СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(1.01–16.01)

2018 № 1

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(1.01–16.01)
№ 1

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

2.01.2018
Как отключить рекомендованные публикации в Instagram

Instagram начал показывать в основной ленте пользователей «Рекомендуемое вам». Среди предлагаемого контента появляются фотографии из аккаунтов тех пользователей, которые, по мнению сервиса, должны быть вам интересны. В каждой подборке содержится от 3 до 5 публикаций (InternetUA).

В интервью изданию TechCrunch представитель Instagram заявил, что «рекомендуемое» не мешается в основной ленте, а будет появляться только после просмотра всех новых постов от пользователей, на которых вы подписаны. К этому заявлению пользователи относятся неоднозначно: одним новая функция все равно мешает и «навязанные» посты им не нужны, а другие их вовсе не замечают или даже считают полезными. К счастью для первых, рекомендуемые посты можно отключить.

***

2.01.2018
Facebook попросила прощения за «ошибки» модерации

Количество пользователей Facebook давно превысило 2 млрд и продолжает расти, так что задача контроля за соблюдением правил сообщества становится всё более сложной. Незавидная работа возложена на плечи команды модераторов, насчитывающей 7500 человек (помимо алгоритмов сайта), которые просматривают множество неприглядных публикаций, начиная с террористических материалов и заканчивая изображениями жестокого обращения с детьми.

Докладніше

***

3.01.2018
Корпоративный мессенжджер Slack обзавёлся сервисом для совершения звонков

Теперь телефонные звонки можно проводить прямо из приложения Slack, которое сейчас является лидером рынка мессенджеров для корпоративного общения. Разработка бота Click2call была осуществлена компанией DirectPhone.

Докладніше

***

9.01.2018

В Twitter появилась новая функция

В соцсети микроблогов Twitter появилась новая функция. Теперь людям со слабым зрением можно будет получить всю информацию об опубликованных фото. Приложение работает как в десктопной версии, так и на смартфонах (InternetUA).

Разработчики сообщили, что эта функция активируется очень просто, нужно лишь зайти в опции и поставить галочку в категории «специальные возможности». И в веб-версии и в мобильном приложении активация происходит одинаково.

Помимо этого, теперь пользователи Twitter могут редактировать описание изображений. После активации функции под каждым кадром появляется строчка, куда можно вписать нужный текст.

***

9.01.2018

Facebook отключит виртуального помощника M спустя 2,5 года после запуска

Компания Facebook отключит виртуального помощника M, предназначенного для Facebook Messenger и работающего на базе технологий искусственного интеллекта. Об этом сообщает The Verge. Сервис перестанет работать 19 января 2018 года (IGate).

«Мы запустили этот проект, чтобы узнать, что нужно людям от помощника. Мы получили необходимую информацию, которую собираемся использовать в других ИИ-проектах Facebook. Мы по-прежнему довольны рекомендациями M для пользователей Facebook Messenger, предоставленными в ходе эксперимента», – заявили в компании.

Facebook запустила M в августе 2015 года. Компания предлагала использовать сервис для решения повседневных задач. Например, поиска заведения, заказа еды, конвертации валют и других.

Разработчики M рассчитывали, что пользователи будут обращаться к помощнику обычными просьбами, а не командами.

***

10.01.2018

Раскрыт главный секрет обновленного WhatsApp

Обновленная версия мессенджера WhatsApp получит более глубокую интеграцию с сервисом Instagram. В частности, пользователи смогут публиковать «истории» одновременно в Instagram и в WhatsApp, сообщает TechCrunch со ссылкой на пользователя из Бразилии (InternetUA).

В настоящее время функция находится в режиме тестирования. Помимо WhatsApp, делиться историями также можно будет и в Facebook.

***

10.01.2018

Facebook представила новый протокол шифрования для групповых чатов

Исследователи из компании Facebook опубликовали на портале GitHub новый протокол шифрования для групповых чатов, получивший название Asynchronous Ratcheting Tree (ART) (InternetUA).

По словам исследователей, в ART решены проблемы безопасности, присутствующие в таких приложениях, как WhatsApp, Facebook Messenger, Signal и пр. Как отмечают специалисты, несмотря на то, что шифрование сообщений в переписке между двумя собеседниками в данных приложениях реализовано на достаточно высоком уровне, функции шифрования для групповых чатов оставляют желать лучшего. Скомпрометировав одного из участников группового чата, злоумышленник может перехватывать сообщения на протяжении неограниченного количества времени.

Протокол использует модель asymmetric prekeys (ассиметричные ключи), позволяющую абонентам получать защищенные групповые ключи. Помимо этого, в протоколе используется одноразовый ассиметричный одноразовый ключ настройки, с помощью которого администратор группы может генерировать закрытые ключи для всех участников чата при создании группы.

Как отметили эксперты, ART позволяет вести защищенную групповую переписку, даже если один из ее участников был полностью скомпрометирован.

ART был опубликован на следующий день после того, как директор Федерального бюро расследований США Кристофер Рей заявил о проблемах, которые ведомство испытывает из-за шифрования на мобильных устройствах.

***

10.01.2018

Екатерина Шпачук

Facebook тестирует «местную» ленту новостей

Компания Facebook намерена облегчить для американцев поиск местных новостей из проверенных источников. Социальная сеть тестирует новую опцию под названием «Сегодня». Это лента, полностью состоящая из локальных новостей, событий и объявлений.

Докладніше

***

12.01.2018

Skype приступил к тестированию шифрования чатов // Пока функция Private Conversations доступна только части пользователей

Microsoft заключила соглашение с мессенджером Signal, чтобы запустить систему оконечного шифрования в Skype. Об этом говорится в заявлении Signal (IGate).

Мессенджер Signal – это защищённый шифрованием сервис для обмена сообщениями, команда проекта также разработала протокол шифрования Signal Protocol. Этой системой, кроме самого Signal, пользуются WhatsApp, Google и Facebook.

В тестовом режиме Skype получил функцию Private Conversations. Открыть зашифрованный чат смогут только два собеседника, для групповых чатов эта функция недоступна.

Пока Private Conversations могут воспользоваться только владельцы Skype Insider – версии Skype, где тестируются новые возможности сервиса. Дата запуска новой функции для всех пользователей не раскрывается.

***

12.01.2018

Олег Дмитренко

Facebook пішов у наступ на компанії. Охоплення постів брендів незабаром різко знизиться

Засновник Facebook Марк Цукерберг 11 січня на своїй сторінці розповів, що алгоритм відображення записів в стрічках користувачів незабаром різко зміниться. Користувачі бачитимуть в своїй стрічці більше постів від людей, і менше постів від компаній.

Докладніше

***

15.01.2018

В мобильный YouTube добавят режим инкогнито и ряд других полезных функций

Компания Google выпустила обновление фирменного приложения YouTube до версии 13.01. На первый взгляд, в ней нет новых функций, но после детального изучения в программе были обнаружены намёки на ряд важных нововведений (InternetUA).

Тёмная тема

В настольной версии YouTube тёмная тема уже доступна, а вот в мобильном приложении компания Google пока не предлагает такой опции.

Очевидно, что Google уже тестирует тёмную тему для мобильного приложения YouTube.

Режим инкогнито

Функция уже давно предлагается в браузере Chrome и клавиатуре Gboard. В будущих обновлениях возможность отключить сохранение просматриваемых видео в истории появится и в YouTube.

Свайп, чтобы пропустить рекламу

Сейчас при просмотре видео в приложении YouTube рекламу обычно можно пропустить спустя 5 секунд, нажав на соответствующую кнопку. В будущих обновлениях реклама будет убираться свайпом.

Настройки автовоспроизведения

Функция автовоспроизведения сейчас находится в отдельном разделе. В новых версиях она будет перемещена в «Общие».

***

16.01.2018

Стало известно, чем удивит следующая версия WhatsApp

Разработчики WhatsApp готовят к выходу следующую версию мессенджера, которая получит новую возможность, сообщает XDA Developers (InternetUA).

Речь идет о функции переключения режима звонка. Например, если пользователи начали общаться голосом, то они смогут продолжить разговор в режиме видео, не прерывая вызов.

Данная функция доступна в бета-версии 2.18.4 WhatsApp для операционной системы Android. Чтобы переключиться из голосового в видеорежим, одному из пользователей достаточно нажать кнопку с изображением камеры. После этого у его абонента на экране появится сообщение с предложением включить видео. Если он откажется, то звонок продолжится в прежнем режиме.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

8.01.2018

Госорганы Украины запустили рождественский флешмоб в Twitter

Сергей Гусовский поделился на своей странице в Facebook примером своевременной коммуникации и командной работы государственных организаций. Официальные аккаунты Министерства иностранных дел, Министерства финансов, Нацбанка Украины, Администрации Президента, Министерства экономического развития, Нацполиции, Министерства внутренних дел, Нацгвардии, Министерства образования, Госпогранслужбы, «Нафтогаза», Министерства юстиции, «Укрпочты», Министерства

информационной политики и другие по строчке выложили рождественскую колядку «Народився Бог на санях» украинского поэта Богдана-Игоря Антонича (Marketing Media Review).

***

12.01.2018

Киев: подать жалобу на Печерские ЖЭКи теперь можно через Facebook и Viber

На ЖЭКи Печерского района Киева теперь можно пожаловаться через Facebook и Viber (InternetUA).

В Печерской РГА советуют жителям района сообщать свои предложения или претензии по поводу неэффективной работы коммунальных служб и ЖЭКов. Также к сообщениям можно прикрепить фото-доказательства.

Принимаются запросы через официальную страницу РГА в Facebook.

***

13.01.2018

Вибори президента РФ-2018: У соцмережах Путіна не буде

Прес-секретар передвиборчого штабу кандидата в президенти РФ Володимира Путіна Андрій Кондрашов заявив, що у соцмережах сторінок у Путіна – ні особистих, ні офіційних – не буде (Українська правда).

Про це Кондрашов заявив у коментарі телеканалу RT.

«Офіційних або особистих сторінок і акаунтів, в тому числі і каналу у Telegram, у кандидата в президенти Володимира Путіна не буде, лише офіційний сайт передвиборного штабу», – заявив Кондрашов.

За його словами, усю роботу соцмереж забезпечуватимуть волонтери і прихильники Путіна.

***

15.01.2018

У соцмережах закликають румун виходити на акцію протесту

Маріанна Присяжнюк

У соціальних мережах румун закликають виходити на протест 20 січня. Про це повідомляє УНН з посиланням на Facebook.

У суботу, 20 січня в Румунії анонсується масштабна демонстрація «За юстицію». Повідомляється, що цього дня до столиці приїдуть мешканці інших великих міст.

«Ми, громадяни округу Клуж, вирушимо в Бухарест, щоб захистити нашу свободу і верховенство закону. Ми вважаємо, що це остання демократична річ,

яку ми можемо зробити, і ми закликаємо всіх протестувати у Бухаресті», – сказано в одному з анонсів.

Крім того, в одній з груп повідомляється, що в Бухаресті розпочнеться збір біля Північного вокзалу (Gara de Nord), де люди будуть зустрічати своїх співгромадян, які до них приєднаються.

Нагадаємо, в Румунії проходять масові демонстрації проти зменшення повноважень прокуратури і збереження незалежності судової системи. Крім того, додатковим каталізатором є правки до Податкового кодексу.

***

15.01.2018

У соцмережах зріє бойкот для АЗС через постійне зростання цін на паливо // Небувале зростання цін на бензин може змусити киян піти на безпрецедентні заходи

У соцмережах жителі столиці стали закликати бойкотувати АЗС, як це роблять в Європі. Тим самим кияни планують змусити бензинових магнатів знизити вартість продукції.

Докладніше

***

16.01.2018

Адвокати Януковича через соцмережі шукають свідків

Адвокати екс-президента Віктора Януковича запрошують бажаючих розповісти відому їм інформацію про події часів Євромайдану 2013-2014 років.

Відповідне звернення оприлюднив у Facebook один з представників захисту Віталій Сердюк (Українська правда).

«Ми просимо відгукнутися всіх, хто готовий допомогти встановити істину і розповісти народу України правду про події 2013-2014 років», – йдеться в зверненні.

Адвокатів Януковича зокрема цікавлять відомості щодо організаційної структури Штабу національного опору, підпорядкованості бійців самооборони політичним лідерам Євромайдану, наявності зброї на Майдані і т.д. і т.п.

Захист стверджує, що відомості збираються згідно ст.20 Закону України «Про адвокатуру» та обіцяють конфіденційність звернень.

***

16.01.2018

«Селфі в музеї». Львів'ян закликають приєднатись до міжнародного флешмобу

Катерина Родак

Львівські музеї приєднуються до міжнародної акції «Селфі в музеї» 17 січня запрошують львів'ян сфотографуватись з улюбленими експонатами (Львівський портал).

Львівська галерея мистецтв закликає мешканців активно робити селфі протягом дня у музеях Львова і запощувати їх у соцмережі.

***

16.01.2018

Канадський депутат приєднався до флешмобу #УкраїнаЄдина

Депутат парламенту Канади від опозиційної Консервативної партії Джеймс Безан приєднався до міжнародної акції «Україна єдина» (ZIK).

Про це він написав на своїй сторінці у мережі Твіттер.

«Впродовж чотирьох років український народ хоробро захищає свою Батьківщину від безжальної російської агресії. Я підтримую акцію #УкраїнаЄдина, метою якої є припинення незаконної російської військової агресії проти України», – йдеться у повідомленні.

Свою позицію Безан проілюстрував фотографією з плакатом зі словами «United Ukraine», тобто «Україна єдина».

***

15.01.2018

Франківські матусі розпочали флешмоб на підтримку щеплень

Франківські матусі в соцмережі розпочали новий флешмоб на підтримку вакцинування. Зокрема франківчанка Іванна Кошель для збільшення довіри до вакцинації започаткувала флешмоб #япротикору #явакцинованавідкору.

Докладніше

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

3.01.2018

В 2018 году прибыль Facebook, Amazon и Google продолжит расти

Екатерина Шпачук

Аналитики Уолл-стрит прогнозируют рост прибыли компаний, которые входят в так называемую группу FANG (Facebook, Amazon, Netflix, и Google), в 2018 году.

По их прогнозам, 2018 год станет успешным для этих компаний и ряда других технологических гигантов, которые делают ставку на электронную коммерцию, онлайн-видео, интернет-рекламу и приложения для смартфонов.

