СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(27.03–9.04)

2019 № 7

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(27.03–9.04)
№ 7

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 2019

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Маніпулятивні технології

28.03.2019
Ирина Фоменко
IT-гиганты помогут Трампу в борьбе с фейковыми новостями

Бюро переписи населения США обратилось к техническим гигантам Google, Facebook и Twitter с просьбой помочь в борьбе с кампаниями фейковых новостей, которые могут нарушить предстоящий подсчет 2020 года.

Докладніше

***

3.04.2019
Цукерберг: Facebook не может гарантировать безопасные выборы в ЕС

Марк Цукерберг заявил, что хотя Facebook гораздо лучше, чем в 2016 году, борется с вмешательством в выборы, но не может гарантировать, что сайт не будет использован для подрыва выборов в Европейский парламент, которые состоятся в мае. Об этом сообщает Reuters (InternetUA).

«Это постоянная гонка вооружений, в которой мы постоянно наращиваем оборону, и эти изощренные правительства также развивают свою тактику», – сказал Цукерберг.

Отмечается, что после того, как Россия использовала Facebook и другие социальные сети, чтобы повлиять на выборы и привести к победе Дональда Трампа, Facebook мобилизировал все свои ресурсы и персонал на защиту выборов в ЕС 26 мая.

«Мы, безусловно, добились большого прогресса. Но нет, я не думаю, что кто-то может гарантировать в мире безопасность и полностью решить эту проблему, так как есть целые государства, которые пытаются вмешаться в выборы», – сказал Цукерберг.

Под давлением со стороны ЕС сделать больше для защиты от иностранного вмешательства в предстоящие выборы, Facebook на прошлой неделе ужесточил свои правила политической рекламы в Европе. Соцсеть также объявила о планах наращивания усилий по борьбе с дезинформацией в преддверии голосования и сотрудничестве с немецким информационным агентством DPA, чтобы усилить проверку фактов.

***

3.04.2019

В Сингапуре тоже готовят закон о запрете фейковых новостей

Первого апреля в парламенте Сингапура был зачитан закон, согласно которому власти получат право удалять все публикации, которые, по их мнению, нарушают государственные нормы (InternetUA).

После имплементации закона под ударом, помимо обычных СМИ, окажутся Facebook, Google и Twitter, штаб-квартиры которых находятся в Сингапуре. За не удаленную вовремя фейковую, по мнению чиновников, новость они вынуждены будут платить миллионные штрафы.

По заявлению премьер-министра Сингапура Ли Сянь Луна, в последние годы город-государство стал «объектом враждебных информационных кампаний», поэтому этот закон будет эффективным инструментом для борьбы с дезинформацией (собственно, так говорят все авторитарные правительства, принимая такие законы). По новому закону издания будут обязаны указывать, когда и где в их материалах был фейк, и исправлять недостоверную информацию.

«В экстремальных и неотложных случаях законодательство также требует, чтобы новостные онлайн-источники удадяли фейковые новости до того, как будет нанесен непоправимый ущерб», – сказал Ли.

Естественно, формулировка, что такое «фейковые новости», прописана в законе нечетко, что оставляет множество трактовок в пользу властей.

Сингапур, который и так достаточно жестко цензурирует свои СМИ, поддерживает тенденцию, распространенную в Юго-Восточной Азии, направленную на ужесточение законодательства, в котором многие усматривают угрозу свободе информации. Похожие законы в поледние годы были приняты во Вьетнаме и Малайзии. Согласно рейтингу свободы прессы «Репортеров без границ», Сингапур находится на 151 месте из 180-ти. Даже Россия со своими законами об «фейковых новостях» и «ответственности за оскорбление власти» обошла Сингапур на три пункта и находится на 148 месте.

Спецслужби і технології «соціального контролю»

27.03.2019

В Запорожье разоблачили очередного антиукраинского интернет-агитатора

В Запорожье мужчина распространял в соцсети антиукраинские призывы. Об этом сообщает пресс-служба СБУ (InternetUA).

26 марта сотрудники службы безопасности провели у интернет-агитатора обыски, а также прекратили его противоправную деятельность.

Выяснилось, что таким образом российские спецслужбы пытаются повлиять на избирательный процесс в Украине.

Для этого кураторы из РФ использовали в соцсетях более 50 сообществ, где и публиковали антиукраинские материалы.

В настоящее время устанавливаются все подробности. Также решается вопрос о привлечении причастных лиц к уголовной ответственности.

***

6.04.2019

В Одесской области СБУ разоблачила антиукраинского интернет-агитатора

В Одесской области сотрудники Службы безопасности Украины разоблачили антиукраинского интернет-агитатора. Как сообщили в пресс-центре спецслужбы, мужчина действовал в интересах страны-агрессора, сообщает «Сегодня» (InternetUA).

Было установлено, что злоумышленник регулярно размещал на персональных страницах в социальных сетях информацию с призывами к изменению государственной границы и конституционного строя Украины, а также занимался пропагандой так называемых «Л/ДНР».

Тексты для своих публикаций агитатор получал из российских пропагандистских интернет-изданий, а также с сепаратистских сайтов боевиков.

Сотрудники СБУ обнаружили в квартире агитатора компьютерную технику и мобильные устройства с материалами. Было открыто уголовное производство по статье «посягательство на территориальную целость и неприкосновенность Украины», фигуранту дела сообщили о подозрении.

***

29.03.2019

Росія планувала кібератаку на популярні ЗМІ України, - СБУ

СБУ запобігла спробі хакерів провести підготовчий етап кібератаки, орієнтованої на популярні ЗМІ та телекомунікаційні об’єкти України (Espreso.tv).

Про це повідомляє прес-службу відомства.

Встановлено, що виконавці впродовж кількох попередніх місяців створювали розгалужену інтернет-інфраструктуру. Вона налічує кілька десятків доменів, які за своєю назвою збігаються або походять на офіційні домени популярних українських електронних засобів масової інформації, операторів зв’язку і великих телекомунікаційних компаній.

Повідомляється, що доменні імена вперше зафіксовані на потужностях дата-центрів кількох російських інтернет-провайдерів, а облікові записи раніше застосовувалися для кібератак на старий сектор протягом минулого року.

Зокрема, з їх допомогою створений ряд командно-контрольних серверів для управління вірусними атаками відомого хакерського угруповання РФ.

В СБУ припускають, що задум кібератаки цілком ймовірно полягав у створенні максимального суспільного резонансу і негативного інформаційного впливу напередодні проведення виборів президента України.

***

27.03.2019

Twitter блокирует аккаунты пользователей из-за розыгрыша

На официальной страничке технической поддержки социальной сети Twitter появилось оповещение, в котором говорится о том, что в течение последних суток аккаунты пользователей Twitter массово блокируются (InternetUA).

Причина заключается в том, что пользователи меняют дату своего рождения с реальной на 2007 год. Система автоматически срабатывает и блокирует учетную запись, так как в Twitter есть возрастное ограничение, сервисом можно пользоваться по достижению 13-летнего возраста.

А менять дату своего рождения пользователи начали после того, как кто-то распространил ложную информацию о том, что после этих действий вы получите доступ к секретной цветовой схеме в приложении Twitter.

Отдел технический поддержи сообщает, что вы можете разблокировать свою учетную запись, следуя инструкции и предоставив копии документов, подтверждающих ваш возраст.

***

28.03.2019

Facebook будет блокировать проявления белого национализма и сепаратизма

С начала апреля компания Facebook заблокирует проявления белого национализма и сепаратизма в своей соцсети, а также в Instagram. Об этом говорится на сайте компании.

Докладніше

***

28.03.2019

Російські спецслужби активізувалися в українському інформаційному просторі

Співробітники Служби безпеки України у ході виконання завдань з контррозвідувального забезпечення інформаційної безпеки протягом 2019 року фіксують потужну активізацію спецслужб РФ в інформаційному просторі нашої держави напередодні виборів Президента.

Докладніше

***

30.03.2019
Twitter рассматривает возможность маркировки твитов Трампа

Twitter рассматривает возможность маркировки твитов, которые нарушают правила социальной сети, но должны оставаться на платформе, потому что они представляют общественный интерес. Об этом сообщает The Washington Post (InternetUA).

«Мы сейчас работаем над тем, каким образом маркировать опасные твиты. Как мы можем дать понять пользователям, что этот контент на самом деле нарушает наши правила, но выполняет определенную цель, поэтому остается на платформе», – заявила глава юридического и политического отделов соцсети Виджая Гадде.

Ранее социальная сеть подвергалась критике за то, что не удаляет и не реагирует на твиты президента США Дональда Трампа, хоть они и нарушают стандарты Twitter (буллинг, дегуманизация и язык ненависти).

Гадде рассказала о возможном способе маркировки. Перед тем, как увидеть «опасный твит», у пользователя всплывет окно «вы действительно хотите увидеть содержание твита?» По ее словам, таким образом, у людей будет выбор.

***

30.03.2019
Facebook ужесточает правила онлайн трансляций

После двойного теракта в Крайстчёрч (Новая Зеландия) Facebook ужесточает правила онлайн трансляций. Об этом заявила главный операционный директор компании Шерил Сэндберг. «В качестве реакции на произошедший теракт, мы принимаем три меры: ужесточение правил для Facebook Live, усиление борьбы с возбуждением ненависти на наших платформах и поддержка Новой Зеландии», – цитирует ее слова агентство AFP (InternetUA).

Как пояснила Сэндберг, в будущем компания запретит использование функции Facebook Live для тех пользователей, кто ранее был замечен в нарушении установленных стандартов сообщества. Кроме того, Facebook инвестирует в программное обеспечение для быстрого обнаружения отредактированных версий видеороликов или других изображений насилия.

Власти Австралии тем временем объявили, что в будущем будут привлекать к ответственности социальные сети, если те не удалят записи террористических атак со своих платформ. Ожидается, что соответствующие законы внесут в парламент страны уже на следующей неделе. Компаниям-

нарушителям грозят миллиардные штрафы, а их менеджерам – тюремное заключение.

Ведущие социальные сети «несут ответственность за принятие любых возможных мер, гарантирующих, что их технологии не будет использованы террористами», – заявил в минувшую субботу глава правительства Австралии Скотт Моррисон. Он отметил, что призовет и другие государства G20 заставить соцсети взять на себя ответственность за нераспространение видеороликов, содержащих записи терактов и другие сцены насилия.

***

2.04.3019

Владимир Кондрашов

В нацкомиссии раскритиковали «пророссийский» законопроект о блокировках сайтов

Национальная комиссия, осуществляющая госрегулирование в сфере связи и информатизации, считает нецелесообразным принятие проекта закона, которым устанавливается уголовная ответственность за распространение недостоверных сведений в СМИ и интернете, а на НКРСИ ложится функция принимать решение об обязательствах операторов, провайдеров телекоммуникаций о приостановлении доступа абонентов к ресурсу сети Интернет.

Докладніше

***

4.04.2019

У Франції Twitter заблокував урядову рекламу, посилаючись на закон проти інформаційних маніпуляцій

МВС Франції запустило кампанію #Ouijevote (так, я голосую), яка закликає громадян зареєструватися на вибори до Європарламенту, що пройдуть 26 травня. Утім соціальна мережа не дала у повній мірі оплатити твіти з цим повідомленням (InternetUA).

Як пише Le Figaro, такий спосіб агітації розробили у Міністерстві внутрішніх справ Франції. Він координується Державною інформаційною службою (SIG). Кампанія закликає зареєструватися громадян на виборах до Європарламенту та проголосувати на них.

Twitter заблокувала рекламу постів кампанії #Ouijevote, оскільки новий закон проти інформаційних маніпуляцій вимагає від інформаційних платформ ознайомлювати користувачів з тим, хто оплачує політичну рекламу.

«Поки що Twitterне розробив таких механізмів, тому було вирішено повністю прибирати рекламні оголошення, які мають політичний характер», – відповіла компанія на звернення SIG.

Утім у відомстві наголошують, що інформаційна кампанія є просвітницькою, а не політичною та не представляє жодну політичну партію. Також вони називають такі дії Twitter спробою повернутися за стіл переговорів щодо норм закону.

***

5.04.2019

Австралия будет сажать руководителей соцсетей в тюрьму за «отвратительные» посты

В Австралии принят первый в демократическом мире закон об уголовном наказании для владельцев соцсетей за содержание постов на их платформах – вплоть до многолетнего тюремного заключения.

Докладніше

***

6.04.2019

Ирина Фоменко

Что скрывается за внезапным принятием государственного регулирования Facebook

Генеральный директор Facebook Марк Цукерберг призвал к усилению государственного надзора и даже регулирования Интернета. По его словам, пришло время для правительств во всем мире активизировать работу и помочь обуздать Интернет.

Докладніше

***

8.04.2019

Британия обяжет Facebook, Twitter и Instagram фильтровать контент

Правительство Великобритании планирует обязать Facebook, Twitter, Instagram внимательнее фильтровать контент. В противном случае корпорациям грозят крупные штрафы, сообщает «ЛІГА.net» (InternetUA).

Департамент цифровых технологий, культуры, медиа и спорта Британии уже внес такое предложение на рассмотрение правительства. Сессия по принятию новых норм закона продлиться 12 недель. По ее завершению будет принято окончательное решение.

Чиновники считают, что руководства популярных социальных сетей недостаточно следят за наличием жестокого контента.

«Интернет-компании должны начать брать на себя ответственность за свои платформы и помогать восстанавливать доверие общественности», – заявила примьер-министр Британии Тереза Мэй.

Інформаційно-психологічний вплив мережевого спілкування на особистість

27.03.2019
В Калифорнии школьникам хотят запретить смартфоны

Ассамблея штата Калифорния представила законопроект, который ограничивает использование мобильных телефонов в школах. С инициативой выступил демократ Альберт Мурацучи.

Докладніше

***

27.03.2019
Ирина Фоменко
Исследование: чрезмерное использование смартфона вызывает потерю сна

Согласно австралийскому исследованию, обнаружившему скачок «техноференции» за последние 13 лет, из-за чрезмерного использования мобильных телефонов люди теряют сон и становятся менее продуктивными.

Докладніше

***

29.03.2019
Почему нельзя пользоваться телефоном перед сном: ответ эксперта

Многие из нас любят полистать ленту новостей в постели, проверить уведомления или пообщаться в мессенджере. Существует даже специальное название такого явления: прокрастинация перед сном. То есть вы намеренно откладываете сон без явной необходимости. В результате вы позже засыпаете и спите меньше, чем могли бы, сообщает «Сегодня» (InternetUA).

Еще один вредный фактор – это холодный голубой свет, продуцируемый LCD-экранами гаджетов. Он сообщает нашим биологическим часам, что наступило утро. Голубой свет нарушает наш внутренний биоритм. Он влияет на внутренние биологические часы, определяющие работу различных органов, и подавляет выработку мелатонина – важного гормона, отвечающий за здоровый цикл сна-бодрствования и восстановление тела. Это не только ухудшает качество сна, но может спровоцировать метаболический синдром, ожирение, депрессию и даже рак.

Что же делать?

«Никаких секретов: качественный сон, сбалансированное питание и физическая нагрузка – это составляющие нашего хорошего самочувствия, –

утверждает психотерапевт Вячеслав Халанский. – Эксперты советуют выключать все гаджеты за час-два до сна. Намного лучше провести это время за чтением книги или занятием йогой. Это поможет организму расслабиться. Также можно установить на смартфон специальные приложения вроде Twiglight, уменьшающие голубое излучение экрана к концу дня. А запустить биологические часы отлично помогает короткая утренняя прогулка.

***

4.04.2019

Вчені дізналися, як зазвичай люди реагують на негативні новини в соцмережах

Американські вчені провели дослідження і дізналися, як зазвичай люди реагують на негативні новини в соцмережах. Ці звістки містили негативні відомості про життя їхніх близьких і знайомих (Cikavosti).

Для цього було створено три типи новин, кожна наступна з них була більш серйозною і трагічною, ніж попередня. У першій йшлося про розставання з близькою людиною, у другій – про несподіване онкологічне захворювання родича, а в третій – про смерть близького друга. Кожному випробуваному давали можливість відреагувати на цю звістку так, як йому хочеться. Можна було написати коментар, поставити лайк, використовувати різні сумні смайлики, або і зовсім залишити новину без реакції.

Після цього людям пропонували заповнити анкету, де у них запитували про те, які звістки для них виявилися найскладнішими і емоційними, а також як вони б воліли їх отримувати. Результати виявилися досить несподіваними. Практично всі випробувані вважали за краще дізнатися про всіх три новини в особистій розмові, а не через соцмережі. Окремо вчені відзначили активність людей. Виявилося, що більш комунікабельні з них охоче залишали свої коментарі і ділилися відповідними переживаннями.

Вчені відзначають, що їх дослідження стосувалося новини про близьких людей, тому реакція їх випробовуваних була більш різкою. У разі звісток про абсолютну чужу людину, переживання були б відчутно слабкішими

***

5.04.2019

Создатель Linux назвал Twitter, Facebook и Instagram болезнью

Создатель операционной системы Linux Линус Торвальдс в недавнем интервью изданию Linux Journal коснулся темы социальных сетей. Его спросили, что бы он хотел изменить в мире технологий, если бы мог. И его ответом оказались социальные медиа (InternetUA).

– Я абсолютно ненавижу современные социальные медиа – Twitter, Facebook, Instagram. Это болезнь. Выглядит так, словно они поощряют плохое поведение, – цитирует Linux Journal спикера.

Линус считает, что в социальных сетях сложнее заметить реакцию получателя сообщения. Из-за чего могут возникать конфликты, которые не случились, будь ты лицом к лицу с собеседником.

– Вся модель лайков и репостов – это просто мусор. В этом нет никаких усилий и контроля качества, – подчеркнул Линус, жалуясь на клик-бейт и вещи, которые нацелены на генерацию морального негодования.

– Некоторые люди путают анонимность и конфиденциальность. Думают, что оба этих понятия идут рука об руку и защита конфиденциальности означает, что должна быть защищена и их анонимность. Это неправильно. Анонимность важна, если вы информатор. Но если вы не можете доказать свою личность, то ваша сумасшедшая тирада на какой-нибудь социальной платформе не должна быть видна.

Business Insider отмечает, что такую критику интересно услышать от человека, который не отличается вежливым поведением и не терпит дураков. Его частенько можно было заметить за публичной поркой людей, которые не соответствуют его стандартам профессионализма или мотивации.

***

8.04.2019

Хмельницькі школярки побили 14-річну дівчину та виклали відео у Facebook

Насилля та цькування заради здобуття авторитету. Назва такого поширеного в українських школах явища – булінг. Переважно винуватцями учнівської «травлі» стають юнаки, які бажають самоствердитися за рахунок інших або ж просто прагнуть влитися в колектив чи здобути собі авторитет серед однолітків таким жорстоким способом (InternetUA).

