СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(2.01–16.01)

2019 № 1

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(2.01–16.01)
№ 1

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

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

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2019

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

3.01.2019
Соцсети: что ждет Facebook, Instagram, Twitter, YouTube в 2019-ом

Один из редакторов The Verge (специализируется на Кремниевой Долине) Кейси Ньютон попросил читателей поделиться прогнозами для социальных сетей на 2019 год. В итоге он срезюмировал ряд трендов, добавив к ним несколько своих собственных умозаключений.

Докладніше

***

4.01.2019
Instagram опубликовал рейтинг самых популярных пользователей

В последние годы популярность Instagram продолжает набирать обороты (InternetUA).

В 2018 году число зарегистрированных пользователей составляло более одного миллиарда человек. Пользователи делятся фотографиями с друзьями, следят за жизнью знаменитостей, а некоторые, даже зарабатывают на этом деньги, размещая рекламу у себя на странице.

Список самых высокооплачиваемых пользователей прошлого года возглавила Кайли Дженнер. Рекламодатели платят более 1 млн долларов за один пост на ее странице.

Самым популярным пользователем, является футболист Криштиану Роналду. Он первым набрал 150000000 подписчиков, тем самым, установив своеобразный рекорд.

На втором месте здесь певица Селена Гомес, набравшая 144500000 подписчиков.

Тройку лидеров завершает еще одна американская певица Ариана Гранде. На ее страницу подписаны уже 141300000 пользователей.

***

7.01.2019
В YouTube для Android усовершенствован голосовой поиск

В YouTube для Android обновлен голосовой поиск. Теперь с его помощью вы можете открыть необходимый раздел приложения (InternetUA).

Нововведения появятся в версии приложения 13.50.52. Нажав на строку поиска, вы увидите иконку микрофона в нижней части экрана. Переместиться в нужный раздел можно будет с помощью голосовой команды Show me – так вы сможете открыть историю просмотров, тренды или подписки.

Ранее YouTube для Android побило отметку в пять миллиардов установок.

Напомним, приложение по умолчанию установлено на всех Android-смартфонах в пакете программ Google. Получается, каждый активированный Android-смартфон увеличивает этот показатель.

***

9.01.2019

Чехи створили соцмережу для поетів

Близько 16 тис. осіб вже приєдналися до чеської соцмережі для поетів Poetizer, яка поки доступна чеською, англійською та іспанською мовами. Чеською версією користуються 10 тис. осіб (Голос українською).

У планах авторів цього цікавого проекту зробити франкомовну версію і рекламувати сайт до Канади. В майбутньому планується залучати творчих особистостей з Латинської Америки і Близького Сходу.

Всього на даний момент на сайті розміщено приблизно 38 тис. віршів.

За задумом, у мережі Poetizer не можна (за рідкісним винятком) публікувати фотографії або інші ілюстрації. Можна використовувати анонімний профіль.

Проект витворили чеський публіцист і бізнесмен Лукаш Седлачек і його дружина Йоганна Вамберская. Спочатку Poetizer був додатком для смартфонів, але з-за популярності було вирішено зробити окрему соцмережу. Кошти вклали два інвестора, імена яких вони не розкривають.

Поезія в інтернеті – далеко не новинка, є, наприклад, так звані Instapoets – поети з Інстаграму. За творчістю канадської поетеси Рупи Каур стежать в Інстаграммі 3,2 млн осіб. Її перший друкований збірник розійшовся накладом 2,5 млн примірників і потрапив в список бестселерів видання The New York Times.

***

9.01.2019

Ирина Фоменко

Появились новые приложения для знакомств, фильтрующие неподходящих кандидатов

В отличие от Tinder, Facebook Dating, Hinge или большинства других приложений для знакомств, в этих эксклюзивных версиях требуется, чтобы пользователи подали заявку, которую должны одобрить. Самые популярные приложения для «серьезных» знакомств – Raya и The League.

Докладніше

***

10.01.2019

WhatsApp получил новую функцию защиты

В обозримом будущем пользователи популярной системы обмена мгновенного сообщениями WhatsApp получат дополнительный способ защиты личных сообщений, который скроет переписку от любопытных глаз других пользователей, даже если у них в руках окажется уже разблокированный смартфон (InternetUA).

После небольшого праздничного перерыва команда разработчиков WhatsApp вернулась к улучшению мессенджера, планируя в ближайшее время добавит в него важное средство защиты персональных данных.

В компании подтвердили, что уже в бета-версии WhatsApp 2.19.3, которая выйдет в ближайшее время, появится опциональная возможность аутентификации пользователя по отпечатку пальца. Разработчики заявили, что данное нововведение позволит сделать мессенджер еще более безопасным и защищенным, а сообщения будут показаны только после того, когда пользователь подтвердит свою личность отпечатком пальцев. Еще раз обращаем ваше внимание, что возможность будет опциональной.

Нововведение будет работать на смартфонах с Android Marshmallow и более новыми версиями этой ОС, которые оснащены дактилоскопическими датчиками.

***

10.01.2019
Ольга Карпенко
В YouTube Music добавили рейтинги: можно узнать о хитах в Украине и мире

В YouTube недавно сделали рейтинги доступными в YouTube Music, в том числе, эта функция работает и в Украине. С помощью рейтингов фанаты музыки могут узнать о хитах в своей стране и в мире. Хит-парады популярной музыки основываются на количестве просмотров от 1 млрд пользователей, которые посещают YouTube ежемесячно (AIN.UA).

Хит-парады доступны в виде списков воспроизведения, которые можно посмотреть на домашнем экране YouTube Music или в поиске. Всего есть пять плейлистов с чартами: три из них основаны на популярности в отдельной стране, а два – в мире. В YouTube Music доступны такие хит-парады, как «Топ-100 песен: самые популярные композиции на YouTube» – глобальные и локальные чарты, «Топ-100 музыкальных видео: самые популярные композиции на YouTube» – глобальные и локальные чарты, «20 лучших музыкальных клипов» – локальный хит-парад и т.д. Как формируются чарты на YouTube, можно прочесть в официальном руководстве.

***

10.01.2019
Дмитрий Демченко

Twitter запускает открытое бета-тестирование новых функций. Подать заявку может каждый

В Twitter объявили о скором запуске открытого бета-тестирования новых функций соцсети. Любой пользователь сможет подать заявку, а компания отберет из них несколько тысяч. Об этом сообщает Engaget (AIN.UA).

В Twitter собираются таким образом получить реакцию пользователей на новые возможности для общения в рамках соцсети. Это касается нового вида ответов, которые компания тестирует на протяжении нескольких месяцев. Twitter планирует полностью изменить вид сообщений под твитами, разбив их на «ветки» и изменив цвет.

Кроме этого, соцсеть планирует запустить особый формат твитов, которые будут закрепляться сверху профиля. В компании уверены, что такое нововведение будет провоцировать «здоровые» дискуссии между пользователями.

Концепция открытого бета-тестирование предполагает, что пользователи, участвующие в программе, смогут рассказывать о новых функциях и публиковать их скриншоты. Сам Twitter будет просить тестеров делиться своим мнением по поводу того или иного нововведения.

***

11.01.2019

Instagram тестирует одно из самых ожидаемых новшеств

Социальная сеть Instagram начала тестировать публикацию одного поста через несколько аккаунтов для операционной системы iOS. Об этом сообщил в среду портал TechCrunch со ссылкой на разработчиков (InternetUA).

«Мы внедряем эту функцию, чтобы сделать наш сервис удобнее для людей, которые часто публикует сообщения в нескольких аккаунтах», – заявил представитель Instagram.

Уточняется, что новая функция пригодится тем, кто размещает в соцсети рекламу, используя при этом не один профиль.

В настоящее время неизвестно о сроках запуска нововведения на Android. При этом Instagram тестирует новый способ по импортированию фотографий для этой операционной системы – скоро их можно будет загружать непосредственно из Google Photos.

***

13.01.2019

Twitter годами фиксировал точные GPS-координаты пользователей

Международная группа исследователей разработала инструмент, который способен в течение нескольких минут с 92,5 % точностью определить, где

живёт человек, используя данные Twitter. С его помощью также можно узнать, где пользователь работает, а также проводит своё свободное время.

Докладніше

***

15.01.2019

Михаил Сапитон

Что тестирует Twitter: цветные твиты, отказ от лайков и новые статусы

Twitter объявил о запуске публичной программы тестирования. В ее рамках несколько тысяч пользователей получат ранний доступ к экспериментальным функциям и смогут повлиять на планы компании по их запуску.

Докладніше

***

15.01.2019

В YouTube добавили систему управления, как в Instagram Stories

В приложении YouTube появилась новая система управления жестами. Технически она похожа на Instagram Stories и доступна на смартфонах и планшетах (Буквы).

Об этом сообщает издание TechCrunch.

Теперь пользователь может листать видео свайпами вправо и влево. В первом случае он откроет следующее, рекомендованное ему видео, а во втором, соответственно, последнее просмотренное.

При этом ролик запустится с момента, на котором пользователь его остановил. Новая функция YouTube напоминает функцию Stories в Instagram, которая популяризировала пролистывание контента по горизонтали.

YouTube заявляет, что 70 % времени занимает просмотр видео с мобильных устройств, а нововведение даст пользователям возможность лучше контролировать их воспроизведение.

***

16.01.2019

В Viber появилась новая функция

В Viber появилась функция проведения опросов в групповых чатах и сообществах (Goodnews.ua).

Новая опция предоставляет дополнительную возможность для получения обратной связи и взаимодействия в группах, тем самым оптимизируя коммуникацию пользователей и позволяя им быстрым и удобным способом выражать свое мнение по конкретной теме.

Благодаря новой функции все участники чата в режиме реального времени смогут узнать мнение собеседников по какому-либо вопросу, не путаясь в бесчисленном количестве ответов и комментариев в истории переписки.

Участники групповых чатов и администраторы сообществ теперь могут легко создать опрос, нажав в меню чата на значок опроса, который доступен в новейшей версии приложения Viber. Затем нужно ввести сам вопрос, а также до 10 возможных вариантов ответа на выбор. Все участники группового чата или сообщества могут проголосовать, нажав на «лайк» напротив понравившегося варианта. Результаты голосования обновляются в режиме реального времени по мере того, как добавляется новый голос.

В групповых чатах пользователи могут посмотреть, за какую опцию проголосовал каждый из участников, нажав на соответствующий вариант ответа, в то время как голосование в сообществах проходит анонимно.

Создание опроса – прекрасный способ вовлечь аудиторию в коммуникацию, дать ей возможность выразить свое мнение, а также мотивировать как можно больше пользователей чаще принимать участие в обсуждении различных тем.

***

16.01.2019

Україна потрапила в топ-50 найбільш «інстаграмних» країн світу

Україна потрапила в топ-50 найбільш «інстаграмних» країн світу в 2019 році. Відповідний рейтинг опублікував портал Big 7 (Еспресо).

Зазначається, що рейтинг створили базуючись на популярність хештегів країн в Instagram, оцінок експертів з подорожей і думці читачів туристичного порталу.

У трійку лідерів увійшли Австралія, Гонконг і Канада. Україна в рейтингу зайняла 39 місце.

Серед найбільш популярних місць української столиці, які виставляють у Instagram, відзначені Печерська Лавра, Арка дружби народів, Майдан Незалежності, Михайлівський собор, 18-метрова копія Ейфелевої вежі, Бессарабський ринок, монумент «Батьківщина-мати».