Докладніше

***

6.01.2018

В Facebook могут появиться криптовалюты

Марк Цукерберг опубликовал на своей странице пост, в котором сообщил, что заинтересован в изучении криптовалют и способах их интеграции в крупнейшую в мире социальную сеть Facebook. По его словам, децентрализованные валюты обладают большим потенциалом и могут дать обычным людям новые возможности, которыми было бы глупо пренебрегать (IGate).

Основатель Facebook отметил, что Интернет становится слишком централизованным и почти полностью подконтролен нескольким крупным компаниям, тогда как люди хотят, чтобы Интернет был бы более децентрализованным – это позволит увеличить влияние на него со стороны обычных людей.

Цукерберг признал, что даже Facebook не работает так, как должен был работать по его изначальной задумке, поэтому у пользователей складывается впечатление, что социальная сеть, наоборот, усиливает контроль над Интернетом со своей стороны, позволяя корпорациям и правительствам всё больше влиять через Facebook на общество.

«Но это не совсем так, поэтому мы продолжим работать, чтобы исправить это», – написал CEO Facebook на своей странице.

Цукерберг уверен, что криптовалюта и блокчейн, равно как и другие современные технологии защиты информации, смогут дать обычным людям возможности, которых они были лишены ранее – таким образом они смогут влиять на важные общественные события и высказывать свою точку зрения.

***

9.12.2018

Олег Дмитренко

Telegram випустить власну криптовалюту

Месенджер Telegram планує створити власну блокчейн-платформу і криптовалюту. Платформа отримає назву Telegram Open Network (TON), а криптовалюта буде називатися Gram.

Докладніше

***

14.01.2018

Руперт Мердок пригрозил следить за изменениями в новостной ленте Facebook

Американский предприниматель, владелец The Wall Street Journal, The Times и New York Post Рупер Мердок заявил, что намерен «внимательно следить» за изменениями в новостной ленте социальной сети Facebook, передает Bloomberg (InternetUA).

Мердок приветствовал изменения, которые направлены на поощрение качества и борьбу с кликбейтом, однако добавил, что пока неясно, каким образом нововведения отразятся на издателях. Он уточнил, что продолжит «давление» на Facebook, чтобы побудить пользователей подписываться на свои газеты через социальную сеть.

Кроме того, Мердок добавил, что будет тщательно следить за тем, чтобы новости, попадающие в ленту, не были отобраны по политическим мотивам.

***

16.01.2018

В Британии разрешили платежи через мессенджеры

Начиная с 13 января 2018 года девять крупнейших банков Великобритании, обслуживающие основную часть населения, больше не смогут блокировать финансовые операции сторонних компаний. Фактически это означает разрешение платежей через Facebook Messenger, Google Wallet и их аналогов.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

3.01.2018

Желание на Новый год: социальные сети по-лучше – Bloomberg

Компаниям пора задуматься, чтобы сделать свои сайты менее «эксплуататорскими» и вредными для пользователей. Соцсети должны стать более человечными.

Докладніше

***

8.01.2018

Акционеры просят Apple изучить зависимость подростков от iPhone

Несколько крупных акционеров Apple написали руководству компании открытое письмо, в котором приводят примеры исследований негативного влияния смартфонов на молодых людей. Авторы послания просят корпорацию провести собственное исследование и расширить возможности родительского контроля в iOS (InternetUA).

Приведенная информация об исследовании Альбертского университета тревожная: из 2300 опрошенных преподавателей 67 % заявили, что растет число студентов, которые отвлекаются во время занятий на смартфоны, из-за чего падает их способность фокусироваться на учебе.

Также сообщается о повышенном риске депрессии, недосыпа (что приводит к другим проблемам со здоровьем) и суицида у подростков, которые излишне много времени проводят за мобильниками.

Акционеры отмечают, что некоторые исследования могут быть неточными. Поэтому Apple должна провести собственное исследование о том, как технологии влияют на развитие детей.

Вместе с этим рекомендуется добавить в iOS дополнительные функции родительского контроля: например, система должна ограничивать время работы со смартфоном в зависимости от возраста пользователя, уменьшить число доступных социальных сервисов, предоставить родителям ребенка возможность просмотра истории посещений и другие опции.

***

13.01.2018

Роман Черный

Почему Билл Гейтс и Стив Джобс ограждали своих детей от технологий

В последнее время психологи все чаще твердят, что смартфоны и соцсети могут быть опасными для психического здоровья подрастающего поколения. Исследование, проведенное учеными Университета Сан-Диего, показало, что восьмиклассники, проводящие много времени в социальных сетях, страдают от депрессии на 27 % чаще своих сверстников, менее увлеченных интернетом.

Докладніше

***

13.01.2018

Смартфон делает тебя глупым, замкнутым и больным. Почему бы не отложить его в сторону?

Михаил Сапитон

Про вред смартфонов трубит каждое второе исследование – однако журналист канадского издания The Globe and Mail Эрик Эндрю-Ги постарался сложить из этого максимально полную картину. Оказалось, что зависимость от

«синих экранов» наносит по-настоящему комплексный вред: под угрозой память, когнитивные способности и отношения.

Докладніше

Маніпулятивні технології

2.01.2018

Учёные выявили связь между поддельными аккаунтами в соцсетях и здоровьем

Специалисты Медицинской школы Кека при Университете Южной Калифорнии провели ряд исследований и пришли к выводу, что поддельные аккаунты в социальных сетях негативно сказываются на здоровье человека. В частности, речь идёт о публикации неправдоподобных новостей, связанных с медицинской тематикой (InternetUA).

В качестве примера исследователи рассмотрели случай с поддельным аккаунтом актрисы Дженни Маккарти, который публиковал сообщения о том, что прививки вызывают аутизм. И это несмотря на то, что утверждение было неоднократно развенчано.

«Сейчас в Южной Калифорнии зафиксированы вспышки кори, потому что люди делились личными историями о том, как вакцинация якобы вызвала у их ребёнка аутизм. Социальные боты, возможно, не имеют звёздной силы Дженни Маккарти, но нехватку славы они компенсируют количеством и настойчивостью. Они призваны продвигать конкретную идею 24 часа в сутки, 7 дней в неделю», – рассказал Джон-Патрик Аллем, ведущий автор исследования.

Стоит отметить, что в прошлом году компании Google и Facebook активно начали бороться с поддельными новостями в интернете.

***

4.01.2018

Макрон представить закон проти фейкових новин

Президент Франції Еммануель Макрон заявив, що в найближчі тижні буде представлений проект закону, спрямованого проти фейкових новин в мережі. Про це повідомляє Reuters (Espreso.tv).

За його словами, неправдива інформація становить загрозу для ліберальних демократій. Французький президент також нагадав, що він і його команда стали жертвами фейкових новин і серйозного злому даних у ході виборчої кампанії минулого року.

Макрон має намір запропонувати переглянути французьке законодавство щодо засобів масової інформації з метою боротьби з фейковими новинами.

«Якщо ми хочемо захистити ліберальні демократії, у нас має бути сильне законодавство», – сказав Макрон в зверненні до журналістів.

Він також зазначив, що зміни до законодавства будуть в тому числі стосуватися соціальних мереж, особливо в період виборів.

***

11.01.2018

Шахраї від імені полтавського боксера ошукують людей у Мережі

Створюючи «липові» акаунти, зловмисники просять довірливих людей поповнити картку «ПриватБанку». Про це повідомив на своїй сторінці у «Фейсбуці» полтавський боксер Олександр Хижняк (InternetUA).

– З'явилася інформація, що від мого імені люди знову починають займатися шахрайством, просять гроші й поширюють недостовірну інформацію! Моєї сторінки немає в соціальній мережі «ВКонтакті», не підписуйтеся на цю сторінку і не ведіть діалогу, бо це фейк! – написав спортсмен.

***

15.01.2018

У ЄС запрацювала команда протидії фейковим новинам. Чим вона буде займатися

У Європейському Союзі зібрали команду фахівців, що допоможе протидіяти фейковій інформації у ЗМІ (Espreso.tv).

Про це повідомляє Deutsche Welle з посиланням на єврокомісара з питань цифрової економіки Марію Габріель.

У Брюселі розпочала роботу група експертів, що протидіятиме неправдивій інформації у ЗМІ. За словами Габрієль, комісія розробить механізми з розпізнавання фальшивих даних та обмеження їх поширення.

Перше завдання групи – дати визначення поняттю «фейкові новини» та підготувати пропозиції для подальших дій Єврокомісії.

Група складається з 40 експертів. Серед них присутні фахівці з соціальних мереж, працівники ЗМІ, активісти та вчені. Керівник команди - юристка з Нідерландів Мадлен де Кок Бунінг.

Спецслужби і технології «соціального контролю»

4.01.2018

СБУ прекратила деятельность украинцев, снимавших пропагандистское видео для российских СМИ

Двое жителей столицы выкладывали отснятые сюжеты в Интернет (InternetUA).

Сотрудники Службы безопасности Украины прекратили деятельность двух украинцев, снимавших пропагандистское видео для российских СМИ. Об этом сообщает пресс-служба СБУ.

Так, двое жителей столицы по заданию российских спецслужб размещали в сети Интернет антиукраинские видеоматериалы, впоследствии транслировались российскими СМИ. Злоумышленники периодически выезжали в РФ, где получали от своих кураторов соответствующие инструкции и деньги за выполненную работу.

Правоохранителями была обнаружена студия, обустроенная в частном доме в Киеве. Подготовленные видеоматериалы содержат призывы к совершению насильственных действий против существующего конституционного строя, государственной власти, а также оправдывают экстремистские и террористические действия.

Продолжаются следственные действия.

***

1.01.2018

В России вступил в силу запрет на анонимное использование мессенджеров

С 1 января в России вступил в силу запрет на анонимное использование приложений, позволяющих обмениваться сообщениями, передает «Эхо Москвы» (InternetUA).

Согласно новым правилам, все пользователи мессенджеров должны быть зарегистрированы, то есть аккаунты должны быть привязаны не к анонимному адресу электронной почты, а к конкретному номеру телефона.

Все паспортные данные владельцев сим-карт есть у операторов сотовой связи и могут быть затребованы для проверки правоохранительными органами.

За неисполнение нового закона нарушители могут быть оштрафованы. Физические лица – на сумму до 5 тыс. руб. (2,4 тыс. грн), юридические – до 1 млн руб. (487,6 тыс. грн).

***

1.01.2018

Трамп оценил блокировку Ираном Telegram и Instagram

Президент США Дональд Трамп в своем Twitter раскритиковал решение иранских властей о блокировке доступа к сервисам Telegram и Instagram (InternetUA).

«Иран, государство номер один по спонсированию терроризма, ежечасно нарушающее права человека, теперь закрыло доступ в интернет, чтобы мирные демонстранты не могли общаться. Нехорошо!», – написал Трамп.

Ранее 31 декабря иранские власти на фоне проходящих в стране массовых акций протеста заблокировали доступ к популярному в республике мессенджеру Telegram и фотосервису Instagram. Меры были приняты по распоряжению Высшего совета национальной безопасности. Создатель Telegram Павел Дуров написал в Twitter, что власти решили заблокировать мессенджер после отказа администрации проекта закрыть каналы мирных протестующих.

Антиправительственные демонстрации в Иране начались в ночь на 28 декабря. Акции протеста, проходящие во многих городах страны, в том числе в Тегеране, сопровождаются столкновениями с силовиками и нападениями на государственные учреждения.

***

3.01.2018

В Беларуси начали применять «налог на Google»

На территории Республики Беларусь с января этого года начинают применяться на практике ранее внесенные поправки в Налоговый кодекс государства, получившие в СМИ неофициальное название «налог на Google» (News.UA).

В частности, предусмотрено, что теперь в Беларуси нужно обязательно уплачивать НДС в размере 20 % со всех электронных услуг, оказываемых и предоставляемых зарубежными предприятиями. Налог будет поступать в бюджет государства ежеквартально и должен уплачиваться в национальной валюте.

Министерство по налогам и сборам РБ сообщает, что применение соответствующего налога на электронные услуги (использование ПО, рекламу в Сети, доступ к электронным книгам и др.) является распространенной практикой в других странах, включая не только соседнюю Российскую Федерацию, но и государства Европейского союза.

***

3.01.2018

Власти Германии начинают штрафовать соцсети за оскорбительные посты

1 января Германия начала исполнять закон, направленный на борьбу с разжиганием ненависти в соцсетях и предусматривающий штрафы до 50 млн евро за несвоевременное удаление запрещённой информации (IGate).

Так называемый «закон о Facebook» был принят в конце июня, накануне парламентских выборов в Германии. В действие он вступил 1 октября.

Исполнение закона было отложено на более поздний срок, чтобы соцсети могли подготовиться к его соблюдению.

Закон направлен на издателей и социальные сети с аудиторией от 2 млн человек, включая Facebook, Twitter, Reddit и YouTube.

Согласно новым правилам, соцсети должны удалять посты и комментарии, содержащие угрозы и призывы к насилию, а также дезинформацию в течение 24 часов после получения уведомления о нарушении. В отдельных случаях этот срок может быть продлён до семи дней. В противном случае им будет грозить штраф.

Проект закона был разработан в марте 2017 года. Канцлер Германии Ангела Меркель поддержала идею регулирования контента в соцсетях. По её мнению, это позволит бороться с популистскими движениями, которые получают всё большее распространение во всей Европе.

***

7.01.2018

Twitter назвал условия для избежания блокировки аккаунтов

Социальная сеть Twitter сообщила, что не будет блокировать учетные записи «мировых лидеров», чтобы сохранить доступ к информации. Об этом сказано в официальном заявлении, опубликованном в блоге компании (InternetUA).

«Блокировка мирового лидера из Twitter или удаление их спорных сообщений скроют от людей важную информацию, которую должны видеть и о которой дискутировать… Мы работаем над тем, чтобы сделать Twitter лучшим местом для свободного обсуждения всего, что имеет значение. Мы считаем, что это лучший способ помочь нашему обществу добиться прогресса», – говорится в сообщении.

Заявление было сделано после требований некоторых пользователей заблокировать аккаунт президента США Дональда Трампа, якобы угрожавшего Северной Корее ядерным оружием.

Всего в мире насчитывается около 300 миллионов пользователей Twitter. Из них более 46 миллионов читают страницу американского лидера.