Днями Хмельницький сколихнула чергова звістка про булінг. Цього разу учасниками стали дівчата, учениці 7 та 8 класів двох хмельницьких шкіл, які знаходяться у різних мікрорайонах міста. Сталося все 5 квітня, неподалік від ліцею №15, що знаходиться по вулиці Проскурівського Підпілля. Моменти побиття зняли на відео і опублікували його у Facebook. На ньому видно, як група учениць школи №28 по черзі б’ють рукою по обличчі дівчину. Остання стояла і не захищалася.

Поліція вже встановила всіх учасниць підліткової «розправи». Наразі з дівчатами спілкуються правоохоронці. Вони побачили відео у соцмережах та відреагували на події, що сталися. Заяву про насильницькі дії над неповнолітньою ученицею ліцею №15 до поліції ніхто не писав.

Проблема захисту даних. DDOS та вірусні атаки

27.03.2019

Чем опасны предустановленные приложения для Android

Приложения, которые производители предустанавливают на свои смартфоны, зачастую могут оказаться не менее опасными, чем шпионское ПО из ненадежных источников. Об этом предупреждают исследователи Мадридского университета им. Карлоса III при сотрудничестве экспертов из Международного института компьютерных наук Беркли и Университета штата Нью-Йорк в Стоуни-Брук.

Докладніше

***

27.03.2019

Новая функция в Android убережет вас от мошенников

Согласно сообщению издания Android Police, вскоре в приложение Google Phone может быть добавлена новая функция, которая будет активно блокировать некоторые входящие вызовы.

Докладніше

***

27.03.2019

Трамп продовжив режим надзвичайного стану через кіберзагрози

Президент США Дональд Трамп продовжив на рік режим надзвичайного стану через «умисні шкідливі дії в кіберпросторі», введений його попередником Бараком Обамою (Espreso.tv).

Відповідний указ опубліковано на сайті Білого дому.

Зазначається, що для зовнішньої політики та економіки США подібні дії «становлять загрозу національній безпеці».

«У зв'язку з цим я визнав за необхідне продовжити режим надзвичайного стану, оголошеного у виконавчому указі 13694», – йдеться в заяві Трампа.

Указ про запровадження надзвичайного стану в країні було підписано 1 квітня 2015 року 44-м президентом США Бараком Обамою.

***

28.03.2019

Рассылал e-mail-адреса с паролями: в Черновцах малолетнему хакеру назначили наказание

В Шевченковском районном суде Черновцов вынесли приговор несовершеннолетнему хакеру, который рассылал электронные адреса с паролями пользователей и получал за это деньги на свой bitcoin-кошелек (InternetUA).

Прокуратура установила, что злоумышленник в декабре 2017 года хакерском форуме выложил для общего доступа файл с электронными ящиками 350 тысяч пользователей и паролями к ним.

Затем в сентябре 2018 года через Telegram он стал вести переписку с различными пользователями и передавал им файлы с e-mail-адресами людей.

В результате он передал 5 пользователям более 3 миллионов адресов.

Удалось также доказать, что малолетний хакер в одном из случаев заработал деньги, которые ему перечислили на bitcoin-кошелек. Сам парень признал свою вину.

Суд принял решение назначить ему наказание – 3 года лишения свободы с испытательным сроком 2 года. Также у него конфисковали телефон, компьютер и другую технику, которую он использовал в своих хакерских делах.

Родителей нарушителя обязали заплатить более 4000 гривен на проведение экспертиз.

***

28.03.2019

В технологии 4G обнаружены десятки серьезных уязвимостей

Исследователи безопасности из Южной Кореи обнаружили в технологии 4G (она же LTE) 36 новых уязвимостей, которые открывают для злоумышленников целый спектр атак. С помощью этих дыр хакеры могут нарушать работу базовых станций связи, блокировать входящие вызовы или полностью отключать связь конкретным пользователям, отправлять фальшивые SMS, перехватывать интернет-трафик (IGate).

Результат исследования будет официально представлен в мае, но соответствующая статья уже доступна онлайн.

Для обнаружения дыр ученые Корейского института передовых технологий разработали полуавтоматический инструмент под названием LTEFuzz. С его помощью они создавали вредоносные соединения в мобильной сети, а потом наблюдали, как сеть отреагирует на атаку. В общей сложности это позволило выявить 51 уязвимость, но 15 из них ранее уже были обнаружены и описаны другими командами исследователей.

Специалисты уже уведомили о проблемах консорциум 3GPP и организацию GSMA. Также связались с производителями железа, на котором тестировался инструмент для взлома. Другим производителям 4G-оборудования также будут предоставлены данные об уязвимостях. А вот широкой публике о конкретных методах атак исследователи, по понятным причинам, рассказывать не будут.

***

28.03.2019

Мобильный троян Gustuff нацелен на клиентов крупных банков

Специалисты Group-IB зафиксировали активность мобильного Android-трояна Gustuff. Среди его целей – клиенты международных банков, пользователи мобильных криптокошельков, а также крупных e-commerce ресурсов.

Докладніше

***

28.03.2019

Владимир Кондрашов

CERT-UA зафиксировала массовую рассылку вредоносных электронных писем

Команда реагирования на компьютерные чрезвычайные события Украины Госспецсвязи (CERT-UA) сообщает о массовой рассылке фишинговых писем о якобы превышении лимита отправки писем, объема памяти и тому подобное. Цель рассылки – кража электронного адреса и пароля к нему (InternetUA).

Как сообщается, фишинговые письма побуждают перейти по ссылке для восстановления доступа или недопущения удаления аккаунта и ввести учетные данные (адрес электронной почты и пароль) в форму на сайте.

Ссылки ведут на следующие сайты:

hxxps://lofty-noun[.]000webhostapp[.]com/

hxxp://subadmnnotifcatio[.]eu5[.]net/form[.]php

hxxp://wydawnictwo[.]edytawittchen[.]pl/pero/Login[.]html

– Призываем не открывать вложения и не переходить по ссылке из писем, которые вы не ожидали получить. Проверяйте (в телефонном режиме или в любой другой способ), действительно ли адресовано вам сообщение с вложением или ссылкой, – предупреждают в CERT-UA.

***

28.03.2019

Иранские кибершпионы атакуют компании в США и Саудовской Аравии

В течение последних трех лет кибершпионская группировка Elfin (другое название APT33), предположительно финансируемая правительством Ирана, активно атакует организации в США и Саудовской Аравии.

Докладніше

***

28.03.2019

Производитель шпионского ПО хранит перехваченные данные в открытой базе данных

Производитель приложений для слежки потребительского класса, позволяющих перехватывать чужие телефонные звонки и сообщения, хранит более 95 тыс. изображений и 25 тыс. аудиозаписей в незащищенной базе данных. Получить доступ к БД через интернет может любой желающий, сообщает исследователь безопасности Трой Хант (Troy Hunt), первым изучивший ее содержимое (InternetUA).

Хант обнаружил на незащищенном сервере две папки с разнообразными данными, начиная от фотографий интимного характера и заканчивая аудиозаписями телефонных разговоров. Всего на сервере хранится 16 ГБ изображений и порядка 3,7 ГБ аудиозаписей в формате MP3.

Первым БД обнаружил исследователь безопасности Сиан Хисли (Cian Heasley), сообщивший о своей находке изданию Motherboard. По его словам, БД находится в открытом доступе как минимум шесть недель. Более того, новые изображения и аудиозаписи загружаются в нее практически каждый день.

Несмотря на многочисленные попытки Motherboard связаться с компанией и сообщить о проблеме, сервер до сих пор находится в открытом доступе. В связи с характером хранящейся на нем информации название компании не раскрывается.

Неназванная компания пополнила весьма немалый список производителей шпионского ПО (предназначенного для слежки за детьми, нерадивыми сотрудниками и неверными супругами), не позаботившихся о надлежащей защите данных своих клиентов. В список «штрафников» уже входят такие компании, как Retina-X (дважды), FlexiSpy, Mobistealth, Spy Master Pro, SpyHuman, Spyfone, TheTruthSpy, Family Orbit, mSpy, Copy9 и Xnore.

***

29.03.2019

Европейский Союз принял закон о защите авторских прав, угрожающий свободному Интернету

Европейский Союз принял новый закон о защите авторских прав, который сильно повлияет на развитие Интернета в Старом Свете. Он призван дать правообладателям больше контроля над распространением своего контента и ограничить влияние таких технологических гигантов, как Google и Facebook.

Докладніше

***

29.03.2019

Обнаружен крадущий деньги вирус для Android

Киберпреступники активно используют Android-троян Gustuff, который нацелен на клиентов международных банков, пользователей мобильных криптокошельков, платежных систем и мессенджеров. Его обнаружили специалисты компании Group-IB (InternetUA).

Gustuff используется для вывода криптовалюты со счетов пользователей. Заражение смартфонов на Android происходит через СМС с вредоносными ссылками.

Жертвами вируса стали пользователи 32 приложений для хранения криптовалют и клиенты более 100 банков. Анализ показал, что под угрозой находятся пользователи мобильных приложений крупнейших банков и криптокошельков.

В текущей версии вирус также нацелен на юзеров приложений онлайн-магазинов, платежных систем и мессенджеров. Среди них – PayPal, Western Union, eBay, Walmart, Skype, WhatsApp, Gett Taxi.

Троян научился показывать фейковые push-уведомления. При переходе пользователь видит загруженное с сервера фишинговое окно. Жертва сама вводит данные банковской карты или криптокошелька.

Сообщается, что автором вируса является русскоязычный киберпреступник, однако Gustuff «работает» исключительно на международных рынках.

***

31.03.2019

Сотни сайтов на Wordpress и Joomla распространяют вредоносное ПО

Более чем 500 взломанных web-сайтов, работающих на популярных платформах Wordpress и Joomla, распространяют различное вредоносное ПО, в том числе вымогатель Shade (другое название Troldesh), бэкдоры, фишинговые ссылки и другой вредоносный контент. Новую кампанию заметили специалисты из Zscaler.

Докладніше

***

31.03.2019

Владимир Кондрашов

На сайте ЦИК семь месяцев не могли закрыть опасную уязвимость

На сайте Центральной избирательной комиссии как минимум семь месяцев просуществовала опасная уязвимость, которая позволяла атакующему внедрить клиентский сценарий в web-страницы, просматриваемые другими пользователями.

Докладніше

***

31.03.2019

Сайт Державного реєстру виборців «впав»: українці не можуть знайти себе у списках

У день президентських виборів в Україні перестав працювати сайт Державного реєстру виборців. Спочатку сторінка довго завантажується, а потім – показує помилку (InternetUA).

Проблему фіксують від полудня 31 березня. Відтак, українці не можуть перевірити, чи є вони у списках виборців, а також уточнити місце розташування дільниць.

Найімовірніше, сайт перестав працювати через надмірну кількість запитів від виборців або ж – DDos-атаку.

Така інформація з'являється при переході на сайт Держреєстру виборців

Додамо, що сайт Держреєстру перебуває у розпорядженні Центрвиборчкому.

***

1.04.2019

Десятки шпионских приложений в Google Play оказались связаны с государствами

Как стало известно изданию VICE, хакеры заразили сотни пользователей несколькими вредоносными приложениями для Android, которые годами размещались в официальном магазине Google Play Store. Предположительно, это делалось по государственному заказу.

Докладніше

***

1.04.2019

Голосовые сообщения пользователей «ВКонтакте» обнаружили в открытом доступе

Часть голосовых сообщений, которые отправляли друг другу пользователи «ВКонтакте», оказались в открытом доступе. Отыскать их можно было через раздел поиска по документам (InternetUA).

Для того чтобы прослушать чужое аудиосообщение, достаточно было в строке поиска ввести запрос audiocomment.3g. В настоящее время эта возможность уже закрыта – поиск по такому образцу не выдает ни одного результата.

Представители соцсети подчеркнули, что речь не идет об уязвимости в механизме самого сайта. По данным «ВКонтакте», в открытый доступ могли попасть аудиозаписи, которые пользователи загружали через неофициальные клиенты, передает RNS.

Администрация соцсети также добавили, что соцсеть не использует формат аудиосообщений audiocomment.3g. Чтобы избежать подобных утечек, в компании порекомендовали пользоваться официальными приложениями «ВКонтакте».

***

2.04.2019

Взлом по клику: в Google Play стало больше вредоносных программ из-за рекламы в приложениях

Скликиваемая реклама помогает хакерам взламывать пользователей. Теперь геймерам грозит опасность (InternetUA).

Google провёл исследование, в результате которого удалось установить, что за последний год количество вредоносных программ в Google Play увеличилось в два раза. В 2017 году он составил 0,02 %, а в 2018 – уже 0,04 %. По словам представителей компании, основная причина заключается в том, что во многие приложения хакеры стали внедрять «мошеннический клик». В процессе игры время от времени появляется реклама. Когда геймер нажимает на крестик, чтобы её убрать, она автоматически отправляет его на сайт рекламы, где пользователя уже ждут злоумышленники.

Реклама в приложениях всегда была раздражающим фактором, а теперь из-за неё стало ещё больше пострадавших и жалоб от них. Взлом по клику в 2018 году стал очень популярным среди мошенников. При этом само руководство отмечает, что несмотря на тенденцию, пока то гораздо безопаснее устанавливать приложения именно из Google Play, а не из Google Play Store. Известно, что среди всех установленных из Play Store вредоносных программ на мошенничество с помощью клика приходится половина случаев. Вслед за ними иду трояны.

Как указали представители Google, в настоящее время территории, где крайне распространён такой способ мошенничества, ограничиваются тремя странами: США, Бразилией и Мексикой. Однако эксперты отмечают, что, если расширится географический фактор, то резко возрастёт и статистика. Сейчас есть специальная защита Google Play Protect от Android. Сообщается, что она смогла предотвратить 1,6 миллиарда попыток установки вредоносных программ. Даже несмотря на то, что система не может полностью обезопасить пользователей, руководство рекомендует данное приложение к установке на гаджеты.

***

2.04.3019

Кіберполіція викрила двох хакерів, які крали особисті дані користувачів форумів про криптовалюти

Кіберполіція виявила двох хакерів, які заволоділи персональними даними користувачів форумів та чатів, присвячених криптовалютам, повідомляє прес-служба МВС (InternetUA).

Підозрюваних затримали у Хмельницькій області. Зловмисники самостійно створювали, а також купували та модифікували шкідливе програмне забезпечення. Ці програмні засоби вони поширювали під виглядом ліцензійного ПЗ. Насправді ж, користувачі завантажували на свій пристрій вірус.

Ці віруси збирали на інфікованих комп'ютерах інформацію, в тому числі і конфіденційну. Серед такої – паролі, логіни до різних ресурсів, інформація про гаманці криптовалют, файли з персональною інформацією тощо.

Зібрану інформацію зловмисники отримували на спеціально налаштований сервер. Вона дозволяла їм віддалено керувати інфікованими пристроями на правах адміністратора, в тому числі спостерігати за жертвами та прослуховувати їхні розмови.

Викрадена особиста інформація використовувалась для подальших протиправних дій та частково продавалася на відповідних форумах. У підозрюваних правоохоронці провели обшуки.

За цим фактом поліція розпочала провадження за ч. 2 ст. 361 (несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу.

***

3.04.3019

Ирина Фоменко

Эксперты обнаружили новый способ хранения злоумышленниками вредоносного ПО

Исследователи безопасности Zscaler обнаружили, что киберпреступники используют скрытые «известные» каталоги сайтов HTTPS для хранения и обслуживания вредоносных программ.

Докладніше

***

3.04.2019

Facebook запрашивает пароли от электронной почты у новых пользователей

Некоторых новых пользователей Facebook для авторизации попросили предоставить пароли от их электронной почты. После ввода соцсеть начинала без спроса импортировать их контакты, пишет Business Insider (InternetUA).

Ранее издание The Daily Beast сообщило, что пользователей с аккаунтами некоторых провайдеров, включая Яндекс и популярный в западных странах

GMX, соцсеть просила подтвердить почтовый адрес, введя пароль от него прямо в Facebook. Пользователи Gmail такой запрос не получали.

Также BI обнаружил, что если новый пользователь вводил пароль от почты на Facebook, у него всплывало окно с уведомлением, что соцсеть «импортирует контакты» – не спрашивая на это разрешение. Хотя какие именно контакты импортировались, BI выяснить не смог.

Эксперты в области кибербезопасности резко осудили подобную практику. По их словам, она ничем не отличается от фишинговой атаки и повышает риск взлома почтовых аккаунтов. Обычно интернет-пользователям советуют никогда не вводить пароли в сторонние сервисы помимо тех, для которых они были созданы.

Даже несмотря на то, что Facebook принимает меры для защиты полученных паролей, с учётом наличия более простых альтернативных вариантов авторизации, этот сомнительный способ выманивания пользовательских контактов совершенно не обоснован и заставляет пользователей поставить под угрозу свою безопасность.

В форме верификации также указано, что Facebook не собирает полученные пароли, но проверить это, пишет BI, невозможно. Недавно стало известно, что соцсеть хранила пароли сотен миллионов своих пользователей в незашифрованном виде, доступном её сотрудникам в виде текста.

Представитель Facebook подтвердил, что она не собирает пароли. Он добавил, что инструмент авторизации в первый раз по почтовому паролю появился у очень небольшой группы людей и что они всегда могут выбрать другой способ – SMS-код или ссылку на email. Но компания понимает, что такой инструмент это «не лучший вариант», поэтому откажется от него. О сроках ничего не сказано.

***

3.04.2019
Facebook снова допустил утечку персональных данных

Исследователи компании UpGuard обнаружили существование двух баз, содержащих персональные данные пользователей Facebook (Espreso.tv).

В своем блоге UpGuard уверяет, что более 540 млн записей с подробными комментариями, ругательствами, названиями учетных записей были найдены на мексиканской цифровой платформе Cultura Colectiva, где публикуется материал, который затем пользователи выкладывают в социальные сети.

Кроме того, данные 22 тысяч человек, включая имена, пароли, адреса электронной почты, были доступны в уже несуществующем приложении At the Pool. Пароли, как сообщается, хранились в виде открытого текста. Отмечается, что UpGuard не знает, как долго в приложении хранились данные пользователей.

Оба набора данных хранятся в облачном хранилище Amazon S3 и могут быть доступны практически любому. Ни один из них не был защищен паролем.

***

5.04.2019

Facebook стал торговой площадкой для киберпреступников

В Facebook обнаружено более 70 групп с более 385 000 участниками, в которых продавались услуги по краже информации с кредитных карт, личных данных, взлому сайтов и электронной почты. Об этом сообщили исследователи по кибербезопасности Talos, подразделения по анализу угроз для технологической компании Cisco, передает Euronews (InternetUA).

По словам исследователей, некоторые подобные группы в соцсети ведут свою деятельность уже около 8 лет. Обширный «черный рынок» в соцсети был обнаружен случайно, когда исследователи искали подтверждения других фактов мошенничества в Сети.

