethereum. Однако разрабатывать и запускать криптовалюты клиенты не смогут, а все данные о транзакциях будут доступны правительству – для этого компании создадут специальные «наблюдательные узлы».

Проект Tencent и Huawei демонстрирует отношение Пекина к технологии распределенного реестра. Китай готов развивать новое направление, о потенциале которого говорит даже председатель КНР Си Цзиньпин, но это развитие должно укладываться в строгие нормативные рамки. К криптовалютам китайские чиновники относятся примерно хуже, поэтому их оборот и даже открытое обсуждение в стране не допускаются. Но это не мешает Центробанку Китая работать над собственным проектом «цифровой фиатной валюты», а государству превращаться в мировую блокчейн-сверхдержаву.

(вгору)

Додаток 36

24.10.2018
Ирина Фоменко
Как выжить в кибератаке

«Есть несколько возможностей ограничить уровень разрушений от кибератак», – заявил адмирал Майкл Роджерс. – «Нужно знать цель злоумышленника, и какой вектор он пытается использовать для ее достижения. Не зацикливайтесь на одном» (InternetUA).

По словам Роджерса, пишет CNBC, во время его пребывания на должности в Агентстве национальной безопасности (NSA), в NSA сосредоточились на финансовом секторе.

«Все дело в доверии. Речь идет о способности поддерживать эти миллионы глобальных транзакций одновременно с идеей о том, что я знаю, у кого сколько средств и какие денежные потоки», – считает Майкл.

Роджерс отметил нападение Северной Кореи на Sony Pictures Entertainment в 2014 году и NotPetya 2017 года в качестве двух атак, непосредственно коснувшихся адмирала. Атака на Sony имела особенно сильные последствия, поскольку президент впервые говорил о кибербезопасности и критиковал государственного преступника.

«Президент США заявил, что произошедшее – дело рук Северной Кореи», – рассказал адмирал. Это, в свою очередь, привело к изменениям в политике, включая санкции против северокорейских граждан и институтов.

Роджерс планирует присоединиться к израильскому аналитическому центру кибербезопасности Team8, который возглавляет его бывший коллега в израильских силах обороны Надав Зафрир. Роджерс и Зафрир сотрудничают с несколькими крупными корпорациями, чтобы инвестировать в фонд, который поможет создать новые компании по кибербезопасности: Wal-Mart, SoftBank, Airbus, Barclays, Munich RE, Moody’s и Nokia.

Зафрир согласился с Роджерсом о значимости нападения на Sony и атаки NotPetya. Эти инциденты привели к «осознанию того, что мы перешли от простой связи к гиперсвязи». «Теперь это деловая проблема. Это то, что может уничтожить любую компанию», – заявил Зафрир.

Упор на устойчивость, отсутствие истории

По словам Зафрира, увеличение числа нападений требует большего внимания к восстановлению от кибератак, а не к попыткам предотвратить их. Представители отделов безопасности нескольких компаний, присоединившихся к партнерству, согласились с тем, что устойчивость к атакам является ключевым фактором.

«Восприимчивость к атакам намного более изменчива, тогда как устойчивость – постоянна», – убежден главный специалист по информационной безопасности Moody's Дерек Вадала.

«Реабилитация также жизненно важна, поскольку сегодняшние кибератаки намного менее предсказуемы, чем исторические катастрофы. В то время как страховщики могут полагаться на 100-летние данные, связанные с погодой, для написания корпоративной политики в отношении ураганов или наводнений, данным о кибератаках только два десятка лет», – заявил член совета директоров Munich RE Торстен Джеворек. – «Даже если вы их возьмете, вспомните, что еще 15 лет назад смартфонов не существовало».

Для борьбы с этой проблемой компании все чаще полагаются на данные, собранные специалистами кибернетической разведки, чтобы помочь заполнить «пробелы в рисках».

Число смарт-устройств – от цифровой одежды до умной «кожи» – в ближайшие годы будет экспоненциально расти. По словам главного технического директора Nokia Bell Labs Маркуса Уэлдона, инженеры Nokia представляют мир, в котором каждый человек имеет до 100 подключенных устройств, а его компания представляет мир «триллионов подключенных девайсов».