***

8.01.2018

Екатерина Шпачук

Facebook и Google намерены оспорить отмену сетевого нейтралитета

Торговая группа, представляющая Facebook, Google и Netflix и десятки других IT-компаний, планирует подать в суд на Федеральную комиссию по связи (FCC) за отмену принципа сетевого нейтралитета. Об этом сообщает издание Duluth News Tribune (InternetUA).

Интернет-ассоциация в своем заявлении отметила, что вступит в правовую борьбу против решения Федеральной комиссии.

Стоит напомнить, что 14 декабря комиссия проголосовала за отмену принципа сетевой нейтральности. Сетевой нейтралитет – это принцип, согласно которому провайдеры интернет-услуг (ISP) должны обрабатывать все виды данных, каких либо ресурсов, одинаково, без предпочтений. При отмене сетевого нейтралитета такие провайдеры, как AT&T, Comcast и Verizon, смогут блокировать контент, веб-сайты и приложения, замедлять или ускорять услуги по своему усмотрению.

«Окончательная версия распоряжения главы Федеральной комиссии по связям Аджита Пая, как и ожидалось, ликвидирует защиту сетевого нейтралитета для потребителей. Это решение бросает вызов большинству американцев, и ставит под угрозу свободный и открытый интернет. Интернет-ассоциация намерена выступить в качестве посредника в судебных разбирательствах против этого решения», – говорится в заявлении президента и генерального директора группы Майкла Беккермана.

В Федеральной комиссии по связи отказались от комментариев.

***

14.01.2018

Чем Apple Watch не угодили Белому дому

Администрация Белого дома в Вашингтоне запретила посетителям носить Apple Watch и другие носимые устройства. Нововведения коснулись западного крыла резиденции Президента США, где работает сам чиновник и основная часть сотрудников (InternetUA).

Как сообщает ABC News, запрет коснулся личных смартфонов, ноутбуков, умных часов, фитнес-трекеров и любых других девайсов, которые используют для подключения беспроводные интерфейсы вроде Wi-Fi и Bluetooth. Основной целью указа является прекращение утечки данных из Белого дома. Помимо этого, сотрудники смогут меньше отвлекаться на личные дела.

Теперь всем посетителям необходимо сдавать Apple Watch и другую носимую электронику перед посещением западного крыла, тогда как ранее они могли спокойно проносить подобные устройства.

***

14.01.2018

В РФ хочуть блокувати сайти без суду. «Як у Китаї»

Глава Слідчого комітету РФ Олександр Бастрикін пропонує запровадити у Росії позасудовий механізм блокування екстремістських сайтів (InternetUA).

Про це Бастрикін заявив в інтерв'ю урядовій газеті РФ «Российская газета».

Глава СК РФ висловив думку про доцільність ухвалити «більш оперативний механізм блокування таких сайтів».

На думку Бастрикіна, необхідно передбачити позасудовий порядок включення матеріалів сайтів до федерального списку екстремістських матеріалів і зазначив, що така практика існує у Китаї.

Він нагадав, що наразі блокування таких сайтів можливе на підставі судового рішення, що вимагає часу, протягом якого ресурс продовжує роботу.

«Для блокування екстремістських сайтів мною на оперативних нарадах, проведених у федеральних округах, дано вказівку активніше взаємодіяти з органами прокуратури та Роскомнадзором і оперативно направляти туди отримані у ході слідства матеріали, що підтверджують поширення в інтернеті протиправної інформації», – зазначив Бастрикін.

***

15.01.2018

Власти Ирана разблокировали Telegram из-за «серьёзных убытков» бизнеса

Правительство Ирана сняло блокировку с мессенджера Telegram. Об этом сообщаетReuters со ссылкой на государственное информационное агентство IRNA (IGate).

По данным агентства, власти объяснили своё решение по возобновлению доступа к сервису тем, что «сотни компаний, использующих мессенджер для маркетинга и продаж, понесли серьёзные убытки» из-за ограничений доступа к социальным сетям.

Сейчас Иран продолжает блокировать другие социальные сети – Facebook и Twitter.

***

15.01.2018

Тисячу молодих датчан звинуватили у поширенні дитячого порно через Facebook

Більше тисячі молодих людей у Данії можуть опинитися на лаві підсудних за звинуваченням у поширенні порнографічних матеріалів (Espreso.tv).

Про це інформує BBC.

За даними правоохоронців, підозрювані поширювали відео сексу двох 15-річних школярів, обмінюючись ним в месенджері Facebook.

Поліція повідомила, що їм інкримінують поширення дитячої порнографії, оскільки підліткам, зафіксованим на відео, не виповнилося 18-ти років. Про інцидент з відео датська поліція дізналася від американської влади, яка, у свою чергу, отримала інформацію від Facebook.

В цілому у цій справі проходять 1004 людини. За даними поліції, вони обмінювалися порнороликом в мессенджері восени минулого року. Деяким підозрюваним вже виповнилося 18 років, тому в поліцейські відділки їх викликали особисто. Підлітків молодше 18 років було повідомлено через батьків.

Представник датської поліції заявив, що ця справа повинна послужити попередженням молоді про наслідки, які можуть виникнути в результаті обміну секс-відео. У разі визнання провини підозрюваним загрожує умовний тюремний термін приблизно на 20 днів. Також, якщо їх визнають винними, вони на 10 років опиняться в списку людей, викритих в поширенні дитячої порнографії.

Проблема захисту даних. DDOS та вірусні атаки

2.01.2018

Хакерские атаки 2018 года возглавит искусственный интеллект

Искусственный интеллект эволюционирует все быстрее и уже в 2018 году станет опасным оружием в руках хакеров. Он научится адаптироваться и взламывать защитные системы, перехватывать контроль над голосовыми помощниками и даже выдавать себя за человека.

Докладніше

***

2.01.2018

Недобросовестные сотрудники угрожают кибербезопасности компании

Многие сотрудники офисов используют доступ в интернет на работе в личных целях, что может стать угрозой для кибербезопасности целой компании. Подчиненные могут посещать сомнительные и даже опасные веб-сайты с рабочих компьютеров и не подозревать, что открывают хакерам доступ к корпоративной сети и информации, содержащейся в ней.

Докладніше

***

3.01.2018

Эксплойт для 0-day в роутерах Huawei вышел в люди

Код эксплойта, который использовался для загрузки IoT-ботов Satori на роутеры производства Huawei, стал достоянием общественности. Эксперты

предупреждают, что злоумышленники не преминут воспользоваться публикацией для построения новых ботнетов с целью проведения DDoS-атак.

Докладніше

***

3.01.2018

Злоумышленники используют пиратское ПО для скрытого майнинга

Эксперты «Лаборатории Касперского» обнаружили скрытый майнер NiceHash в пиратских дистрибутивах популярных программ. Список продуктов включает как платные Adobe FineReader, Outlook, PowerPoint, так и свободное ПО вроде OpenOffice. В каждом из них исследователи нашли программную закладку для майнинга криптовалют.

Докладніше

***

3.01.2018

В Opera появилась защита от криптомайнеров

Компания Opera выпустила 50-ю версию фирменного браузера. Апдейт включает сразу несколько важных возможностей, в том числе нацеленных на защиту пользователей от нового типа злоумышленников. Сразу отметим, что на данный момент Opera 50 находится на стадии бета-тестирования, но все желающие уже могут опробовать новую версию (Центр информационной безопасности).

Первым нововведением Opera 50 стала расширенная поддержка 360-градусных видео для Oculus и Chromecast. Вторым и более значимым изменением является защита от злоумышленников, использующих компьютеры пользователей для майнинга криптовалют. Сейчас всё большую популярность набирает вид атак, когда при посещении вредоносного сайта ваш компьютер внезапно нагружается до максимума. В этот момент злоумышленники используют его для добычи криптовалюты. Вы можете закрыть сайт или браузер, но процесс будет продолжаться. Поэтому в Opera разработали инструмент для борьбы с любителями лёгкой наживы.

В настройках Opera 50 появилась функция NoCoin, находящаяся в разделе блокировки рекламных объявлений. При её активации встроенные в страницы скрипты для добычи криптовалют будут заблокированы так же, как блокируется реклама.

***

8.01.2018

Секретная настройка в Google Chrome спасает от всех видов угроз

В самом начале этого года компания Intel объявила о том, что ее сотрудники обнаружили критический дефект во всех фирменных процессорах. Позже выяснилось, что встретить уязвимость можно даже в ARM-процессорах, которые установлены во все современные смартфоны и планшеты.

Докладніше

***

9.01.2018

McAfee распространяет свою защиту на личные данные

Фирма McAfee, предоставляющая антивирусное ПО более, чем 375 млн клиентов, анонсировала расширение своего бизнеса на защиту от кражи личных данных (Компьютерное Обозрение).

В условиях, когда взломы информационных систем с похищением персональных данных учащаются и приобретают все более угрожающие масштабы, McAfee Identity Theft Protection предоставит пользователям упреждающий подход к обеспечению безопасности со средствами персонального/финансового мониторинга и восстановления данных.

Этот сервис сканирует онлайновый теневой рынок и предупреждает пользователей о появлении там их персональных данных, а также об адресах, связанных с их номером социального страхования, указывающих на возможные поддельные учётные записи. Отслеживание кредитной истории позволяет держать пользователей в курсе любых изменений их кредитоспособности.

На CES 2018 в Лас-Вегасе (штат Невада), где McAfee сделала это объявление, она анонсировала партнёрские соглашения с различными провайдерами оборудования, ПО и широкополосных сервисов в целях защиты клиентов соответствующих компаний. В частности, она сообщила, что обеспечит безопасность нового Wi-Fi-маршрутизатора D-Link AC2600 и Samsung Secure Wi-Fi – для европейских пользователей Galaxy Note8.

Новейшие продукты и сервисы компании включают, помимо McAfee Identity Theft Protection, также McAfee Secure Home Platform, McAfee Safe Family и McAfee Safe Connect.

***

9.01.2018

Вредонос маскируется под приложение Uber для Android

Исследователи Symantec обнаружили вредоносную программу, которая маскируется под приложение Uber для Android. Целью вредоноса являются пароли пользователей (Компьютерное Обозрение).

Чтобы похитить информацию пользователя, программа регулярно показывает сообщение с предложением ввести логин и пароль от учетной записи Uber. Для сокрытия кражи данных она показывает местоположение

пользователя, используя ссылки на настоящие сервисы Uber. Поэтому жертва не сомневается, что открыла настоящее приложение.

К счастью, фишинговая атака не распространена широко, так как вирус маскируется под версию приложения Uber, которой нет в Google Play. В Symantec считают, что вредоносную программу со стороннего магазина загрузили в основном пользователи русскоговорящих стран.

***

10.01.2018

Хакери поширили троян через український сайт бухгалтерських програм

Хакери використовували сайт українського розробника бухгалтерського програмного забезпечення Crystal Finance Millennium (CFM) для поширення банківського трояна ZeuS.

Інформацію оприлюднила компанія Cisco Talos, що спеціалізується на кібербезпеці, повідомляє AIN (Espreso.tv).

Фахівці порівняли атаку ZeuS з вірусом NotPetya, яка поширювався через бухгалтерські програми українського розробника MEDoc.

На відміну від NotPetya, в даному випадку шкідливий вірус поширюється не через вразливий сервер, а через сайт компанії CFM. Жертв заражали по електронній пошті. У листах містився ZIP-архів з файлом JavaScript, який працював як завантажувач, через який шкідливий вірус надходив в систему з домену, пов'язаного з сайтом CFM.

Опинившись на комп'ютері, вірус активовував перманентний сплячий режим, в іншому випадку створювався запис реєстру для забезпечення виконання при кожному запуску системи. Далі програма намагалася підключитися до різних C & C-серверів. В рамках розслідування інциденту фахівці зафіксували 11 925 626 спроб зв'язатися з сервером від 3216 унікальних IP-адрес.

***

10.01.2018

Владимир Кондрашов

В Минюсте открыли уголовное дело из-за слива данных, но забыли закрыть уязвимость

За фактом вмешательства в работу серверов Главного территориального управления юстиции в Одесской области и установки вредоносного программного обеспечения открыто уголовное производство по ст.361 Ч 1. Уголовного кодекса Украины (InternetUA).

Об этом сообщает InternetUA со ссылкой на пресс-службу ГТУ Юстиции в Одесской области.

Санкция статьи, по которой открыто уголовное производство, предусматривает наказание в виде штрафа от шестисот до тысячи необлагаемых минимумов доходов граждан или ограничение свободы на срок от двух до пяти лет, или лишение свободы на срок до трех лет, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет с конфискацией техсредств.

Как сообщает пресс-служба ГТУЮ, вмешательство в работу серверов одесской юстиции и установку вредоносного ПО обнаружили сотрудники Причерноморского управления киберполиции Департамента киберполиции НПУ, что немного не соответствует действительности. Уязвимости портала ГТУ Юстиции в Одесской области обнаружили белые хакеры Украинского киберальянса в рамках акции #FuckResponsibleDisclousure рано утром 6 января. Сообщалось об утечке сотен гигабайт документов.

***

10.01.2018

Чтобы закрыть фундаментальную «дыру» в Wi-Fi по всему миру, создается новый протокол WPA3

Wi-Fi Alliance готовит новый стандарт безопасности Wi-Fi-соединений WPA3, который должен будет прийти на смену уязвимому протоколу WPA2.

Докладніше

***

10.01.2018

Популярнейшие китайские смартфоны заподозрили в шпионаже

Планы Huawei начать продавать свои устройства через американских сотовых операторов терпят крах. Власти США подозревают производителя смартфонов в тесных связях с китайским правительством и, опасаясь шпионажа, оказывают на крупнейшие телекоммуникационные компании страны политическое давление.

Докладніше

***

10.01.2018

Малоизвестная функция MS Word может использоваться для кражи паролей

Исследователи из компании Rhino Labs описали новый способ кражи учетных данных Windows с помощью малоизвестной функции MS Word под названием subDoc, позволяющей загружать документ в тело другого документа. Функционал также может применяться для удаленной загрузки subDoc файлов

в основной документ, что позволяет проэксплуатировать его во вредоносных целях.

Докладніше

***

11.01.2018

В пакете Dell EMC Data Protection Suite обнаружены серьезные уязвимости

Исследователи безопасности из компании Digital Defense обнаружили в пакете программ для защиты данных Dell EMC Data Protection Suite несколько серьезных уязвимостей, позволяющих злоумышленнику получить контроль над системой.