После того, как исследователи присоединились к группам в соцсети, связанными с мошенничеством в индустрии видеоигр, Facebook начал предлагать присоединиться к другим подобным группам, занимающимся более серьезной преступной детальностью в Интернете.

«Алгоритм Facebook, предназначенный для связи пользователей с похожими увлечениями, также учитывает ключевые слова между этими различными типами преступных групп», – сказал Клэйг Уильямс, директор Talos.

«К сожалению, вместо того, чтобы связывать людей с позитивными увлечениями, он выводит их на преступный путь, рекламирующий инструменты взлома для широкой публики», – подытожил Уильямс.

Представители Facebook подтвердили, что данная проблема действительно существует. В руководстве соцсети заявили, что большинство вышеупомянутых группы было создано в 2018 году. Facebook удалили группы и запретил их бывшим администраторам создавать новые, также были удалены учетные записи и страницы, связанные с киберпреступниками.

***

5.04.2019

Ирина Фоменко

BBC: интернет-вирус смог дорисовать к скану пациента раковую опухоль

В ходе лабораторных испытаний вредоносная программа изменила 70 изображений и сумела обмануть трех радиологов, заставив их поверить, что у пациентов был рак. Измененные изображения также сумели обмануть автоматизированные системы скрининга.

Докладніше

***

5.04.2019

Eset обнаружила фишинговую атаку в WhatsApp

Эксперты антивирусной компании Eset предупреждают о новой фишинговой атаке в мессенджере WhatsApp – пользователи устанавливают вредоносное расширение, якобы предназначенное для изменения цвета интерфейса (Компьютерное Обозрение).

Как считает Eset, атака направлена на жителей Бразилии и испаноговорящих стран – сообщения составлены на португальском и испанском языках. Примечательно, что приложение стремится подписать пользователей на уведомления с русскоязычного ресурса.

Потенциальные жертвы получают сообщение, которое предлагает изменить зеленый цвет интерфейса WhatsApp на любой другой. Для активации пользователя вынуждают перейти по ссылке и установить вредоносное разрешение или программу.

В зависимости от операционной системы и устройства, которое использует жертва, загрузка программы происходит по двум сценариям.

Пользователям ПК и ноутбуков рекомендуется загрузить расширение для браузера Chrome под названием Black Theme for WhatsApp. После открытия мессенджера установленное расширение автоматически разошлет «заманчивое» предложение по списку контактов и групповым чатам. Данное расширение до сих пор доступно в интернет-магазине Chrome. В настоящий момент число загрузок достигло почти шестнадцати тысяч.

У пользователей смартфонов иной сценарий заражения – они получают уведомление о необходимости поделиться ссылкой с 30 друзьями или 10 чатами, только после этого появится возможность изменить цвет. Далее пользователь получает сообщение о необходимости скачать APK-файл под названием best_video.apk и подписаться на уведомления с русскоязычного ресурса. Если пользователь выполнит все инструкции, его мобильный телефон будет заражен трояном для показа рекламы, который продукты Eset NOD32 детектируют как Android/Hiddad. Пользователь изначально не замечает присутствие вредоносного ПО – демонстрация рекламных баннеров начинается только во время использования WhatsApp.

***

5.04.2019

Итальянская компания распространяла шпионское ПО через Google Play

В Италии ведется следствие в отношении производителя шпионского ПО, заразившего вредоносными приложениями как минимум 1 тыс. пользователей Google Play (InternetUA).

В конце прошлой недели специалисты организации «Безопасность без границ» (Security Without Borders) сообщили об обнаружении новой шпионской

платформы для Android-устройств, которое они назвали Exodus. Платформа состоит из двух компонентов – Exodus One и Exodus Two. За период с 2016-й по 2019 год исследователи собрали множество образцов вредоноса.

Образцы Exodus также были обнаружены в Google Play – злоумышленники в течение двух лет распространяли их под видом сервисных приложений от мобильных операторов. Несколько месяцев приложения находились в магазине, а затем добавлялись авторами заново.

Сами приложения, как и их страницы в магазине (в настоящее время все 25 приложений уже удалены из Google Play), были оформлены на итальянском языке. Каждое приложение было загружено по несколько десятков раз, но в одном из случаев число загрузок составило 350 раз. Все жертвы вредоноса проживают в Италии.

Exodus представляет собой мощное шпионское ПО с функцией сбора и перехвата данных. Хуже всего то, что вносимые вредоносом модификации делают зараженное устройство уязвимым к дальнейшим атакам.

Автором вредоносных приложений оказалась итальянская компания eSurv, специализирующаяся преимущественно на технологиях видеонаблюдения. Судя по материалам из открытых источников, с 2016 года eSurv занялась производством программного обеспечения для проникновения. Компания является подрядчиком государственной полиции Италии, однако неизвестно, использовалось ли ПО Exodus правоохранительными органами.

По данным итальянских СМИ, еще до публикации сообщения специалистов «Безопасности без границ» прокуратура Неаполя возбудила уголовное дело в отношении eSurv. Три недели назад правоохранители провели обыск в офисах компании по подозрению в незаконном перехвате данных и изъяли все компьютеры. C&C-инфраструктура Exodus была отключена.

***

6.04.2019

В браузере Chrome обнаружена опасная уязвимость

Уязвимость позволяет злоумышленнику удаленно выполнить произвольный код на системе жертвы. Проблема уже исправлена в V8 (JavaScript-движке браузера), но патч пока еще не добавлен в стабильную версию Chrome 73, используемую на более чем 1 млрд устройств.

Докладніше

***

6.04.2019

Обнаружен вредоносный код, атакующий пользователей онлайн-магазинов

Новый вредоносный код, обнаруженный компанией Group-IB, позволяет хакерам перехватывать данные банковских карт, адреса электронной почты, логины и пароли во время совершения онлайн-покупок (InternetUA).

В отчете компании говорится, что при заражении сайта так называемым JS-сниффером, пострадать могут все конечные пользователи, платежные системы, банки и крупные компании, торгующие своими товарами и услугами через интернет.

Специалисты Group-IB проанализировали почти 2,5 тыс. зараженных онлайн-магазинов. В некоторых случаях мошенникам достаточно просто перехватить данные. В других им приходится использовать поддельную платежную форму, которая подгружается с другого сайта.

Виктор Окороков, аналитик отдела кибербразведки Group-IB:

«Это такой тип вредоносного кода, который внедряется на сайт онлайн-магазина. Он предназначен для одной простой цели – красть данные кредитных карт пользователей, которые оплачивают покупки на этих сайтах. Дальше данные уже используются злоумышленниками для собственного обогащения: они либо продают это другим злоумышленникам, либо используют сами для оплаты покупок и последующей перепродажи товаров. Например, при помощи этих карт они могут получить iPhone, продать его и получить с этого наличные. Пока сайт заражен, страдает каждый, кто осуществляет там покупки».

По словам специалиста, пользователи почти беззащитны перед такими угрозами. Единственный способ обезопасить себя – это использование отдельной карты для совершения онлайн-покупок. Это поможет свести риски к минимуму даже в случае компрометации карты.

***

7.04.2019

Instagram отобрал никнейм пользователя и передал его королевской семье

Ваш никнейм в Instagram – это не личная собственность, которая безоговорочно принадлежит вам. Именно это познал на себе житель Великобритании, когда он проснулся утром и обнаружил, что его имя пользователя в Instagram было у него отобрано и передано более популярному пользователю.

Докладніше

***

8.04.2019

Большинство онлайн-банков содержат опасные уязвимости

Эксперты компании Positive Technologies оценили уровень защищенности онлайн-банков в 2018 г. и выяснили, что 54 % из обследованных систем позволяют злоумышленникам похитить денежные средства, а угрозе

несанкционированного доступа к личным данным и банковской тайне подвержены все онлайн-банки.

Докладніше

***

8.04.2019

Киберполиция начала масштабную операцию «Пираты»

Департамент киберполиции Национальной полиции Украины сообщил о начале операции «Пираты». Ее основной задачей является усиление противодействие преступлениям, совершаемым в сфере нарушений авторских прав правообладателей. Операция стартовала по всей стране и продлится до конца апреля (InternetUA).

В ведомстве напомнили, что в 2019 году Киберполиция уже прекратила деятельность 100 пиратских онлайн-кинотеатров, действующих на территории Львовской и Закарпатской областей, а также в Киеве.

«Мы должны научиться уважать интеллектуальный труд, ведь на первый взгляд, просмотр видеоленты на пиратском ресурсе не несет никакой угрозы для безопасности общества, но в то же время такие действия провоцируют злоумышленников в обход законодательства нарушать права других граждан, чьей собственностью и являются эти ленты», – сказал начальник департамента киберполиции Сергей Демедюк.

Он также добавил, что пираты не заинтересованы в предоставлении гражданам бесплатного доступа к просмотру видеопроизведений – основной их целью является получение денег за размещение рекламных объявлений на пиратских ресурсах.

«Такой заработок может стартовать от $500 долларов в месяц с одного сайта. При этом, нет гарантии того, что этот ресурс не несет в себе вредоносного программного обеспечения», – подчеркивает Демедюк.

Для эффективного противодействия пиратству в Украине Национальная полиция налаживает государственно-частное партнерство: уже подписан ряд меморандумов о сотрудничестве с медиагруппами «Старлайт Медиа», «Медиа Группа Украина», «Телерадиокомпания “Студия 1+1”», а также с Discovery Networks, Ассоциацией музыкальной индустрии Украины и «Украинской антипиратской ассоциацией», представляющей в Украине интересы крупнейших мировых медиа-корпораций.

Киберполиция также призывает правообладателей обращаться в подразделение с сообщениями о нарушении их авторских прав, заполнив форму обратной святи.

***

9.04.2019

Пользователям iOS угрожают шпионские приложения, записывающие звонки

Эффективность всевозможных барьеров, защищающих iOS от вредоносных приложений, находится на весьма высоком уровне. Поэтому даже если в App Store и проникают программы, которые ведут не совсем правомерную деятельность, их ждет незамедлительное удаление, а пострадавших – компенсация. Но как быть в ситуациях, когда ПО, ведущее слежку за пользователями, было установлено не из App Store, но при этом имеет официальный сертификат самой Apple (Украинский телекоммуникационный портал)?

По данным экспертов компании Lookout, им удалось зафиксировать еще несколько случаев злоупотребления программой Apple Enterprise Program, которая предназначена для сертификации приложений для корпоративного использования. Недобросовестные разработчики выдавали шпионское ПО за утилиты для улучшения качества сотовой связи в Италии и Туркмении. А поскольку доступ в App Store им был закрыт, они распространяли его через интернет, подписывая сертификатом компании Apple.

Шпионские приложения для iOS

Как и следовало ожидать, такие приложения не улучшали качество сотовой связи, а просто вели сбор данных о перемещениях пользователей, сохраняли их SMS-сообщения, контакты, фотографии, а также занимались прослушкой их телефонных разговоров. Примечательно, что вся собранная информация направлялась на сервер, с которым связаны вредоносные приложения для Android с компонентом Exodus. Таким образом не следует исключать, что злоумышленники могут начать распространение своих разработок и в других странах, в том числе в России.

Злоупотребление программой Apple Enterprise Program давно переросло из исключения в правило. Ранее в этом году Apple уличила Google и Facebook в распространении приложений для сбора данных. Компании подписывали свое ПО сертификатом Apple, нарушая соглашение, и привлекали к их установке пользователей, готовых делиться информацией о своих перемещениях и других действиях за деньги. В результате Apple отозвала сертификаты, но потом снова вернула их нарушителям.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

29.03.2019

У соціальних мережах проходить флешмоб на підтримку кримських татар

У соціальних мережах проходить флешмоб «Я солідарний з кримськими татарами». Акцію було організовано першим кримськотатарським телеканалом

ATR. Уповноважена Верховної Ради з прав людини Людмила Денисова однією з перших підтримала акцію, організовану активістами (День).

ATR закликає всіх небайдужих приєднатися до флешмобу, висловивши свій протест проти незаконних арештів і облав ФСБ на кримських татар в окупованому Криму.

Для участі у флешмобі необхідно в соцмережах опублікувати фото, вказавши хештег: #я_солідарний_з_кримськими_татарами.

***

2.04.2019

А як же зуб даю: у соцмережах нова хвиля – хештег #хочубачитидебати

У соцмережах набирає популярності новий флешмоб, у межах якого українські користувачі вимагають дебатів між кандидатами у президенти Петром Порошенком та Володимиром Зеленським перед другим туром виборів, який відбудеться 21 квітня.

До своїх дописів українці додають хештег #хочубачитидебати.

У Стамбулі приєдналися до флешмобу на підтримку затриманих кримських татар

***

3.04.2019

У Стамбулі приєдналися до флешмобу на підтримку затриманих кримських татар

Українці та кримські татари, які мешкають у Стамбулі, а також співробітники Генерального консульства України приєдналися до флешмобу «Я солідарний з кримськими татарами» (UA/TV).

Про це повідомляє прес-служба консульства на своїй сторінці в Facebook.

Захід організовано за ініціативи кримськотатарського телеканалу ATR. Учасники флешмобу висловили свою підтримку кримським татарам, заарештованим окупантами в результаті облав 27 березня на території незаконно анексованого півострова.

***

5.04.2019

Вибори 2019: соцмережі вибухнули жартами через аналізи Порошенка і Зеленського // Обидва кандидати здали аналізи, хоча і в різних лабораторіях

П’ятого квітня, кандидати на пост президента України Петро Порошенко і Володимир Зеленський, які вийшли до другого туру президентських перегонів, здали аналізи (НАРОДНА ПРАВДА).

Варто відзначити, що вчинок обох кандидатів викликав бурхливе обговорення в мережі, при цьому екс-чемпіон світу з боксу Володимир Кличко заявив, що готовий допомогти з організацією здачі аналізів кандидатів на пост президента України за міжнародними стандартами – у Світовому антидопінговому агентстві (WADA).

«Сьогоднішні ранкові новини про здачу “допінг контролю” кандидатами в президенти України мене здивували і трохи розсмішили! (Справді, якби так спортсмени здавали тести на допінг, то були б усі суперменами). Адже кожен зробив це окремо і причому в “своїй лабораторії“. Якщо ви так відкриті і зацікавлені в об’єктивному результаті, то зробіть це репутаційно перевіреним методом у міжнародній організації World Anti-Doping Agency (WADA)», – зазначив він на своїй сторінці в Facebook.

***

5.04.2019

Депутати Кропивницької міськради демонструють тенденції до публічності в соцмережах

Дмитро Сінченко

Кількість зареєстрованих профілів депутатів місцевих рад у соціальній мережі Facebook свідчить про позитивну тенденцію – діяльність депутатів місцевих рад з кожним роком стає все публічнішою.

Докладніше

***

8.04.2019

Концерт в Боярці та Ліга сміху: соцмережі обговорюють можливу дату проведення дебатів

Голова фракції БПП у Верховній Раді Артур Герасимов заявив, що президент Петро Порошенко згодний на дебати у будь-який день, зокрема і 19 квітня, як пропонував інший кандидат у президенти Володимир Зеленський (Прямий).

«Ми сподіваємося вже найближчим часом отримати відповіді на всі ключові питання, які цікавлять українське суспільство на дебатах. До речі, Петро Порошенко чекає Зеленського на дебати, по суті, і 14 квітня, і 19 квітня. Як то кажуть, “стадіон – так стадіон”», – сказав Герасимов.

Користувачі соцмереж почали активно обговорювати заяву Герасимова. У мережі з’явилася велика кількість коментарів та фотожаб.

***

9.04.2019

Рятувальники Київщини підтримали всеукраїнський флешмоб #«Не перешкоджай! Я рятую твоє життя!»

Останнім часом фіксується все більше випадків, коли рятувальники стикаються з агресивною поведінкою громадян. Тому вогнеборці Київщини долучаються до всеукраїнського флешмобу #«Не перешкоджай! Я рятую твоє життя».

Докладніше

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

27.03.2019

Соцсеть Pinterest официально объявила о планах выйти на биржу

Компания Pinterest, развивающая одноименную социальную сеть и фотохостинг, подала официальную заявку на первичное публичное размещение своих акций на бирже. Об этом сообщило информагентство «Рейтер» со ссылкой на данные Комиссии по ценным бумагам и биржам США (SEC) (InternetUA).

Pinterest планирует провести IPO в «ближайшее время». Газета The Wall Street Journal (WSJ) пишет, что компания может стать публичной в середине апреля 2019 года.

В поданной SEC заявке Pinterest утверждает, что продолжает искать новые способы заработка и находится на «ранних стадиях своей монетизации». Стратегия роста зависит от числа привлеченных рекламодателей, масштабирования бизнеса и улучшения рекламных инструментов, считает компания.

Pinterest позволяет хранить коллекции изображений и обмениваться ими. Пользователи сервиса могут добавлять в закладки понравившиеся картинки (пины) и создавать из них тематические коллекции (boards). К изображениям можно добавлять описание.

В сентябре 2018 года аудитория Pinterest превысила 250 млн человек, за год увеличившись на 50 млн пользователей.

За время работы с 2009 года компания привлекла в общей сложности 1,5 млрд долларов инвестиций. В 2017 году инвесторы оценивали Pinterest в 12,3 млрд долларов. WSJ пишет, что в рамках IPO будет стремиться к оценке рыночной капитализации в 12 млрд долларов.

***

28.03.2019

Исследование: как постят бренды и блогеры в украинском Instagram

Сервис аналитики профилей в украинском Instagram 22flr.com проанализировал около 300 000 публикаций, чтобы понять, в какое время и дни чаще всего публикуют блогеры и бренды. Ниже ключевые выводы исследования (Marketing Media Review):

Статистика по брендам. В 00 минут любого часа (e.g. 12:00, 13:00, 14:00 и т.д.) выходит в 2,5 раза больше постов, чем в любое другое время. На втором месте постинг в 30 минут (e.g. 12:30, 13:30, 14:30 и т.д.). Такую привязку к графику можно объяснить использованием сервисов отложенного постинга и следованию контент-планам, в которых тоже обычно указывают круглое время.

Также бóльшая активность по постингу приходится на первую половину дня. После 18:00 активность по постингу падает. Помимо прочего, активность брендов на выходные меньше, чем в будние.

Статистика по блогерам. Здесь более плавное распределение по часам и минутам, блогеры меньше привязаны к четкому графику, хотя в аналитике заметны небольшие скачки активности в 00 и 30 минут, т.е. часть лидеров мнений пользуются графиком либо сервисами отложенного постинга.

Также бóльшая активность по постингу приходится на вторую половину дня, что противоположно активности брендов.

Из аналитики можно догадаться, что во время, когда публикует большинство (9:00, 9:30, 10:00 и т.д.) конкуренция между постами будет выше и соответственно их увидит меньше людей.