Найбільш «інстаграмні» країни світу-2019: Австралія, Гонконг, Канада, Індонезія, Південна Африка, Мальдіви, Індія, Сполучені Штати Америки, Дубай, Сінгапур, Об’єднане Королівство, Італія, Франція, Таїланд, Японія, Марокко, Малайзія, Іспанія, Нідерланди, Туреччина, Аргентина, Росія, Мексика, Португалія, Бразилія, Греція, Німеччина, Колумбія, Венесуела, Швеція, Китай, Бахрейн, Ірландія, Тайвань, Кувейт, Норвегія, В’єтнам, Польща, Україна, Йорданія, Австрія, Швейцарія, Філіппіни, Південна Корея, Нова Зеландія, Ізраїль, Іран, Перу, Чехія, Єгипет.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

2.01.2019

Як соцмережі реагували на самовисунення Зеленського через канал Коломойського

Як відомо, 31 грудня о 23.55 на каналі 1+1 олігарха Коломойського транслювали самовисунення коміка Зеленського у президенти, а передноворічне вітання чинного Президента перенесли і показали вже після опівночі (ТЕКСТИ.ORG.UA).

Артист і художній керівник «Студії Квартал 95» Володимир Зеленський заявив, що візьме участь у наступних виборах президента України. Про це він сказав під час трансляції новорічного ефіру програми «Вечірній квартал». «1+1» показав його заяву в той же час, коли інші канали транслювали привітання глави держави. При цьому традиційне привітання президента України показали уже в перші хвилини 2019 року.

Медіаексперт Наталя Лігачова також несхвально відгукнулась на поведінку телеканалу 1+1.

Спортивний журналіст Костянтин Андріюк пише: «[Коломойський] попер війною на Порошенка, бо вже прорахував завчасно всі ризики. А глядач, якого плюси так дбайливо виховують, 95 кварталами та іншими подібними продуктами, все одно це “схаває”».

Прихильники абсолютних прав приватних власників (відомі на постсовку як «атланти») виправдали поведінку Коломойського. Блогер Юрій Гудименко у саркастичній формі говорить про зв’язок Володимира Зеленського із олігархом Ігорем Коломойським (власником каналу «1+1»). «Циніки» заговорили про досконалий піар-хід, який «витиснув» Порошенка і зробив будь-яку його реакцію смішною.

***

2.01.2019

Мэр Ивано-Франковска через Facebook назначил дополнительный выходной

Мэр Ивано-Франковска Руслан Марцинкив назначил в городе дополнительный выходной день на 8 января. Об этом он заявил на своей странице в Facebook 2 января (InternetUA).

«На Рождество, 8 января, будем отдыхать. Такое решение приняли на местном уровне и будем рекомендовать организациям отработать этот рабочий день в субботу, 5 января. Если Киев не хочет отмечать Рождество, это не значит, что и мы в праздник должны идти на работу. Рождество – это время,

которое следует проводить с семьями, пойти в церковь! А поработаем другой день», – написал он.

***

2.01.2019

СМИ подсчитали твиты Трампа за прошедший год

Президент США Дональд Трамп за 2018 год три тысячи раз написал в твиттер, сообщает The Hill (InternetUA).

По данным издания, американский президент сделал 2860 постов, включая ретвиты. Отмечается, что он 139 раз написал фразу «охота на ведьм» – так Трамп называет расследование предполагаемого российского вмешательства в выборы в США, проводимое специальным прокурором Робертом Мюллером.

Кроме того, 193 раза Дональд Трамп упомянул «фейковые новости».

***

4.01.2019

У митрополита Епифания появились первые фейковые странички в соцсетях

В соцсетях появилось много фальшивых страниц митрополита Киевского и всея Украины Епифания. В Православной церкви Украины призвали верующих использовать информацию лишь с единственной автентичной страницы митрополита в Facebook. С таким призывом обратился к верующим архиепископ Черниговский и Нежинский Евстратий (InternetUA).

«После ряда одинаковых вопросов в мессенджерах – решил ответить для всех здесь. На фото внизу – ЕДИНСТВЕННАЯ аутентичная ФБ-страница Митрополита Епифания. Эта страница – не личная, а представительство Митрополита как публичного лица и религиозного деятеля. Адрес: https://www.facebook.com/epifaniy/. Другие страницы, где в названии используется имя “Епифаний” или созвучное – клоны/фальшивки», – написал он в Facebook.

***

6.01.2019

У соцмережі Facebook запустили флешмоб на підтримку популярної спільноти «Варта-1»

#ПоверністьВарту – з таким хештегом розпочався 5 січня у соцмережах флешмоб на підтримку видаленої нещодавно популярної львівської спільноти «Варта-1» (032.ua).

Про це повідомляє кореспондент сайту 032.ua із посиланням на офіційну сторінку засновника ГО «Варта-1» Ігора Зінкевича.

Творець спільноти попросив підтримки користувачів соцмережі Facebook у відновленні «Варти-1» та опублікував покрокову інструкцію про те, як долучитися до флешмобу.

Тим часом, поки спільнота видалена, творці «Варта-1» уже зареєстрували резервну однойменну спільноту, куди постять актуальні новини міста. У резервну групу додалося вже майже 23 тисячі людей.

Нагадаємо, 4-го січня, Facebook видалив сторінку найпопулярнішої львівської спільноти «Варта-1», яка налічувала 400 тисяч користувачів. Наразі причини видалення групи невідомі.

***

8.01.2019

Візит Порошенка у Луцьк: в соцмережах волинян закликають задати питання Президенту

Волинян запрошують поставити запитання Президенту, коли він 11 січня з візитом приїде до Луцька.

У Фейсбуці створили сторінку «Постав запитання президенту 11 січня. Волинь», на якій закликають усіх охочих прийти на Театральний майдан міста Луцька, де виступатиме Петро Порошенко і поставити йому актуальні питання, які турбують кожного (Волинські новини).

Зокрема, ветеран батальйону «Донбас», волинянин Богдан Пташник закликав краян не ігнорувати візит, а запитати Президента про наболіле.

«Шановні волиняни! У зв'язку з радісною звісткою про приїзд Порошенка в Луцьк 11 січня в межах своїх повноважень – з релігійною місією, закликаю всіх не ігнорувати чинного гаранта Конституції. Давайте також приїдемо, прийдемо, приповземо, але послугаємо мудре слово і може й самі щось скажемо! Це буде вияв нашої любові і вдячності... ПС. Добиратись треба самостійно, оскільки влада і так витратиться на довезення чітко визначених бюджетників, але хіба це перешкода прибути і поставити запитання?» – пише Пташник у Фейсбуці.

Разом з тим, на сторінці спільноти акцентують, що «це – особиста справа і право кожного громадянина», тому жодної координації дій не планують.

***

8.01.2019

Замість соцмереж – книга: між школярами Хмельницького шириться патріотичний флешмоб

Надія Свінціцька

Учні по черзі читають книгу Лариси Ніцой «Незламні мураші».

Аби під час зимових канікул учні хмельницьких шкіл займалися самоосвітою, в обласному центрі стартував флешмоб «Плекаймо українську

мову». Ініціатором його стала заступник міського голови Галина Мельник (ye.ua).

«Знаю з практики, що діти на канікулах читати не хочуть, натомість днями просиджують в соцмережах. Саме тому ми запустили в Хмельницькому флешмоб “Плекаймо українську мову”. Мета його полягає в тому, що учні по черзі читають книгу відомої письменниці Лариси Ніцой “Незламні мураші”. Після прочитання вони залишають у соцмережах свій відгук з хештегом #плекаємоукраїнськумову. Цим флешмобом ми хочемо навчити дітей відпочивати правильно, а з огляду на тематику книги – привити у них патріотизм та любов до рідної землі», – розповіла Галина Леонтіївна.

У розпорядження школярів надано 30 книг, які по черзі читають учні. За словами чиновниці, до флешмобу долучилися вже близько сотні школярів.

«Долучитися до читання цієї книги можуть не лише діти, а й дорослі. 31 січня ми підіб’ємо підсумки і парахуємо скільки осіб долучилися до флешмобу. Ймовірно, ми встановимо рекорд з читання книги українського автора», – зазначила Галина Мельник.

***

10.01.2019

Украина требует заблокировать страницу МИД РФ в Крыму в Twitter

Министерство иностранных дел Украины направило жалобу в службу поддержки социальной сети Twitter с требованием заблокировать аккаунт Министерства иностранных дел (МИД) Российской Федерации в оккупированном Крыму. Об этом сообщает РБК-Украина со ссылкой на сообщение МИД Украины в Twitter (InternetUA).

В украинском МИД назвали недопустимым предоставление странице МИД РФ в Крыму статуса официальной.

«Мы отправили официальную жалобу в службу поддержки Twitter. Совершенно недопустимо ставить так называемым МИД России в оккупированном Крыму голубую галочку! Россия незаконно аннексировала Крым, военизировала его и совершала грубые нарушения прав человека. Twitter должен заблокировать этот аккаунт!», – говорится в сообщении.

***

15.01.2019

Ирина Фоменко

Сотрудники Google будут протестовать против IT-гигантов в соцсетях

15 января группа сотрудников Google в Instagram и Twitter начнет протестовать, оказывая давление на технические компании, чтобы они изменили свою практику, связанную с притеснением на работе в

технологической отрасли. Группа планирует еженедельно публиковать в Twitter факты о принудительном арбитраже, а также отзывы сотрудников и интервью с экспертами каждые полчаса в Instagram.

Докладніше

***

15.01.2019

Київські музеї у День музейного селфі: де вас раді бачити

Юлия Семенова

Деякі музеї навіть пропонують різноманітні бонуси 16 січня, в міжнародний День музейного селфі (Вокруг света).

Підтримати всесвітній флешмоб Museum Selfie Day можна, виклавши в соціальних мережах селфі з будь-якого музею та додавши до публікації хештеги #MuseumSelfie, #MuseumSelfieDay. Також можна додати хештег музею та тегнути його сторінку.

Деякі музеї, активно підтримуючи акцію, пропонують відвідувачам особливі умови та різні бонуси. Наприклад, працівники Софії Київської із розумінням поставляться до фотоавтопортретів навіть у тих місцях, де зазвичай фото заборонене (тільки не забудьте хештег #SelfieSophiaKyiv).

Не маєте можливості відвідати музей 16 січня? Не біда. До участі у флешмобі приймаються фото з музеїв, зроблені протягом останнього року.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

4.01.2019

Facebook заполучила Nestle в клиенты корпоративной платформы Workplace

Компания Facebook объявила, что крупнейший глобальный бренд продуктов питания и напитков, Nestle, стал корпоративным клиентом её коммуникационной платформы для бизнеса, Workplace. Эта сделка позволит расширить пользовательскую базу Workplace сотнями тысяч служащих Nestle. За предыдущие месяцы компания уже подключила к этому сервису 210 тыс. сотрудников и планирует добавить к ним многие тысячи в течение 2019 г.

Докладніше

***

4.01.2019

Цукерберг исследует человеческий мозг

Марк Цукерберг и его жена Присцилла Чан продали около 30 миллионов акций Facebook, чтобы профинансировать амбициозный биомедицинский исследовательский проект под названием «Инициатива Чан-Цукерберга» (CZI). Цель проекта – протестировать имплантационные мозговые устройства в рамках кампании по искоренению болезней.

Докладніше

***

9.01.2019

Марк Цукерберг в 2019 году будет проводить постоянные открытые дискуссии о будущем технологий

Марк Цукерберг на своей странице в Facebook пообещал в 2019 году раз в несколько недель проводить открытые публичные дискуссии в разных форматах о будущем технологий (InternetUA).

Беседы с экспертами, другими технологическими бизнесменами и лидерами мнений будут опубликованы в Facebook, Instagram и на других площадках. Пока неизвестно, когда пройдет первая публичная беседа и кто примет в ней участие.

В рамках дискуссий Цукерберг будет рассказывать о проблемах, связанных с технологиями, публичности информации, открытости данных, искусственном интеллекте и его возможностях применения.