Докладніше

***

13.01.2018

«ВК» и RuTracker попали в список крупнейших мировых пиратских ресурсов

Министерство торговли США вновь внесло российскую социальную сеть «ВКонтакте» (принадлежит Mail.ru Group) в список пиратских ресурсов, следует из документа, опубликованном на сайте ведомства (InternetUA).

В документе собраны крупнейшие мировые ресурсы, которые, по мнению американской стороны, нарушают права интеллектуальной собственности. При этом «ВКонтакте» оказывается в списке не в первый раз. Среди других российских проектов, включенных в список, – торрент-трекер Rutracker.org и Rapidgator.net, онлайн-кинотеатр kinogo.cc, а также еще ряд сайтов.

Как сообщает «Интерфакс», всего в список вошли 25 сайта разных стран мира, которые по мнению американской стороны нарушают авторские права. В частности, в него вошел сайт крупнейшего китайского интернет-магазина taobao.com, который принадлежит Alibaba Group.

***

13.01.2018

ЦРУ пришло к выводу, что вирус NotPetya был создан российской разведкой

Центральное разведывательное управление США (ЦРУ) признала российское Главное разведывательное управление (ГРУ) создателем вируса NotPetya. Об этом сообщает The Washington Post (IGate).

Газета, ссылаясь на свои источники, отмечает, что в ноябре 2017 года ЦРУ пришло к выводу, что «с высокой долей уверенности» вирус был создан российским ГРУ. В ЦРУ отказались комментировать информацию.

27 июня на государственные и частные компании Украины была совершена кибератака с использованием вируса-вымогателя NotPetya. Мошенники поразили тысячи компьютеров в десятках организаций страны. Эксперт, опрошенный The Washington Post отмечает, что целью атаки был «подрыв финансовой системы Украины».

***

15.01.2018

СБУ заблокувала розповсюдження в Україні шпигунського програмного забезпечення

Співробітники СБ України спільно з прокуратурою заблокували розповсюдження шкідливого програмного забезпечення, яке призначалося для віддаленого негласного отримання інформації з мобільних терміналів.

Докладніше

***

15.01.2018

Компьютеры Apple начал поражать новый вирус

По данным экспертов по безопасности, компьютеры Apple подвержены атаке нового опасного вируса OSX/MaMi (iLenta.com).

Новый зловред, по словам специалистов, напоминает действовавший в 2012 году троян DNSChanger эстонского «производства», который в свое время успел заразить миллионы компьютеров по всему миру.

OSX/MaMi помогает злоумышленникам воровать персональные данные пользователей компьютеров Apple. Современные антивирусные программы не в состоянии обнаружить этот зловред. Кто его разработал и как он распространяется – пока неизвестно.

Эксперты отмечают, что OSX/MaMi нельзя назвать особо продвинутым, но он способен незаметно проникать в систему и сильно вредить владельцу устройства. Киберпреступники с его помощью могут, к примеру, взять под контроль интернет-трафик.

***

16.01.2018

Хакеры взломали DNS-сервер сервиса BlackWallet и похитили $400 тыс. в криптовалюте

Неизвестные хакеры взломали DNS-сервер сервиса BlackWallet.co, предоставляющего web-кошельки для криптовалюты Stellar Lumen (XLM), и украли более $400 тыс. со счетов пользователей.

Докладніше

***

16.01.2018

Сотрудники Twitter читают переписку пользователей и просматривают их интимные фото

Организация Project Veritas опубликовала снятое скрытой камерой видео, в котором сотрудники Twitter признались в том, что читают личные сообщений пользователей.

Докладніше

ДОДАТКИ

Додаток 1

2.01.2018

Facebook попросила прощения за «ошибки» модерации

Количество пользователей Facebook давно превысило 2 млрд и продолжает расти, так что задача контроля за соблюдением правил сообщества становится всё более сложной. Незавидная работа возложена на плечи команды модераторов, насчитывающей 7500 человек (помимо алгоритмов сайта), которые просматривают множество неприглядных публикаций, начиная с террористических материалов и заканчивая изображениями жестокого обращения с детьми (InternetUA).

Неудивительно, что модераторы не всегда верно понимают суть изображения или публикации (частично из-за двусмысленных рекомендаций самой Facebook). Проблеме распространения ненависти и вражды с помощью крупнейшей социальной сети был посвящён недавний материал некоммерческой организации ProPublica.

Её сотрудники отправили в Facebook набор из 49 примеров (выбранных из 900 публикаций добровольцев) с просьбой объяснить решения модераторов. В большинстве этих случаев сообщения, содержавшие сексистские, расистские или антимусульманские высказывания, остались опубликованными; в нескольких же случаях вполне законное выражение эмоций было удалено. Социальная сеть признала, что её редакторы неверно отреагировали на 22 случая. В шести примерах Facebook сказала, что пользователи запутали модераторов неверно оформленными жалобами или авторы сами удалили сообщения; а в двух случаях не было достаточно информации для реакции. Компания также выступила в защиту решений 19 своих редакторов.

«Мы сожалеем об ошибках, которые допустили, – сказал в заявлении Facebook вице-президент Джастин Ософский (Justin Osofsky). – Мы должны справляться лучше». Руководитель добавил, что в следующем году социальная сеть расширит свою команду по безопасности и защите до 20 тысяч человек, чтобы лучше поддерживать стандарты сообщества. Он добавил, что Facebook

еженедельно удаляет порядка 66 тысяч сообщений, на которые поступают жалобы в распространении ненависти.

Помимо борьбы с дезинформацией, Facebook старается развивать и свои инструменты для удаления чувствительных материалов. Например, в апреле социальная сеть добавила механизм жалоб на «порновозмездие» (Revenge Porn – распространение фото- или видеоматериалов жертвы, запечатлённой во время сексуальной активности или в ином непотребном виде). Появляются и другие инструменты борьбы с агрессивным поведением собеседников и тому подобными тёмными сторонами общения в социальных сетях. Например, благодаря недавним новшествам должен снизиться поток нежелательных сообщений и запросов в друзья.

(вгору)

Додаток 2

3.01.2018

Корпоративный мессенджер Slack обзавёлся сервисом для совершения звонков

Теперь телефонные звонки можно проводить прямо из приложения Slack, которое сейчас является лидером рынка мессенджеров для корпоративного общения. Разработка бота Click2call была осуществлена компанией DirectPhone (ITnews).

Цель его создания – облегчить возможность звонков непосредственно из мессенджера, путем выбора нужных участников команды. Позвонить любому участнику команды можно прямо из приложения или страницы Slack. Каждый имеет возможность в любой момент связаться с партнёрами. Оценить быстроту подключения бота смогут компании, которые работают с клиентами по всему миру. Звонить можно из любой страны в любую точку земного шара, где находится нужный вам человек.

Простота использования сервиса

Установить бот может администратор корпоративного чата. Следующий шаг – настройка рабочей площадки. Затем выполняются выбор языка и привязка бота, для этого используют аккаунт в системе DirectPhone. В результате создаётся счёт, денежные средства на котором принадлежат команде, право пополнять его есть у администратора. Для удобства работы Click2call бот для Slack способен реагировать на специальные команды, исходящие от пользователя. Посредствам команд Бота, можно запросить баланс средств, напомнить логин-пароль, путём отправки данных на электронную почту. Если возникают трудности в процессе работы, можно получить помощь с пояснениями команд. Администратор имеет право добавлять или удалять участников.

Как осуществляются звонки

Разобраться с работой программы очень легко. Пользовательское меню устроено так, чтобы было удобно и просто им пользоваться. В списке

участников указываются номера телефонов, с которыми бот будет осуществлять связь. Каждый член команды может позвонить любому участнику. Соединение устанавливается следующим образом: сначала звонок поступает на исходящий номер, а затем происходит соединение с абонентом. Пользователи Slack уже оценили преимущество Click2call. Это реальная экономия, поскольку звонки в роуминге выливаются в месячном балансе предприятия в огромную сумму. Приоритет использования телефонной связи прямо с сайта в системе DirectPhone в том, что соединение осуществляется мгновенно.

(вгору)

Додаток 3

10.01.2018
Екатерина Шпачук
Facebook тестирует «местную» ленту новостей

Компания Facebook намерена облегчить для американцев поиск местных новостей из проверенных источников. Об этом сообщает издание Recode (InternetUA).

Социальная сеть тестирует новую опцию под названием «Сегодня». Это лента, полностью состоящая из локальных новостей, событий и объявлений.

На данный момент тестирование новой функции проходит в 6 городах США: Новый Орлеан, штат Луизиана; Литл-Рок, штат Арканзас; Биллингс, штат Монтана; Пеория, штат Иллинойс; Олимпиа, штат Вашингтон, и Бингемтон, штат Нью-Йорк. Пользователи Facebook, которые отметили в соцсети, что живут в этих районах, смогут воспользоваться новым разделом, чтобы узнать местные новости. Например, истории локальных изданий или информацию о чрезвычайных ситуациях от местных властей.

В своей новой функции Facebook использует как информацию о пользователях, так и ПО для машинного обучения, чтобы распределять информацию в «местной» ленте новостей. Перед тем как появиться в ленте, локальные издания будут проверены и одобрены командой News Partnerships, которую возглавил бывший ведущий новостей NBC Кэмпбелл Браун.

По словам Facebook, новая опция стала частью инициатив – Journalism Project, которые начались вскоре после последних президентских выборов в США. Многие обвиняют социальную сеть в распространении фейковых новостей, которые могли стать одной из причин внезапной победы Дональда Трампа.

Компания намерена убрать сомнительные новости из своей ленты. Выбор локальных изданий «вручную», который появится в приложении, теоретически должен помочь свести фейковые новости до минимума.

Вопрос состоит лишь в том, поможет ли эта функция местным изданиям. Возможно, это поможет привлечь больше трафика местным веб-сайтам и они

смогут зарабатывать через рекламу. Однако изданиям не удастся заработать деньги с «локального раздела».

Facebook планирует предупредить жителей шести городов, где тестируется эта функция, что вскоре она появится в меню. Отмечается, что здесь находятся десятки других менее используемых разделов приложения, о которых быстро забывают.

Несмотря на это, у Facebook большие надежды на эту опцию и планы внедрить ее в большинстве городов США. По словам представителя компании, пользователи смогут узнавать новости из городов, в которых они уже не живут (например, в родном городе детства).

За последние 18 месяцев «местная» лента новостей стала для Facebook одной из главных тем. Осенью прошлого года компания начала выдавать больше сообщений от местных политиков и расширять Marketplace (платформа, где люди продают подержанные товары своим соседям).

В ноябре Facebook также перезапустила свое приложение «Facebook Local», которое показывает пользователям, где поесть и куда сходить.

(вгору)

Додаток 4

12.01.2018

Олег Дмитренко

Facebook пішов у наступ на компанії. Охоплення постів брендів незабаром різко знизиться

Засновник Facebook Марк Цукерберг 11 січня на своїй сторінці розповів, що алгоритм відображення записів в стрічках користувачів незабаром різко зміниться. Користувачі бачитимуть в своїй стрічці більше постів від людей, і менше постів від компаній (Watcher).

І хоча Цукерберг пояснює все це турботою про людей, про реальні мотиви ми можемо лише здогадуватись.

За словами Марка, стрічка новин в Facebook зміниться так, щоб користувачі могли приділити більше уваги повідомленнями від близьких. Це стане відповіддю на наплив реклами, відео та політичних новин.

Цукерберг пояснив, що став отримувати все більше скарг на те, що масово вироблений контент починає витісняти з новинних стрічок повідомлення від близьких і друзів. «Легко зрозуміти, як це сталося. За останні кілька років відео та інший публічний контент вибуховими темпами поширювалися на Facebook. Через це в вашій стрічці з'являється все більше публічних записів, число записів від друзів і родичів зменшується. Це змінило баланс і відсунуло нас від найбільш важливої справи, для якої призначений Facebook – допомагати нам спілкуватись», – пояснив він.

За його словами, команда соціальної мережі відчуває свою відповідальність за те, щоб Facebook був не просто засобом розваги, але і сприяв «благополуччю» користувачів. Дослідження показали, зазначає

Цукерберг, що соціальні мережі несуть благо тоді, коли використовуються для підтримки контакту між окремими людьми. Перегляд відео та читання статей, хоча і можуть бути більш інформативними, не допомагають соціальній комунікації. Тому порядок формування новинної стрічки буде змінений, і в ній з'явиться більше повідомлень від друзів.

«Хочу пояснити: я готовий до того, що після цих змін скоротиться час, який люди проводять на Facebook, а деякі засоби взаємодії перестануть бути популярними. Але я також сподіваюся, що час, який ви будете тут проводити, стане більш цінним », – написав Цукерберг.

У Facebook діє алгоритм Edge Rank, що відповідає за формування новинної стрічки, і який відбирає найважливіші для користувача повідомлення. Відмовлятися від хронологічного відображення соцмережа вирішила з 2006 року, хоча можливість переключитися на перегляд всіх повідомлень є в налаштуваннях.

Facebook випустив окреме відео, в якому детальніше пояснив, як зміниться алгоритм ранжування контенту в стрічці нови користувача:

Що ж могло змусити Цукерберга так різко розвернути Facebook? Є кілька версій.

Перша – це зростання тиску на соцмережу як з боку влади США, так і з боку суспільства через нездатність боротись з фейковими новинами. Є думка, що у середньотерміновій перспективі Facebook програє боротьбу з фейками, оскільки алгоритми спецслужб та окремих компаній, які їх поширюють, будуть лише покращуватись.

Друга – це банальне бажання заробити більше на корпораціях. Фейсбук є лідером за кількістю часу, який люди щоденно тратять. Це найвпливовіший медіа-канал у світі. І Фейсбук хоче більше заробляти грошей завдяки тому, що ціна на рекламу зросте. Компаніям доведеться платити не лише за виготовлення матеріалів для розміщення на своїх сторінках, а й суттєво збільшити й так вже не малі кошти на рекламу цих постів.

Третя – стрічка новин у Фейсбуку дійсно стала занадто перевантажена різноманітним трешовим контентом. І користувачі шукають для себе більш зручні гавані. Наприклад, протягом минулого року кількість молоді у віці до 21 року, які користуються Фейсбуком, постійно знижувалась. Вони міняли Фейсбук на месенджери або інші, більш зручні сервіси соціальної взаємодії.