Рекомендация сервиса – публиковать в менее активное время, экспериментировать с минутами и часами постинга, чтобы иметь шансы быть увиденными новыми людьми и теми, кто может вас не увидеть в «час пик».

***

2.04.2019

У Facebook хочуть створити окремий розділ з надійними новинами

Марк Цукерберг планує запустити в Facebook окремий розділ, у якому будуть зібрані новинні матеріали від якісних і надійних джерел.

Цю ідею він висловив під час бесіди з главою видавництва Axel Springer Матіасом Депфнером, пише Recode з посиланням на власні джерела. (Espreso.tv).

За задумом Цукерберга, окремий розділ підійде користувачам, які хочуть частіше дізнаватися новини з соцмережі. Щоб забезпечити доступність і якість матеріалів, Facebook може укласти прямі угоди з видавцями, припустив глава компанії.

У 2017 році Facebook тестувала окрему вкладку, в яку були б винесені всі новинні матеріали з основної стрічки, але це тестування закрилося навесні 2018 року. Новий проект, швидше за все, буде виглядати інакше і підійде людям, які хочуть читати Facebook як новинний рідер, пише видання.

Деталі новинного сервісу поки невідомі – у Facebook поки не вирішили, чи варто призначати конкретні виплати виданням або перераховувати їм

частину від рекламних доходів з певною мінімальною платою, каже джерело Recode.

Компанія також не знає, як формувати стрічку: на основі джерел, які вибирає користувач, або з ручним керуванням з боку Facebook, яким може зайнятися команда редакторів. Співрозмовник Recode передбачає, що новинний сервіс може бути запущений до кінця 2019 року.

***

2.04.3019
Андрей Юров
Facebook работает над секретным проектом

Разработчики компании Facebook последние пару ведут разработку секретного проекта по созданию специального интернет-дрона, который планируется к использованию в качестве альтернативного мобильного соединения. Беспилотник Facebook Стало известно, что в борьбе за первенство в интернет-среде, в Facebook приняли решение о запуске ряда проектов по подключению удаленных районов к Интернету. Один из таких, проект Catalina, который был запущен два года назад. В рамках данного проекта специалисты компании Facebook вели разработку над беспилотниками, которые по размеру похожи на птицу. К сожалению, больше информации о данном проекте пока нет (IT новости).

***

3.04.2019
Дмитрий Демченко
Instagram делает ставку на продажу товаров. Потенциально это $10 млрд выручки

Instagram активно развивает свое направление электронной коммерции, вводя новые возможности для покупки товаров прямо в приложении. Аналитики говорят, что такая стратегия станет успешной для соцсети – и принесет ей $10 млрд в 2021 году.

Докладніше

***

8.04.2019
Facebook хоче прокласти кабель навколо Африки, – WSJ

Про це повідомляє The Wall Street Journal (WSJ) (Espreso.tv).

Відповідний проект називається «Сімба». Facebook має намір полегшити собі доступ до користувачів на Африканському континенті.

Завданням даного проекту є збільшення пропускної здатності з'єднання і залучення нових клієнтів. Точний маршрут оптоволоконного кабелю наразі ще не визначений.

Джерела видання зазначають, що проект ще перебуває на стадії обговорення.

Окрім того, для Facebook це не перша спроба підключитися до реалізації подібних проектів. Однак раніше компанія розділяла інвестиції з телекомунікаційними компаніями, які не мали достатніх коштів для самостійного прокладання оптоволоконних трас.

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

27.03.2019

Instagram вплотную приблизился к Facebook по количеству подписчиков

В начале марта 2019 года в Украине насчитывалось около 11 млн пользователей социальной сети для обмена фотографиями Instagram. Об этом сообщило коммуникационное агентство PlusOne, добавив, что за минувшие 12 месяцев в полку почитателей платформы прибыло 3,7 млн украинцев (+50,7 %). А мобильное приложение Instagram вышло на 1-е место в Украине в категории социальные медиа (InternetUA).

Исследователи отметили, что если темпы роста Instagram сохранятся, то уже до конца текущего года число его пользователей вплотную приблизится по объему аудитории к Facebook.

В разрезе областных центров самое высокое проникновение Instagram – в Черновцах (71,5 %). И только на втором месте – Киев (68,5 %). Позиции с третьей по пятую также принадлежат западноукраинским городам: Тернополь (64 %), Ивано-Франковск (63,7 %) и Львов (63,3 %).

Наибольшей популярностью соцсеть для «фоточек» пользуется среди украинцев в возрасте 18-24 года – это 2,8 млн или 91 % представителей этой возрастной группы.

Более зрелые соотечественники менее привержены Instagram: среди 25-35-летних – 4 млн пользователей (54,3 %), в категории 36-45 лет – 1,8 млн (28,9 %).

Среди мобильных операционных систем (ОС), используемых для посещения этой социальной платформы, 2,6 млн – iOS и 8,5 млн – Android. Еще 100 тыс. заходили в Instagram с обеих ОС.

Самые популярные среди украинских «инстаграммеров» бренды смартфонов: Samsung – 3 млн, iPhone – 2,5 млн, Xiaomi – 2,5 млн, Huawei – 1,6 млн.

***

27.03.2019

Подтверждено появление ночного режима в WhatsApp для Android

WhatsApp, невзирая на статус самого популярного мессенджера современности, долгое время старался избегать трендов и игнорировал такое явление, как ночной режим. Однако, не сумев выстоять перед натиском пользователей, для которых возможность перевести интерфейс приложения в темные цвета стала настоящим культом, разработчики мессенджера сдались и приняли решение реализовать давно напрашивавшуюся функцию. Правда, пока только в предварительной версии (Украинский телекоммуникационный портал).

Ночной режим появился в последней бета-версии WhatsApp, однако все еще остается недоступным по умолчанию. Видимо, нововведение находится в ранней стадии тестирования, а потому не предназначается для массового пользователя. Тем не менее, те, кому все-таки посчастливилось оценить ночной режим, утверждают, что его активация переводит цвета интерфейса мессенджера в темно-серые тона, а не чисто черные, как это бывает в случае с подавляющим большинством приложений.

В чем польза ночного режима

Впрочем, даже такая реализация позволит одновременно решить две проблемы. Во-первых, темные тона снизят нагрузку на глаза при использовании мессенджера в условиях недостаточного освещения, а, во-вторых, окажут положительное влияние на автономность устройства. Ведь, как признала сама Google, даже IPS-экранам требуется существенно меньше ресурсов на отображение черных и серых цветов, чем белых, желтых или, скажем, зеленых.

Однако лично я, испытав ночные режимы в десятках приложений, так и не смог оценить их положительно. По непонятной для меня самого причине, темные цвета интерфейса с констрастирующими на нем белыми символами не только не успокаивает мои глаза, но, напротив, вынуждает их напрягаться еще больше. Как следствие, уже через пару минут безуспешных попыток расслабиться и убедить себя в том, что мне комфортно, я со слезящимися глазами спешил отключить ночной режим.

***

27.03.2019

Как и почему изменятся социальные сети в 2019 году

Если в 2018 году самые популярные соцсети были сосредоточены на мобильном видео, прямых трансляциях и поиске товаров, то в текущем году приоритеты поменялись. Согласно прогнозам Hootsuite, крупнейшие игроки рынка сделали ставки на новые технологические форматы и способы привлечения аудитории.

Докладніше

***

28.03.2019

Названо області, де найактивніше користуються «ВКонтакте»

Найбільше в Україні користуються забороненою соцмережею «ВКонтакте» в Донецькій, Дніпропетровській області та в місті Києві (InternetUA).

Про це свідчать результати дослідження «”Русский мир” та вибори в Україні: про що говорять у “ВКонтакте”».

«Перше місце за кількістю активних профілів “ВКонтакте” займає Донецька область. Друге – Дніпропетровська. Третє – Київ», – йдеться в опублікованому 27 березня дослідженні громадської організації «Інтерньюз-Україна».

Зазначається, що на четвертому місці Луганська область, але від неї не надто відстає Харківська та Одеська.

Дослідження проводилося з 1 листопада 2018 року до 14 лютого 2019 року. Аналітики дослідили 1 млн профілів українського сегменту VK та майже 10 млн постів.

***

28.03.2019

Skype сможет сам переключаться на говорящего участника группового звонка

Участникам программы предварительного тестирования Skype предложено протестировать новую функцию групповых звонков – Speaker view. С ней программа будет крупно показывать на экране только говорящего в данный момент участника группового звонка (InternetUA).

Режим Speaker view запущен на всех платформах в приложении версии 8.42.76.54 или более новой. На мобильных устройствах он активируется касанием переключателя вида в верхнем правом углу, на десктопах – в меню дополнительных параметров видео (также в верхней правой части экрана). Новшество наверняка будет полезно коммерческим пользователям Skype, часто проводящим собрания и собеседования в режиме группового видеозвонка. В дружеских и семейных беседах, где все галдят одновременно, удобнее будет прежний режим Grid View.

Ещё несколько улучшений для групповых звонков пока реализовано только в приложениях для Windows (8.42.76.55 и 14.42.54.0). Речь о возможности подключения к групповым звонкам с отключённым видео, а также автоматического размытия фона сразу после включения видео-изображения. Skype запомнит предпочитаемые вами настройки и самостоятельно применит их при следующем звонке. Кроме того теперь прямо во время звонка можно перейти в профиль одного из его участников,

просмотреть нужную информацию о нём и отправить личное сообщение, например.

Наконец, в приложении Skype для Microsoft Store (14.42.54.0) была реализована поддержка глобальных горячих клавиш. Теперь для отмены звонка, отключения и включения микрофона, не нужно вызывать на передний план окно Skype. Достаточно воспользоваться сочетаниями клавиш Ctrl+E и Ctrl+M.

***

28.03.2019

В WhatsApp для Android появилась новая функция

Разработчики популярного мессенджера WhatsApp выпустили свежую бета-версию 2.19.83 для мобильных устройств, которые работают под управлением операционной системы Android (InternetUA).

Помимо ночного режима Dark Mode, пользователи теперь могут опробовать возможность распознавания по отпечатку пальцев, без которого приложение попросту не откроется.

Функция идентификации по отпечаткам пальцев может быть активирована в разделе «Настройки» > «Учетная запись» > «Конфиденциальность» > «Использовать отпечатки пальцев».

WhatsApp также предоставляет пользователям возможность выбора времени автоматической блокировки через 1 минуту, 10 минут или 30 минут. Несколько неудачных попыток запустить WhatsApp при помощи не того отпечатка пальца заблокируют приложение на несколько минут.

Стоит добавить, что эта функция уже доступна на устройствах с iOS, причем кроме аутентификации по отпечатку пальца, пользователи также могут запустить приложение, используя распознавание лиц через Face ID.

Совсем скоро эти нововведения будут реализованы в стабильной версии мессенджера.

***

29.03.2019

В Instagram скоро добавят функцию перемотки видеороликов

Известная блогерша Джейн Вонг (Jane Manchun Wong), которая часто добывает инсайдерскую информацию, подтвердила, что в Instagram скоро появится функция перемотки видеороликов (InternetUA).

Свое сообщение Джейн Вонг подкрепила доказательством того, что ролик в Instagram действительно можно проматывать на нужную отметку.

Стоит добавить, что первая информация о тестировании данной функции появилась еще в январе этого года, однако этой очень простой возможности до сих пор нет у пользователей.

В Instagram по-прежнему действует максимальное ограничение в 60 секунд для видеороликов. В IGTV, сервисе на базе Instagram, можно загружать видеоролики продолжительностью до 60 минут, которые изначально можно было проматывать.

***

1.04.2019

Facebook позволил пользователям управлять новостной лентой

Facebook представил новую функцию для всех пользователей – «Почему я вижу этот пост». Открыв меню любой публикации, можно увидеть, почему она отображается в ленте (Marketing Media Review).

– Почему пост попал в выдачу: он от друга или группы/страницы, на которую вы подписаны.

– Какая информация больше всего повлияла на порядок постов: частота взаимодействия с контентом профиля, частота взаимодействия с записями определенного жанра, популярность постов.

– Инструменты для персонализации ленты.

Также Facebook обновил инструмент «Почему я вижу эту рекламу», которому уже более 4 лет. Теперь в нем будет отображаться информация о том, когда рекламодатель загрузил данные в соцсеть, и привлекал ли он стороннюю маркетинговую организацию.

***

3.04.2019

В WhatsApp добавили запрет на добавление в групповые чаты без разрешения

Месседжер WhatsApp позволил пользователям указывать, кто может добавлять их в групповые беседы.

Докладніше

***

5.04.2019

Instagram закрывает приложение для Windows Phone

Популярный социальный фото-сервис Instagram сообщил владельцам смартфонов с Windows о скором отказе от приложения для этой платформы. В качестве альтернативы им предлагается использовать веб-версию в браузере (InternetUA).

Решение вступает в силу 30 апреля, с этого дня «приложение Instagram для Windows Phone будет недоступно». Чтобы продолжить использование сервиса, пользователям предлагается обратиться к веб-сайту сервиса, который вряд ли полностью заменит им приложение.

Заметим, что предупреждение об отказе от приложения получили и пользователи Windows 10 Mobile, то есть под Windows Phone вероятно подразумеваются все смартфоны с Windows. Можно предположить, что доля обладателей этих устройств среди пользователей Instagram снизилась до совсем крошечных цифр и дальнейшая поддержка приложения более нецелесообразна. Нет нужды в мобильном приложении Instagram и у Microsoft. Даже если гибридный смартфон со складным экраном Andromeda когда-нибудь доберётся до полок магазинов, его пользователям будет доступно PWA-приложение для Windows 10.

***

9.04.2019
Viber нанес «удар» по WhatsApp и Telegram

В тройку самых популярных в мире сервисов для общения входят WhatsApp и Telegram, которые активно конкурируют друг с другом, а их прямым конкурентом является белорусский мессенджер Viber, создатели которого постоянно добавляют в него новые возможности. Девятого апреля 2019 года, всем пользователям данного программного обеспечения стала доступна такая возможность, которой нет в сервисах-конкурентах, и это должно стать его визитной карточкой, считают разработчики (Украинский телекоммуникационный портал).

Создатели Viber добавили в приложение такую функцию, как «Местные номер», а переводится она как Local Number. С ее помощью можно получить себе в постоянное пользование европейский или же американский номер, чтобы с его помощью совершать звонки и отправлять сообщения SMS, хотя он также подходит для того, чтобы их принимать. Это реальная возможность получить доступ к таким функциональным возможностям, которые ранее всегда были недоступны, по крайне мере в WhatsApp, Skype, Telegram и их аналогах.

Как считает администрация сервиса для общения, новая функциональная возможность превращает Viber в идеального спутника во время путешествия, так как за совсем скромную сумму денег абонент может сам выбрать любой желаемый номер телефона, который станет его на 30 дней или иной промежуток времени.

В эту сумму уже включены безлимитные звонки и сообщения SMS на местные номера, то есть, например, купив номер США, можно будет бесконечно много и долго общаться с жителями страны, а предоставлять при этом каких-либо паспортных данных не придется. При этом приложение Viber является чем-то вроде платформы для управления номером, ведь можно не только совершать звонки, но и принимать их. В настоящее время имеется возможность оформить номера для Великобритании, США и Канады, но в скором будущем их станет больше.

***

8.04.2019

Пользователи YouTube получили новую бесплатную функцию

Режим «Картинка в картинке», который ранее был доступен только в платной Android-версии YouTube, становится доступным обычным пользователям (InternetUA).

Два года назад компания Google представила режим «Картинка в картинке» (PiP) для приложения YouTube в Android, однако, воспользоваться им могли только пользователи платных подписок RED/Premium.

В июне 2018 стало известно, что все пользователи приложения YouTube в США получили доступ к данной функциональности, даже не имея платной подписки, сообщает Ixbt.

Тогда мы предположили, что Google сделает функциональность доступной и в других регионах мира. Так и случилось, однако для этого компании потребовалось не несколько дней/недель, а чуть ли не целый год.

Пока что поступили подтверждения от рядовых пользователей YouTube из Италии. Как ожидается, в ближайшие дни эта возможность появится в остальных регионах Европы.

При использовании режима «Картинка в картинке» приложение YouTube сворачивается и вы видите видеоролик в небольшом плавающем окне на домашнем экране.

Данный режим включается в разделе «Настройки»>«Общее», но он поддерживается не всеми видеороликами. Минимальной версией операционной системы является Android 8.0 Oreo.

***

9.04.2019

Объявлен «закат» видеохостинга YouTube

Видеохостинг YouTube находится в глубоком кризисе из-за нескольких факторов, которые оказали большое влияние на сервис и его роль в жизни интернет-сообщества, пишет The Verge.

Докладніше

ДОДАТКИ

Додаток 1

27.03.2019

В Калифорнии школьникам хотят запретить смартфоны

Ассамблея штата Калифорния представила законопроект, который ограничивает использование мобильных телефонов в школах. С инициативой выступил демократ Альберт Мурацучи (InternetUA).

Он предлагает ввести полный или частичный запрет на применение гаджетов в учебных заведениях и на прилегающих территориях. Если закон примут, то нести ответственность за соблюдение новых правил будет администрация школы.

Как поясняет CBS Sacramento, учащимся разрешат брать с собой гаджеты, но использовать их можно будет только в экстренной ситуации или в учебных целях на занятиях.

«Беспрепятственный доступ к смартфонам мешает школам выполнять педагогические задачи, снижает успеваемость, разжигает травлю в интернете, а также вызывает тревожность, провоцирует депрессию и суициды», – говорится в законопроекте.

Мурацучи ссылается на исследование Лондонской школы экономики (Великобритания), проведенное в 2015 году. Эксперименты показали, что учащиеся школ, в которых смартфоны запрещены, демонстрировали более высокие результаты на тестировании. Исследователи приравняли эффект от запрета гаджетов к эффекту от недели дополнительных занятий.

Законопроект также упоминает результаты опроса, который обнаружил связь между депрессией и временем, проведенным в интернете. Восьмиклассники, которые проводят в сети больше 10 часов в неделю, считают себя счастливыми в полтора раза реже реже, чем их сверстники.

Аудитория мобильных устройств молодеет с каждым годом, и дети все больше времени проводят в интернете. Согласно опросу, проведенному в 2011 году, дошкольники в среднем проводят около четырех часов в день за экранами мобильных устройств, компьютеров и телевизоров.

Другое исследование показало, что 78 % подростков не могут обойтись без смартфона больше часа. Половина респондентов признала, что испытывает зависимость.

Многие калифорнийские школы уже ограничили детям доступ к мобильным телефонам. Учащихся младших и средних классов обязаны отключать устройства на время занятий, а старшеклассникам позволяют включать гаджеты только после получения разрешения от учителя.

Во Франции учащимся запретили приносить в школу смартфоны и планшеты еще в августе прошлого года.