(вгору)

Додаток 37

25.10.2018

Владимир Кондрашов

Украинские хакеры украли банковские данные с помощью приложения для знакомств

Украинские полицейские ищут распространителя вредоносного программного обеспечения, позволяющего несанкционированно вмешиваться в работу мобильных Android-устройств для последующего списания денежных средств с банковских счетов и электронных кошельков пораженных смартфонов (InternetUA).

Об этом говорится в определении Королевского районного суда Житомира.

Напомним, ранее мы уже писали о том, что два студента, 24-летний волынянин и 19-летний уроженец Херсонщины, получили условные сроки за разработку мобильного приложения, которое под видом приложения для знакомств «ДругВокруг» получало доступ к банковским счетам пользователей мобильного банкинга и передавало эти данные злоумышленникам.

Студенты разработали и распространяли вредоносное ПО «SexDrugWokrug.apk». Данная программа устанавливается под видом системного процесса как SystemUpdate, а после первого запуска просит предоставить дополнительные полномочия для доступа в систему. Получив полномочия, программа удаляет свою «иконку-ярлык» и переходит в фоновый режим, пытаясь соединиться с сервером и передать персональные сведения «жертвы» и всю ее адресную книгу. Получив данные, программа проверяет наличие установленного «мобильного банкинга» на телефоне «жертвы», отправляя смс-запросы на запрограммированные специальные номера, и, при положительном результате, пытается завладеть денежными средствами потерпевшего.

Несмотря на то, что создатели приложения ещё в марте получили приговоры по 3 года лишения свободы с освобождением от отбывания наказания и испытательным сроком в 2 года и конфискацией орудий преступления, их «дело продолжает жить». В частности, досудебным расследованием установлено, что в период с 9 августа этого года по настоящее время установленное следствием лицо, используя возможности всемирной сети Интернет и путем создания собственных сайтов, распространяет это вредоносное ПО.

Также удалось выяснить, что житель Житомирской области совместно с неустановленными лицами, «создает и распространяет вредоносное программное обеспечение, осуществляющее несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), и приводит к утечке и искажение процесса информации».

– В ходе оперативно-розыскных мероприятий установлено, что подозреваемый вмешивается в работу мобильных терминалов граждан путем модификации программного обеспечения операционной системы «Android» (а именно вредоносное программное обеспечение «SexDrugWokrug.apk»), что определяется как «Троян», «Passwordstealer». В дальнейшем с помощью указанного программного обеспечения появляется возможность осуществлять несанкционированное вмешательство в работу мобильных терминалов на правах суперпользователя «root». Распространение модифицированного программного обеспечения вышеуказанное лицо осуществляет с помощью собственных сайтов, и в дальнейшем получает удаленный доступ к управлению устройствами и проводит несанкционированные операции с платежными системами мгновенных интернет расчетов «WebMoney», «Qiwi», – говорится в определении суда.

(вгору)

26.10.2018

Ирина Фоменко

Миллионы пассажиров пострадали из-за хакерской атаки на авиакомпанию

В Cathay Pacific Airways Ltd сообщили, что хакеры получили личную информацию 9,4 млн клиентов. Это крупнейшее в мире хищение данных авиакомпании, пишет The Star Online (InternetUA).

Акции авиакомпании впервые так сильно упали за 2 года – на 3,8 %, что привело к потере Cathay Pacific Airways Ltd 201 млн долларов рыночной стоимости. Причиной стало раскрытие гонконгским перевозчиком несанкционированного доступа к данным спустя семь месяцев после обнаружения нарушения.

В компании заявили, что безопасность полетов не была скомпрометирована, а каких-либо доказательств неправомерного использования украденных данных – нет.

«Вероятно, это самое большое хищение данных в авиационном секторе», – прокомментировал основатель авиационной консалтинговой фирмы Endau Analytics в Малайзии Шукор Юсоф.

Ранее в этом году British Airways Plc и Delta Air Lines Inc сообщали о краже данных сотни тысяч клиентов. Эти перевозчики увеличили расходы на кибербезопасность после хакерской атаки.

«Неясно, наложат ли на Cathay Pacific государственные штрафы за такое нарушение», – заявил аналитик Bocom International Holdings Co Джеффри Ченг.