(вгору)

Додаток 5

15.01.2018

У соцмережах зріє бойкот для АЗС через постійне зростання цін на паливо // Небувале зростання цін на бензин може змусити киян піти на безпрецедентні заходи

У соцмережах жителі столиці стали закликати бойкотувати АЗС, як це роблять в Європі. Тим самим кияни планують змусити бензинових магнатів знизити вартість продукції.

«Усім водіям! Відмінна ідея як боротися з цінами на бензин! Ціни на паливо стрімко ростуть, ще трохи і ми побачимо 30-35 гривень за літр, а може бути і більше. В Європі водії намагалися боротися з цінами акцією “Не купуй паливо один день”, яка пройшла кілька місяців тому. Виробники палива лише посміялися над цим, розуміючи, що довго тривати це не може: наслідки для автовласників виявляться більш згубні, ніж для них.

Але на основі цієї акції виникла ідея нової, куди більш ефективною! Коли ціни продовжують рости з такою гнітючою стабільністю – ми повинні вживати заходів! Щоб зробити це без будь-яких незручностей для себе, протягом двох місяців не купуємо бензин і дизельне паливо на заправці найбільшого постачальника регіону. Якщо паливо не будуть купувати довгий період – продавець буде змушений знижувати ціни. Коли вони знизять ціни – інші продавці будуть змушені зробити те ж саме! Але для досягнення ефекту, нам потрібно, щоб ці компанії втратили дійсно тисячі клієнтів», – написала Еліна Галва.

При цьому план дуже простий і хитрий: не купувати бензин у найбільшого постачальника. Адже бойкотувати всіх неможливо, а ось якщо найбільший учасник ринку буде змушений знизити ціни, за ним це зроблять і інші.

При цьому автор публікації впевнена, що спільними зусиллями до акції можна підключити величезну кількість людей.

«Просто надсилайте це повідомлення і люди перестануть купувати. Якщо кожен, кому набридло платити корпораціям шалену ціну за бензин з надр своєї землі, перешле це повідомлення наступним 10 людям – вже через тиждень у цій акції братимуть участь 300 мільйонів чоловік», – стверджує вона.

Ідея моментально знайшла підтримку у інших користувачів, які впевнені, що навіть один день колективного бойкоту може вплинути на зниження цін.

(вгору)

Додаток 6

15.01.2018

Франківські матусі розпочали флешмоб на підтримку щеплень

В Україні набирає обертів епідемія кору. Кількість, людей які захворіли на цю хворобу, збільшилася в 70 разів порівняно з минулим роком (Бліц-інфо).

За даними МОЗ, за 10 місяців 2017-го в Івано-Франківській області захворіли 877 людей. За словами медиків від початку року в області вже захворіли 100 людей. Через збільшення кількості хворих на кір у франківських школах продовжили на тиждень канікули.

Дитсадків вимушені канікули не торкнулися, проте батьків схвилювало розпорядження Департаменту освіти Про продовження канікул в якому був пункт «Заборонити відвідувати заклади освіти не вакцинованих дітей».

Втім, директор Департаменту освіти у коментарі ЗМІ запевнив, що довідок про щеплення у дитсадках не вимагають, а опубліковене розпорядження тільки чернетка, яку не мали викладати. Також освітянин сказав, що з батьками будуть проводити бесіди, щодо необхідності вакцинування.

Водночас франківські матусі в соцмережі розпочали новий флешмоб на підтримку вакцинування. Зокрема франківчанка Іванна Кошель для збільшення довіри до вакцинації започаткувала флешмоб #япротикору #явакцинованавідкору.

Умови флешмобу прості:

1. Коротко розповісти про вакцинацію власну чи дітей та яке було самопочуття.

2. При можливості фото картки з календарем вакцинації.

3. Поставити тег #япротикору #явакцинованавідкору

Варто зауважити, що франківські мамусі активно долучаються до флешмобу і розповідають чому вирішили вакцинувати дітей чи себе.

(вгору)

Додаток 7

3.01.2018

В 2018 году прибыль Facebook, Amazon и Google продолжит расти

Екатерина Шпачук

Аналитики Уолл-стрит прогнозируют рост прибыли компаний, которые входят в так называемую группу FANG (Facebook, Amazon, Netflix, и Google), в 2018 году. Об этом сообщает издание Fortune (InternetUA).

По их прогнозам, 2018 год станет успешным для этих компаний и ряда других технологических гигантов, которые делают ставку на электронную коммерцию, онлайн-видео, интернет-рекламу и приложения для смартфонов.

«Как мы видим, группа FANG будет в лидерах в 2018 году вместе с PayPal и Shopify. Конечно, через год все может поменяться. Но в ближайшем будущем у Amazon, PayPal, Netflix, Shopify, Google и Facebook будут хорошие показатели», – считает аналитик Джеймс Чакмак из Monness, Crespi, Hardt & Co.

Отмечается, что акции Facebook выросли, поскольку крупнейшая в мире социальная сеть продолжала увеличивать доходы от рекламы. Компания еще не обнародовала данные за четвертый квартал, но доход Facebook в размере 27,7 млрд долларов за девять месяцев 2017 года уже показал рост на 47 %. Чистая прибыль выросла на 76 % – до 11,7 млрд долларов.

«С финансовой точки зрения у Facebook очень «здоровые показатели», несмотря на увеличение расходов. Между тем, Instagram вместе с Messenger и WhatsApp продолжают дышать в спину», – отметил Чакмак.

Компания Amazon обеспечила себе фундамент в физическом мире, купив сеть супермаркетов Whole Foods. Продажи компании выросли на 27 % до 117 млрд долларов за первые девять месяцев 2017 года, в то время как чистая прибыль снизилась на 27 % до 1,2 млрд. долларов.

Компания Netflix потратила в 2017 году около 6 млрд долларов на производство оригинального контента. Это было не зря, Netflix взяла несколько статуэток престижной премии Emmy за свои сериалы – «Очень странные дела», «Корона» и «Карточный домик». Доход компании за первые девять месяцев 2017 года увеличился на 32 % до 8,4 млрд долларов. Аналитик Wells Fargo Кен Сена считает, что акции Netflix могут вырасти еще на 15 %. Компания инвестирует в собственный контент, в том числе кино.

«Ожидается, что производство фильмов и сериалов в следующем году должно способствовать дальнейшему укреплению позиций Netflix среди подписчиков», – пишет Сена.

Google в прошлом году столкнулась с рядом разногласий, но тем не менее финансовые результаты компании по-прежнему выглядели убедительными. Доход Google вырос на 22 % и составил 78,5 млрд долларов, а чистая прибыль увеличилась на 11 %, достигнув 15,7 млрд долларов.

«В 2018 году Google продолжит занимать лидерские позиции по мобильному поиску и YouTube. Сейчас у них слишком мало конкурентов, которые бы смогли повлиять на ситуацию на этом рынке», – отмечает Чакмак.

Несмотря на внушающие результаты компаний группы FANG, были компании, которые показали более значительный рост. Так, акции компании Micron Technology (производит чипы памяти) выросли на 88 %, PayPal – на 87 %, а производителя графических карт Nvidia на 81 %.

Худшие результаты в 2017 году показали компании Hewlett-Packard Enterprise (акции упали на 38 %), Xerox с падением на 17 % и Western Union – на 13 %.

(вгору)

Додаток 8

9.12.2018
Олег Дмитренко
Telegram випустить власну криптовалюту

Месенджер Telegram планує створити власну блокчейн-платформу і криптовалюту. Платформа отримає назву Telegram Open Network (TON), а криптовалюта буде називатися Gram – пише techCrunch (Watcher).

Для випуску власної криптовалюти компанія проведе ICO (Initial Coin Offering, первинне розміщення монет криптовалюти або токенів – записів в реєстрі блоків транзакцій, які можуть підтверджувати наявність у їх власника

прав на певні об’єкти). Telegram планує залучити $500 млн на перепродажі токенів, тобто в рамках всього ICO компанія може залучити від $3 млрд до $5 млрд.

За даними TechCrunch, блокчейн-платформа TON дозволить убезпечити всі платежі між користувачами Telegram, який себе позиціонує як захищений месенджер, і децентралізована блокчейн-платформа дозволить убезпечити всі операції між користувачами, як всередині, так і ззовні, включаючи уряди різних країн, які борються з Telegram через питання приватності, відзначає TechCrunch.

Крім віртуальних валют користувачі також зможуть через свій електронний гаманець в Telegram переводити і звичайні гроші. Електронний гаманець може бути запущений в четвертому кварталі 2018 року. Також планується, що через платформу зможуть працювати сервіси від сторонніх розробників і боти – для цього у другому кварталі 2019 року буде запущений TON Services.

У white paper вказано, що для продажу інвесторам буде доступно 44 % валюти Gram. Ще 4 % залишиться у власності команди Telegram на чотири роки. При цьому наголошується, що щонайменше 52 % всієї видобутої криптовалюти залишиться у компанії, щоб уникнути спекуляцій.

Деталі майбутнього ICO наведені і в презентації в каналі «Телеграм-маркетинг». У цьому документі йдеться про те, що закритий пресейл токенів може відбутися в січні, а основне ICO – в березні цього року. Залучені кошти планується використовувати для розвитку Telegram і TON. У цій презентації наголошується, що в додаток Telegram будуть вбудовані криптогаманці TON, завдяки чому мільйони користувачів зможуть безпечно зберігати свої кошти в блокчейні. Доступ до цього гаманця буде зберігатися в режимі наскрізного шифрування за допомогою ключа, який буде відомий тільки власнику гаманця.

У недавньому інтерв’ю агентству Bloomberg Дуров назвав біткоіни «цифровим золотом» і заявив, що близько чотирьох років тому купив 2 тис біткоінів за ціною $750 за «монету». Загальний обсяг інвестицій склав $ 1,5 млн. У грудні вартість криптовалютного портфеля підприємця перевищувала $ 35 млн.

(вгору)

Додаток 9

16.01.2018

В Британии разрешили платежи через мессенджеры

Начиная с 13 января 2018 года девять крупнейших банков Великобритании, обслуживающие основную часть населения, больше не смогут блокировать финансовые операции сторонних компаний. Фактически это означает разрешение платежей через Facebook Messenger, Google Wallet и их аналогов, пишет Quartz (InternetUA).

Новые правила, получившие название Open Banking, вынуждают крупные банки – Allied Irish Bank, Bank of Ireland, Barclays, Danske, HSBC, Lloyds, Nationwide, RBS и Santander – внедрять API-интерфейсы, которые стандартизируют безопасный допуск к данным клиентов с их согласия.

Новые правила дают полную свободу для развития платежных продуктов Facebook и Google, которые уже не первый год хотят войти в банковское дело, фактически не становясь банками. Раньше им нужно было вести переговоры напрямую с каждым из банков, чтобы получить доступ к данным учетной записи пользователя. Стартапам, не имеющим таких ресурсов, приходилось каждый раз запрашивать у пользователей логин и пароль, а затем отправлять их на сайт банка для проведения оплаты. Все это затрудняло «быстрые платежи» через приложения, которые широко используются в США и Китае.

Быстрые платежи позволяют оплатить свою часть счета в кафе, просто отправив сообщение вида «$15» в мессенджере Facebook или по электронной почте, используя Google Wallet. «В следующий раз, когда вам нужно будет отправить другу деньги, то вместо того, чтобы открыть свое скучное банковское приложение, возиться с поиском банковских реквизитов, а затем несколько раз подтверждать оплату, вы просто наберете „+10 фунтов“ в WhatsApp», – говорит финансовый консультант Дэвид Берч.

Использование быстрых платежей также означает, что когда вы покупаете что-то на сайте Amazon, продавцу не придется обращаться к третьей стороне для связи с Visa или Mastercard для проведения платежа. Этот платеж спишется непосредственно с вашего банковского счета.

С введением новых правил транзакции через чаты будут использоваться в Великобритании так же свободно, как в США, где пользователи так оплачивают поездки и покупают товары в обычных магазинах, пишет издание.

(вгору)

Додаток 10

3.01.2018

Желание на Новый год: социальные сети по-лучше – Bloomberg

Компаниям пора задуматься, чтобы сделать свои сайты менее «эксплуататорскими» и вредными для пользователей (Зеркало недели. Украина).

Соцсети должны стать более человечными.

Для бизнеса социальных сетей новый год стал очередным мрачным вестником. Кажется, каждый день пионеры сферы выражают сожаление и предостережения, извиняются за технологию, которая развивается стремительными темпами.

Один из бывших исполнительных директоров Facebook Inc Шамат Пализапития недавно сказал, что сеть «разрывает социальное полотно». Бывший инженер компании предупредил о надвигающейся «дистопии». Другой

ветеран признал, что компания «использует уязвимости человеческой психологии».

Об этом пишет в редакционной статье Bloomberg, добавляя, что в Кремниевой долине инсайдеры в последнее время говорят об аналогичных беспокойствах, а также о страхах, что бизнес-модель социальных сетей может подорвать благосостояние пользователей. И все больше исследователей предполагают, что эти страхи, вероятно, оправданы.

Среди молодежи социальные сети, возможно, играют определенную роль в росте уровня распространения депрессий и самоубийств. Похоже, они стали одной из причин возникновения чувства зависти, тревоги и неполноценности.

«Кроме того, они способствуют снижению самооценки, нарушают сон, вредят обучению и поощряют антисоциальное поведение. Около двух третей детей теперь говорят, что они бы были не против, если бы соцсетей не существовало вовсе», – пишет издание.

Проблема в том, что отказаться от использования соцсетей трудно. Вооружившись большими запасами данных, компании придумали хитрые способы удерживать пользователей на своих сайтах. Они развили мощные инструменты, такие как пуш-уведомления, «лайки», автовоспроизведение видео, которые эксплуатируют выверты человеческой психологии для создания чего-то подобного к зависимости.

«Суммируйте все это и неприятная правда всплывет: людей вовлекли в потребление продукта, который заставляет их чувствовать себя кошмарно. Ряд решений для этой дилеммы уже обсуждался. Попробуйте “электронные детоксикаторы”»,– говорят одни. Разработайте новую этику и стандарты для дизайнеров программного обеспечения, – говорят другие. Используйте Facebook больше, – говорит Facebook. В конце концов, именно бизнес социальных сетей может сделать свои продукты более человечными и менее эксплуататорскими», – говорится в статье.

Ранее издание Washington Post писало, что социальные сети изменили суть войны. Современные войны ведутся не только за территории, но и за то, как люди воспринимают события, которые с ними происходят. И часто это восприятие становится решающим.