Масштабные исследования о влиянии гаджетов на детскую психику пока дают противоречивые результаты. Недавно американские эксперты выяснили, что под влиянием мобильных устройств школьники 11-13 лет становятся нелюбознательными, а подростки в возрасте от 14 до 17 лет теряют способность концентрироваться на задачах.

(вгору)

Додаток 2

27.03.2019

Ирина Фоменко

Исследование: чрезмерное использование смартфона вызывает потерю сна

Согласно австралийскому исследованию, обнаружившему скачок «техноференции» за последние 13 лет, из-за чрезмерного использования мобильных телефонов люди теряют сон и становятся менее продуктивными. Об этом сообщает Gadgets Now (InternetUA).

Исследователи из Квинслендского технологического университета (QUT) в Австралии опросили 709 пользователей мобильных телефонов в возрасте от 18 до 83 лет в 2018 году, используя опрос 2005 года.

Затем они сравнили результаты и обнаружили значительное увеличение числа людей, обвиняющих свои телефоны в потере сна, продуктивности, бдительности во время вождения, а также о наличии большего количества заболеваний.

«Когда мы говорим о техноференции, мы имеем в виду ежедневные “вторжения и перерывы”, которые люди испытывают из-за мобильных телефонов. Наше исследование показало, что техноференция среди мужчин и женщин увеличилась во всех возрастах. Например, самоотчеты, касающиеся потери сна и продуктивности, показали, что количество негативных результатов значительно возросло за последние 13 лет», – заявил Оскар Овьедо-Треспаласиос из QUT.

Результаты, опубликованные в журнале Frontiers in Psychiatry, показывают, что мобильные телефоны потенциально все больше влияют на аспекты дневного функционирования из-за недостатка сна и растущего неисполнения обязанностей.

Согласно опросу, каждая пятая женщина (19,5 %) и каждый восьмой мужчина (11,8 %) теперь теряют сон из-за времени, которое они тратят на смартфон.

Около 12,6 % мужчин заявили, что их производительность снизилась как прямой результат времени, которое они проводят за телефоном – по сравнению с отсутствием в 2005 году – и 14 % женщин также заметили падение уровня производительности.

Более 54 % женщин считают, что их друзьям будет трудно связаться с ними, если у них нет мобильного телефона (по сравнению с 28,8 %), и 41,6 % мужчин думают так же.

По словам исследователей, около 8,4 % женщин и 7,9 % мужчин страдают от заболеваний, которые они связывают с использованием мобильных телефонов.

Результаты опроса также показали, что телефоны использовались в качестве стратегии выживания: каждая четвертая женщина и каждый шестой мужчина говорят, что они предпочли бы использовать свой телефон, а не решать более насущные проблемы.

«Быстрые технологические инновации за последние несколько лет привели к кардинальным изменениям в современной технологии мобильных телефонов – они могут улучшить качество жизни пользователей, но также могут привести к некоторым негативным результатам. К ним относятся беспокойство и, в некоторых случаях, рискованное поведение с серьезными последствиями для здоровья и безопасности, такими как отвлечение от вождения», – прокомментировал Овьедо-Треспаласиос.

(вгору)

Додаток 3

28.03.2019
Ирина Фоменко
IT-гиганты помогут Трампу в борьбе с фейковыми новостями

Бюро переписи населения США обратилось к техническим гигантам Google, Facebook и Twitter с просьбой помочь в борьбе с кампаниями фейковых новостей, которые могут нарушить предстоящий подсчет 2020 года. Об этом сообщает The Star Online (InternetUA).

Среди доказательств предстоящих кампаний – чаты на платформах типа 4chan со стороны отечественных и зарубежных сетей, стремящихся подорвать исследование. Перепись является важной целью, поскольку формирует избирательные округа США.

Заместитель директора Бюро Рон Джармин подтвердил, что организация предвидит кампании по дезинформации и заручается поддержкой крупных технологических компаний для отражения угрозы. «Мы ожидаем, что (перепись) станет целью для такого рода усилий в 2020 году», – заявил Джармин. – «С 2017 года представители Бюро проводят многочисленные встречи с техническими компаниями».

Пока что Бюро заручилось поддержкой Google, Twitter Inc и Facebook Inc. Представитель Facebook Адам Стоун подтвердил встречи с госучреждениями, но не предоставил подробностей о каких-либо согласованных действиях. Twitter и Google отказались от комментариев.

По словам представителей Бюро, организация приступила к «онлайн-захвату земли» для контроля сайтов, похожих на ресурсы госучреждения. Эти сайты могут оказаться в руках людей, которые хотят помешать переписи.

«Мы составили список из 20-30 URL-адресов. Контролируем как минимум два негосударственных веб-сайта с переписью – 2020census.com и 2020census.org – через маркетинговую компанию Reingold», – поделился пресс-секретарь Census Стивен Бакнер.

Бюро переписей до сих пор в основном молчало о планах борьбы с дезинформацией. Усилия подчеркивают проблемы, которые Интернет-эпоха ставит перед десятилетним сбором данных о населении Америки.

По мнению кибер-экспертов, так называемые стратегии «фейковых новостей» могут принимать множество форм: выдавать себя за

демографическую группу, которая передает ложную информацию под предлогом защиты интересов; распространение фейковых данных путем размещения рекламы и новостей; или распространение поддельной информации, чтобы вызвать страх и противодействие.

«Активисты будут пытаться заставить людей не участвовать в переписи, запугивая или говоря им, что это не важно, или, например, что уплата налогов автоматически засчитается в перепись», – считает Джармин.

Помощь от Силиконовой долины

Бывший директор Бюро Джон Томпсон заявил, что первый брифинг об угрозе дезинформации – вскоре после президентских выборов 2016 года – побудил организацию действовать.

Год спустя Бюро переписей организовало в Силиконовой долине форум, частично посвященный угрозе дезинформации в 2020 году, в котором приняли участие местные должностные лица и представители технологических компаний, включая Twitter, Uber Technologies и Microsoft Corp. Во время этой встречи представители Бюро также посетили кампусы Facebook и Google, чтобы встретиться с руководителями.

Согласно отчетам Reuters, Google сообщил Бюро, что рассмотрит вопрос о создании специального поискового проекта, связанного с переписью. Twitter также согласился помочь снизить количество дезинформации.

На встрече с Facebook чиновники обсуждали возможность присоединения компании к беседам между Бюро и Министерством обороны США о безопасности; создание групп в Facebook на темы переписи; и обучение работников Бюро через технологию Facebook.

(вгору)

Додаток 4

28.03.2019

Facebook будет блокировать проявления белого национализма и сепаратизма

С начала апреля компания Facebook заблокирует проявления белого национализма и сепаратизма в своей соцсети, а также в Instagram. Об этом говорится на сайте компании (InternetUA).

«Сегодня мы объявляем о запрете похвалы, поддержки и представления белого национализма и сепаратизма в Facebook и Instagram, который мы начнем применять на следующей неделе. Понятно, что эти концепции тесно связаны с организованными группами ненавистников и им нет места в наших сервисах», – говорится в сообщении.

Отмечается, что политика компании уже давно запрещает ненавистническое обращение с людьми, основанное на таких признаках, как раса, этническая принадлежность или религия. Изначально в Facebook не применяли такое же обоснование к выражениям белого национализма и сепаратизма, потому что имели в виду более широкие концепции национализма

и сепаратизма – например, такие, как американская гордость и баскский сепаратизм. Они, по мнению Facebook, являются важной частью идентичности людей.

Но представители гражданского общества и ученые-эксперты в области расовых отношений подтвердили, что белый национализм и сепаратизм невозможно отделить от идеи превосходства белой расы и организованных групп ненависти.

В Facebook подчеркивают, что хотя в дальнейшем люди все еще смогут демонстрировать гордость за свое этническое наследие, компания не потерпит похвалы или поддержки белого национализма и сепаратизма.

Контент, исполненный ненависти, будут находить и удалять с платформ компании, заявляют в Facebook.

Также в компании говорят, что людей, которые ищут термины, связанные с превосходством белых, будут перенаправлять на ресурсы, которые нацелены на то, чтобы помочь людям избавится от ненависти. Для этого будет задействована организация Life After Hate, которая была основана бывшими воинствующими экстремистами. Ее деятельность направлена на кризисную работу, образование и поддержку.

Ранее Facebook разрешал какой-либо контент, касающийся белого национализма, который он не рассматривал как расистский.

После стрельбы в начале этого месяца в Новой Зеландии несколько мировых лидеров призвали руководителей социальных сетей взять на себя больше ответственности за экстремистские материалы, размещаемые на их платформах.

Премьер-министр Новой Зеландии Джасинда Ардерн сказала, что социальные сети являются «издателем, а не просто почтальоном», имея в виду их потенциальную ответственность за материалы, которыми обмениваются пользователи аккаунтов.

(вгору)

Додаток 5

28.03.2019

Російські спецслужби активізувалися в українському інформаційному просторі

Співробітники Служби безпеки України у ході виконання завдань з контррозвідувального забезпечення інформаційної безпеки протягом 2019 року фіксують потужну активізацію спецслужб РФ в інформаційному просторі нашої держави напередодні виборів Президента (InternetUA).

Країна-агресор всіма засобами намагається вплинути на виборчий процес через маніпулятивний вплив на електоральні настрої громадян України з використанням загальнодоступних та соціальних ресурсів мережі Інтернет.

Упродовж січня - березня 2019 року оперативники СБ України викрили та припинили протиправну діяльність розгалуженої та глибоко законспірованої

агентурної мережі Інтернет-агітаторів, до якої входили жителі Київської, Одеської, Миколаївської, Запорізької, Дніпропетровської, Сумської та Чернігівської областей. Учасники мереж за вказівкою своїх російських кураторів через соціальні мережі «Facebook», «ВКонтакте» та «Twitter» поширювали в регіональних і загальнодержавних сегментах мережі Інтернет деструктивні матеріали, спрямовані на штучне загострення суспільно-політичної ситуації напередодні та під час проведення президентських виборів у країні.

Лише за перший квартал 2019 року оперативні працівники СБУ задокументували сімнадцять фактів втручання російських спецслужб у виборчі процеси в країні через проплачене поширення фейкової інформації для маніпуляції суспільною свідомістю користувачів соціальних мереж. Зокрема, 26 березня у Запоріжжі співробітники СБ України під процесуальним керівництвом прокуратури викрили чергового антиукраїнського Інтернет-агітатора, який діяв на користь країни-агресора.

Правоохоронці встановили, що для протиправної діяльності кураторами з РФ використовувались понад п’ятдесят груп у соціальних мережах з аудиторією понад півтора мільйона користувачів.

Наразі продовжується проведення контррозвідувальних заходів та вирішується питання щодо притягнення причетних осіб до кримінальної відповідальності.

Служба безпеки України у рамках своєї компетенції здійснює комплекс вичерпних заходів з протидії втручанню країни-агресора у виборчий процес та вкотре звертається до українських користувачів Інтернету з проханням бути уважними і у разі отримання від невідомих осіб пропозицій щодо поширення в соцмережах фейкової інформації, насамперед антиукраїнського спрямування, повідомляти на гарячу лінію СБУ (0 800 501 482).

(вгору)

Додаток 6

2.04.3019

Владимир Кондрашов

В нацкомиссии раскритиковали «пророссийский» законопроект о блокировках сайтов

Национальная комиссия, осуществляющая госрегулирование в сфере связи и информатизации, считает нецелесообразным принятие проекта закона, которым устанавливается уголовная ответственность за распространение недостоверных сведений в СМИ и интернете, а на НКРСИ ложится функция принимать решение об обязательствах операторов, провайдеров телекоммуникаций о приостановлении доступа абонентов к ресурсу сети Интернет (InternetUA).

Как мы уже сообщали ранее, 12 марта нардеп от «Народного фронта» Игорь Лапин зарегистрировал законопроект № 10139 «О внесении изменений в

некоторые законодательные акты Украины относительно предотвращения распространения недостоверных сведений в средствах массовой информации», которым предлагается установить уголовную ответственность за распространение недостоверных сведений в СМИ и интернете. При этом ответственность наступает независимо от того, сознательно ли СМИ распространили недостоверную информацию или сделали непреднамеренную ошибку. Кроме того, специалисты телеком-отрасли сразу же указали на схожесть украинского законопроекта с печально известным российским законом о «запрете фейков». Против законопроекта высказались участники коалиции «За свободный Интернет!».

– Законопроектом в Законы Украины «О выборах Президента Украины» и «О выборах народных депутатов Украины» предлагается включить положения, которыми предусматривается, что в случае установления судом при рассмотрении избирательного спора повторного или одноразового грубого нарушения СМИ требований соответствующего закона, суд принимает решение, в частности, об обязательстве оператора, провайдера телекоммуникаций о приостановлении доступа абонентов к соответствующему ресурсу в сети Интернет. Также законопроектом полномочия НКРСИ, предусмотренные статьей 18 ЗУ «О телекоммуникациях», предлагается дополнить полномочием о принятии решения об обязательстве операторов, провайдеров приостанавливать доступ абонентов к ресурсу в сети Интернет, распространяющем недостоверную информацию, до момента её опровержения (при наличии соответствующего решения суда), – объяснили в НКРСИ.

По результатам рассмотрения законопроекта в аппарате НКРСИ предложили утвердить вывод о выражении позиции о нецелесообразности принятия законопроекта в связи с замечаниями к нему.

– Во-первых, указанные положения законопроекта не согласовываются между собой: в одном законе предусматривается решение суда, а в другом – решение НКРСИ о соответствующем обязательстве оператора, провайдера. Во-вторых, касательно реализации предложенного законопроектом полномочия НКРСИ: законопроектом не определена информация, которая должна содержаться в решении суда об опровержении недостоверной информации для надлежащего его исполнения. В-третьих, в изменениях в законы «О выборах Президента Украины» и «О выборах народных депутатов Украины» не определены временные рамки приостановления доступа абонентов к соответствующему ресурсу, а именно то, когда оператор, провайдер должны возобновить соответствующий доступ, а изменениями ЗУ «О телекоммуникациях» не определены источники, через которые операторы, провайдеры телекоммуникаций должны узнать об опровержении недостоверной информации для возобновления доступа. В-четвертых, учитывая то, что услугу доступа к Интернету предоставляют около 5,5 тысяч операторов, провайдеров, возникает вопрос о механизмах информирования таких субъектов об упомянутых решениях, – считают в НКРСИ.

Позицію о нецелесообразности принятия данного проекта закона члены НКРСИ поддержали единогласно.

(вгору)

Додаток 7

5.04.2019

Австралия будет сажать руководителей соцсетей в тюрьму за «отвратительные» посты

Трансляция террористом бойни в двух мечетях Новой Зеландии на Facebook спровоцировала резкую реакцию законодателей в соседней стране: не имеющий аналогов закон принят подавляющим большинством и без особых обсуждений (InternetUA).

В Австралии принят первый в демократическом мире закон об уголовном наказании для владельцев соцсетей за содержание постов на их платформах – вплоть до многолетнего тюремного заключения. Страна, где техногигантов уже обязали предоставлять властям все данные о пользователях, устанавливает новые барьеры. И жители это одобряют, отмечает New York Times.

Новый закон стал резкой и быстрой реакцией на бойню в Крайстчерче. 28-летний расист Брентон Таррант расстрелял 50 человек в двух мечетях, ведя прямую трансляцию своих преступлений с помощью Facebook Live.

Со времени этого теракта не прошло и месяца, а законопроект был принят за пять дней – без обсуждения и почти единодушно. Что вполне отразило позицию большинства австралийцев о том, что соцсети должны нести ответственность за размещенный у них пользователями контент.

Но по-настоящему закон выделяется не направленностью, а жесткостью: соцсети предлагается штрафовать на сумму до 10 % годовой прибыли. А их руководителям, которые откажутся удалить «отвратительный контент», грозит до трех лет тюрьмы.

Под «отвратительным» австралийские законодатели имеют в виду четыре категории: изображения террористических актов, убийств, изнасилований или похищений.

Австралийские медиа и IT-гиганты выступили против закона, указав, что он ограничит свободу слова, а отвечающие теперь своими миллиардами за контент компании в момент появления не в силах его оценить.

Google, Facebook и Amazon добавили, что закон навредит отношениям Австралии с другими странами, поскольку предполагает «проактивную» слежку за пользователями со всего мира.

Механизм реализации закона пока неясен. Например, прописано требование «оперативно» удалять информацию, и такая расплывчатая формулировка сама по себе может вызвать длительные обсуждения в судах по поводу того, как соцсети могут и должны соблюдать новое уложение.

В Германии похожий закон касается нелегального контента – например, пиратских копий фильмов – и его требуется удалять «в течение 24 часов». Даже

такой срок – неизвестно, насколько «оперативный» по меркам австралийских законодателей – часто представляет серьезную трудность для местных провайдеров.

Если сроки будут более сжатыми, потребуются иные механизмы, которые могут привести к широким оперативным блокировкам.

Усилить регулирование соцсетей требуют и британские парламентарии. По итогам масштабного расследования, занявшего полтора года, практики ведения бизнеса Facebook там сравнили с действиями гангстеров.

(вгору)

Додаток 8

6.04.2019

Ирина Фоменко

Что скрывается за внезапным принятием государственного регулирования Facebook

Генеральный директор Facebook Марк Цукерберг призвал к усилению государственного надзора и даже регулирования Интернета. По его словам, пришло время для правительств во всем мире активизировать работу и помочь обуздать Интернет, пишет Tech News World (InternetUA).

Главный контроль должен быть над «вредным контентом». Цукерберг утверждал: только обновив правила для Интернета можно будет сохранить лучшее – в том числе позволить людям свободно выражать свое мнение, а предпринимателям – создавать новые вещи.

4 области регулирования

Цукерберг нацелен на четыре области усиления государственного регулирования: вредный контент, честность выборов, конфиденциальность и переносимость данных.

Что касается вредоносного контента, то замечания Цукерберга позволяют предположить – он не считает, что социальные сети должны отвечать за различие между действительной «свободой слова» и «опасной речью».

Вместо этого регуляторы должны определить, что может расцениваться как пропаганда терроризма или разжигание ненависти, а интернет-компании – нести ответственность за соблюдение установленных ими стандартов.

Цукерберг отметил, что некоторые законодатели уже жаловались, что у Facebook слишком много полномочий для суждений о том, что на самом деле является вредоносным контентом.

Цукерберг также призвал принять закон, который обеспечит большую защиту для выборов. Facebook уже внес изменения в процессы покупки политической рекламы, включая создание архива с возможностью поиска, который показывает, кто фактически заплатил за подобные объявления.

Что касается вопросов конфиденциальности и защиты данных: граждане всего мира призвали к всеобъемлющему регулированию конфиденциальности, которое будет соответствовать Общему регламенту по защите данных (GDPR).