«Мы очень сожалеем за любые причиненные неудобства, связанные с кражей данных. Мы пытаемся связаться с пострадавшими пассажирами, используя несколько каналов связи и предоставляя им информацию о действиях, которые они могут предпринять для своей защиты», – сообщается на веб-сайте перевозчика.

Какие данные украли?

– Имена, национальности, даты рождения, номера телефонов, электронная почта, физические адреса, номера паспортов, удостоверения личности и программы часто летающих пассажиров, а также информация о путешествиях.

– 403 номера кредитных карт с истекшим сроком действия.

– 27 номеров кредитных карт без CVV.

– Около 860000 номеров паспортов.

– 245 000 гонконгских ID.

Комиссар по конфиденциальности в Гонконге выразил серьезную обеспокоенность по поводу утечки данных и сообщил, что офис проведет юридическую экспертизу. Специальный веб-сайт infosecurity.cathaypacific.com предоставляет информацию об инциденте и плане действий для пострадавших пассажиров.

Некоторые местные законодатели раскритиковали Cathay Pacific за молчание о нарушении на протяжении семи месяцев. «Многие возмущены, авиакомпания должна была уведомить клиентов в первый же день утечки данных», – заявил член комитета безопасности Legislative Council Лам Чеук-тинг.

В свою очередь, в Cathay Pacific «открыли расследование», привлекли фирму по кибербезопасности и улучшили системы сетевой безопасности.

Взлом British Airways длился две недели в течение августа и сентября, компрометируя данные кредитных карт около 380000 клиентов. В прошлом году было украдено платежную информацию «нескольких сотен тысяч клиентов» Delta в результате кибератаки.

(вгору)

Додаток 39

29.10.2018

В Google Play обнаружено несколько десятков вредоносных банковских приложений

Компания ESET сообщает об обнаружении в официальном магазине Google Play ряда троянских приложений, нацеленных на похищение банковских данных пользователей. Программы маскируются под приложения для очистки и ускорения работы устройств, контроля состояния аккумулятора и даже тематические приложения для просмотра гороскопа (Компьютерное Обозрение).

Специалисты ESET обнаружили 29 таких приложений и сообщили компании Google, которая в свою очередь удалила все выявленные нелегитимные программы из своего магазина. Однако к тому времени фальшивые программы уже успели установить почти 30 тысяч пользователей.

После загрузки троянские программы способны маскироваться под любые приложения на устройствах жертв с помощью специальных фишинговых форм. Кроме этого, вредоносные программы могут перехватывать и перенаправлять текстовые сообщения для обхода двухфакторной аутентификации на основе SMS, перехватывать журналы вызовов, а также загружать и устанавливать другие программы на зараженном устройстве. Приложения загружались от имени различных разработчиков, однако сходство кодов свидетельствует о том, что все программы созданы одной группой злоумышленников.

В отличие от большинства фальшивых банковских приложений, которые распространяются под видом легитимных финансовых программ и отображают фальшивые экраны для входа, обнаруженные приложения обладают сложной функциональностью и расширенными возможностями маскировки на устройствах жертв.

В случае запуска на устройстве жертвы вредоносные приложения отображают ошибку с сообщением об удалении из-за несовместимости с

устройством. После этого поддельные программы пытаются оставаться незаметными как можно дольше или предоставляют обещанную функциональность, например, показ гороскопов. Наиболее важной особенностью этих троянских приложений является то, что они могут маскироваться под любое приложение, установленное на зараженном устройстве. После запуска легитимного приложения троянская программа способна незаметно для пользователя перекрывать его фиктивными формами.

Обнаруженные вредоносные приложения не имеют особых функций для обеспечения устойчивости и защиты от удаления из зараженных устройств, поэтому их можно легко деинсталлировать. Удалить вредоносное приложение можно в разделе Настройки > (Общие) > Диспетчер приложений/Программы. После этого следует проверить банковский счет на наличие подозрительных транзакций и изменить PIN-код банковской карты, а также пароль для входа в Интернет-банкинг.