В свою очередь, издание The Economist писало, что социальные сети могут угрожать демократии. Любой, кто листал Facebook, знает, что вместо того, чтобы распространять мудрость, система подбирает контент, который только усиливает человеческие иллюзии и предубеждения. Это еще больше ухудшает политику презрения, которая продолжается в США, по меньшей мере, с 1990-х годов. Поскольку различные стороны видят разные факты, в них нет никакой эмпирической базы для того, чтобы достичь компромисса. Из-за того, что люди погрязли в воронке мелочности, скандальности и возмущения, они утратили видение того, что важно для общества, в котором они все живут. Это может дискредитировать компромиссы и тонкости либеральной демократии.

(вгору)

Додаток 11

13.01.2018

Роман Черный

Почему Билл Гейтс и Стив Джобс ограждали своих детей от технологий

В последнее время психологи все чаще твердят, что смартфоны и соцсети могут быть опасными для психического здоровья подрастающего поколения. Исследование, проведенное учеными Университета Сан-Диего, показало, что восьмиклассники, проводящие много времени в социальных сетях, страдают от депрессии на 27 % чаще своих сверстников, менее увлеченных интернетом. Дети, которые используют смартфон более трех часов в день, более склонны к суициду. Свежая статистика показывает, что количество подростковых самоубийств в США превысило количество убийств, совершенных несовершеннолетними. И ученые уверены, что именно смартфоны являются движущей силой этих изменений (IGate).

Впрочем, некоторые исследователи не видят в этой информации ничего нового. Недавно в свет вышла книга Джо Клемента и Мэтта Майлза «Школьники у экрана: два учителя-ветерана объясняют, как злоупотребление технологиями делает наших детей глупее». В ней авторы утверждают, что людям следовало насторожиться еще десять лет назад.

По наблюдениям Клемента и Майлза, Билл Гейтс и Стив Джобс, ключевые фигуры мира технологий, всячески ограждали своих детей от собственных технологий. «Что такого знают эти технологические гиганты о своих разработках, что не известно простым потребителям?», – задаются вопросом исследователи. Ответ, по их мнению, заключается в гипнотической силе цифровых технологий.

Лимит «экранного» времени

В 2007 году Билл Гейтс, бывший генеральный директор Microsoft, установил для своей дочери лимит времени нахождения у монитора, когда у нее развилась нездоровая зависимость от видеоигр. Также он не позволял своим детям пользоваться мобильными телефонами, пока им не исполнилось 14 лет. Сегодня же первый мобильный телефон появляется у ребенка в возрасте примерно десяти лет.

Стив Джобс, бывший генеральный директор Apple, признавался, что не позволял своим детям пользоваться iPad. «Мы стараемся предельно ограничивать использование технологий у себя дома», – говорил он.

В книге «Школьники у экрана» Клемент и Майлз утверждают, что наиболее влиятельные персоны Кремниевой долины всерьез воспринимают потенциальную опасность смартфонов, планшетов и компьютеров, хотя сами же часто зарабатывают на жизнь, создавая подобные технологии. «Интересно думать, что в современной школе, где ученики должны использовать

электронные устройства, такие как iPad, дети Стива Джобса были бы одними из немногих, кто бы от этого отказался», – пишут исследователи.

Дети Джобса уже закончили школу, так что остается только гадать, как бы отреагировал на современные образовательные технологии основатель Apple. Но Клемент и Майлз полагают, что если бы сегодня Дети Джобса ходили в среднестатистическую американскую школу, они бы пользовались технологиями в классе намного чаще, чем дома.

Впрочем, это справедливо только для общеобразовательных школ. Во многих профильных учебных заведениях дела обстоят иначе. К примеру, частная Вальдорфская школа в Кремниевой долине использует подчеркнуто низкотехнологичные методы обучения. Там, где в других школах используются планшеты и сенсорные дисплеи, в частных заведениях в ходу меловые доски и карандаши.

Персонализированное обучение

Впрочем, Билл Гейтс не считает, что детей нужно полностью изолировать от технологий. Нужно лишь изменить подход. К примеру, Гейтс неоднократно подчеркивал, что он является сторонником идеи персонализированного образования. По его мнению, технологии могут помочь внедрить такое образование повсеместно.

В посте в своем блоге Гейтс рассказал об одной из школ в Сиэтле, которая работает над постановкой индивидуальных целей для каждого конкретного ученика. Если ученик запланировал поступление в конкретный колледж, школа предлагает ему индивидуальную учебную программу и подробный план действий для поступления. Учителя в этом случае выступают в роли тренеров, которые натаскивают подопечных на конкретный результат.

По словам Гейтса, технологии в таких условиях используются адресно. Они применяются для развития ученика, а не для его развлечения. «Персонализированное обучение не станет панацеей, но именно этот подход поможет многим молодым людям использовать свои таланты максимально эффективно», – пишет Гейтс.

(вгору)

Додаток 12

13.01.2018

Смартфон делает тебя глупым, замкнутым и больным. Почему бы не отложить его в сторону?

Михаил Сапитон

Про вред смартфонов трубит каждое второе исследование – однако журналист канадского издания The Globe and Mail Эрик Эндрю-Ги постарался сложить из этого максимально полную картину. Оказалось, что зависимость от «синих экранов» наносит по-настоящему комплексный вред: под угрозой память, когнитивные способности и отношения. Редакция AIN.UA приводит сокращенный перевод материала (AIN.UA).

Для начала Эндрю-Ги вспоминает о пророческой шутке из британского журнала Punch. Под заголовком «Предсказание на 1907» издание выпустило карикатуру, изображающую состоятельную пару, которая сидела в парке и пользовались подобием телеграфа. Публикация отсылала к трагическим событиям 1906 года – тогда Сан-Франциско пострадал от сильнейшего землетрясения, а сигнал SOS получил международный статус. Подпись сообщала: «Эти двое не общаются между собой. Леди получает любовное послание, а джентльмен – результаты гонок».

Автор подмечает, что столетие спустя Стив Джобс подарил миру iPhone – и теперь гротескная карикатура похожа на реальность. Смартфоны появились у двух миллиардов людей по всему миру.

И они меняют то, как мы делаем множество вещей, от съемки фото до заказа такси. Но смартфоны также изменили нас: нашу натуру на самом базовом уровне, заново сформировали наш образ мышления и взаимодействия с миром.

Журналист уверен, что несмотря на все сопутствующие удобства, пора уже признать – смартфоны также наносят вред. Это подтверждают многочисленные исследования, проведенные психиатрами, неврологами, экспертами в области здравоохранения. Они предупреждают: смартфоны по-настоящему вредят уму и телу. Мы не можем удержать внимание дольше нескольких секунд, ухудшаются когнитивные способности, смещается баланс между работой и жизнью, мы уделяем меньше времени семье.

Помимо того, что гаджеты сделали нас забывчивыми, беспокойными и заставили игнорировать близких, они еще и вызывают привыкание. Для иллюстрации Эндрю-Ги приводит результаты опроса после первых пяти лет «эры смартфонов»: 28 % опрошенных говорили, что интернет уменьшает количество времени, проведенного с семьей. Изначально таких было всего 11%. Сегодня «пострадавших» оказалось бы намного больше.

При этом нигде проблему не воспринимают так серьезно, как в Калифорнии. Бывшие сотрудники Google, Apple и Facebook начали подымать тревогу.

Крис Марселлино, который помог Apple разработать пуш-уведомления, рассказал The Guardian, что по результатам скана мозговой активности использование смартфонов можно сравнить с азартными играми и употреблением наркотиков. Шон Паркер, экс-президент Facebook, недавно признался, что крупнейшая социальная сеть была разработана так, чтобы стимулировать пользователя «дофаминовыми инъекциями». Признание в ощущении собственной вины высказал и Чамат Палихапитиа, бывший старший президент по росту пользовательской базы в Facebook.

Главным глашатаем оказался бывший звездный продакт менеджер Google Тристан Харрис. Последние несколько лет он рассказывает людям о том, что они должны тратить меньше времени на технологии. Также Харрис основал неприбыльную организацию Time Well Spent. К нему прислушиваются и политики. В прошлом сентябре, на Global Progress Summit с Харрисом

встретился канадский премьер-министр Джастин Трюдо. Тем временем уже этой осенью Франция планирует запретить сотовые телефоны в начальных и средних школах.

Обеспокоены и бизнесмены. В недавнем блог-посте Дэн Никсон, аналитик Банка Англии, отметил, что у сотрудников уходит 25 минут на то, чтобы вновь сфокусироваться на задаче после раздражителя вроде электронного письма.

Люди всегда были обеспокоены подъемом новых технологий. Сократ полагал, что письменность перемелет мозги юных афинян, подрывая их способность к запоминанию. Эразм проклинал «рой новых книг», захвативших Европу эпохи Гутенберга. Во времена зарождения телевидения его называли «выжженной пустошью».

Однако Харрис говорит, что в этот раз все иначе – в отличие от телевизоров или десктопных ПК, смартфоны преследуют нас повсюду. Кроме того, они знают нас и пользуются возможностями алгоритмов, чтобы подольше удерживать внимание. По мнению Эндрю-Ги, в такой нездоровой ситуации нет ничего удивительного – большинство сайтов не берут денег за доступ, поэтому в интернете все платят вниманием. Чем больше времени вы тратите на Google и Facebook, тем больше они могут заработать на рекламодателях.

Согласно некоторым оценкам, среднестатистический человек поглядывает на смартфон более 150 раз за день и вдвое больше, чем он предполагает сам. В Северной Америке средняя продолжительность использования смартфона от трех до пяти часов. По итогу всей жизни, большинство проведет около семи лет наедине с экраном.

Таких успехов технологическим компаниям удалось добиться благодаря использованию естественных человеческих слабостей. Одна из них называется «эффектом новизны» – именно благодаря ему соцмедиа так налегают на нотификации, а Facebook сменил их цвет с нейтрального синего не тревожный красный.

Создатели приложений справедливо уверены, что заинтересованность людей в уведомлениях спровоцирована неуверенностью и желанием получать позитивный фидбек. Особенно активно это эксплуатирует Instagram – разработчик Мэтт Мэйбери говорит, что все в Долине знают о манипуляциях соцсети с показом лайков.

Если Instagram решает, что вам следует больше пользоваться сервисом, то сначала покажет лишь малую долю лайков на определенной публикации, в надежде, что вы расстроитесь и вернетесь через пару минут.

Однако есть и менее очевидные уловки. Одна из них – установленный профессором Скиннером принцип «переменчивых наград». Если подопытные менее уверены в успешном получении награды после реакции на раздражитель, то будут совершать больше попыток, чем при предсказуемом раскладе. Это стоит за работой алгоритмической ленты Facebook или привычкой без конца проверять почту.

Эндрю-Ги вновь обращается к истории первого iPhone – и отмечает важность экрана в «седативном» эффекте смартфона. Стив Джобс особенно настаивал на увеличении его размера – последние изменения в конструкцию внесли за несколько недель до первой демонстрации. И теперь мы начинаем ощущать последствия такого решения. Согласно результатам исследования канадского подразделения Microsoft, средний период концентрации человеческого внимания между 2000 и 2013 годами упал с 12 до 8 секунд. Профессор Джон Райти и вовсе проводит параллели между состоянием активных пользователей смартфонов и людей, страдающих синдромом дефицита внимания – его домыслы также подтверждает исследование, проведенное в Китае при участии 7000 студентов.

Растет и количество данных вокруг. В 2007 году среднестатистический американец через телевидение, переписку и интернет поглощал столько информации, что она бы поместилась на 174 газетах – и это было впятеро больше, чем за два десятилетия до того. Сегодняшние показатели только выросли. Мозг больше не в силах различать важные и неважные сведения, из-за чего мы отвлекаемся на мелочи вроде уведомлений на экране iPhone.

Более того, даже попытки контролировать использование смартфона сказываются на мышлении. Это проверили в Техасском университете, где попросили три группы отложить смартфоны и пройти интеллектуальные тесты – чем ближе находился девайс, тем сильнее ухудшались результаты. Наконец, в числе опасных проблем Эндрю-Ги называет и чувство отчужденности – особенно между родителями и детьми. Ученые даже исследуют последствия текстинга женщин во время грудного кормления – ведь зрительный контакт матери с ребенком важен для развития младенца.

Впрочем, проблемы возникают и в более позднем возрасте: по результатам опроса Гарвардской медицинской школы, среди 1000 детей в возрасте от 4 до 18 лет, множество заявили, что не идут с порога поприветствовать родителей – взрослые слишком заняты смартфонами. У этих жалоб есть реальные последствия: с 2006 по 2011 среднее количество совместно проведенного времени в американских семьях упало на треть, с 26 до 18 часов. Возможна даже связь с детскими травмами: их количество в период между 2007 и 2010 годами возросло на 12 % после длительного периода спада. Это можно списать на плохие времена для американской экономики, но статистика совпадает и с временем подъема iPhone.

Однако идет и обратный процесс – в обществе и культуре постепенно распространяются мысли о вреде гаджетов. В качестве примера Эндрю-Ги приводит скетчи Уилла Фаррела, созданные в рамках компании #DeviceFreeDinner. В них комик играет пристрастившегося к смартфону отца, которого пытается вразумить его семейство. Тем временем в Калифорнии на месте бывших отелей хиппи возникают восстановительные кемпы «без подключений».

Но технологических скептиков вроде Тристана Харриса это не утешает – проблемы актуальны еще для миллиардов людей. Он воображает, что когда-

нибудь Facebook будет доставлять все нотификации единожды в день: как по почте. Другие полагают, что технологическим компаниям пора задуматься о защите внимания пользователей – и платить им будут по двойному тарифу.

Проблема в реформировании этих продуктов, конечно, такова – их нынешние версии слишком удивительны, забавны в использовании и удобны. Вот почему они так аддиктивны. Однако урок, который мы начинаем изучать, заключает в том, что это не безвредные орудия. Пока они используются как сейчас, то останавливают нас от улучшения самих себя.

Проблема лишь в том, что мы можем вовремя этого не осознать.

(вгору)

Додаток 13

2.01.2018

Хакерские атаки 2018 года возглавит искусственный интеллект

Искусственный интеллект эволюционирует все быстрее и уже в 2018 году станет опасным оружием в руках хакеров. Он научится адаптироваться и взламывать защитные системы, перехватывать контроль над голосовыми помощниками и даже выдавать себя за человека (InternetUA).