В 2018 году вокруг компании Facebook прошло огромное количество скандалов, связанных с проблемами с конфиденциальностью данных пользователей.

***

14.01.2019

Дурова предупредили, что при ликвидации Telegram Messenger LLP права и имущество отойдут Великобритании

Британский государственный реестр юридических лиц предупредил Павла Дурова, что в случае ликвидации Telegram Messenger LLP, её права и имущества перейдут Великобритании. Это произойдёт в течение двух месяцев после одобрения заявки о ликвидации компании.

Докладніше

***

15.01.2019

Ощадбанк запустил чат-бота в популярном мессенджере

Теперь виртуальный помощник Ощадбанка есть и в Facebook Messenger чат-бот. Начиная с января 2019 года клиенты Ощадбанка – пользователи

Facebook могут связываться с банком с помощью чат-бота в Messenger. Об сообщила пресс-служба госбанка.

Найти виртуального помощника можно в Messenger – m.me/Oschadbot, или на странице Ощадбанка – https://www.facebook.com/oschadbot/. Ранее банк запустил чат-ботов на своем сайте и в Telegram (@Oschadbot). С помощью чат-бота можно: проверять баланс карточного счета и счета мобильных сбережений; заказывать выписки со счета по электронной почте; проверять состояние задолженности по карточному счету; блокировать и активировать карточки, снимать лимиты; уточнять статусы карточки, последней транзакции и доставки карты, статус денежного перевода; подключать SMS-банкинг; продлевать срок действия карты; активировать возможность снятия наличных без карты и др. По информации пресс-службы госбанка, список этих услуг будет расширяться. Если клиенту нужно получить консультацию относительно банковских продуктов, он может заказать обратный звонок консультанта контакт-центра Ощадбанка (PaySpace).

***

16.01.2019
Facebook потратит $300 миллионов на журналистику

Facebook объявил о трехлетнем плане инвестировать $300 млн в «новостные проекты, партнерства и контент», передает CNN. Часть средств будет напрямую направлена некоммерческим организациям вроде фонда Пулитцера, а также на «локальные новостные экосистемы» (InternetUA).

Местные газеты и сайты были «уничтожены цифровой революцией», в том числе из-за появления Facebook, от изменений в новостной ленте которого напрямую стал зависеть трафик многих изданий, поясняет CNN.

Соцсеть попала в череду скандалов и «сражается на нескольких других фронтах», но также поставила задачу улучшить свою репутацию в медиаиндустрии: пилотный проект поддержки СМИ Facebook запустил два года назад, добавляет телеканал.

«Мы не хотим, чтобы издатели зависели от нас, мы хотим поддержать их», – заявил CNN вице-президент Facebook по новостному партнерству Кэмпбелл Браун.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

9.01.2019

Ученые рассказали об опасности увлечения «селфи»

Любители фотографировать сами себя быстрее глупеют и теряют память. К такому выводу пришли британские специалисты (InternetUA).

По словам ученых, любители «селфи», которые хотят продемонстрировать всему миру, как им хотелось бы жить, не удовлетворены реальностью. Как утверждают исследователи, постановочные позы на фото, не естественная мимика и частые публикации в социальных сетях приводят к тому, что личность человека стирается.

Кроме того, во время этого процесса человек не «напрягает» свою память. Таким образом зависимые от «селфи» личности склонны становиться глупее.

Ученые заявляют, что лучший способ проверить себя на измененное сознание – пройти простой тест. Необходимо взять снимки пятилетней давности и вспомнить детали запечатленного момента. Тем, кто кроме факта мероприятия не удается больше ничего вспомнить, следует чаще тренировать память.

***

9.01.2019

46 % интернет-пользователей сократили время, проведенное в сетях, в 2018

Исследование GlobalWebIndex отмечает, что сокращение времени, проведенного в сетях, стало растущим трендом в прошлом году. Исследование обнаружило, что 46 % интернет-пользователей в США уменьшили время, проведенное в сетях. Об этом же заявили и 41 % пользователей в Великобритании. Молодые люди более всего заинтересованы в том, чтобы проводить меньше времени в социальных медиа. Про это заявили 58 % пользователей от 16 до 24 лет по сравнению с 43 % пользователей от 35 до 44 лет. Шесть из 10 пользователей отметили, что значительно уменьшили время, проведенное в сетях. Женщины стали меньше проводить времени в Facebook, а мужчины стали чащи заходить в Instagram (Marketing Media Review).

***

10.01.2019

Смартфоны хотят использовать, чтобы обнаруживать депрессию у подростков

Исследователи в США хотят использовать смартфоны, чтобы определять депрессию у подростков. Они пришли к выводу, что в последние годы молодые американцы стали чаще страдать от депрессий и совершать самоубийства отчасти по причине пользования социальными сетями (InternetUA).

В результате клин решили вышибать клином. Ведётся разработка приложения, которое поможет определять ментальные проблемы. Назвали проект «смартфонная психиатрия».

В программе использован искусственный интеллект. Приложение анализирует всё: от скорости написания текстов, до тона голоса и выбора слов. Исследователи говорят, что есть около 1000 разных параметров, изменения в которых могут указать на возможную депрессию или намерение подростка причинить себе вред.

В рамках исследования ведут наблюдение за двумя сотнями старшеклассников, включая детей из неполных или неблагополучных семей, а также тех, кто пережил смерть близких или издевательства в школе. Они отвечают на вопросы о своём настроении, а также о том, что на него влияет.

Полученные ответы сравнивают с данными, которые собирает система искусственного интеллекта.

***

11.01.2019

Сколько времени на самом деле ребенку можно играть с гаджетами?

Новые рекомендации британского Королевского колледжа педиатриии и детского здоровья противоречат общепринятой точке зрения.

В отчете содержится призыв более внимательно изучить влияние гаджетов и Интернета (в частности, социальных сетей) на здоровье детей, поскольку в данный момент выводы делаются на основании слишком расплывчатых данных и не учитываются многие дополнительные факторы.

Докладніше

***

16.01.2019

Ні небезпечним пранкам та приниженню дітей: як YouTube змінив правила публікації відео

YouTube оновив призначені для користувача правила. Тепер на відеохостингу заборонено публікувати ролики із небезпечними челенджами і пранками, під час виконання яких люди отримують або можуть отримати травми.

Докладніше

***

16.01.2019

8 вещей, которые психологи советуют не размещать в соцсетях

Социальные сети оказывают сильное воздействие на нашу повседневную жизнь, и зачастую далеко не в лучшую сторону. Соцсети также могут крайне

вредоносно воздействовать на наши жизни, если мы будем недостаточно осторожны.

Докладніше

Маніпулятивні технології

3.01.2019
Ирина Фоменко
Через ваш аккаунт в Twitter могут распространять исламистскую пропаганду

Хакеры взламывают и используют бездействующие аккаунты Twitter для распространения террористической пропаганды. Твиты с измененным стилем написания или языком говорят о взломанном аккаунте – иногда достаточно даже одной публикации на арабском языке, восхваляющей Аллаха, или ретвит такой пропаганды.

Докладніше

***

4.01.2019
Мошенники создали фейковый аккаунт ПриватБанка в Instagram

На днях мошенники создали в соцсети Instagram поддельный аккаунт ПриватБанка. Об этом сообщил на своей странице в Facebook руководитель направления Инноваций в ПриватБанке Егор Аветисов (InternetUA).

На канале проходит акция – первым 10 тыс подписчиков обещают выплатить по 500 гривен. Для этого нужно подписаться на каналы банка в Telegram и Instagram (ссылки на фейковые аккаунты приведены в профиле), запостить сториз со ссылкой на поддельный аккаунт, выслать номер карты в личных сообщениях.

«Люди реально отправляют свои деньги и реквизиты карт этим товарищам, а потом приходят на наш официальный аккаунт и начинают рассказывать, что они выполнили условия акции», – Егор Аветисов, руководитель направления Инноваций в ПриватБанке

***

2.01.2019
Соцмережі розчиняють науку та перетворюють її на «клікбейт»
Євген Корольов

Наукові новини дуже складно передавати звичайним людям. Труднощі відчувають навіть традиційні ЗМІ, які часто не повністю передають усі

особливості наукового дослідження, неправильно тлумачать його результати та акцентують увагу не на тому, про що розповідають вчені.

Потрапляючи в соцмережі, ці вже спотворені публікації починають ще більше деформуватися, втрачаючи важливі факти на користь кричущого заголовка та утримання уваги читачів.

Докладніше

***

16.012.019

Выборы-2019: польские СМИ пророчат масштабную атаку российских «троллей» на Украину

С приближением выборов российская дезинформационная активность в отношении Украины только усилится. Об этом сообщает Польске радио (Realist).

На каждую тысячу случаев дезинформации в прокремлевских СМИ 461 касался Украины, – заявляют эксперты группы EU vs Desinformation.

«Эта тенденция, однако, усилится еще больше, ведь в марте на украинское государство ждут президентские выборы, а в ноябре – парламентские», – утверждает политолог Петр Андрусечко.

По словам экспертов, фейковые сообщение направляются адресатам в России, Украине и других государствах. Россиянам демонстрируют материалы, в которых украинцы представлены как нелюди, а представители власти в Киеве – как наследники нацистов. Украинский адресатов пытаются деморализовать, например, сообщениями о слабости их армии. Зато людям Запада и в целом международному сообществу российские тролли представляют украинцев как виновных в конфликте с Россией.

С поступлением выборов российская дезинформационная активность в отношении Украины только усилится. Киев бьет тревогу, что Россия различными способами попытается повлиять на их ход.

Спецслужби і технології «соціального контролю»

2.01.2019

В России «Первый канал» отключил комментарии под новогодним обращением Путина, собравшим более 70 тыс. «дизлайков»

Новогоднее обращение президента РФ Владимира Путина, которое разместил телеканал «Россия 1», оценили как «не понравилось» 33 тыс. пользователей – в 11 раз больше, чем те, кому понравилось, сообщает интернет-издание «ГОРДОН» (InternetUA).

Российский «Первый канал» отключил на своей странице в YouTube комментарии под новогодним обращением президента РФ Владимира Путина,

когда количество дизлайков превысило 70 тысяч. Об этом 1 января в Facebook сообщил писатель Евгений Шестаков.

«Не долюбил народец нынче кощеюшку. Плохих слов “Первому каналу”" принес, тот все их стер, комментарии отключил», – написал он.

Шестаков также разместил скриншот YouTube-страницы «Первого канала», где видно, что после почти 922 тыс. просмотров обращение Путина собрало 13 тысяч «лайков» и 77 тысяч «дизлайков».

Сейчас на странице «Первого канала» с обращением Путина комментарии отключены, а количество «лайков» и «дизлайков» – скрыто.

Новогоднее видео, размещенное на том же видеосервисе телеканалом «Россия 1», по состоянию на 3.50 2 января не было ограничено. «Не понравилось» его обозначили 33 тыс. пользователей – это в 11 раз больше, чем те, кому понравилось.

В комментариях пользователей присутствует ненормативная лексика в адрес Путина. В частности, его называют «главным врагом России», «вороватым» и «лицемерной рожей».

***

2.01.2019

Власти Ирана объявили сотрудничество с криптовалютой Gram от Telegram угрозой национальной безопасности

Правительство Ирана предприняло дальнейшие шаги, направленные на противодействие криптовалюте Gram, разработкой которой занимается мессенджер Telegram. Об этом 31 декабря сообщило издание Tehran Times (InternetUA).

В заявлении секретаря рабочей группы по определению уголовного содержания Джавад Джавидния, любое сотрудничество с приложением по запуску токена Gram будет считаться действием против национальной безопасности и угрозой национальной экономике.