(вгору)

Додаток 40

29.10.2018

Данные сотрудников украинской «дочки» Сбербанка России утекли в сеть

Имена и адреса электронной почты примерно 420 тыс. сотрудников Сбербанка России попали в сеть. Причину утечки в банке не раскрывают, возможный вариант – «злонамеренные действия одного из сотрудников». Глобальными проблемами Сбербанку подобная утечка данных не грозит, хотя его персонал может стать жертвой массовых фишинговых рассылок. В данном случае важнее репутационный риск: клиенты могут усомниться, что российский госбанк, не сумевший защитить данные собственных сотрудников, хорошо обеспечивает безопасность другой информации (InternetUA).

На днях на специализированном форуме phreaker.pro была выложена база данных сотрудников Сбербанка. База представляет собой текстовый файл размером около 47 мегабайт, в котором содержится свыше 421 тыс. записей с ФИО сотрудников и их логинами для входа в операционную систему, которые в большинстве случаев совпадают с адресами их почты. Также можно узнать, в каком подразделении работает сотрудник. В базе содержатся данные о сотрудниках дочерних организаций Сбербанка, в том числе зарубежных (в частности, в Украине). При этом размер базы превышает численность всех сотрудников группы Сбербанка, которая, согласно данным МСФО по итогам первого полугодия 2018 года, составляла почти 300 тыс. человек. Связано это может быть с тем, что в базе содержатся данные о некоторых (не всех) уволенных сотрудниках. База была выложена неизвестным пользователем. Доступна бесплатно.

Проверка показала, что информация в базе актуальна на 1 августа 2018 года (найти сотрудников, трудоустроенных позже, не удалось). Для проверки

подлинности данных Коммерсант сравнил адреса электронной почты некоторых непубличных менеджеров Сбербанка с собственной базой данных, есть в базе и три e-mail президента банка Германа Грефа. Подлинность базы также подтвердили один из сотрудников Сбербанка и представитель сторонней организации, связанной с информационной безопасностью банка. В пресс-службе Сбербанка также сообщили, что там известно о публикации части адресной книги сотрудников.

Опубликованная информация «не представляет никакой угрозы автоматизированным системам и клиентам», заверили в банке. Эта адресная книга доступна всем сотрудникам Сбербанка и «не несет угрозы раскрытия их персональных данных», подчеркнули в пресс-службе банка. Причины утечки там не раскрыли. По словам источников, наиболее вероятны «злонамеренные действия» кого-то из действующих или бывших сотрудников.

Об утечке данных сотрудников Сбербанка осведомлен также департамент информационной безопасности ЦБ России, и там считают ситуацию «малоприятной». Однако подтвердить эту информацию официально, а также выяснить, принимает ли ЦБ в связи с этим какие-либо меры (например, обращался ли в международную организацию FIRST для разделегирования доменов, на которых база выложена), не удалось: в пресс-службе Банка России не ответили на запрос.

По мнению главы управления информбезопасности ОТП-банка Сергея Чернокозинского, для банка с серьезной информационной защитой подобная утечка данных несет в первую очередь репутационные, а не кибернетические риски. «Данные могут быть использованы для массовой рассылки фишинговых писем, рекламы, спама, но серьезные банки с подобными проблемами умеют справляться», – считает он.

Веб-аналитик «Лаборатории Касперского» Владислав Тушканов отметил, что утечки данных в последнее время происходят достаточно часто, им подвержены и финансовые компании, и здравоохранение, и государственные ведомства. «Для самого предприятия это может быть чревато репутационными потерями, также утечки несут угрозу непосредственно тем, чьи данные попадают в открытый доступ», – полагает господин Тушканов. По словам управляющего партнера экспертной группы Veta Ильи Жарского, клиенты банка могут усомниться, что банк, не сумевший защитить данные собственных сотрудников, хорошо обеспечивает безопасность клиентской информации.

(вгору)

Додаток 41

29.10.2018
Владимир Кондрашов
Информационный «стриптиз» государственных сайтов продолжается

Флешмоб Украинского киберальянса #fuckresponsibledisclousure, начатый около года назад, несмотря официальное окончание, похоже, заканчиваться и

не собирается. Причина тому – наплевательское отношение органов власти к собственной кибербезопасности (InternetUA).