Летом 2016 семь команд хакеров прибыли в Лас-Вегас, чтобы принять участие в Cyber Grand Challenge, мероприятии, в котором одни автоматические системы соревновались, взламывая другие. Победителем стала машина под названием Mayhem, которая теперь выставлена в Национальном музее американской истории в Вашингтоне как первое нечеловеческое «существо», занявшее первое место в престижном конкурсе хакеров.

В 2017 году Mayem не смог повторить свой подвиг и проиграл команде людей. По всей видимости, машине не хватило творческого подхода, интуиции и мотивации. Но в 2018 году все изменится. Прогресс в теории и практике искусственного интеллекта, а также прорывы в кибербезопасности указывают на то, что алгоритмы машинного обучения станут ключевыми элементами киберзащиты и кибератаки.

Большинство специалистов по информационной безопасности (62 %, согласно опросу компании Cylance), считают, что хакеры станут использовать ИИ как кибероружие уже в 2018 году. На Defcon 2017 датолог из Endgame (фирмы-распространителя систем безопасности) продемонстрировал работу автоматизированной программы, которая изучила среду OpenAI Gym и научилась прятать вредоносный файл от антивирусов. Еще несколько подобных инструментов и инноваций – и будет несложно представить себе, как ИИ поднимается еще на одну ступеньку вверх по эволюционной лестнице и создает системы, способные адаптироваться, выискивать компьютерные уязвимости и использовать их во вред человеку, пишет Wired UK.

Такой ИИ сможет выдавать себя за дружественную человеку систему, например, голосового помощника, который составляет наше расписание, проверяет нашу почту и управляет нашим умным домом. Но что если его

подменит вредоносный ИИ? И что если он станет настолько развитым, что сможет выдать себя за человека, которому вы доверяете, например, подделав его голос по телефону, манеру изложения мыслей в письменном сообщении или цифровую подпись на документе?

(вгору)

Додаток 14

2.01.2018

Недобросовестные сотрудники угрожают кибербезопасности компании

Многие сотрудники офисов используют доступ в интернет на работе в личных целях, что может стать угрозой для кибербезопасности целой компании. Подчиненные могут посещать сомнительные и даже опасные веб-сайты с рабочих компьютеров и не подозревать, что открывают хакерам доступ к корпоративной сети и информации, содержащейся в ней (InternetUA).

Согласно результатам недавно проведенного исследования, почти половина офисных сотрудников выходят в интернет с рабочих мест по своим личным делам. Фактически, это снижает их производительность труда, поскольку на такой веб-серфинг ежедневно тратится в районе 2 часов рабочего времени, но, помимо этого, недобросовестные коллеги добавляют работы IT-отделу или системному администратору. Опасность для компании заключается в первую очередь в посещении сотрудниками зараженных сайтов и скачивании им программ сомнительного качества с ресурсов, доверия тоже не вызывающих. В итоге работа офиса может застопориться, к примеру, из-за вируса, пойманного одним из сотрудников и успешно распространившегося по сети.

Подобное поведение сотрудников офисов прослеживается во многих странах мира, и мотивация у сотрудников всегда одна: компьютер им не принадлежит, и в случае возникновения той или иной ситуации системный администратор все поправит. Все это на руку кибер-преступникам, использующим подобную халатность в своих целях для кражи, в первую очередь, информации, которая может оказаться весьма чувствительной. Владельцы компаний и IT-отделы все чаще сталкиваются с ситуацией, когда простых мер по фильтрации контента становится недостаточно. Профессий, связанных с ежедневным использованием Сети, становится все больше, и запрет на доступ к нему перестает быть лекарством от всех бед. Эксперты видят два способа выхода из подобной ситуации: среди сотрудников можно проводить тренинги и ликбезы с наглядной демонстрацией последствий необдуманного веб-серфинга, но этот путь выбирают не все. Второй вариант – это переход на концепцию BYOD или Bring Your Own Device, когда сотрудник работает в офисе на собственном ПК или ноутбуке, принесенном из дома и просто подключенным к корпоративной сети. В этом случае, согласно

статистике, работники намного более ответственно подходят к использованию Всемирной Паутины.

(вгору)

Додаток 15

3.01.2018

Эксплойт для 0-day в роутерах Huawei вышел в люди

Код эксплойта, который использовался для загрузки IoT-ботов Satori на роутеры производства Huawei, стал достоянием общественности. Эксперты предупреждают, что злоумышленники не преминут воспользоваться публикацией для построения новых ботнетов с целью проведения DDoS-атак (Центр информационной безопасности).

Вредоносный код, выложенный в открытый доступ на Pastebin.com, обнаружил Анкит Анубхав (Ankit Anubhav) из NewSky Security. Исследователь идентифицировал свою находку как эксплойт к CVE-2017-17215, который использовался для распространения модификации IoT-зловреда Mirai, известной как Satori и Mirai Okiru, и построения многотысячной бот-сети, центры управления которой были недавно отключены.

«Код попал в общий доступ, и это означает, что его теперь начнут использовать другие злоумышленники, – комментирует Майя Горовиц (Maya Horowitz), руководитель подразделения Check Point по исследованию интернет-угроз. – Можно предположить, что этот эксплойт будет поставлен на коммерческую основу и IoT-ботнеты, пытающиеся использовать разные уязвимости, начнут добавлять CVE-2017-17215 в свой арсенал».

Брешь нулевого дня CVE-2017-17215 в домашних роутерах HG532 от Huawei исследователи из Check Point идентифицировали в конце ноября. Вендор уже выпустил соответствующие обновления, отметив, что данную уязвимость можно эксплуатировать удаленно посредством подачи на порт 37215 вредоносных пакетов для внедрения команд, влекущих исполнение произвольного кода.

«Этот код стал известен сообществу “черных” хакеров, – пишет Анубхав в блоге NewSky. – Теперь его, как и прочие SOAP-эксплойты, слитые для безвозмездного пользования, начнут осваивать разные скрипт-кидди и киберпреступники».

Исследователь также отметил, что, по данным NewSky, эксплойт к CVE-2017-17215 реализован не только в Satori, но и в другом зловреде, ориентированном на IoT-устройства, – Brickerbot. «Этот эксплойт-код уже использовали два известных IoT-ботнета – Brickerbot и Satori, а теперь, когда он стал общедоступным, его начнут внедрять и в другие боты», – сетует Анубхав.

«Следует отметить, что эти роутеры [Huawei HG532] используются в основном в домашних сетях, владельцы которых не имеют обыкновения регистрироваться для входа в интерфейс и не всегда обладают специальными знаниями, – предупреждает Горовиц. – По этой причине стоит ожидать, что

многие из таких устройств сохранят уязвимость. Производителям IoT-устройств давно пора понять, что обеспечение безопасности имеет первостепенное значение и эту ответственность нельзя перекладывать на плечи пользователей».

(вгору)

Додаток 16

3.01.2018

Злоумышленники используют пиратское ПО для скрытого майнинга

Эксперты «Лаборатории Касперского» обнаружили скрытый майнер NiceHash в пиратских дистрибутивах популярных программ. Список продуктов включает как платные Adobe FineReader, Outlook, PowerPoint, так и свободное ПО вроде OpenOffice. В каждом из них исследователи нашли программную закладку для майнинга криптовалют (Центр информационной безопасности).

Злоумышленники распространяют зараженные файлы через множество одинаковых сайтов, которые различаются только названием продвигаемого ПО: abby-finereader.ru, thecoreldraw.ru, thevisio.ru. После установки пользователь действительно получает взломанный продукт, который зачастую можно найти и на торрент-площадках. Если на компьютере нет антивируса, то о скрытом функционале можно догадаться только по снижению производительности ПК.

Разработчики майнеров стараются как можно дольше оставаться незамеченными и максимально использовать ресурсы зараженной машины. К примеру, специальная утилита прячет окно майнера за системный трей, а некоторые установщики распределяют по системе множество ярлыков для запуска вредоноса. В зависимости от модификации майнер может получать данные с удаленного сервера либо работать по вшитой в код инструкции.

Авторы отчета отмечают, что распространенность скрытых майнеров за последние четыре года выросла в 8 раз. Только в первые три квартала 2017 года «Антивирус Касперского» обнаружил такое ПО почти на 1,7 млн машин. К концу года аналитики прогнозируют рост этого показателя до 2 млн компьютеров. Злоумышленники создают для добычи токенов масштабные ботнеты – например, одна из недавно обнаруженных сетей объединяла более 5 тысяч машин, на которых был скрытно установлен легальный продукт Minergate.

Скрытые майнеры подвергают компьютер или мобильный гаджет более серьезным угрозам, чем проблемы с производительностью. Такие программы умеют отключать защитное ПО, отслеживать пользовательскую активность, включая запуск приложений, проникать в автозагрузку и переустанавливаться, если их удаляют. Длительная работа процессора на максимальной загрузке может и физически уничтожить устройство – например, недавний Android-троян Loapi может всего за два дня вывести из строя аккумулятор смартфона.

Аналитики «Лаборатории Касперского» посвятили отдельный дайджест угрозам для криптовалют в 2018 году. В материале отмечается, что эпидемии

зловредов-вымогателей повышают спрос на цифровые деньги, а развитие майнеров в свою очередь будет подталкивать и шифровальщики. В грядущем году можно ожидать усиление целевых атак на крупные организации –попытки использовать корпоративные мощности предпринимались уже и в России.

Веб-майнинг в скором будущем может стать популярным источником прибыли как для владельцев ресурса, так и злоумышленников, которые будут пытаться незаметно встроить скрипт на сайт. Так, с недавнего времени активным атакам подвергаются сайты на базе WordPress – злоумышленники пытаются скомпрометировать веб-сервер и установить добытчик валюты Monero.

Тем временем суды уже начали выносить первые приговоры по делам о скрытой установке таких программ. В законодательстве пока нет специальной статьи, оговаривающей наказание за это преступление, поэтому мошенники получают срок за взлом информационных систем. Если же майнингом на корпоративных ресурсах решит заняться собственный сотрудник компании, например системный администратор, то его могут обвинить только в краже электроэнергии.

(вгору)

Додаток 17

8.01.2018

Секретная настройка в Google Chrome спасает от всех видов угроз

В самом начале этого года компания Intel объявила о том, что ее сотрудники обнаружили критический дефект во всех фирменных процессорах. Позже выяснилось, что встретить уязвимость можно даже в ARM-процессорах, которые установлены во все современные смартфоны и планшеты (Украинский телекоммуникационный портал).

Благодаря этой бреши в системе защиты, любое вредоносное ПО может получить доступ к ядру процессора в обход любых ограничений. Оно хранит секретную информацию, включающую в себя логины и пароли. Сегодня компания Google сообщила о том, что секретная настройка в веб-браузере Chrome спасает от всех видов угроз, в том числе и от уязвимостей Meltdown и Spectre, которые представляют из себя критический дефект в процессорах, установленных практически в 99 % электронных устройств.

Речь идет о секретной функции под названием «Strict Site Isolation». Она позволяет обрабатывать каждую страницу в сети Интернет в отдельности от всех остальных, за счет чего достигается изоляцию от вредоносного ПО.

Активировать секретную настройку в Google Chrome очень просто. Достаточно запустить интернет-обозреватель, после чего в адресной строке ввести фразу chrome://flags/#enable-site-per-process. Должно открыться секретное меню со списком скрытых от рядовых пользователей настроек. Необходимо найти пункт «Strict Site Isolation», после чего нажать на кнопку

«Включить». Затем следует нажать на кнопку «Перезапустить» в нижнем правом углу.

После включения функции «Strict Site Isolation» каждая вкладка в браузере Chrome будет представлять из себя изолированный процесс, в результате чего вредоносное программное обеспечение ни при каком раскладке не сможет попасть на компьютер. Компания Google сообщает, что это экспериментальная настройка, поэтому она может работать не совсем корректно.Кроме того, стоит учитывать, что включение этой опции приведет к тому, что на работу с браузеров будет уходить приблизительно на 20-25% больше ресурсов компьютера, поскольку процессору придется обрабатывать больше процессов со всеми дополнениями для их работы. На компьютере с небольшим объемом оперативной памяти функцию «Strict Site Isolation» лучше не включать, так как она значительно увеличивает расход ОЗУ при работе со вкладками.

(вгору)

Додаток 18

10.01.2018

Чтобы закрыть фундаментальную «дыру» в Wi-Fi по всему миру, создается новый протокол WPA3

Wi-Fi Alliance готовит новый стандарт безопасности Wi-Fi-соединений WPA3, который должен будет прийти на смену уязвимому протоколу WPA2 (InternetUA).

Уязвимость как повод для разработки нового стандарта Wi-Fi Alliance, отраслевая группа, ответственная за стандартизацию беспроводных сетевых соединений, анонсировала выпуск нового протокола шифрования – WPA3. Этот шаг предпринят после того, как осенью 2017 г. в протоколе WPA2, используемом в миллиардах устройств по всему миру, была обнаружена критическая уязвимость, получившая название KRACK.

Уязвимость позволяет хакеру перехватывать трафик, проходящий между точкой доступа Wi-Fi и подключенными к ней устройствами. Свое название эта брешь получила от эксплуатирующей ее атаки – Key Reinstallation Attacks, «атаки переустановки ключей».

Четыре функции

Протокол WPA3 должен будет решить ряд проблем, связанных с безопасностью. На данный момент «официальный черновик» WPA3. Его обещают представить ближе к середине 2018 г. Пока же известно, что протокол будет насчитывать четыре новые защитные функции.

Первая позволит заблокировать попытки брутфорса: после нескольких неуспешных попыток залогиниться процесс аутентификации будет заблокирован. Подобные меры давно применяются для защиты веб-приложений от «словарных» атак. Но беспроводные сети до сих пор такой защиты были лишены.

Вторая функция – это возможность использования любого Wi-Fi-устройства в качестве панели настроек для других устройствах. Иными словами, любой смартфон можно будет использовать для того, чтобы настроить располагающиеся в пределах досягаемости IoT-устройства, лишенные собственных экранов, – «умные» замки, осветительные приборы и так далее.

Очевидно, что для этого устройство с экраном должно быть авторизовано для настройки IoT-устройств, но тут возникает вопрос с «заводскими» логинами и паролями и возможностью злоупотребления этой функцией.