«Одним из наиболее важных факторов при запрете Telegram было ощущение серьезной экономической угрозы, которую несет его деятельность. К сожалению, эта угроза была оставлена без внимания из-за неразберихи в политической атмосфере страны», – сказал Джавидния.

Первые ограничительные меры в отношении Telegram Иран принял в апреле 2018 года, когда верховный лидер аятолла Али Хаменеи запретил его использование сотрудникам правительственных учреждений. Позже в том же месяце власти этой ближневосточной страны полностью запретили использование биткоина и других криптовалют. Впоследствии Telegram был полностью запрещен на территории Ирана.

Официальные лица страны также заявляли, что первоначальное предложение монет (ICO), которое Telegram провел в прошлом году, потенциально «подрывало национальную валюту Ирана». Высший совет по киберпространству одобрил предложенный запрет, согласившись, что в

потенциале доступ к криптовалютному токену Gram могут получить все иранские пользователи приложения.

***

4.01.2019
В ЕС не доверяют китайским технологиям

Европейский Союз (ЕС) требует более тщательного изучения потенциальных рисков, связанных с китайскими технологическими компаниями. Такое решение в организации возникли на фоне растущей киберпреступности со стороны Пекина (InternetUA).

Дипломат, который давал комментарий изданию Financial Times, рассказал, что с предстоящим внедрением мобильной технологии 5G самое время поставить под сомнение намерения Китая по продвижению технологии другим странам.

Все больше стран обеспокоены поведением Китая в сфере кибербезопасности. Страны ЕС, включая Испанию, Италию и Финляндию, в 2018 году уже провели аукционы на частоты 5G, а ряд других государств запланировали такие аукционы на 2019 год. Мы призываем не совершать поспешных действий, о которых можно пожалеть потом, из комментария дипломата для Financial Times.

Так, в прошлом месяце США обвинили двух граждан Китая в совершении крупнейшей хакерской кампании. Кроме того, обвинения были представлены и представителям Народно-освободительной армии Китая, которые скомпрометировали систему дипломатических коммуникаций ЕС. В частности, последний инцидент в Пекине отрицают.

Также довольно-таки подозрительной является арест Мэн Ваньчжоу, финансового директора компании Huawei. Женщина задержана по запросу американских властей, ее обвинили в нарушении торговых санкций США с Ираном. При этом Huawei отрицает какие-либо нарушения Мэн.

***

9.01.2019
Facebook звинуватили у порушенні кібербезпеки

В'єтнам звинуватив Facebook у порушенні закону про кібербезпеку за дозвіл користувачам залишати антиурядові коментарі (Espreso.tv).

Про це повідомляє Reuters.

Як вважають представники влади, компанія Facebook порушила новий закон про кібербезпеку, дозволяючи користувачам розміщувати антиурядові коментарі.

У Міністерстві інформації і зв'язку В'єтнаму заявили, что Facebook дозволяє користувачам друкувати пости, які містять нібито наклепницький зміст проти окремих осіб і організацій.

Зазначимо, що незважаючи на економічні реформи, Комуністична партія В'єтнаму зберігає жорстку цензуру в засобах масової інформації.

***

9.01.2019

Google и Facebook оштрафовали за скрытие информации

Генпрокурор американского штата Вашингтон принял решение оштрафовать компании Google и Facebook за сокрытие данных, связанных с публикацией на их сайтах политической рекламы. Агитационные материалы размещали и оплачивали местные кандидаты на политические посты. Интернет-компании нарушили Fair Campaign Practices Act, который был принят в 1972 году (Украинский телекоммуникационный портал).

Этот закон требует полного раскрытия всей информации, касающейся финансирования политических кампаний и лоббирования. Fair Campaign Practices Act регулирует требования штата Вашингтон к финансированию избирательных кампаний, в том числе требуя отчётности перед общественностью о финансировании политических кампаний, расходах лоббистов и финансовых делах государственных должностных лиц и кандидатов.

Кандидаты во время избирательных кампаний использовали интернет-ресурсы Google и Facebook для публикации агитационной информации. В соответствии с отчётами кандидатов, за десять лет размещения политической рекламы они заплатили Google $1,5 млн, а Facebook – $5,1 млн.

По итогам судебного расследования принято решение о штрафе, так как Google и Facebook с 2013 года не выполняли требование о сборе, хранении и публикации информации о заказчиках такой рекламы, как того требуют законы штата. Google оштрафован на 217 тысяч долларов, а Facebook заплатит 238,5 тысячи долларов. Иски в суд в июне 2018 года направил Боб Фергюсон, генпрокурор штата Вашингтон.

***

9.01.2019

Антиукраїнська діяльність у соцмережах: в СБУ розповіли про масштаби пропаганди та арешти модераторів груп

За антиукраїнську пропаганду до відповідальності притягнуто 49 осіб, які займались адмініструванням груп у соцмережах. Про підозру повідомлено 29 з них (Ракурс).

20 вироків суду у справах про антиукраїнську пропаганду набрали чинності, повідомляє прес-центр Служби безпеки України.

Протягом 2018 року СБУ виявила та блокувала 360 кібератак на українські сайти. Також співробітниками Служби безпеки було попереджено

вісім терористичних актів, які зловмисники намагалися скоїти на території України.

Військова контррозвідка СБУ виявила 152 учасників терористичних організацій Л/ДНР, 54 з них було затримано.

Як раніше повідомляв «Ракурс», у держзраді та шпигунстві СБУ запідозрила 50 українців у 2018 році.

***

14.01.2019

Власти Венесуэлы начали блокировать доступ к «Википедии»

Власти Венесуэлы начали блокировать доступ местных пользователей к интернет-энциклопедии «Википедия». Об этом сообщает организация NetBlocks, которая собрала доказательства ограничения доступа ко всем разделам энциклопедии (InternetUA).

Сообщается, что блокировку ввела государственная компания CANTV, которая является крупнейшим телекоммуникационным оператором в стране. Предположительно причиной блокировки стала борьба со статьей «Википедии» о политическом кризисе в Венесуэле, в которой новый глава парламента страны (Национальной ассамблеи) Хуан Гуайдо был назван «47-м президентом Боливарианской Республики Венесуэла». По данным NetBlocks, доступ был ограничен также к некоторым местным сайтам.

***

14.01.2019

Facebook выявил российское администрирование на многих украинских сообществах

Чтобы посмотреть местоположение администрации сообщества необходимо нажать на вкладку «Информация и реклама» (InternetUA).

Социальная сеть Facebook начала показывать страны, из которых ведется администрирование популярных страниц соцсети. При этом выяснилось, что на многих украинских сообществах администрацией занимаются люди из РФ. Об этом сообщает Наташа Белова на своей странице в Facebook.

Она предоставила скриншоты нескольких популярных сообществ, на котрых видно, их администрированием занимались люди из России.

Информация о местоположении администрации сообщества находится во вкладке «Информация и реклама».

Стоит отметить, что в августе 2018 года компания Facebook обязала администраторов популярных американских сообществ подтвердить свои данные и местоположение с помощью геолокации и паспорта.

Такие меры были приняты в связи с выборами президента США. Чтобы никто из иностранного правительства не смог повлиять на выборы с помощью Facebook-сообществ.

***

16.01.2019

Facebook ужесточает правила размещения политической рекламы для Украины

Компания Facebook расширит некоторые из своих правил политической рекламы и инструменты для сдерживания вмешательства в выборы на Украину, Индию, Нигерию и Европейский Союз.

Докладніше

Проблема захисту даних. DDOS та вірусні атаки

4.01.2019

Свыше 5 млн. пользователей Google Play установили в декабре ПО с рекламными троянцами

В течение месяца в Google Play было выявлено множество вредоносных и нежелательных программ. Среди них – рекламные троянцы Android.HiddenAds.343.origin и Android.HiddenAds.847, распространявшиеся под видом игр и полезных приложений. После запуска они скрывали свой значок с главного экрана и начинали показывать рекламу.

Докладніше

***

4.01.2019

Google исправила уязвимость безопасности Chrome через три года после обнаружения

Google устранила критический баг в Chrome для Android, о котором стало известно более трёх лет назад, пишет TechRadar (InternetUA).

Уязвимость обнаружили баг-хантеры из Nightwatch Cybersecurity в мае 2015 года. Однако проблема оставалась нерешённой до момента, пока специалисты Google не поняли, что она несёт угрозу безопасности.

В процессе работы браузеры отправляют на веб-серверы различную информацию, например о себе, о запущенных приложениях и операционной системе, что считается нормальным. Но из-за бага в мобильном Chrome происходила утечка данных об устройстве, в том числе о его модели и прошивке. В десктопной версии такой проблемы нет.

Названия гаджетов, которые высылал Chrome для Android, были неполными (к примеру «C6606»), но по ним в готовых базах можно было легко найти точную модель (Sony Xperia Z).

Как подчёркивают в Nightwatch Cybersecurity, более опасным является раскрытие подробностей о микропрограммном обеспечении устройств. По ним часто можно вычислить поставщика и его страну. На сайтах производителей и поставщиков можно запросто получить номера сборки, а по ним – определить уровень безопасности смартфонов и уязвимость к отдельным видам атак.

Частичный патч вышел вместе с Chrome 70 в октябре 2018 года, но браузер по-прежнему высылает информацию о моделях устройств, а два компонента Android (включая встроенный браузер WebView) – номер билда прошивки.

***

4.01.2019

Хакеры опубликовали личные данные сотен немецких политиков

Неизвестные хакеры опубликовали личные данные и документы, имеющие отношение к сотням немецких политиков, сообщает телерадиостанция RBB. Отмечается, что в массиве данных есть информация на членов всех партий, представленных в бундестаге, кроме ультраправой «Альтернативы для Германии» (InternetUA).

Среди данных оказались сотни телефонных номеров и адресов членов бундестага, а также земельных парламентов. Опубликованы партийные документы, посвященные съездам и их участникам. Некоторые документы уже устарели и касаются событий, произошедших несколько лет назад.

Журналисты не смогли выявить какой-либо принцип, по которому были выбраны цели для взлома. Поэтому неясен и источник взлома – настолько разнообразные данные вряд ли могли быть получены в одном месте.

С политической точки зрения опасных документов там, на первый взгляд, нет. Но ущерб, вероятно, будет значительным хотя бы в силу того, насколько много различных данных было опубликовано (нем. яз.).

***

4.01.2019

Торговцы потеряют $130 млрд из-за хакеров – прогноз на пять лет

По данным недавнего исследования Juniper, розничные торговцы потеряют более $130 млрд в период с 2018 по 2023 года в связи с цифровым мошенничеством (InternetUA).

В отчете говорится о том, что онлайн-продацы в основном фокусируются на мониторинге транзакций, сеансов и поведения клиентов, а также проверке личности пользователя перед проведением транзакций. Эксперты настоятельно рекомендуют им уделять больше внимания предотвращению CNP (card not present) мошенничества.

По прогнозам Juniper, в 2023 году компании в сфере цифровых платежей будут тратить около $9,6 млрд в год на решения FDP (Fraud Detection & Prevention), а именно обнаружение и предотвращение мошенничества.

Необходимо отметить, что результаты исследования Juniper были ожидаемыми. По данным 2017 года, онлайн-торговцы, особенно на территории США, оказались в зоне риска. Рост онлайн-продаж и повсеместный переход на использование чипованных карт стандарта EMV, оставил продавцов уязвимыми для мошенничества типа CNP.

EMV недавно объявила о модернизации своего протокола для предотвращения мошенничества такого типа. Обновления включают в себя усовершенствования для поддержки новых процедур аутентификации во время онлайн-шоппинга, которые помогут остановить незаконные CNP-транзации.