Цукерберг также писал, что любое регулирование Интернета должно гарантировать принцип переносимости данных, поэтому, если информация используется совместно с одним сервисом, ее можно переместить в другой. Это дало бы индивидуальный выбор, позволяя разработчикам внедрять инновации и конкурировать.

Резкая смена курса Facebook

Время «манифеста» Цукерберга примечательно, поскольку федеральные прокуроры США начали расследование действий Facebook, связанных с обменом данными с другими крупными технологическими компаниями. Европейские чиновники также пристально наблюдают за социальной платформой из-за предполагаемых нарушений обмена данными.

Facebook уже столкнулся с Федеральной торговой комиссией США (FTC) и многомиллиардным штрафом, сейчас компания ведет переговоры о возможном урегулировании, чтобы закончить годичное расследование FTC о конфиденциальности.

FTC пристально следит за действиями компании, включая то, как она собирает и обрабатывает данные. Информация о пользователях используется в рекламном бизнесе Facebook, поэтому вполне вероятно, что призывы Цукерберга к регулированию могут быть связаны не столько с сохранением Интернета, сколько с сохранением прибыльной бизнес-модели социальной платформы.

Необходимость регулирования

Каким бы ни было обоснование для Цукерберга в отношении регулирования, оно запоздало. «Я рад видеть, что есть признание необходимости регулирования со стороны Цукерберга. Facebook контролировал “диалог” о границах конфиденциальности около десяти лет. Само собой разумеется, что компания не очень хорошо справилась с этой задачей; государственному и частному сектору необходимо определить соответствующее законодательство в партнерстве, чтобы сбалансировать масштабы для пользователей и интернет-платформ», – заявил главный аналитик Netpop Research Джош Крэндалл.

Также настало время, когда некоторые интернет-гиганты, в том числе Facebook, должны играть по основным правилам – регулирующим то, как компании могут конкурировать на равных в США и даже на мировых рынках. Вопрос в том, что должен включать такой контроль?

«Более строгие условия конфиденциальности и использования данных – это одна из областей, которую можно улучшить. Другой способ – заставить платформы принять открытые стандарты и протоколы для часто используемых сервисов, таких как идентификация и гео – например, карты, – которые будут управляться общественной организацией и финансироваться платформами», – считает Крэндалл.

Для отвода глаз?

Кредо Цукерберга может оказаться не более чем обманом. Как часто лидер отрасли предлагает нормативные акты, которые должно ввести

правительство? Это может быть случай предложения только того, что человек готов отказаться.

«Призыв “спасти интернет” – для отвода глаз. Цукберг прекрасно знал, что его бизнес-модель основана на продаже нашей личной информации, особенно поведения. Все разговоры о том, чтобы принести извинения за нарушения конфиденциальности и попытки это исправить – чепуха», – заявил консультант по социальным медиа Лон Сафко.

Что может означать большее регулирование

Если призывы Цукерберга к регулированию будут приняты, могут быть компромиссы для всех участников. «Нормативный надзор заставит компанию пересматривать свои решения, что почти всегда сокращает инновации и замедляет разработку новых продуктов и процессов. Однако регулируемые компании в определенной степени защищены от конкуренции, поскольку контроль создает барьеры для выхода на рынок», – утверждает вице-президент Competitive Enterprise Institute Иэн Мюррей.

Таким образом, римская концепция «Кто устережет самих сторожей?» отражена в том, кто регулирует контролирующие органы. «Однако возможно и обратное: прежние регулирующие органы начинают укомплектовывать компанию, что снижает вероятность оспаривания действий контролирующей организации. Любая версия регулятивного захвата усиливает эффект барьеров выхода на рынок. В CEI мы придерживаемся мнения, что, хотя регулирование может принести пользу компании, устанавливая эти барьеры, компромиссы всегда вредны для отрасли в целом, конкуренции, потребителей и самой компании в долгосрочной перспективе», – убежден Мюррей.

Против регулирования

Ряд факторов может помешать любому такому регулированию Интернета. Первая поправка к Конституции США является, пожалуй, самым большим препятствием. Тем не менее, по словам Мюррея, другие страны могут легко навязать подобное регулирование, например, запрет на публикацию «кощунственного» контента.

Стоимость регулирования на свободном рынке является еще одним фактором. «Регулирование конфиденциальности потребителей может строго ограничивать то, для чего Facebook и его партнеры используют данные пользователей, и может настаивать на том, чтобы потребители имели право удалять свои данные и переносить их в другое место», – прокомментировал Мюррей. – «Регуляторы ЕС налагают штрафы на успешные технологические компании, которые, по их мнению, нарушают правила конкуренции».

Основанием для более строгого регулирования является создание свода правил для всех игроков. «Именно правительственные инвестиции в DARPA создали фундамент, на котором были построены сегодняшние платформы. Без разумного регулирования трудно понять, как интернет-платформы будут делать это самостоятельно. Существуют риски, связанные с любыми изменениями, и новые правила ничем не отличаются от других рыночных сил. В идеале,

правильная комбинация правил даст возможность следующему поколению предпринимателей самим создавать ценности», – считает Крэндалл.

Обход правил

Другим соображением для любого предложенного регулирования будет то, является ли оно обязательным для исполнения. Опытные пользователи находят обходные пути.

«Мы уже наблюдаем более широкое использование виртуальных частных сетей в ЕС для обхода ограничений GDPR. В некотором смысле это отражает использование VPN в репрессивных режимах; регулирование контента почти наверняка приведет к использованию даркнета для передачи цифрового самиздата. Чем более ограничено регулирование контента, тем больше вероятность того, что люди, которые ранее пользовались социальными сетями, обнаружат, что изучают даркнет», – заявил Мюррей.

Последний фактор – это «конфиденциальность», но во многих случаях люди действительно обеспокоены «безопасностью» данных. «Они рады поделиться своими данными с другими, чтобы получить какую-то выгоду, будь то скидки в супермаркетах или бесплатные продукты. Они недовольны тем, что эта информация остается в небезопасности. Непонятно, в какой степени государственное регулирование может обеспечить защиту без ущерба для выгод, которые нравятся людям», – пояснил Мюррей.

(вгору)

Додаток 9

27.03.2019

Чем опасны предустановленные приложения для Android

Приложения, которые производители предустанавливают на свои смартфоны, зачастую могут оказаться не менее опасными, чем шпионское ПО из ненадежных источников. Об этом предупреждают исследователи Мадридского университета им. Карлоса III при сотрудничестве экспертов из Международного института компьютерных наук Беркли и Университета штата Нью-Йорк в Стоуни-Брук. Они изучили более 1700 устройств 214 брендов и пришли к выводу, что поставляемое с ними ПО может подвергать их владельцев необоснованному риску (InternetUA).

Проблема, как ни странно, кроется не в факте предустановки приложений на смартфоны, а в системе разрешений Android, которую они эксплуатируют. Из-за того, что эти программы устанавливаются на устройства самим производителем, то они по умолчанию имеют те привилегии, которые сам пользователь, возможно, им бы ни за что не предоставил. В результате приложения могут беспрепятственно отслеживать действия пользователя и отправлять их удаленный сервер.

Предустановленные приложения для Android

Ситуация осложняется еще и тем, что предустановленные приложения в подавляющем большинстве случаев не подлежат удалению. Взять хотя бы

Facebook, который, будучи установленным «из коробки», уже не может быть стерт из памяти устройства. Единственное, что предлагает производитель – остановить работу клиента социальной сети, что, однако не является его полным удалением, не говоря уже о приложениях-компаньонах, которые также анализируют всю вашу деятельность на устройстве.

По словам представителей Google, компания тщательно следит за приложениями, которые производители устанавливают на свои смартфоны. Якобы все они прошли проверку безопасности и, следовательно, не могут считаться вредоносными. Тут Google совершенно явно лукавит. Действительно, ни Facebook, ни Firmware scanner, ни Lumen Privacy Monitor не воруют данные банковских карт и не выдают себя за легитимное ПО. Зато они ведут слежку за вашими перемещениями и отправляют эти данные рекламодателям. Но Google не считает это проблемой, поскольку сама грешит тем же.

(вгору)

Додаток 10

27.03.2019

Новая функция в Android убережет вас от мошенников

Аналитики говорят, что 50 % звонков, полученных на ваш мобильный телефон в этом году, будут либо спамом, либо совершены с целью мошенничества. Это означает, что каждый раз, когда вы слышите, как звонит ваш телефон, есть большая вероятность, что вызов поступает от кого-то, кого вы не знаете, и, вероятнее всего, этот кто-то звонит, потому что хочет разлучить вас с вашими кровно заработанными (Украинский телекоммуникационный портал).

У Федеральной комиссии по связи (США) есть специальные фреймворки STIR и SHAKEN, для технологий обработки и аутентификации звонков, которые могут использовать мобильные и стационарные провайдеры для определения того, является ли номер, с которого поступает входящий звонок, настоящим. Телефонные мошенники специально подделывают номера так, чтобы они походили на те, что используют в вашем регионе, ведь так шанс, что вы поднимите трубку, намного выше. На данный момент только мобильный оператор США T-Mobile предлагает услуги с использованием STIR и SHAKEN, чтобы вы могли сразу узнать, является ли номер, с которого поступает звонок, настоящим. Но уже до конца этого года подобные услуги должны внедрить и другие операторы.

С одним пожилым гражданином США случился такой неприятный инцидент. Он пользовался простым кнопочным телефоном, и ему более 20 раз днем и ночью поступали входящие вызовы с белорусского номера. Каждый такой звонок продолжался всего одну секунду, но если вызов принимали, то на том конце провода автоматически включалась заранее подготовленная запись на белорусском языке. Звонок, к сожалению, в данном случае не мог быть

заблокирован, так как использовался простой кнопочный телефон. Но в чем смысл этих звонков?

Подобные звонки рассчитаны на любопытство пользователя. Мошенники надеятся, что жертва заинтересуется, кто же так настырно звонит, и решит позвонить в ответ. Тот пожилой мужчина трижды попробовал перезвонить на высветившийся номер мошенников и каждый раз с его счета списывалось 8 долларов за международный звонок, а мошенники получали от этих денежных списаний процент. А теперь умножьте это на миллионы звонков, совершаемых каждый день миллионом людей. К счастью, для того старика все закончилось благополучно и его мобильный оператор компенсировал ему все, потраченные на мошеннические международные звонки, средства.

Теперь, если у вас есть смартфон, вы можете заблокировать звонки с номеров мошенников. Согласно сообщению издания Android Police, вскоре в приложение Google Phone может быть добавлена новая функция, которая будет активно блокировать некоторые входящие вызовы. Часть Android-пользователей уже получили новое меню настроек с четырьмя новыми функциями, которые можно включать или отключать, но по умолчанию они отключены. В активированном состоянии одна из функций будет блокировать входящие вызовы с номеров, которых нет в вашем списке контактов. Другая функция позволит вам заблокировать звонки тех, кто предпочел скрыть свой номер телефона. Новые функции также позволяют блокировать звонки с платных телефонов и звонки от неустановленных абонентов.

До сих пор новые функции отображались только на смартфонах с установленной бета-версией Android Q, и то не на всех. Если новые настройки все же перекочуют в финальную сборку Android Q или даже станут доступны для более старых версий Android, это позволит владельцам устройств на «зеленом роботе» существенно снизить шансы на получение входящего вызова от очередного мошенника, желающего поживится за счёт неосведомленности некоторых пользователей.

(вгору)

Додаток 11

28.03.2019

Мобильный троян Gustuff нацелен на клиентов крупных банков

Специалисты Group-IB зафиксировали активность мобильного Android-трояна Gustuff. Среди его целей – клиенты международных банков, пользователи мобильных криптокошельков, а также крупных e-commerce ресурсов. Gustuff – «представитель» нового поколения вредоносных программ с полностью автоматизированными функциями, нацеленными, в том числе, на вывод фиатных денег и криптовалюты со счетов пользователей. Троян использует Accessibility Service – сервис для людей с ограниченными возможностями (Компьютерное Обозрение).

Анализ образца Gustuff показал, что потенциально троян нацелен на клиентов, использующих мобильные приложения крупнейших банков, таких как: Bank of America, Bank of Scotland, J.P.Morgan, Wells Fargo, Capital One, TD Bank, PNC Bank, а также на криптокошельки Bitcoin Wallet, BitPay, Cryptopay, Coinbase и др. На данный момент, специалистам Group-IB известно, что среди целей Gustuff пользователи 32 приложений для хранения криптовалют и клиенты более 100 банков, среди которых 27 – в США, 16 – в Польше, 10 – в Австралии, 9 – в Германии и 8 – Индии.

Изначально созданный, как классический банковский троян, в текущей версии Gustuff значительно расширил список потенциальных объектов для атаки. Помимо Android-приложений банков, финтех-компаний и криптосервисов, Gustuff нацелен на пользователей приложений маркетплейсов, онлайн-магазинов, платежных систем и мессенджеров. В частности, PayPal, Western Union, eBay, Walmart, Skype, WhatsApp, Gett Taxi, Revolut, и других.

Для Gustuff характерен «классический» вектор проникновения на Android-смартфоны через SMS-рассылки со ссылками на APK (Android Package Kit, формат архивных исполняемых файлов-приложений для Android). При заражении Android-устройства трояном, по команде сервера может произойти дальнейшее распространение Gustuff'а по базе контактов инфицированного телефона, либо по базе данных сервера. Функциональные возможности Gustuff рассчитаны на массовое заражение и максимальную капитализацию бизнеса своих операторов – в нем присутствует уникальная функция «автозалива» в легитимные мобильные банковские приложения и криптокошельки, что позволяет ускорить и масштабировать кражу денег.

После загрузки на телефон жертвы Gustuff, используя сервис для людей с ограниченными возможностями Accessibility Service, получает возможность взаимодействовать с элементами окон других приложений (банковских, криптовалютных, а также приложений для онлайн-шоппинга, обмена сообщениями и др.), выполняя необходимые для злоумышленников действия. К примеру, по команде сервера троян может нажимать на кнопки и изменять значения текстовых полей в банковских приложениях. Использование механизма Accessibility Service позволяет трояну обходить механизмы защиты, используемые банками для противодействия мобильным троянам прошлого поколения, а также изменения в политике безопасности, внедренные Google в новые версии ОС Android. Так, Gustuff «умеет» отключать защиту Google Protect: по заверениям автора, данная функция срабатывает в 70 % случаев.

Также Gustuff может демонстрировать фейковые PUSH-уведомления с иконками легитимных мобильных приложений. Пользователь кликает на PUSH-уведомление и видит загруженное с сервера фишинговое окно, куда сам вводит запрашиваемые данные банковской карты или криптокошелька. В другом сценарии работы Gustuff происходит открытие приложения, от имени которого демонстрировалось PUSH-уведомление. В этом случае вредоносная программа по команде сервера через Accessibility Service может заполнять поля формы банковского приложения для мошеннической транзакции.

В функциональные возможности Gustuff также входят отправка на сервер информации о заражённом устройстве, возможность чтения/ отправления SMS-сообщений, отправление USSD-запросов, запуск SOCKS5 Proxy, переход по ссылке, отправление файлов (в том числе фотосканы документов, скриншоты, фотографии) на сервер, сброс устройства до заводских настроек.

Впервые система киберразведки Threat Intelligence Group-IB обнаружила Gustuff на хакерских форумах в апреле 2018 г. По данным разработчика, скрывающегося под ником Bestoffer, Gustuf стал новой улучшенной версией вредоносной программы AndyBot, которая с ноября 2017 г. атакует телефоны с ОС Android, для кражи денег используя фишинговые веб-формы, маскирующиеся под мобильные приложения известных международных банков и платежных систем.

(вгору)

Додаток 12

28.03.2019

Иранские кибершпионы атакуют компании в США и Саудовской Аравии

В течение последних трех лет кибершпионская группировка Elfin (другое название APT33), предположительно финансируемая правительством Ирана, активно атакует организации в США и Саудовской Аравии (InternetUA).

Как сообщают специалисты компании Symantec, жертвами группировки стали представители разных сфер. Помимо правительственного сектора, Elfin также интересуют производственные, инженерные и химические предприятия, исследовательские организации, консалтинговые фирмы, финансовые и телекоммуникационные компании и пр.

За последние три года жертвами Elfin стали 18 организаций в США, в том числе компании из списка Fortune 500. Некоторые из них были атакованы с целью осуществления дальнейших атак на цепочку поставок. В одном случае крупная американская компания и принадлежащая ей фирма на Среднем Востоке стали жертвой Elfin в один и тот же месяц.

Последняя волна атак была зафиксирована в феврале нынешнего года. Для их осуществления злоумышленники пытались эксплуатировать известную уязвимость в утилите WinRAR (CVE-2018-20250), позволяющую устанавливать файлы и выполнять код на системе.

Эксплоит попал на компьютеры двух сотрудников атакуемой организации через фишинговое письмо со вложенным вредоносным файлом JobDetails.rar. После его открытия на систему загружался эксплоит для CVE-2018-20250.

Elfin была замечена исследователями в декабре 2018 года в связи с новыми атаками Shamoon. Незадолго до атаки Shamoon одна из компани Саудовской Аравии была заражена вредоносным ПО Stonedrill из арсенала Elfin. Поскольку атаки последовали сразу одна за другой, эксперты

предположили, что между ними может быть связь. Тем не менее, на сегодняшний день никаких других свидетельств причастности Elfin к атакам Shamoon обнаружено не было.

Помимо бэкдора Stonedrill, группировка также использует бэкдор Notestuk, открывающий доступ к файлам на атакуемой системе, и кастомизированный бэкдор на языке AutoIt. Наряду с инструментами собственного производства злоумышленники также применяют ПО, купленное на черном рынке, в том числе трояны Remcos, DarkComet, Quasar RAT и пр.

(вгору)

Додаток 13

29.03.2019

Европейский Союз принял закон о защите авторских прав, угрожающий свободному Интернету

Европейский Союз принял новый закон о защите авторских прав, который сильно повлияет на развитие Интернета в Старом Свете. Он призван дать правообладателям больше контроля над распространением своего контента и ограничить влияние таких технологических гигантов, как Google и Facebook. Однако, директива вызвала много критики, так как содержит спорные пункты, которые в итоге могут иметь противоположный эффект и дать больше власти технологическим гигантам, а также затруднить свободное распространение информации в Сети (Компьютерное Обозрение).

Особо экспертов беспокоит имплементация двух пунктов закона, которые могут иметь непредвиденные последствия.

Статья 11 предписывает платформам, которые размещают чужой контент, получать лицензии на ссылки или использование фрагментов новостей, статей и пр. Она призвана помочь СМИ получать прибыль от служб агрегации, каких как Google Новости, которые отображают их заголовки и части материалов.

Критики закона считают, что от этой нормы издатели только пострадают, так как им самим станет труднее делиться новостями и статьями, а крупные агрегаторы и соцсети не будут платить за лицензии и просто перестанут отображать результаты новостей из многих источников.