Третья функция – «персонализированное шифрование данных» – позволяет шифровать соединения между каждым устройством и роутером (или точкой доступа), в то время как четвертая – это новый криптографический стандарт с 192-битным ключом, аналогичный алгоритму из комплекта CNSA (Commercial National Security Algorithms – Коммерческих алгоритмов для защиты национальной безопасности). Разработкой этого набора занимался Комитет по системам обеспечения национальной безопасности США.

WPA3 должен будет увидеть свет в ближайшие месяцы после принятия чернового варианта, однако пройдет еще какое-то время прежде, чем пользователи смогут купить на открытом рынке устройства с поддержкой WPA3.

Куда больше времени уйдет, прежде чем небезопасные устройства на базе WPA/WPA2 уйдут с рынка.

Последовательность протоколов

WPA – это стандарт сертификации устройств беспроводной связи, заменивший предыдущий протокол того же назначения под названием WEP. По сравнению с другими решениями WPA отличается большей защищенностью данных и усиленным контролем доступа, а также более широкой совместимостью.

WPA2, утвержденный в июне 2004 г., пришел на смену WPA. В нем присутствует протокол шифрования CCMP и шифрование AES, что повышает его безопасность по сравнению с WPA первого поколения. В марте 2006 г. поддержка WPA2 стала стандартом сертификации устройств Wi-Fi. В 2017 г. в нем была найдена фундаментальная уязвимость, поставившая под угрозу беспроводные устройства во всем мире.

Как отметил Мати Ванхеф (Mathy Vanhoef), эксперт по безопасности, который является автором атаки KRACK, стандарты, положенные в основу WPA3, существуют уже длительное время и реализованы на аппаратном уровне, однако слишком редко используются на практике. Теперь, возможно, все изменится, поскольку производители Wi-Fi-устройств будут стремиться получить сертификат совместимости с WPA3 – из коммерческих соображений.

(вгору)

Додаток 19

10.01.2018

Популярнейшие китайские смартфоны заподозрили в шпионаже

Планы Huawei начать продавать свои устройства через американских сотовых операторов терпят крах. Власти США подозревают производителя смартфонов в тесных связях с китайским правительством и, опасаясь шпионажа, оказывают на крупнейшие телекоммуникационные компании страны политическое давление (InternetUA).

Как сообщает со ссылкой на источники The Wall Street Journal, на проходящей в Лас-Вегасе выставке потребительской электроники CES Huawei должна была объявить о партнерстве с одним из крупнейших в США сотовых операторов – AT&T. Однако в последний момент американская компания отказалась продавать через свои салоны смартфоны Huawei.

По данным The Information, это стало результатом политического давления – конгрессмены и сенаторы обратились в Федеральную комиссию по связи AT&T задуматься о возможных рисках в области безопасности. Политики подозревают Huawei в тесных связях с Компартией и спецслужбами Китая и опасаются, что в ее смартфонах могут скрываться шпионские «закладки».

Как пишет AndroidPolice.com, с аналогичными проблемами столкнулся и другой крупнейший сотовый оператор США, Verizon, также ведущий переговоры с Huawei о продаже ее смартфонов.

Формально Huawei, являющаяся третьим производителем смартфонов в мире после Samsung и Apple, смартфоны в США уже продает – через онлайн-магазин. Однако реалии рынка в стране таковы, что 90 % продаж аппаратов происходят через салоны ведущих операторов. Они предлагают клиентам разнообразные гибкие варианты оплаты – например, когда стоимость смартфона «размазывается» в виде ежемесячной добавки к платежам за услуги связи. Если продукция производителя не представлена в операторской рознице, шансов завоевать значительную долю рынка в США у него нет.

Huawei, тем не менее, представила на проходящей в Лас-Вегасе выставке CES2018 ранее анонсированный в Европе Huawei Mate 10 Pro. Как пишет The Verge, в конце презентации глава подразделения потребительских продуктов Huawei Ричард Ю рассказал о срыве соглашения с AT&T и отметил, что это сокращает возможности выбора для американцев. «Это большая потеря для нас, и также для операторов, но еще большая потеря для потребителей, потому что у них не будет наилучшего выбора», – сказал Ю.

Он напомнил, что шесть лет назад, когда уже глобально признанный производитель телеком-оборудования Huawei выходил на рынок смартфонов, ему пришлось завоевывать доверие с нуля. «Мы завоевали доверие китайских операторов, завоевали доверие развивающихся рынков... и также мы завоевали доверие операторов по всему миру, всех операторов в Европе и Японии, – сказал он. – Мы обслуживаем миллионы человек по всем миру. Мы доказали наше [высокое] качество, защиту приватности и безопасность».

(вгору)

Додаток 20

10.01.2018

Малоизвестная функция MS Word может использоваться для кражи паролей

Исследователи из компании Rhino Labs описали новый способ кражи учетных данных Windows с помощью малоизвестной функции MS Word под названием subDoc, позволяющей загружать документ в тело другого документа. Функционал также может применяться для удаленной загрузки subDoc файлов в основной документ, что позволяет проэксплуатировать его во вредоносных целях (InternetUA).

Новая техника основана на классической атаке Pass-the-hash – одном из видов атаки повторного произведения. Она позволяет атакующему авторизоваться на удаленном сервере, аутентификация на котором осуществляется с использованием протокола NTLM или LM. Данный метод может быть использован против любого сервера/сервиса, применяющего протокол аутентификации NTLM или LM, вне зависимости от используемой на компьютере жертвы операционной системы. В системах, использующих протокол аутентификации NTLM, пароли никогда не передаются по каналу связи в открытом виде. Вместо этого они передаются соответствующей системе (такой, как контроллер домена) в виде хешей на этапе ответа в схеме аутентификации Вызов-ответ.

Для осуществления атаки злоумышленники могут сформировать файл Word, загружающий поддокумент с подконтрольного им вредоносного SMB-сервера, перехватить SMB-запросы и получить доступ к NTLM-хешу. В настоящее время существует немало инструментов, позволяющих взломать хеш и извлечь учетные данные. Владея этой информацией, атакующие могут получить доступ к компьютеру или компьютерной сети жертвы под видом оригинального пользователя. Данный вид атаки эффективен для целевых фишинговых кампаний, направленных на высокозначимые объекты, такие как предприятия или государственные учреждения, указывают эксперты.

По словам экспертов, на данный момент описанный ими метод атаки не является широкоизвестным, поэтому антивирусные решения не распознают его. Исследователи разместили на GitHub инструмент под названием SubDoc Injector, позволяющий создавать вредоносные документы Word. Данный инструмент позволит системным администраторам и специалистам в области безопасности провести собственное тестирование.

(вгору)

Додаток 21

11.01.2018

В пакете Dell EMC Data Protection Suite обнаружены серьезные уязвимости

Исследователи безопасности из компании Digital Defense обнаружили в пакете программ для защиты данных Dell EMC Data Protection Suite несколько серьезных уязвимостей, позволяющих злоумышленнику получить контроль над системой. Об этом сообщило издание ZDNet (InternetUA).

Специалисты выявили три уязвимости, затрагивающие Avamar Installation Manager (AVI) – общий компонент, используемый в пакете программ. Злоумышленник может скомпрометировать уязвимую систему путем эксплуатации данных проблем и изменения файлов конфигурации.

Первая уязвимость CVE-2017-15548 позволяет обойти аутентификацию в сервисе SecurityService. Аутентификация пользователя выполняется через запрос POST, включающий в себя имя пользователя, пароль и параметр wsUrl. Данный параметр может быть произвольным, что дает злоумышленникам возможность самим генерировать действительные запросы протокола обмена сообщениями SOAP. По словам исследователей, данная проблема может быть удаленно проэксплуатирована для обхода аутентификации и получения прав администратора.

Вторая уязвимость CVE-2017-15549 представляет собой проблему произвольного доступа к файлу, позволяющую аутентифицированным пользователям загружать произвольные файлы с правами суперпользователя. Проблема возникает в связи с тем, что метод getFileContents класса UserInputService не выполняет проверку параметра имени файла перед его извлечением с сервера Avamar.

Третья уязвимость CVE-2017-15550 позволяет авторизованным пользователям загружать произвольные файлы в произвольные локации с правами суперпользователя. В сочетании с двумя предыдущими уязвимостями данная проблема может позволить злоумышленнику получить полный контроль над системой.

«При совместной эксплуатации трех уязвимостей можно полностью скомпрометировать виртуальное устройство путем изменения файла sshd_config для предоставления прав суперпользователя, загрузки нового файла authorized_keys и web-оболочки для перезапуска службы SSH. После этого злоумышленник может выполнять команды с теми же привилегиями, что и пользователь с учетной записью администратора», – пояснили исследователи.

Компания Dell уже выпустила исправления безопасности для устранения уязвимостей.

(вгору)

Додаток 22

15.01.2018

СБУ заблокувала розповсюдження в Україні шпигунського програмного забезпечення

Співробітники СБ України спільно з прокуратурою заблокували розповсюдження шкідливого програмного забезпечення, яке призначалося для

віддаленого негласного отримання інформації з мобільних терміналів (InternetUA).

Оперативники СБ України встановили, що група зловмисників з різних регіонів України розробила програму для прихованого зняття інформації з мобільних пристроїв. Свої «послуги» вони продавали клієнтам через спеціально створені веб-ресурси.

Замовник, заповнивши на сайті відповідну заявку, отримував спочатку тестовий доступ до «сервісу». Йому надходило посилання, яке він мав фізично «закачати» на телефон потрібної йому особи. Програма запускалася автоматично при включенні мобільного телефону, не виявляла ознак активності під час роботи та діяла приховано від власника.

Можливості хакерського забезпечення дозволяли перехоплювати телефонні розмови, СМС- та ММС-листування, фіксувати місцезнаходження абонента, «знімати» спілкування через популярні месенджери та електронну пошту, надавали доступ до фото- і відеофайлів, що зберігаються на мобільному пристрої.

Усі отримані дані зберігалися для клієнта в «особистому кабінеті» на веб-ресурсах зловмисників. Для постійного користування «сервісом» замовник повинен здійснити оплату на необхідний йому термін через електронні платіжні системи.

Співробітники Управління СБ України в Харківській області провели низку обшуків в офісах та за місцями мешкання учасників групи, під час яких вилучили докази протиправної діяльності зловмисників.

За висновками фахівців, виявлене програмне забезпечення, встановлене на мобільному пристрої, є спеціальним технічним засобом негласного отримання інформації.

Кримінальне провадження здійснюється за ознаками злочинів, передбачених ч. 2 ст. 359 (незаконне використання спеціальних технічних засобів негласного отримання інформації) та ч. 1 ст. 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України.

Вирішується питання про оголошення фігурантам справи підозри в скоєнні злочинів. Тривають невідкладні слідчо-оперативні дії.

(вгору)

Додаток 23

16.01.2018

Хакеры взломали DNS-сервер сервиса BlackWallet и похитили $400 тыс. в криптовалюте

Неизвестные хакеры взломали DNS-сервер сервиса BlackWallet.co, предоставляющего web-кошельки для криптовалюты Stellar Lumen (XLM), и украли более $400 тыс. со счетов пользователей (InternetUA).

Атака произошла 13 января, когда злоумышленникам удалось перехватить DNS-запись домена BlackWallet.co и перенаправить ее на свой собственный сервер. По словам администратора BlackWallet, инцидент произошел после того, как некто получил доступ к учетной записи хостинг-провайдера.

По словам исследователя безопасности Кевина Бомона (Kevin Beaumont), занимавшегося расследованием инцидента, в ходе взлома на сайт был внедрен вредоносный код, автоматически отправлявший средства пользователей на кошелек злоумышленников, если на счету было более 20 XLM. По предварительным оценкам, преступникам удалось похитить порядка 669 тыс. XLS или около $400 тыс. по курсу на 15 января 2018 года. Вскоре после взлома администрация приостановила работу сайта.

Команда BlackWallet и владельцы криптовалюты XLM пытались предупредить пользователей на ресурсах Reddit, Twitter, GitHub, Stellar Community и GalacticTalk, однако множество пользователей продолжали регистрироваться на домене BlackWallet.co и вводить свои учетные данные.

14 января злоумышленники начали переводить средства со своей учетной записи XLM на криптовалютную биржу Bittrex. Вероятно, таким образом хакеры попытались замести следы, обменяв XLM на другую криптовалюту. В настоящее время администраторы BlackWallet ведут переговоры с Bittrex касательно блокировки учетной записи злоумышленников.

«Я также веду переговоры с моим хостинг-провайдером, чтобы получить как можно больше информации о хакере. Посмотрим, что можно сделать», – добавил представитель администрации BlackWallet.

Пользователям порекомендовали переместить свои средства с BlackWallet на другой кошелек с помощью сервиса Stellar Account Viewer.

(вгору)

Додаток 24

16.01.2018

Сотрудники Twitter читают переписку пользователей и просматривают их интимные фото

Организация Project Veritas опубликовала снятое скрытой камерой видео, в котором сотрудники Twitter признались в том, что читают личные сообщений пользователей. По словам старшего инженера по сетевой безопасности Клэя Хэйнса (Clay Haynes), в компании «есть целая команда или, по крайней мере, триста-четыреста человек», которым платят за просмотр фотографий и переписки, в том числе интимного характера (InternetUA).

Как сообщил инженер Twitter Пранай Сингх (Pranay Singh), на его сервере хранятся все пересылаемые пользователями секс-сообщения и интимные фото. «Вы не можете их удалить, они все уже на моем сервере, – заявил инженер. Все ваши законные жены и девочки, с которыми вы

развлекались, теперь на моем сервере. Я отправлю их вашей жене, и она использует их в бракоразводном процессе».

По словам сотрудников Twitter, пользователи платят за возможность пользоваться сайтом не деньгами, но своими персональными данными. На самом деле люди раскрывают о себе гораздо больше информации, чем думают. Сотрудники компании собирают их персональные данные и составляют «виртуальные профили», которые затем продают рекламодателям.

«Для того чтобы получить от рекламодателей деньги, мы должны доказать, что этой действительно ваши данные. Поэтому мы используем электронный адрес, cookie-файлы и еще что-то в этом роде для отслеживания вас», – сообщил инженер Twitter Михай Флоря (Mihai Florea).

В базах данных Twitter хранятся сведения даже о тех, у кого нет учетной записи в сервисе, сообщил бывший инженер Twitter Конрадо Миранда (Conrado Miranda). «Как защитить себя, если эти данные попадут не в те руки? Никак. Это просто невозможно», – отметил инженер.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, Голосіївський просп., 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
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.