***

6.01.2019

Шахраї придумали нову аферу з номерами телефонів та соцмережами

Про нову схему шахрайства розповіли в прес-службі поліції. Зловмисники телефонують оператору, називають номер телефону «жертви» і кажуть, що втратили телефон із карткою. Називають співробітнику компанії останні контакти. Після цього ваш номер опиняється «в руках» злочинців. За його допомогою можуть зламати пошту, акаунти в соціальних мережах і навіть банківський рахунок.

Докладніше

***

8.01.2019

Новая атака через побочный канал опасна для любого ПК с Windows и Linux

В работе, опубликованной 7 января на сервере arXiv, пять специалистов в информатике и компьютерной безопасности описали новую атаку по побочным каналам (Side-Channel Attack, SCA), эффективную против операционных систем, таких как Windows и Linux, а возможно и macOS (она выходила за рамки данного исследования).

Докладніше

***

8.01.2019

Надежность Face ID поставлена под сомнение

В 2017 году Apple представила инновационную технологию распознавания лиц Face ID. По заверениям представителей компании, новый способ биометрической аутентификации гораздо надежнее чем Touch ID.

Возможно это и так, но, как известно, любую систему защиты можно обойти – если знать её уязвимые места. По утверждениям специалиста по безопасности Виш Ву, ему таки удалось найти слабое место Face ID (Украинский телекоммуникационный портал).

Продемонстрировать свой метод взлома хакер планировал на мероприятии Black Hat Asia в марте 2019 года. По словам хакера, им была найдена брешь, которая позволяет без каких-либо затруднений обойти систему распознавания лиц Face ID. Впрочем, работает данная уязвимость только на iPhone X. Более новые модели, как выяснилось, не подвержены взлому.

Но, судя по всему, метод обхода не будет показан общественности. Как сообщает издание Reuters, выступление хакера было внезапно отменено из-за новых «обстоятельств». Вполне возможно, что к этому могла быть причастна Apple. Совершенно очевидно, что демонстрация взлома может негативно повлиять на репутацию компании, которая изначально позиционировала собственную технологию как предельно надежную и безопасную.

Впрочем, надо отдать должное Apple – до этого момента, ещё никто из хакеров не представил рабочий способ обхода Face ID. В то время как аналогичные разработки конкурентов практически сразу подвергаются обоснованной критике. Взять за пример тот же Samsung Galaxy S9 или Galaxy Note 9. Несмотря на наличие на борту устройств систем распознавания лиц, пользователи всё еще не могут подтверждать транзакции через Samsung Pay. Поставив такое ограничение, корейская компания красноречиво расписалась в несостоятельности собственной технологии.

***

8.01.2019

Google Chrome для Android стал оружием в руках злоумышленников

Google Chrome для Android в течение длительного времени мог быть причиной утечки приватной информации о пользователях, выяснили исследователи в области информационной безопасности компании Nightwatch.

Докладніше

***

8.01.2019

С помощью умных зеркал Google будет следить за вами даже в ванной

Кажется, голосовые ассистенты пытаются проникнуть буквально в каждый предмет и в каждую комнату. Правда, до сих пор они не особо претендовали на ванную, но и это изменилось. В рамках выставки CES 2019 Компания Capstone Connected Home представила умное зеркало Smart Mirror под управлением голосового ассистента Google (IGate).

Зеркалом можно управлять при помощи голосовых команд или сенсорного дисплея. Через ассистента зеркало позволяет пользователю управлять другими устройствами умного дома, узнавать о погоде и проверять состояние дорожного трафика еще во время утренних сборов. Также зеркало позволяет проверять соцсети, почту, отвечать на электронные письма, открывать YouTube, запускать музыку. В общем, устройство можно назвать гибридом планшета и смарт-колонки под зеркальной оболочкой.

Технология распознавания голоса Google позволяет настраивать профили для шести разных пользователей. Каждого человека зеркало узнает по голосу. Таким образом, если вы попросите ассистента озвучить запланированные события, тот по ошибке не выдаст вам секретов другого члена семьи.

С точки зрения дизайна гаджет выглядит как обычное настенное зеркало, а потому будет уместно смотреться в любом доме. В общем, теперь Google будет следить за вами даже в ванной.

Цена зеркала пока не озвучивается, но гаджет поступит в продажу в течение ближайших месяцев.

***

8.01.2019

Ирина Фоменко

Google Play опять «грузит» пользователей Android вредоносным софтом

В Google Play в очередной раз обнаружили вредоносные приложения. Исследователи из Trend Micro обнаружили десятки приложений, популярные утилиты и игры, у которых есть масса обманчиво отображаемой рекламы (чтобы выжать как можно больше денег из ничего не подозревающих пользователей Android), в том числе – полноэкранной, скрытой и фоновой.

Докладніше

***

9.01.2019

Експертка з інформаційної безпеки: Додати друга у соцмережі – все одно, що пустити незнайомця додому

Катерина Баркалова

Чого не можна робити в мережі, чим небезпечні фейки про маніяків, що викрадають дітей та чому тест «Який ти сир?» потрібно оминати десятою дорогою.

Докладніше

***

10.01.2019

Владимир Кондрашов

В Украине ищут интернет-мошенников, которые вымогали деньги от имени МВД Беларуси

Украинская полиция помогает правоохранителям Республики Беларусь в расследовании случая компьютерного саботажа. Интернет-злоумышленники вымогали деньги от имени Министерства внутренних дел Республики Беларусь за разблокировку браузера пользователя. Следы мошенников ведут в Украину.

Докладніше

***

10.01.2019

В Сети выложен простой инструмент для преодоления двухфакторной защиты

Новое средство тестирования проникновения, опубликованное на GitHub в начале года, позволяет автоматизировать фишинговые атаки и даже преодолевать двухфакторную аутентификацию (2FA). Оно представляет собой так называемый обратный прокси-сервер, модифицированный для работы с трафиком для страниц входа и фишинговых операций.

Докладніше

***

10.01.2019

Пользователи обнаружили в Инстаграме ссылки на детскую порнографию

Война хештегов развернулась между пользователями, которые распространяли ссылки на детскую порнографию, и подростками, намеренными это остановить.

Докладніше

***

11.01.2019

Китайское приложение для смартфонов украло данные 10 миллионов пользователей со всего мира

Как стало известно, китайский производитель бытовой электроники TCL собирал данные с мобильных телефонов, не спрашивая разрешения пользователей. Получение информации производилось с помощью бесплатного приложения для смартфонов с прогнозом погоды, которое с момента его выпуска в декабре 2016 года было загружено пользователями со всего мира более 10 миллионов раз.

Докладніше

***

15.01.2019

Google избавила Google Play от сотни вредоносных программ для Android

За последние два месяца Google удалила из Google Play более сотни вредоносных и потенциально опасных приложений. Об этом рассказали официальные представители компании.

Докладніше

***

15.01.2019

Владимир Кондрашов

Facebook «кормит» украинцев рекламой сомнительных и пиратских веб-сервисов

В последнее время стало появляться всё больше жалоб на рекламу в украинском сегменте Facebook: от имени сомнительных компаний (а иногда даже и ничего не подозревающих пользователей) рекламируются некачественные товары, пиратские сервисы или даже покупка аккаунтов для российской фабрики троллей. Однако обнаруженный нами вид рекламы ставит под сомнение какую-либо модерацию объявлений популярнейшей в мире соцсети (InternetUA).

Сегодня в Facebook была замечена рекламная кампания, сообщающая пользователям о том, что BitTorrent официально выпустил µTorrent Web, торрент-клиент для Windows, якобы работающий через Интернет, который позволяет загружать и воспроизводить торренты внутри браузера. Такая реклама противоречит Условиям предоставления услуг Facebook, которыми запрещено публиковать содержимое, нарушает права интеллектуальной собственности других лиц, в том числе авторские права и права на торговую марку.

Кроме того, реклама с Facebook ведет непосредственно на фейковую страницу, созданную для заражения устройств пользователей вирусами. Страница, размещенная на сайте консалтинговой компании из Люксембурга неизвестными, имитирует страницу новостного технологического издания, где и сообщается о торрент-клиенте для Windows.

***

15.01.2019

Распространяемый через торренты поддельный видеофайл подменяет результаты поиска в Google

Распространяемое через The Pirate Bay и замаскированное под видеофайл вредоносное ПО заражает компьютеры под управлением Windows и выполняет

ряд вредоносных функций. К примеру, вредонос способен внедрять подготовленный злоумышленником контент на такие популярные сайты, как Википедия, Google или Яндекс.

Докладніше

***

15.01.2019

«Умные» телевизоры дешевеют, продавая информацию о пользователях

В сезон рождественских праздников в США были проданы миллионы телевизоров компаний Vizio (США) и TCL (Китай) с поддержкой 4K и HDR. Стоимость такой модели, которая останется актуальной ещё много лет, с диагональю экрана 65" составляла порядка $500. Но такая низкая цена связана с оговоркой, на которую большинство людей не обращают внимания: некоторые производители собирают данные о пользователях, а затем продают их третьим сторонам.

Докладніше

***

15.01.2019

США звинуватили українця у зламі бази даних Комісії з цінних паперів

США висунули звинувачення українському хакеру і ще кільком особам через проникнення в базу даних Комісії з цінних паперів і бірж США (SEC).

Докладніше

***

16.01.2019

Владимир Кондрашов

Украинские хакеры поиздевались над официальным вестником Кабинета Министров

Спикер Украинского киберальянса, известный в сети под ником Шон Таунсенд, опубликовал на своей странице в Facebook скриншот видоизменного сайта официального вестника Кабинета Министров Украины «Урядовий кур’єр». Хактивисты УКА, используя XSS-уязвимость на сайте правительственного вестника, изменили содержимое ряда публикаций (InternetUA).

Таким образом УКА в рамках флешмоба #fuckresponsibledisclosure уже не первый раз пытается привлечь внимание властей к безопасности государственных информационных ресурсов.

Тем не менее, даже «банальная» XSS-уязвимость сайта «Урядовий кур'єр» (уязвимость ПО, позволяющая атакующему внедрить клиентский сценарий в web-страницы, просматриваемые другими пользователями – Ред.) может стать серьезным оружием в руках врага в информационной войне. XSS можно успешно использовать для кражи паролей.

ДОДАТКИ

Додаток 1

3.01.2019
Соцсети: что ждет Facebook, Instagram, Twitter, YouTube в 2019-ом

Один из редакторов The Verge (специализируется на Кремниевой Долине) Кейси Ньютон попросил читателей поделиться прогнозами для социальных сетей на 2019 год. В итоге он срезюмировал ряд трендов, добавив к ним несколько своих собственных умозаключений (InternetUA).

LIGA.net публикует резюме колонки Ньютона.

1. Пора платить

Может появиться больше платных социальных сетей. В традиционных представлениях, чем больше людей зарегистрировано в конкретной социальной сети, тем лучше она работает. Но судя по всему, это не так. Посмотрите, к примеру, на рост платных каналов на Slack.

Одна из мыслей – Apple или Google еще раз попробуют создать свою социальную сеть. Мы точно знаем, что вундеркинд Майкл Сайман готовит что-то вроде социального приложения для Google, поэтому предположение кажется правдоподобным.

2. Оправдание блокировки

Еще одна мысль: «Главы государств с автократической идеологией используют обеспокоенность насчет Фейсбука как оправдание блокировки доступа, национализации или полного запрета социальных сетей на территории своих стран». Предпосылки этому уже есть.

Так что возможно, мы увидим, как принимаются шаги в направлении регуляции национальных положений о конфиденциальности, которым препятствуют участники вооруженных конфликтов.

3. Падающий спрос

Читатели прогнозируют в Северной Америке снижение использования соцсетей. Возможно, будут разработаны сообщества с платным членством. Кейси Ньютон также считает, что снижение активности пользователей соцсетей в 2019 году произойдет из-за повышения уровня модерации контента и проблем внешнего вмешательства. И я не предсказываю, что в 2019 году история Фейсбука закончится.