На прошлой неделе мы рассказывали об обнаруженных уязвимостях 5 ресурсов органов власти (если прямой доступ без пароля к административной панели вообще можно считать уязвимостью, а не халатностью), однако поток дыр, судя по всему, неиссякаем: в пятницу, 26 октября, спикер Украинского киберальянса, известный в сети под ником Sean Townsend, опубликовал информацию об уязвимостях ещё 5 государственных ресурсов.

Напомним, украинские хактивисты в рамках флешмоба #fuckresponsibledisclousure уже почти год выявляют и публикуют в открытом доступе сведения об уязвимостях украинских государственных Интернет-ресурсов. Публичная огласка уязвимостей, считают участники флешмоба, позволяет чаще добиваться желаемого результата: государственные органы реагируют на подобную информацию намного оперативней, устраняя бреши и проблемы на своих ресурсах.

Согласно опубликованной информации, на пяти государственных информационных ресурсах обнаружены XSS- и SQl-уязвимости. В список «жертв» флешмоба на этот раз попали сайты «Киевпастранса», Национальной академии государственного управления при Президенте Украины, Фонда государственного имущества (дважды), Прилуцкого городского совета и Управления образования Днепровской районной в Киеве государственной администрации.

На момент написания материала, вечер 28 октября, спустя 48 часов после сообщения об уязвимостях, брешь на сайте «Киевпастранса» уже закрыта, на сайте Фонда государственного имущества всё ещё остаются «дыры», а ресурс Национальной академии государственного управления при Президенте Украины вовсе оказался недоступным.

В комментарии нашему изданию Sean Townsend отмечает: злоумышленники могут использовать эти уязвимости самыми разными способами.

– Обнаруженные уязвимости на сайтах госструктур свидетельствуют о том, что любой профессиональный хакер пройдёт через всю государственную и критическую инфраструктуру, как нож сквозь масло. Зачастую речь идёт даже не об уязвимостях, а о мисконфигурации. Вплоть до того, что пароли администраторов лежат в открытом доступе, или важная информация лежит онлайн, – говорит спикер УКА. – К примеру, Максим Литвинов из ситуационного киберцентра СБУ на конференции по безопасности UISGCON14 рассказывал о взломе сайта ГП "Антонов" (см. слайд ниже – Ред.), если мы посмотрим на слайд внимательно, то увидим, что сайт был взломан через уязвимость типа SQLi (мы часто находили подобные же), и даже вмешательство СБУ не помогло выявить уязвимость и привести сайт в порядок, чем немедленно воспользовались (предположительно российские хакеры). Через три месяца сайт взломали повторно. В данный момент он выключен. Такая же история была с сайтом Донецкой ОВЦА: даже после того как ДП

"УСС" перенастроили полностью всю сеть, уязвимость осталась на месте. И дело не в сайте как таковом, а в том, что с веб-сервера, как правило, доступна внутренняя сеть организации, что само по себе является грубой ошибкой.

Акция #fuckresponsibledisclousure стартовала почти год назад. Спикер УКА говорит, что подсчета количества обнаруженных уязвимостей за это время не вели.

– Не вижу смысла подсчитывать, я был бы доволен, если бы хотя бы в одном случае из нескольких сотен (включая центральные органы власти) увидел бы адекватную реакцию на инцидент безопасности, – говорит Sean Townsend. – Акция закончена, у различных участников была разная мотивация. Дмитрий Орлов хотел, чтобы особо злостные разгильдяи были наказаны, я хотел проверить определённые политические тезисы (которые касаются законодательных, и не только, инициатив в области кибер- и национальной безопасности), я лично не вижу смысла продолжать флешмоб, хотя акция открытая, и все желающие могут присоединиться.

За время с начала акции, отмечает спикер УКА, в отношении государства к безопасности собственных Интернет-ресурсов существенно ничего не поменялось:

– Появилась первая программа баг-баунти в госсекторе (этим занимается BRDO), многочисленным центрам удаётся выявлять какие-то уязвимости, а иногда реальные атаки, но качественно не изменилось ничего. По-прежнему, в случае как «учебной», так и реальной атаки, нет людей, которые способны исправлять ошибки и общаться с публикой. Единственное, что стало полностью очевидным – полная неготовность Украины к кибератакам. Никакой кибербезопасности в Украине нет, и с существующим порядком вещей не будет. Те же выводы разделяют и другие эксперты в области информационной безопасности.

(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.