Статья 13, в свою очередь, требует от платформ прикладывать активные усилия для получения лицензий на контент, защищенный авторским правом, до его загрузки на свои сайты. Ранее, сервисам достаточно было просто выполнять запросы на удаление материалов, нарушающих авторские права. Из-за этой нормы, платформы скорее всего будут вынуждены использовать строгие фильтры при загрузке пользовательского контента.

Однако, небольшие и начинающие сервисы, которые позволяют пользователям загружать контент, не смогут конкурировать с гигантами вроде YuoTube и Facebook, которые смогут выделить огромные ресурсы на модерацию контента. Критики также считают, что эта директива слишком расплывчато сформулирована, а ее внедрение может сильно ограничить

творчество в Интернете. Может дойти до абсурдной ситуации, считают они, когда создание мемов или обзоров на произведения станет невозможным из-за того, что компании не будут рисковать и запретят выкладывать такой контент на своих сервисах.

Новый закон вызвал как поддержку, так и неприятие в различных кругах. Многие знаменитости, задействованные в создании контента, поддержали инициативу. Однако, технологические эксперты в основном настроены скептично. Изобретатель Всемирной паутины Тим Бернерс-Ли раскритиковал спорные моменты закона, а основатель Википедии Джимми Уэйлс отметил, что итоги голосования стали поражением в битве за бесплатный и открытый Интернет, а также увеличат вероятность появления монополий.

Также стоит отметить, что много чего будет зависеть от конкретной реализации норм закона. У каждой страны-члена Европейского Союза теперь есть два года, чтобы принять свое соответствующее законодательство. От строгости имплементации директивы во всех странах и будет зависеть, какие последствия она будет иметь на свободный обмен информации в Интернете.

(вгору)

Додаток 14

31.03.2019

Сотни сайтов на Wordpress и Joomla распространяют вредоносное ПО

Более чем 500 взломанных web-сайтов, работающих на популярных платформах Wordpress и Joomla, распространяют различное вредоносное ПО, в том числе вымогатель Shade (другое название Troldesh), бэкдоры, фишинговые ссылки и другой вредоносный контент. Новую кампанию заметили специалисты из Zscaler. По их словам, для компрометации сайтов злоумышленники используют уязвимости в различных плагинах, темах и расширениях (InternetUA).

В настоящее время неясно, кто является организатором атак. Для своих целей организаторы кампании задействуют скрытые служебные папки на сайтах, использующих защищенное HTTPS-соединение. Данные папки позволяют удостоверяющим центрам (УЦ) получить информацию о домене, однако их могут использовать и злоумышленники для хранения вредоносного ПО.

За последние несколько недель исследователи зафиксировали рост числа угроз, распространяемых посредством скрытых папок. Чаще всего этот способ используется для заражения вымогательским ПО Shade.

«Обычно спам-сообщение содержит ссылку на страницу на скомпрометированном сайте, с которой загружается вредоносный ZIP файл. Если после распаковки архива пользователь откроет содержащийся в нем файл JavaScript, на устройство загрузится программа-вымогатель», – поясняют эксперты.

Отметим, по данным компании Sucuri, в 2018 году примерно 90 % атак на системы управления контентом пришлись на сайты под управлением WordPress. Далее со значительным отрывом следуют Magento (4,6 %), Joomla (4,3 %) и Drupal (3,7 %).

(вгору)

Додаток 15

31.03.2019
Владимир Кондрашов
На сайте ЦИК семь месяцев не могли закрыть опасную уязвимость

На сайте Центральной избирательной комиссии как минимум семь месяцев просуществовала опасная уязвимость, которая позволяла атакующему внедрить клиентский сценарий в web-страницы, просматриваемые другими пользователями (InternetUA).

Об этом журналисту InternetUA сообщил спикер Украинского кибералья́нса, известный в сети под ником Шон Таунсенд.

Напомним, 21 августа прошлого года мы сообщали, что хактивисты обнаружили на сайте Государственного реестра избирателей ЦИК XSS-уязвимость – тип уязвимости программного обеспечения, который позволяет атакующему внедрить клиентский сценарий в web-страницы, просматриваемые другими пользователями. Благодаря этой уязвимости, злоумышленники могли «убедительно нарисовать любое дурацкое заявление» на сайте ЦИК – например, изобразить для российских СМИ очередную «победу Яроша», как это было сделано в 2014-м. Тогда же спикер УКА отмечал, что несмотря на то, что через веб-сайт реестра избирателей невозможно попасть в сам реестр, обнаруженное прежде всего показывает отношение к информационной безопасности в ЦИК.

22 августа в Центризбиркоме выступили с заявлением, в котором назвала Украинский кибералья́нс «малоизвестной организацией, которая пытается ассоциировать себя с кибербезопасностью», а само заявление – «неуклюжей попыткой обвинить специалистов ГРИ в некомпетентности и поставить под сомнение надлежащий уровень защищенности сайта Реестра».

Уже на следующий день после «ответа», 23 августа, на сайте ЦИК (теперь уже на основном – Ред.) также была обнаружена XSS-уязвимость.

О ней было поставлено в известность руководство Центризбиркома, но, как оказалось, «закрыли» брешь только за несколько дней до выборов, то есть, спустя семь месяцев с момента обнаружения, – после того, как наличие уязвимости обнаружил специалист по кибербезопасности под ником Ochumelec.

– Всё это время дырка была на месте, её ещё один человек нашел повторно и пнул Стельмаха, только тогда и закрыли. На днях, – сообщил спикер Украинского кибералья́нса.

Отметим также, что в марте этого года представители Центральной избирательной комиссии должны были отчитываться о кибербезопасности ЦИК перед депутатами-членами Комитета ВРУ по информатизации и связи, однако отчет, после переноса заседания Комитета, из повестки дня исчез.

Неофициально нашему изданию сообщили в Комитете, что в ЦИК слишком заняты, чтобы отчитываться.

(вгору)

Додаток 16

1.04.2019

Десятки шпионских приложений в Google Play оказались связаны с государствами

Как стало известно изданию VICE, хакеры заразили сотни пользователей несколькими вредоносными приложениями для Android, которые годами размещались в официальном магазине Google Play Store. Предположительно, это делалось по государственному заказу (InternetUA).

В прошлом как правительственные хакеры, так и те, кто работает на преступные организации, загружали вредоносные приложения в Google Play. Этот случай еще раз подчеркивает ограничения фильтров Google, которые предназначены для предотвращения проникновения на платформу вредоносного ПО, отмечает издание. В этом случае более двадцати вредоносных приложений остались незамеченными компанией Google в течение примерно двух лет.

VICE также узнал о новом виде вредоносных программ для Android в магазине Google Play, который был продан итальянскому правительству компанией, которая занимается камерами наблюдения. Анонимные эксперты сообщили автору текста, что он мог «заманить в ловушку невинных жертв». Эксперты по правовым вопросам и правоохранительным органам сообщили, что шпионские программы могут быть незаконными.

Шпионские программы были обнаружены и изучены в ходе совместного исследования некоммерческой организации «Безопасность без границ», которая часто расследует угрозы в адрес диссидентов и правозащитников. В пятницу исследователи опубликовали подробный технический отчет о результатах своей работы.

«Мы обнаружили ранее неизвестные шпионские приложения, которые успешно загружались в Google Play Store несколько раз в течение более двух лет. Эти приложения будут недоступны в Play Store на пару недель, но в конечном итоге их загрузят снова», – пишут исследователи.

Лукас Стефанко, исследователь фирмы ESET, специализирующейся на вредоносных программах для Android, но не участвовавший в исследовании, отметил, что это тревожно, но неудивительно, что вредоносное ПО продолжает проникать через фильтры Google Play Store.

(вгору)

Додаток 17

3.04.3019

Ирина Фоменко

Эксперты обнаружили новый способ хранения злоумышленниками вредоносного ПО

Исследователи безопасности Zscaler обнаружили, что киберпреступники используют скрытые «известные» каталоги сайтов HTTPS для хранения и обслуживания вредоносных программ. Об этом сообщает Security Week (InternetUA).

Были обнаружены взломанные веб-сайты WordPress и Joomla с вирусами-вымогателями Shade/Troldesh, майнерами, бэкдорами, перенаправителями, фишинговыми страницами и другими угрозами. На скомпрометированных сайтах WordPress запущены версии 4.8.9–5.1.1 CMS.

Как утверждают в Zscaler, злоумышленникам удалось получить доступ к установкам с помощью устаревших плагинов/тем CMS или серверного программного обеспечения.

Общим для скомпрометированных веб-сайтов было использование SSL-сертификатов, выданных Automatic Certificate Management Environment (ACME), такими как Let Encrypt, GlobalSign, cPanel и DigiCert.

Преступники использовали хорошо известный скрытый каталог на сайтах HTTPS для хранения своих вредоносных данных. Каталог является префиксом URI для известных местоположений, определенных IETF и используемых для демонстрации владения доменом.

Для веб-сайтов HTTPS, которые используют ACME для управления сертификатами SSL, администраторы помещают в папку уникальный токен, чтобы показать центру сертификации (CA), что они контролируют домен. CA отправляет определенный код, который они помещают в конкретный каталог, и CA сканирует его для проверки домена.

«Злоумышленники используют каталоги, чтобы скрыть вредоносные и фишинговые страницы от администраторов. Эта тактика эффективна, поскольку этот каталог уже присутствует на большинстве сайтов HTTPS и является скрытым, что увеличивает срок службы вредоносного/фишингового контента на скомпрометированном сайте», – заявили в Zscaler.

В прошлом месяце исследователи безопасности обнаружили в скрытом каталоге различные типы угроз, среди которых наиболее распространенным является вирус-вымогатель Shade/Troldesh, а на втором месте – фишинговые страницы.

На каждом скомпрометированном веб-сайте были обнаружены файлы трех типов, а именно – HTML, ZIP и EXE, маскирующиеся под изображения .jpg. Спам обычно используется для распространения вирусов-вымогателей через прикрепленные файлы ZIP, либо ссылки на HTML, которые

перенаправляют на файлы ZIP. Архивы содержат JavaScript, который загружает «полезную нагрузку» и выполняет ее.

Полезная нагрузка – новый вариант Shade/Troldesh. Вредоносное ПО использует клиент TOR для подключения к серверу командования и управления (C&C) и шифрует содержимое и имена целевых файлов.

Фишинговые страницы связаны с Office 365, Microsoft, DHL, Dropbox, Bank of America, Yahoo, Gmail и другими брендами.

(вгору)

Додаток 18

5.04.2019

Ирина Фоменко

BBC: интернет-вирус смог дорисовать к скану пациента раковую опухоль

Исследователи кибербезопасности создали компьютерный вирус, который может добавлять поддельные опухоли к медицинским изображениям. Об этом сообщает BBC (InternetUA).

В ходе лабораторных испытаний вредоносная программа изменила 70 изображений и сумела обмануть трех радиологов, заставив их поверить, что у пациентов был рак. Измененные изображения также сумели обмануть автоматизированные системы скрининга.

Команда из Израиля разработала это вредоносное ПО, чтобы показать, как легко обойти средства защиты для диагностического оборудования. Программа смогла убедительно добавить ложные злокачественные новообразования к изображениям легких, сделанным на машинах МРТ и КТ.

Исследователи из центра кибербезопасности Университета им. Бен-Гуриона заявили, что вредоносное ПО может также удалять фактические злокачественные образования из файлов изображений, создавать другие поддельные заболевания, в том числе опухоль головного мозга, тромбы, переломы или проблемы с позвоночником.

Эксперты утверждают, что изображения и сканы были уязвимы, поскольку файлы, как правило, не имели цифровой подписи и не шифровались. Это означает, что любые изменения будет трудно заметить. По словам специалистов, уязвимости в безопасности могут быть использованы для сеяния сомнений в отношении здоровья правительственных деятелей, саботажа исследований и участия в террористических атаках.

Кроме того, недостатки в способе защиты больницами и медицинскими центрами сетей могут обеспечить злоумышленникам легкий доступ. Как заявил один из экспертов, медучреждения уделяют слишком мало внимания внутренней обработке данных.

«То, что происходит внутри самой больничной системы, к которой ни один обычный человек не должен иметь доступ в целом, к ней, как правило,

относятся довольно снисходительно», – прокомментировал Исроэль Мирский. – «Лучшее использование шифрования и цифровых подписей может помочь больницам избежать проблем, если хакеры попытались изменить изображения».

Больницы и другие организации здравоохранения стали популярной целью для кибератак, и многие из медучреждений пострадали от вирусов-вымогателей, которые шифруют файлы и возвращают данные только за вознаграждение.

(вгору)

Додаток 19

6.04.2019

В браузере Chrome обнаружена опасная уязвимость

Четвертого апреля, исследователь безопасности компании Exodus Intelligence Иштван Куручай (István Kurucsai) опубликовал PoC-эксплоит и демо-видео для неисправленной уязвимости в Google Chrome. Уязвимость позволяет злоумышленнику удаленно выполнить произвольный код на системе жертвы. Проблема уже исправлена в V8 (JavaScript-движке браузера), но патч пока еще не добавлен в стабильную версию Chrome 73, используемую на более чем 1 млрд устройств (InternetUA).

Причина, по которой исследователь решил опубликовать PoC-эксплоит до исправления уязвимости, – желание продемонстрировать изъяны в процессе подготовки патчей. По мнению Куручая, пока Google работает над исправлениями, злоумышленники успевают создать эксплоиты и атаковать пользователей.

Задержка патчей связана с цепочкой поставок Chrome, подразумевающей импорт и тестирование кодов из различных источников. В случае с уязвимостью в движке V8 исправление было готово 18 марта, после чего оно стало доступно в журнале изменений проекта и исходном коде V8. Однако в сам браузер патч пока еще не добавлен.

В настоящее время обновление проходит все этапы сборки, включающие интеграцию с проектом Chromium, интеграцию с кодовой базой Chrome, тестирование в Chrome Canary и Chrome Beta, и только после этого патч будет добавлен в стабильную версию браузера. В результате у злоумышленников появляется «окно» от нескольких дней до нескольких недель, когда подробности об уязвимости уже известны, но стабильная версия Chrome еще не получила обновление.

Опубликованный исследователем PoC-эксплоит в своем нынешнем виде является сравнительно безобидным. Куручай специально не добавил в него возможность обхода песочницы, необходимую для выполнения кода. Тем не менее, злоумышленники могут воспользоваться им вкупе со старыми уязвимостями обхода песочницы и выполнить код на атакуемой системе.

(вгору)

Додаток 20

7.04.2019

Instagram отобрал никнейм пользователя и передал его королевской семье

Ваш никнейм в Instagram – это не личная собственность, которая безоговорочно принадлежит вам. Именно это познал на себе житель Великобритании, когда он проснулся утром и обнаружил, что его имя пользователя в Instagram было у него отобрано и передано более популярному пользователю. В частности, членам британской королевской семьи (InternetUA).

Кевин Кейли, сообщает Би-би-си, – обычный фанат футбольного клуба «Рединг», живущий в Западном Сассексе в Великобритании. Его никнейм в Instagram, sussexroyal, был придуман благодаря псевдониму футбольного клуба и его месту жительства. По-видимому, то же словосочетание пришло в голову герцогу и герцогине Сассекс – принцу Гарри и Меган Маркл.

В итоге ник забрали у Кевина и вместо него ему дали другой – @_sussexroyal_. Важно отметить, что в отличие от многих историй о похищенных хакерами данных, на этот раз злодеем выступает сам Instagram.

Кейли сообщил радио Би-би-си, что ни один представитель соцсети не связывался с ним по поводу передачи имени пользователя sussexroyal другим людям, и что он «раздражен» всем этим. Он говорит, что использовал эту учетную запись в основном для подписки на другие учетные записи и лайков.

Примечательно, что представитель Instagram подтвердил Би-би-си, что соцсеть отобрала у Кейли никнейм, мотивируя это тем, что аккаунт был неактивен и, таким образом, созрел для выбора другими пользователями. Но что именно означает «неактивный»? Может ли редко используемый аккаунт внезапно стать «неактивным» в глазах Instagram в тот момент, когда этого захочет известный человек?

На странице помощи, посвященной объяснению статуса неактивных учетных записей, компания изо всех сил старается предоставить как можно меньше информации.

«Аккаунт определяется как неактивный на основании ряда обстоятельств, включая дату создания аккаунта и того, делился ли владелец аккаунта фотографиями, комментировал ли фотографии, лайкал ли фотографии и входил ли в систему», – говорится на странице. «Имейте в виду, что вы, возможно, не сможете определить, является ли учетная запись в данный момент неактивной, поскольку не все действия учетной записи могут просматриваться публикой».

(вгору)

Додаток 21

8.04.2019

Большинство онлайн-банков содержат опасные уязвимости

Эксперты компании Positive Technologies оценили уровень защищенности онлайн-банков в 2018 г. и выяснили, что 54 % из обследованных систем позволяют злоумышленникам похитить денежные средства, а угрозе несанкционированного доступа к личным данным и банковской тайне подвержены все онлайн-банки. По данным проведенного анализа, большинство изученных онлайн-банков содержат критически опасные уязвимости. В результате работ по оценке защищенности онлайн-банков в каждой исследованной системе были обнаружены уязвимости, которые могут привести к серьезным последствиям (InternetUA).

Угроза несанкционированного доступа к информации клиентов и банковской тайне, например к выпискам по счету или платежным поручениям других пользователей, оказалась актуальной для каждого исследованного онлайн-банка, а в отдельных случаях уязвимости позволяли развивать атаку на ресурсы корпоративной сети банка. Исследования Positive Technologies показывают, что данные входят в ТОП наиболее популярных для продажи в дарквебе продуктов. При этом непосредственно на долю учетных данных и данных банковских карт приходится более 80 % в общем объеме продающихся данных. Средняя стоимость данных одного пользователя онлайн-банка составляет $22.

В ходе анализа в 77 % обследованных онлайн-банков были обнаружены недостатки реализации механизмов двухфакторной аутентификации. В некоторых онлайн-банках одноразовые пароли для критически важных действий (например, для аутентификации) не применяются или имеют слишком большой срок действия. Эксперты связывают это с тем, что банки стремятся найти баланс между безопасностью и удобством использования.

Сравнительный анализ показал, что изученные готовые решения, предлагаемые вендорами, содержат в три раза меньше уязвимостей, чем системы, разработанные банками самостоятельно. А вот количество уязвимостей в продуктивных и тестовых системах сравнялось: согласно статистике, в 2018 г. оба эти типа систем в большинстве случаев содержат как минимум одну критически опасную уязвимость. Эксперты связывают это с тем, что разработчики, единожды протестировав систему на безопасность, склонны откладывать повторный анализ защищенности после внесения изменений в программный код, что неминуемо приводит к накоплению уязвимостей, и со временем их число становится сопоставимо с тем, которое было обнаружено при первичной проверке.