4. Instagram ждет удар?

Есть предположение, что фейсбучизация Инстаграма продолжится, но при этом приложение будет страдать от серьезных утечек персональных данных. Я не могу предсказать конкретно, но считаю, что в 2019 году мы увидим что-то вроде сведения счетов с Instagram. Харизматические основатели ушли, пресса продолжает спрашивать про давно назревшие проблемы, и все больше усиливается чувство, что кто-то следит за предложением, чтобы ударить его побольнее.

5. Twitter и эксперименты с ИИ

Предположение: «Твиттер станет основой для большого количества неоднозначных экспериментов с искусственным интеллектом, но ни одно изменение не будет содержать кнопку «Редактировать». И так, скорее всего, и будет.

Один из читателей утверждает, что Твиттер будет исключен из App Store из-за контента 18+ – прогноз, который может вполне воплотиться в реальность после фиаско Tumblr в этом году.

Кейси же считает, что Twitter выстоит, и остальные будут постоянно называть материть его, но в любом случае продолжат им пользоваться.

6. YouTube и сериалы

Бывший работник Facebook Бен Каннингам прогнозирует, что на YouTube появится многосерийный контент. Возможно, что-то вроде S-Town, Slow Burn или Caliphate. Как один из вариантов, как это может быть реализовано: посмотрите документальный сериал Шейна Доусона, который касается конференции TanaCon.

Никто не прогнозирует, что YouTube справится с проблемой правого экстремизма.

7. Snap – будет трудный год

Каннингем предполагает, что разработки с использованием дополненной реальности будут затмевать собой все остальное, что похоже на правду. Для Snap это будет трудный год.

8. Facebook – фиаско с личными данными

Несмотря на активное развитие в 2018 году, в конце прошлого года Facebook выявил еще одну утечку данных. Эта поразила почти 6,8 миллионов людей, которые дали разрешение 1500 приложениям от 876 различных разработчиков показывать фото, к которым они не должны были иметь доступа. Один из редакторов The VergeДжейк Кастренейкс говорит:

«Facebook утверждает, что у них был баг, связанный с ошибкой доступа к логину Facebook и API фотографий, которая по факту дала доступ разработчикам к фото в рамках своих приложений. Все пострадавшие пользователи вошли в приложения третьих сторон, используя собственные аккаунты Фейсбука и предоставили им доступ к своим фото».

«Мы сожалеем, что подобное случилось», пишет Томер Бар, инженерный директор Фейсбука. Разглашение доступа случилось на следующий день после

открытой презентации Facebook, которая должна была показать людям, как они могут управлять своей приватностью на сайте.

Напомним, в конце сентября баг стал причиной разглашения личной информации 30 миллионов пользователей. В октябре масштаб нарушений только увеличился вместе с докладом, что уязвимость касается не только некоторых емейлов и телефонных номеров пользователей, но также и информации в профиле, включая пол, месторасположение, дни рождения и недавнюю историю поиска. ФБР сейчас расследует данную утечку.

Эти две серьезных уязвимости были обнаружены на протяжении месяца – в этот же год, когда произошел скандал с Cambridge Analytica, которая также коснулась миллионов пользователей Facebook. Если взять все вместе, масштаб провалов просто ошеломляет, ведь они охватывают десятки миллионов людей. Утечка данных не ограничивается только электронной почтой и паролями, она включает и персональную информацию – истории посещений, поисков и фото.

«Последнее время я встречаюсь с друзьями, которые говорят, что ограничивают использование социальных сетей – они просто удаляют свои аккаунты и мобильные приложения, а время от времени заходят на сайты вроде Facebook с помощью компьютера. Что-то подобное сделал и я сам – год назад я отключил все оповещения Facebook, и это помогло мне уменьшить время использования приложения всего до нескольких минут в день. Детали последнего слива, возможно, не вызывают слишком сильного волнения, как это могли показать СМИ. Но я полагаю, что для многих людей именно это стало последней каплей», – пишет редактор The Verge.

9. Facebook: крах секретного отдела

Facebook по-тихому расформировал свой секретный отдел разработки Building 8 (запущен в апреле 2016 для разработок наподобие DARPA – Defense Advanced Research Projects Agency – Ред.), поскольку они изменили порядок тестирования новейших элементов программного обеспечения.

Building 8, которая создавалась как магическая лаборатория в стиле Вилли Вонка, была закрыта – утверждает Регина Даген, бывший сотрудник агентства по перспективным оборонным научно-исследовательским разработкам США. Это уже было очевидно, когда Даген в прошлом году уволилась из конторы, проработав там всего 18 месяцев.

С другой стороны, глава технического отдела утверждает, что ситуацию поняли неправильно: «Исследование, которое мы запустили в Building 8, продолжается в пределах Facebook Reality Labs».

Некоторые из наиболее перспективных экспериментальных продуктов передали в другой отдел – Facebook Reality Labs, а ее технические мощности были перепрофилированы для запуска видео-чата Facebook.

Building 8, тем временем, списали со счетов полностью, как рассказал спикер журналу Business Insider.

10. Facebook ищет новые деньги

Facebook ищет новый источники доходов: количество времени, которое пользователи проводят в соцсети постепенно падает:

На долю Facebook, Messenger, Instagram and WhatsApp приходится меньше 14 % создаваемого контента в ноябре. Для сравнения, два года назад этот показатель был равен 18 %, а год назад – 16 %.

11. Факт-чекеры на Facebook

Facebook на страже правды. Verge спросило 19 факт-чекеров о том, что они думают об их партнерстве с Facebook. Вот, что они рассказали:

Интересная статистика: факт-чекеры, которые проверяют факты на достоверность, в общем итоге за два года пометили как минимум 30000 материалов как ложные. Преследуя собственные цели, факт-чекеры в принципе удовлетворены сотрудничеством с Facebook и ставят ему оценку 3,5 из 5.

Если оценивать это мерками Yelp, которые они применяют для оценки ресторанов, то здесь так себе кухня, но вот отравление вам точно не грозит.

Также сотрудники удовлетворены (3,5 из 5) оплатой, которую они получают от Фейсбука за свою работу. Несмотря на то, что суммы не оглашаются и зависят от сделанных объемов работы, Factcheck.org раскрыл, что в 2018 году Facebook потратил на это $188881.

12. YouTube фильтрует спамеров

Пользователи YouTube могут заметить «значительное уменьшение» количества подписчиков из-за фильтра спамеров.

Официальное сообщение на форуме YouTube говорит, что в рамках текущего обслуживания компания провела зачистку. Удаление спам-аккаунтов помогает сохранить YouTube в качестве «честного игрового поля» для создателей контента. Поэтому платформа борется с искусственным увеличением количества подписчиков на каналах. Правда, еще неясно, сколько каналов использовали подобные инструменты, но YouTube предупреждает, что при обнаружении накрутки на канале его ждет откат назад.

«Мы постоянно проверяем законность аккаунтов и действий на ваших YouTube каналах», – пишут в блоге сервиса. «В рамках таких регулярных проверок мы идентифицируем и удаляем подписчиков, которые заспамляют нашу платформу».

13. Instagram и работа с брендами

Instagram начнет информировать бренды, чьи продукты используют обозначения, которые нельзя использовать для рекламного таргетинга.

Люди любят Инстаграм, но иногда они спрашивают: почему не все мои действия на платформе используются для определения рекламных предпочтений?

За последние месяцы Инстаграм представил инструмент, который позволит пользователям добавлять в закладки интересные продукты. Сейчас Инстаграм работает над инструментом, который показывает брендам, какие именно их продукты сохраняют пользователи, – утверждает Лайла Амжад, продакт-менеджер Инстаграма. Соцсеть планирует сделать эту функцию доступной в первой половине 2019 года.

14. Facebook банит без разбора

Редактору The Verge лично нравятся действия Фейсбука, когда он требует больше информации от политической рекламы – это делает жизнь иностранных агентов непростой, ведь влиять на выборы становится труднее. Конечно, были трудности, но результат – как говорит исполнительный директор Nuyorican Poets Cafe – действительно делает Facebook территорией, где каждое доброе дело не избежит наказания.

«В любом случае, я полагаю, что мы можем поговорить о некоммерческой покупке рекламы, которая может повлиять на результаты выборов. И я действительно считаю, что ее заказ требует более тщательного рассмотрения», – пишет редактор The Verge.

Некоторые оплаченные рекламные кампании, которые запустили его коллеги за последние несколько месяцев, были необъяснимо остановлены как не отвечающие политике Facebook. Фейсбук не дал разрешение прорекламировать культурное некоммерческое мероприятие – Nuyorican Poets Cafe, потому что эта страница «не авторизована для запуска рекламных кампаний, связанных с политикой». Кампания, продвигающая лекцию о скульптуре в Бостонском музее изобразительных искусств была заблокирована, потому что цензоры Facebook ошибочно посчитали, что она касается выборов в Ирландии.

(вгору)

Додаток 2

9.01.2019

Ирина Фоменко

Появились новые приложения для знакомств, фильтрующие неподходящих кандидатов

В отличие от Tinder, Facebook Dating, Hinge или большинства других приложений для знакомств, в этих эксклюзивных версиях требуется, чтобы пользователи подали заявку, которую должны одобрить. Самые популярные приложения для «серьезных» знакомств – Raya и The League (InternetUA).

Журналисты The Verge Эшли Карман и Кейтлин Тиффани, а также генеральный директор The League Аманда Брэдфорд разбирались, почему люди проводят время, обращаясь к этим службам, и зачем были созданы эти приложения.

В чем заключается задача The League?

– Хотелось построить сообщество, где люди были бы амбициозными, ориентированными на карьеру. Им понравилось это друг в друге. Они хотели встречаться с кем-то с такими чертами. Иногда я шучу и говорю, что это приложение для трудоголиков, но, в конце концов это люди, которые действительно серьезно относятся к своей карьере и хотят оказать какое-то влияние на мир.

The League – это люди, которые очень высоко ценят образование. Вы говорите с любой девушкой, которая заканчивает Гарвардскую школу бизнеса,

и она предпочла бы встречаться с кем-то, кто тоже ходил в школу, о которой она слышала, и причина, по которой она этого хочет, не в том, что вы умнее, а в том, что вы цените образование.

The League имеет собственную систему проверки. Как вы определяете, кого можно «впустить» в приложение?

– На самом деле мы единственные, кто имеет двойную проверку. Сначала мы проверяем Facebook, затем LinkedIn, а потом мы ставим всех в список ожидания. Это похоже на приемную комиссию колледжа. Все идут в лист ожидания, а затем мы стараемся привлечь людей, которые потратили время на свои профили.

Мы стараемся, чтобы сообщество было разнообразным. Как и в системе приема в колледж, вы не хотите, чтобы все учили историю или занимались музыкой. Мы пытаемся сделать так, чтобы образование людей было разным. Идея заключается в том, что мы приводим людей в сообщество, но оно – сбалансировано.

Какой процесс подачи заявки?

– Мы узнаем все данные из Facebook и LinkedIn. Пользователь предоставляет немного базовой информации и то, что он хотел бы видеть в графе «О себе». Затем мы ставим его в список ожидания. Так мы видим, кто регистрируется, кто приглашает друзей, кто на самом деле проверяет приложение и выясняет, как все это работает, и мы используем всю эту информацию, чтобы предсказать, кто будет хорошим пользователем в системе.

Алгоритмы других приложений могут, возможно, поощрять расизм, потому что «цветных» пользователей чаще всего свайпают влево, а затем опускают в рейтинге.

– Мы делаем то, что называется двойными предпочтениями. Я всегда использую рост в качестве примера, допустим, что есть шестифутовая женщина и пятифутовый мужчина. Пятифутовый мужчина может встречаться с женщиной любого роста, а шестифутовая женщина – только с мужчинами ростом 5’10" и выше. Мы не покажем шестифутовую женщину пятифутовому мужчине, даже если она соответствует его предпочтениям.

Мы стараемся учесть предпочтения обоих людей и показываем вам только тех, с кем у вас действительно хорошие шансы на совпадение, тогда как многие другие приложения просто покажут вам всех, и вы будете постоянно свайпать влево.

Вы отфильтровываете людей, но в то же время нет бизнес-стимула привлечь больше пользователей. Почему?

– На любом рынке вам нужен «запас». Вы всегда хотите увеличить этот пул кандидатов. Мы действительно стараемся помочь людям подготовить свои профили, поэтому стало меньше «О, вы отклонены. Вы приняты». Это больше похоже на: «Эти люди, очевидно, приняты, потому что они составили действительно хорошую заявку».

Мы не эксклюзивны, мы просто разборчивы в том, кого мы выбираем, а тех, чью заявку отклоняем, стараемся «подтянуть». В наших же интересах

помочь довести их профиль до минимального уровня качества, прежде чем показывать его другим.

Если заявку отклоняют в The League, как пользователь узнает об этом?

– Мы никого не «отвергаем». Просто держим пользователя в списке ожидания, пытаемся побудить внести некоторые изменения в свой профиль. Это также зависит от спроса/предложения. Смотрим на динамику рынка. Допустим, многие люди ищут определенного типа парня, а затем он попадает в список ожидания. Потом мы внезапно привлекаем больше людей, и тогда он становится более востребованным.

Наш показатель приемлемости колеблется от 20 до 30 % в зависимости от города, а затем от людей, которые не получают эти первоначальные 20 или 30 %, многие пользователи не возвращаются и не вносят изменения.

(вгору)

Додаток 3

13.01.2019

Twitter годами фиксировал точные GPS-координаты пользователей

С помощью этих данных можно определить место их проживания и те места, которые они чаще всего посещали (InternetUA).

Международная группа исследователей разработала инструмент, который способен в течение нескольких минут с 92,5 % точностью определить, где живёт человек, используя данные Twitter. С его помощью также можно узнать, где пользователь работает, а также проводит своё свободное время.

Инструмент под названием LPAuditor (Location Privacy Auditor) использует особенности работы функции геолокации в Twitter, позволяющей пользователям указывать в твитах своё местонахождение.

Как выяснилось, в течение нескольких лет после запуска этой функции в 2009 году даже при указании такой широкой категории, как город, Twitter автоматически фиксировал точные GPS-координаты пользователя. Эти данные не видели ни автор поста, ни его подписчики, но они включались в метаданные твита и всё ещё доступны через API Twitter.

Автоматическая передача координат происходила с 2009 по апрель 2015 года. Затем сервис микроблогов изменил свою политику, и теперь пользователи должны дать согласие на передачу их координат. По словам представителя Twitter, на сегодняшний день это делает лишь очень небольшой процент людей. Однако те данные, которые были собраны раньше, по-прежнему доступны через API.

При этом в компании заявили, что отправка геолокационных данных в Twitter всегда была добровольным делом, и у пользователей всегда была возможность удалить эти данные в настройках. Однако ею пользовались немногие.

«Если вы не знаете о проблеме, вы не будете удалять эти данные», – ответил на это исследователь из Иллинойского университета Джейсон Полакис (Jason Polakis).

Исследователи начали извлечение метаданных Twitter через API компании в ноябре 2016 года. Ранее они провели исследование, которое показало возможность получения конфиденциальной информации из твитов с геометками. Теперь они хотели узнать, могут ли они получать эти данные в более широком масштабе и с большей точностью, используя автоматизацию.

В ходе работы специалисты с помощью LPAuditor проанализировали выборку из 15 млн геотаргетированных твитов от примерно 87 тысяч пользователей. Инструмент присвоил каждому твиту место на карте и определил его временной пояс. В результате был сгенерирован кластер твитов на карте с указанием мест, которые пользователь посещал чаще всего – по крайней мере, на момент публикации твитов.

Чтобы определить место проживания пользователя, исследователи анализировали те места, где он проводил больше всего времени на выходных.

Для верификации полученных с помощью инструмента данных исследователи определили группу из примерно 2000 человек и вручную проверили все их твиты, чтобы найти те фразы, которые могли подтверждать нахождение человека дома или на работе, а также соответствующий контекст.

Затем они сравнили местоположение этих твитов с результатами, полученными с помощью инструмента, и пришли к выводу, что точность его работы составляет 92,5 %.

По большей части это исследование было основано на твитах, отправленных до изменения политики Twitter в апреле 2015 года. После обновления получение таких данных стало затруднительным.

Однако исследователи считают, что только изменения политики сервиса недостаточно, ведь через API Twitter собранные ранее данные по-прежнему доступны. И хотя эта информация может быть устаревшей, она всё равно может представлять собой ценность для злоумышленников.

(вгору)

Додаток 4

15.01.2019

Михаил Сапитон

Что тестирует Twitter: цветные твиты, отказ от лайков и новые статусы

Twitter объявил о запуске публичной программы тестирования. В ее рамках несколько тысяч пользователей получат ранний доступ к экспериментальным функциям и смогут повлиять на планы компании по их запуску (AIN.UA).

Журналисты TechCrunch пообщались с директором Twitter по продуктовой разработке и рассказали о ключевых отличиях бета-версии

мобильного приложения соцсети. Редакция AIN.UA приводит сокращенный перевод материала.

В чем особенность новой программы тестирования

У Twitter уже работает программа тестирования под названием Experiments Program. Новый набор пользователей будет отличаться – участников не заставят подписывать NDA. Им разрешат публично обсуждать новые функции. Но количество тестеров ограничат – компания планирует набрать всего несколько тысяч человек.

Кроме того, в отличие от традиционных бета-программ, на тест сообществу будут отдавать не практически готовые к релизу функции, а те, что находятся на раннем этапе разработки. Создатели обещают прислушиваться к отзывам, менять или даже отказываться от функциональности.

Участникам новой программы потребуется установить отдельное приложение. В первой версии упор сделают на редизайне обсуждений.

Вот какие изменения журналисты заметили при первом знакомстве с бета-версией.

Алгоритмическая сортировка ответов

Сейчас отмечать интересные сообщения в длинных Twitter-обсуждениях неудобно. Пользователям приходится «лайкать» сообщения, к которым они собираются вернуться позже или проверять секцию «Твиты и ответы» в профиле топик-стартера.

Twitter хочет облегчить чтение длинных обсуждений. Сейчас соцсеть сначала отображает ответы тех, на кого вы уже подписаны. В будущем наверх могут выносить и другие твиты, которые алгоритм посчитает релевантными. Таким образом, два человека, одновременно читающие одно обсуждение, увидят разные версии. Но в Twitter обещают сохранить возможность хронологического показа.

Отсутствие лайков и других иконок

Чтобы сэкономить место в обсуждениях, Twitter тестирует отказ от лайков и других индикаторов вовлечения. Эта информация все еще будет доступна по тапу на интересующий ответ.

Цветовая индикация ответов

В Twitter хотят сделать акцент на твитах от знакомых вам пользователей. Для этого тестируют использовании цветовой индикации. Выделять будут:

- сообщения от топик-стартера;
- ответы от пользователей, на которых вы подписаны;
- ответы от пользователей, на которых вы не подписаны.

В рамках бета-теста Twitter использует яркий оттенки – в релизном варианте яркость намерены приглушить.

Live-статусы

В Twitter могут заимствовать активные статусы, как в Facebook. В них можно указать, где вы находитесь или чем занимаетесь во время написания твита.

С помощью этой функции компания намерена упростить набор новых пользователей – сейчас им сложно закрепиться на платформе без сформированного круга общения. Статусы, к примеру, помогут объединить незнакомых людей на одном мероприятии.

(вгору)

Додаток 5

15.01.2019

Ирина Фоменко

Сотрудники Google будут протестовать против IT-гигантов в соцсетях

15 января группа сотрудников Google в Instagram и Twitter начнет протестовать, оказывая давление на технические компании, чтобы они изменили свою практику, связанную с притеснением на работе в технологической отрасли. Об этом сообщает Recode (InternetUA).

Кампания направлена на освещение проблем с предприятиями, использующими соглашения о принудительном арбитраже, что является общим условием в трудовых договорах, которое лишает сотрудников права привлекать своих нанимателей к суду по вопросам, связанным с работой.

Исследования показали, что работники реже выигрывают у работодателей в арбитражных разбирательствах, а не через судебную систему. И даже при выигрыше в арбитраже они, как правило, получают меньше денег, чем в судебном процессе.

Кампания является еще одним примером растущего движения сотрудников IT-компаний, публично критикующих общеотраслевую практику, которая, по их словам, ведет к неравенству на рабочем месте. Сторонники кампании утверждают, что прекращение принудительного арбитража является ключевым шагом к созданию более справедливой культуры на работе.

15 января с 9 до 18 часов по восточному времени группа планирует еженедельно публиковать в Twitter факты о принудительном арбитраже, а также отзывы сотрудников и интервью с экспертами каждые полчаса в Instagram.

В ноябре 20000 сотрудников Google уволились с работы в знак протеста против сексуальных домогательств на работе, указав в качестве основного требования прекращение принудительного арбитража. Вскоре после этого Google пообещал изменить политику применения этой практики в случаях сексуальных домогательств и нападений. Несколько других крупных технологических компаний последовали примеру Google.

Однако лидеры движения считают, что они не достигли поставленной цели, поскольку по-прежнему существует принудительный арбитраж по другим типам преследований и дискриминации на рабочем месте, которые не носят сексуального характера. Многие крупные технологические компании

продолжают требовать, чтобы сотрудники отказывались от своих прав на коллективный иск.

Группа, организующая кампанию, изучила контракты около 30 технологических компаний и 10 крупнейших HR-предприятий. Так, ни одна IT-фирма не выполнила свои обязательства по защите прав сотрудников в случаях судебных исков против компаний в связи с проблемами на рабочем месте.

(вгору)

Додаток 6

4.01.2019

Facebook заполучила Nestle в клиенты корпоративной платформы Workplace

Компания Facebook объявила, что крупнейший глобальный бренд продуктов питания и напитков, Nestle, стал корпоративным клиентом её коммуникационной платформы для бизнеса, Workplace. Эта сделка позволит расширить пользовательскую базу Workplace сотнями тысяч служащих Nestle. За предыдущие месяцы компания уже подключила к этому сервису 210 тыс. сотрудников и планирует добавить к ним многие тысячи в течение 2019 г (Компьютерное Обозрение).

«Эффект ощутился незамедлительно с 25-кратным увеличением активности на один пост и очень высокими уровнями задействования мобильных технологий, – написала Кэтрин Флинн (Catherine Flynn), глобальный директор по маркетингу Workplace в Facebook, в блоге, анонсирующем сделку. – Менеджеры используют Live-видео для прямой связи с сотрудниками в разных местах, а отделы продаж используют Workplace для ежедневных проверок, для обмена информацией и передовым опытом».

Инструмент потоковой видеосвязи Live – это одна из нескольких возможностей, которые сервис Workplace унаследовал от соцсети Facebook, и которые выгодно отличают его от более популярных альтернатив, и прежде всего от Slack.

Facebook утверждает, что людям практически не нужно учиться пользованию Workplace, так как интерфейс у него его тот же, что и у самой известной социальной сети. Благодаря этому крупным компаниям проще внедрять его в глобальных масштабах.

Привлечение Nestle стало крупным успехом корпоративного направления бизнеса Facebook: в ноябре 2017 г., когда компания в последний раз публиковала статистику использования Workplace, сеть имела всего 30 тыс. клиентов.