Главной позитивной тенденцией в безопасности финансовых онлайн-приложений в прошлом году стало сокращение доли уязвимостей высокого уровня риска в общем числе всех выявленных недостатков. По данным специалистов Positive Technologies, доля критически опасных уязвимостей снизилась вдвое по сравнению с предыдущим годом. Однако в целом уровень защищенности онлайн-банков остается низким.

(вгору)

Додаток 22

5.04.2019

Депутати Кропивницької міськради демонструють тенденції до публічності в соцмережах

Дмитро Сінченко

Кількість зареєстрованих профілів депутатів місцевих рад у соціальній мережі Facebook свідчить про позитивну тенденцію – діяльність депутатів місцевих рад з кожним роком стає все публічнішою (Перша).

Тенденція загальнонаціональна і пов'язана з різними факторами, які сьогодні зійшлись в одній точці. Візьмемо для прикладу місто Кропивницький – обласний центр середнього розміру, що знаходиться в центральній області, яка відтворює модель України в мініатюрі. Тенденції, притаманні Кропивницькому, можна приміряти загалом до країни.

Отже, станом на сьогодні, за даними кампанії «Атестація депутатів місцевих рад», 39 із 42-х депутатів Кропивницької міської ради сьомого скликання, тобто 93 %, мають зареєстровані профілі у Facebook. У 2013 році, тобто у на той час ще Кіровоградській міській раді шостого скликання – таких було 12 із 76, тобто лише 16 % (відповідно до результатів моніторингового дослідження Асоціації Політичних Наук).

Із цих 39 депутатів лише 10 сторінок можна вважати неактивними, адже за останній місяць на них не з'явилось жодної інформації. Так, малоактивні профілі мають депутати Валерій Шутка, Богдан Товстоган, Олександр Рокожиця, Роман Розгачов, Ігор Захаров, Михайло Демченко, Микола Гамальчук, Тетяна Волкожа та Ігор Волков.

Взагалі не мають профілів у Facebook депутати Олександр Артюх, Віктор Ксеніч та Лілія Матяшова. Депутати, які користуються своїм профілем у Facebook найактивніше, і які особисто спілкуються через свою сторінку з виборцями, відповідаючи на особисті повідомлення, це Михайло Бєжан, Сергій Бойко, Сергій Горбовський, Сергій Капітонов, Олег Краснокутський, Віталій Пінчук, Володимир Смірнов, Дмитро Терзов, Андрій Табалов, Олександр Цертій, Олександр та Катерина Шамардіни, а також Валентина Яремчук.

З чим пов'язане таке стрімке зростання публічності місцевих політиків? Переконаний, на цю ситуацію суттєво вплинули наступні фактори:

1. Майдан

Революційні події кардинально змінили порядок денний української політики. Громадяни почали більше цікавитись політичним життям, і політики змушені задовольняти цей запит. Звідси і купа он-лайн інструментів, відкритих реєстрів, трансляцій засідань органів влади.

2. Зростання популярності соціальних мереж

Соцмережі допомогли робити революцію, і виявилось, що це ще й надзвичайно зручний інструмент для політичної діяльності. Не мати власної сторінки стало немодно. Тим паче, що з 3G s 4G і новими смартфонами

технічно це стало ще простіше. Спершу народні депутати, за прикладом активістів, зареєстрували свої сторінки, потім, наслідуючи «старших колег», зареєструвались і депутати місцевих рад.

3. Блокування російських соцмереж

Раніше те, якій мережі людина надавала перевагу, суттєво залежало від її віку. Учні та студенти (тобто від 14 до 24 років) надавали перевагу Вконтактє, працююча молодь (від 25 до 40) надавала перевагу Facebook, а старша вікова категорія сиділа в Одноклассниках. У той же час, спілкуватись на політичні теми було прийнято передусім у Facebook. Блокування російських соцмереж суттєво збільшило аудиторію ФБ і перетворило її на потужний майданчик для політичної агітації.

4. Децентралізація

Як не дивно, але реформа децентралізації істотно збільшила привабливість депутатства в місцевих радах, а тому посилилась і боротьба за кожен голос виборця, а місцеві політики почали використовувати всі можливі інструменти для роботи з виборцем, і соцмережі виявились одним із найпростіших і найзручніших інструментів.

5. Політична конкуренція

Всі вище перелічені фактори сприяли зростанню політичної конкуренції, і депутатам довелось збільшувати кількість часу на виконання своїх обов'язків. Адже, якщо раніше можна було з'являтись на виборчому окрузі лише один раз – під час виборів, то сьогодні виборець вимагає більшого. Навіть не зважаючи на те, що частина народних обранців доручає вести свою ФБ-сторінку помічникам, час, витрачений на роботу з виборцями, у більшості депутатів значно зріс. Бо в інакшому випадку депутат не матиме шансів переобратись знову.

Отже, остання тенденція свідчить, що якщо політика немає у соцмережах – значить, його не існує.

(вгору)

Додаток 23

9.04.2019

Рятувальники Київщини підтримали всеукраїнський флешмоб "Не перешкоджай! Я рятую твоє життя!"

Останнім часом фіксується все більше випадків, коли рятувальники стикаються з агресивною поведінкою громадян, незважаючи на те, що щодня, ризикуючи власним життям, рятують їх самих, їхню нерухомість та інше майно від нищівної сили стихії (Погляд).

Тож вони закликають не перешкоджати виконанню пожежно-рятувальними підрозділами професійних обов'язків – порятунку людей, забезпеченню проїзду до місць надзвичайних подій, гасінню пожеж.

Передісторією цього флешмобу став ганебний вчинок під час гасіння масштабної пожежі у Ворзелі працівникам ДСНС, коли їм з погрозами перешкоджали заправлятися водою на гідранті.

Тому вогнеборці Київщини долучаються до всеукраїнського флешмобу #«Не перешкоджай! Я рятую твоє життя» і звертаються до жителів Київщини: «Коли Ви телефонуєте на номер 101 – Ми знаємо, що необхідно допомогти! Ми, ризикуючи власним життям та здоров'ям, йдемо у полум'я з ціллю ліквідувати пожежу, яку в більшості випадків провокує саме людина!

Ми добросовісно виконуємо свої обов'язки і намагаємося в найкоротший час здолати стихію, бо знаємо, що кожна секунда зволікання може обернутися трагедією!

То чому ж ви, громадяни, замість підтримки та посильної допомоги, створюєте нам зайві перепони? Ви дозволяєте собі погрожувати та принижувати нас під час виконання покладених державою на нашу службу обов'язків?

Чи готові ви взяти на себе відповідальність за те, що доки ви створюєте нашій роботі перешкоди, може загинути людина?

Що ж…. Ми свою роботу зробимо!!! Нехай з затримкою, але зробимо!!! Але подумайте! Чи хотіли б ви, щоб хтось так саме перешкоджав нам, коли допомога буде потрібна саме вам???».

До акції вже долучилися вогнеборці Тетіївського, Києво-Святошинського та інших районів області.

З їхніми вимогами не можна не погодитися! Шановні жителі Київської області не перешкоджайте рятувальникам виконувати їхній професійний обов'язок: рятувати ваше майно, а найголовніше – життя!

(вгору)

Додаток 24

3.04.2019

Дмитрий Демченко

Instagram делает ставку на продажу товаров. Потенциально это $10 млрд выручки

Instagram активно развивает свое направление электронной коммерции, вводя новые возможности для покупки товаров прямо в приложении. Аналитики говорят, что такая стратегия станет успешной для соцсети – и принесет ей $10 млрд в 2021 году. Об этом сообщает Business Insider (AIN.UA).

В марте Instagram запустил функцию Checkout для некоторых пользователей в США. Она позволяет совершать покупки прямо в соцсети, не покидая приложение. Аналитики Deutsche Bank уверены, что это принесет больше денег Instagram по нескольким причинам:

– Конверсия рекламы в соцсети возрастет – она станет эффективнее, а соответственно, генерировать больший доход.

– Instagram сможет предлагать новые форматы рекламы.

– Instagram будет брать комиссию за покупки в соцсети.

– Пользователи будут больше времени проводить на платформе.

– Instagram будет использовать данные о покупках, чтобы делать рекламу более релевантной.

Кроме этого, новый руководитель Instagram Адам Моссери, который заменил на посту основателей соцсети в сентябре 2018 года, больше нацелен на монетизацию сервиса, чем его предшественники.

В то же время в Deutsche Bank замечают, что Instagram может столкнуться с рядом проблем. Во-первых, возможен конфликт с компаниями-партнерами. Facebook, которой принадлежит Instagram, исторически ограничивает пути, благодаря которым рекламодатели могут использовать данные о своих клиентах. А информация – важная составляющая любого ecommerce-бизнеса.

Во-вторых, пока непонятно, захочет ли среднестатистический пользователь Instagram передавать свои платежные данные соцсети.

(вгору)

Додаток 25

27.03.2019

Как и почему изменятся социальные сети в 2019 году

Если в 2018 году самые популярные соцсети были сосредоточены на мобильном видео, прямых трансляциях и поиске товаров, то в текущем году приоритеты поменялись. Согласно прогнозам Hootsuite, крупнейшие игроки рынка сделали ставки на новые технологические форматы и способы привлечения аудитории (InternetUA).

Они используют в мобильном видео виртуальную и дополненную реальность. Встраивают искусственный интеллект (ИИ), чтобы обеспечить более персонализированные контент и рекламу. А также в соответствии с запросами пользователей вынуждены улучшать свою политику безопасности и защищать конфиденциальную информацию.

Facebook

После скандала с утечкой персональных данных 137 млн пользователей крупнейшая в мире социальная сеть (2,23 млрд пользователей) сосредоточилась на возобновлении утраченного доверия к онлайн-сервисам. Компания объявила о заключении партнерских соглашений для борьбы с фейками, привлечении 20 тыс. новых модераторов и специалистов по безопасности.

Анонсированный в 2018 году инструмент Facebook Stories привлек 150 млн пользователей – теперь в них появится и реклама, Stories Ads. Платформа начала тестирование этой опции в США, Мексике и Бразилии. Ожидается, что в этом году 5-15-секундные ролики станут доступны для всех пользователей по всему миру.

Инновационная разработка Facebook – шлем виртуальной реальности Oculus Quest – должна появиться на прилавках магазинов весной 2019 года.

Устройство соединило в себе беспроводной дизайн, виртуальный контроллер и позволяет играть в игры практически в любом месте.

При этом соцсеть уделит больше внимания развитию сообществ. Новая функция Watch Party позволит участникам Facebook Group совместно просматривать видео и делиться впечатлениями от увиденного. Как пример успешного использования нововведений указана ювелирная компания BaubleBar. С помощью динамически таргетированных объявлений для целевой аудитории в Facebook она увеличила доходность от рекламы на 47 %. И удвоила средний объем ежедневных покупок.

YouTube

Число активных пользователей YouTube за 2018 год выросло с 1,6 млрд до 1,9 млрд. Менее чем за год после запуска потоковый сервис YouTube TV набрал более чем 300 тыс. подписчиков, а к лету 2018-го этот показатель вырос до 800 тыс. В текущем году произойдет дальнейшее расширение: с новыми каналами и издателями, на новых рынках.

Будущее YouTube означает больше контроля, гибкости и интерактивности для пользователей, а также – для рекламодателей. Новые инструменты, такие как Reach Planner в AdWords, позволят персонализировать рекламу и пользовательский опыт.

Работающая в сфере путешествий Majestic Heli Ski ориентировалась на пользователей, которые в интернете искали горнолыжные курорты и некоторые виды лыж. Таким образом за последние пять лет компания увеличила свою клиентскую базу на 400%. Продажи выросли на четверть, а 50% новых клиентов пришли через YouTube.

Snapchat

Хотя в прошлом году сервис Instagram Stories набрал более 400 млн пользователей и обогнал Snapchat, последний остается очень популярным в молодежной среде. В этой сети имеют учетную запись 79 % подростков.

Их прежде всего привлекают такие функции, как Snapstreaks, которая отслеживает, сколько дней подряд пользователи контактировали друг с другом. На вопрос «Какую соцсеть бы вы выбрали, если бы пришлось выбрать только одну?» 44 % ответили – Snapchat.

В 2018 году компания запустила проект Spectacles («очки»), продемонстрировав свое стремление объединить программные и аппаратные решения. На базе этого сервиса в будущем пользователи смогут автоматически конвертировать снятое видео в видеоисторию.

Кроме инвестиций в дополненную реальность, Snapchat регулярно расширял возможности для покупок. Последние новости касались нового инструмента для визуального поиска товаров в сотрудничестве с Amazon. Достаточно навести Spectacles на товар, выбрать и оплатить, не покидая соцсети.

LinkedIn

Принадлежащая Microsoft социальная сеть для профессионалов привлекла свыше 575 млн пользователей из 200 стран мира. Пока LinkedIn

удается успешно избегать проколов с безопасностью, с которыми столкнулись другие платформы.

В 2018 году компания внедрила новый пользовательский интерфейс, новые форматы объявлений и функции видео. LinkedIn подтверждал свою клиентоориентированность интеграцией Microsoft Dynamics 365 (инструмент CRM от Microsoft) и внедрением LinkedIn Recruiter.

Запуск нового аналитического инструмента самообслуживания Talent Insights позволит применять обширную информацию LinkedIn для предоставления информации по запросу миллионам специалистов по подбору и найму персонала. Это поможет профессиональным пользователям LinkedIn понять тенденции рынка, а также позволит вести более качественный целевой поиск.

Twitter

В 2019 году сеть микроблогов повысит уровень безопасности и будет бороться с ботами. После бурных скандалов, связанных с обвинениями в расизме, «языком вражды», спамом Twitter разработает новую политику борьбы с нежелательным контентом.

Компания инвестирует в экосистему разработчиков, поощряя создание новых и инновационных способов использования Twitter. А также вкладывает средства в развитие потоковых сервисов, что не может не заинтересовать бренды и издателей.

Instagram

В 2018 году Instagram преодолел порог в 1 млрд активных пользователей (на месячной основе). Этот впечатляющий рост обеспечили Stories, новые видеофункции и продвинутые опции для рекламодателей.

С новой функцией IGTV, позволяющей снимать вертикальные ролики длительностью до часа, компания подтвердила свой фокус на видео. Вероятно, в текущем году появятся опции для монетизации этого сервиса. Расширятся и возможности для покупок непосредственно в приложении. Эти разработки и самый высокий среди соцсетей уровень вовлеченности предоставляет компаниям и пользователям широкое поле для взаимодействия.

Pinterest

После того, как в 2017 году доходы компании от рекламы достигли $500 млн, в 2018-м Pinterest приблизился к впечатляющему показателю – $1 млрд.

Этот сайт становится все более популярным среди крупных брендов моды, красоты, уюта и стиля жизни. Особенной популярностью у компаний пользуется мобильная реклама – из 250 млн активных подписчиков Pinterest 80% используют его мобильное приложение.

Статистика свидетельствует, что около 90 % пользователей Pinterest используют эту платформу для принятия решений о покупках.

(вгору)

Додаток 26

3.04.2019

В WhatsApp добавили запрет на добавление в групповые чаты без разрешения

Месседжер WhatsApp позволил пользователям указывать, кто может добавлять их в групповые беседы (InternetUA).

«Теперь приложение позволяет запретить пользователям добавлять вас в группы, если они не являются контактами в вашей адресной книге. Кроме того, вы можете запретить кому-либо добавлять вас или оставить этот параметр открытым для всех», – говорится в сообщении.

Отмечается, что эта функция является частью множества изменений, которые вносит служба, чтобы предотвратить распространение дезинформации.

WhatsApp уже ограничил количество переадресаций сообщений, а также теперь помечает переадресованные сообщения, чтобы привлечь к ним внимание.

Второго апреля месседжер запустил в Индии новую службу проверки фактов, которую пользователи могут использовать для проверки достоверности любых отправленных им сообщений.

Пользователи, которые ограничивают тех, кто может добавлять их в группы, могут быть добавлены по личному приглашению. В частности, они получат ссылку, которая дает основную информацию о группе, в которую они были приглашены, и могут присоединиться к ней, если захотят.

В противном случае срок действия ссылки истекает через 72 часа. Ранее на странице поддержки WhatsApp отмечалось, что единственный способ предотвратить добавление в группу – это заблокировать администратора группы.

Доступ к новым настройкам можно получить, перейдя в раздел «Параметры учетной записи» в меню настроек. Выберите «Конфиденциальность», затем «Группы», и вы сможете выбрать, кто именно может добавить вас в группу.

(вгору)

Додаток 27

9.04.2019
Объявлен «закат» видеохостинга YouTube

Видеохостинг YouTube находится в глубоком кризисе из-за нескольких факторов, которые оказали большое влияние на сервис и его роль в жизни интернет-сообщества, пишет The Verge. Как отмечает издание, за последнее время компания стала отказываться от независимых авторов и их контента, предпочитая более традиционные форматы со знаменитостями, напоминающие телевизионные (InternetUA).

В пример журналисты приводят историю авторов канала RackaRacka, Дэнни и Майкла Филиппу (Danny Philippou, Michael Philippou). По словам Дэнни, YouTube, в создании которого он участвовал, мертв, как и их канал.

YouTube в прошлом был площадкой, приветствовавшей необычных, уникальных неизвестных авторов, считает он. Теперь же видеохостинг – место для эпизодов вечерних шоу и музыкальных видео, полагает Филипп.

Поддерживать ролики пользователей сервис начал в конце нулевых годов, когда Google купила YouTube и столкнулась с проблемой пиратства, вспоминает The Verge. Продвижение авторов, снимающих свои собственные видео, помогло YouTube к 2011 году достичь миллиарда просмотров. Авторам дали возможность получать денежные выплаты за просмотры через систему Google AdSense.

Со временем YouTube начал экспериментировать с алгоритмами подбора видеороликов. Вслед за этими переменами авторы каналов стали пытаться менять свои форматы. Несмотря на изменения, к 2015 году сервис находился на пике успеха. Это произошло благодаря запуску платной подписки YouTube Red и специальных шоу, в которых профессионалы и известные на платформе авторы создавали более качественный контент.

Сложности во взаимодействии авторов и руководства компании начались в 2016 году. Все больше рекламодателей начали отказываться от размещения на YouTube или проявлять настороженность к площадке как к месту для своих рекламных кампаний.

Кроме того, на отношение к авторскому контенту повлияли скандалы с популярными YouTube-блогерами, такими как Феликс Чельберг (Felix Kjellberg), более известный как PewDiePie, и Логан Пол (Logan Paul). Ресурс усилил контроль над видео, попадающими в тренды YouTube, и ужесточил требования к роликам, достойным монетизации. После шквала критики видеосервис решил действовать в угоду «того самого голливудского контента, которому они когда-то были альтернативой», подытожил автор The Verge.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, Голосіївський просп., 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
Сайт: http://nbuviap.gov.ua/
http://сіаз.укр/
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.