Для сравнения, Slack в мае сообщила о более 8 млн активных пользователей своего сервиса в день, относящихся к 500 тыс. организаций. Примерно 3 млн этих клиентов имели платную подписку. Конкурирующая платформа Microsoft, Teams, была запущена через несколько месяцев после Workplace, тем не менее, в сентябре она имела 329 тыс. клиентов.

Помимо Nestle, список известных брендов, выбравших Workplace, включает Walmart, Domino’s Pizza, Booking.com и Spotify.

(вгору)

Додаток 7

4.01.2019
Цукерберг исследует человеческий мозг

Чтение личной переписки пользователей Facebook – не единственная забава Цукерберга. Сегодня он вкладывает деньги в гаджет для чтения мыслей стоимостью $5 млрд (Телекритика).

Марк Цукерберг и его жена Присцилла Чан продали около 30 миллионов акций Facebook, чтобы профинансировать амбициозный биомедицинский исследовательский проект под названием «Инициатива Чан-Цукерберга» (CZI). Цель проекта – протестировать имплантационные мозговые устройства в рамках кампании по искоренению болезней. Об этом сообщает Business Insider.

Один из аспектов работы CZI включает в себя разработку интерфейса «мозг-машина», который сможет переводить мысли в команды. Это беспроводной имплантат главного мозга, который может записывать, стимулировать и координировать движения примата в режиме реального времени. Ученые называют такое внедрение «терапией», так как оно предназначено для лечения таких заболеваний, как эпилепсия или болезнь Паркинсона, путем прерывания приступа или другого разрушительного движения.

Редакция научного журнала Nature сообщила, что такое устройство уже разработано и имплантировано в мозг примата. «Наше устройство способно контролировать мозг примата, поэтому вы точно знаете, что происходит», – комментирует Рикки Мюллер (Rikki Muller), соавтор CZ Biohub (некоммерческая медицинская исследовательская группа, связанная с CZI), профессор информатики и инженерии Калифорнийского Университета в Беркли.

«Применение интерфейсов “мозг-машина” имеет перспективное будущее: в то время, как некоторые исследователи сконцентрированы на их использовании, чтобы помочь людям с травмами спинного мозга или другими заболеваниями, влияющими на движение, мы хотим, чтобы это взаимодействие напоминало работу с ноутбуками и смартфонами», – добавляет Мюллер.

Подразделение Facebook, которое ранее называлось Building 8 и компания Илона Маска Neuralink также работают над подобными исследованиями.

В своем докладе Рикки Мюллер и ее научные сотрудники подробно описали устройство Cortera и принцип его работы. К макушке головы обезьяны прикрепляется беспроводное устройство размером с ладонь, подключенное к мозгу животного. Гаджет записывает, стимулирует и изменяет поведение обезьяны в то время, как она перемещает курсор к точке на экране с помощью джойстика, который необходимо удерживать в течение некоторого времени.

Современные устройства для одновременного фиксирования и прерывания действий имеют 128 электродов и проводников, что, примерно, в 31 раз больше, чем в современных компьютерных устройствах. Устройства ж для исследования человеческого мозга ограничиваются 4-8 электродами. По словам Мюллер, Cortera может «чувствовать», когда примат собирается сдвинуть джойстик и остановить это движение целевым электрическим сигналом, посланным в правую часть его мозга.

«Мы хотим, чтобы люди делали невероятные вещи, то, что другие даже не осмелились бы попробовать», – отмечает Джо ДеРизи (Joe DeRizi), сопрезидент CZ Biohub и провессор биофизики Калифорнийского Университета Сан-Франциско.

(вгору)

Додаток 8

14.01.2019

Дурова предупредили, что при ликвидации Telegram Messenger LLP права и имущество отойдут Великобритании

Британский государственный реестр юридических лиц предупредил Павла Дурова, что в случае ликвидации Telegram Messenger LLP, её права и имущества перейдут Великобритании. Это произойдёт в течение двух месяцев после одобрения заявки о ликвидации компании. Об этом сообщило РБК, заявление также появилось на сайте Британского реестра (InternetUA).

Регистр компаний уведомляет, что если причина (ликвидации) не указана в стране, то по истечении двух месяцев с даты, указанной выше, Telegram Messenger LLP будет снят с учёта, а товарищество с ограниченной ответственностью распущено.

После роспуска всё имущество и права, которыми наделено или находится в доверительном управлении LLP, считаются бесхозяйным имуществом и, соответственно, принадлежат короне. Из заявления Британского реестра к Telegram Messenger LLP

10 января СМИ узнали, что Дуров подал заявление о ликвидации Telegram Messenger LLP. Как отметили эксперты, это не повлияет на блокировку мессенджера в России: скорее всего, глава компании сделал это, так как Великобритания вскоре покинет Евросоюз.

Что это значит

На Telegram LLP пока зарегистрированы приложение Telegram X для iOS и классическое приложение Telegram для Windows Phone. Издателем приложения Telegram для iOS значится Telegram LLC, а для Android – Telegram FZ-LLC. Дуров и его брат Николай владеют зарегистрированными на Британских Виргинских островах компаниями Telegram Group Inc. и TON Issuer Inc.

Telegram LLP создана как товарищество с ограниченной ответственностью (Limited Liability Partnerships). Согласно британскому закону,

в случае ликвидации компании имущество и права становятся бесхозяйными, то есть переходят в пользование государством. По нему же компания не имеет права подавать заявление о вычеркивании из реестра, если за последние три месяца осуществляла предпринимательскую деятельность.

Кроме того, процедура ликвидации не является заменой официальной процедуры банкротства, поэтому LLP не может быть вычеркнута из реестра, если в отношении неё осуществляются (или могут начаться) процедуры банкротства. Если LLP было вычеркнуто, у кредиторов и других лиц сохраняется право требовать восстановления партнёрства в реестре.

(вгору)

Додаток 9

11.01.2019

Сколько времени на самом деле ребенку можно играть с гаджетами?

Новые рекомендации британского Королевского колледжа педиатриии и детского здоровья противоречат общепринятой точке зрения (InternetUA).

Новый отчет Королевского колледжа педиатрии и детского здоровья (RCPCH) не содержит рекомендаций по использованию гаджетов с четкими временными рамками (скажем, не более 2 часов в день). Также там сказано, что нет прямых свидетельств о плохом влиянии гаджетов на детское здоровье.

В отчете говорится, что невозможно рекомендовать какие-то конкретные временные ограничения в зависимости от возраста. Но рекомендуется избегать использования гаджетов за час до сна, чтобы улучшить сон. Также в докладе подчеркнута важность физических упражнений, общения с семьей и друзьями – все это, как и сон, ни в коем случае не должно заменяться игрой с гаджетами.

На сегодняшний день считается, что усиленное использование гаджетов детьми связано с ожирением, психическими проблемами, сердечными заболеваниями и низким уровнем образования, но «доказательная база для прямого «токсического» эффекта гаджетов слишком слабая», — говорится в отчете.

Рассел Виннер, профессор Института детского здоровья UCL в Лондоне, говорит: «Мы должны признать, что гаджеты повсеместно распространены в современном мире. Мы не можем загнать джинна обратно в бутылку».

В отчете содержится призыв более внимательно изучить влияние гаджетов и Интернета (в частности, социальных сетей) на здоровье детей, поскольку в данный момент выводы делаются на основании слишком расплывчатых данных и не учитываются многие дополнительные факторы.

Мнение RCPCH расходится с рядом рекомендаций, выпущенных ранее другими организациями и экспертами. Например, в 2016 году Американской академией педиатрии (AAP) рекомендовано ограничивать время перед экраном в зависимости от возраста ребенка: до 18 месяцев – никаких гаджетов, от 2 до 5 лет – не более часа в день, в дальнейшем родители могут решать сами, сколько

времени их чадо может провести перед экраном компьютера, планшета или телефона.

Исследование, проведенное в 2018 году, показало, что если детям ограничивают время перед экраном до двух часов в день, при этом они достаточно спят и двигаются, это приводит к улучшению познавательных способностей.

Однако RCPCH в своем докладе подчеркивает, что предыдущие исследования основаны прежде всего на исключение всякого риска и не учитывают потенциальные преимущества использования гажетов в образовании.

(вгору)

Додаток 10

16.01.2019

Ні небезпечним пранкам та приниженню дітей: як YouTube змінив правила публікації відео

YouTube оновив призначені для користувача правила. Тепер на відеохостингу заборонено публікувати ролики із небезпечними челенджами і пранками, під час виконання яких люди отримують або можуть отримати травми (Еспресо).

Про це йдеться в офіційному повідомленні компанії.

15 січня адміністрація YouTube повідомила про зміни в основних правилах для користувачів. Тепер сервіс забороняє публікувати челенджі (виклики), в яких присутній ризик смерті або учасники можуть отримати серйозні травми. Правило також стосується пранків (розіграшів), де герої впевнені, що знаходяться в небезпечній ситуації. У приклад наведено ситуації про вторгнення в будинок і «проїзд поруч».

«Ми відновили наші зовнішні рекомендації, щоб стало ясно – на YouTube немає місця для Tide Pod Challenge або Fire Challenge, які можуть привести до отримання серйозних травм або смерті», – коментує ком'юніті-менеджер YouTube.

YouTube посилив модерацію зовнішніх посилань, опублікованих в описі до відео або історій. Тепер заборонені прямі посилання на порнографію, шкідливі програми або спам. За порушення правила користувач отримає страйк: три таких протягом 90 днів приведуть до видалення облікового запису.

Адміністрація сервісу також заборонила ставити на мініатюри зображення, що містять сцени насильства чи порнографії. Навіть якщо саме відео чи не порушує правила платформи – користувач отримає попередження.

Окремо в правилах з'явився пункт про важкі емоційні переживання у дітей: тепер на відеохостингу не можна публікувати ролики із «розіграшами», де дітям повідомляють про смерть батьків або ж публічно принижують за помилки.

Нагадаємо, нещодавно надихнувшись фільмом від Netflix «Пташиний короб», користувачі соцмереж почали намагатися виконувати повсякденні справи з зав'язаними очима. Відеоблогер Джейк Пол опублікував ролик, де їде за кермом автомобіля із зав'язаними очима. Через кілька днів відео видалили. До цього 17-річна американка потрапила в аварію через сліпе водіння заради участі в челленджі.

(вгору)

Додаток 11

16.01.2019

8 вещей, которые психологи советуют не размещать в соцсетях

Социальные сети оказывают сильное воздействие на нашу повседневную жизнь, и зачастую далеко не в лучшую сторону (InternetUA).

И хотя это, вне всяких сомнений, крайне полезный способ взаимодействия с людьми, с которыми вы просто не можете видеться каждый день, соцсети также могут крайне вредоносно воздействовать на наши жизни, если мы будем недостаточно осторожны.

Да, я понимаю, что вы можете быть настолько довольны вашей жизнью, что вам постоянно хочется поделиться своею радостью со всем миром в Instagram, но есть определенные вещи, которым не стоит оказываться в общем доступе. Никогда.

Вот, что об этом говорят эксперты в области личных отношений:

1. Ваша сексуальная жизнь должна быть личной, не выставляйте ее на всеобщее обозрение.

То, что происходит за закрытыми дверями вашей спальни между вами и вашим партнером, касается только вас двоих. Сочные подробности вашей интимной жизни ни при каких обстоятельствах не должны попадать в ленту новостей в Instagram.

Разговоры о сексе допустимы разве что в общении с самыми близкими друзьями, да и то в исключительных случаях. Во всех же остальных обстоятельствах помните – это совершенно не касается окружающих.

2. Не выкладывайте в интернет личную информацию, касающуюся вашего партнера.

Ваш партнер и вы – не единое целое, даже если в своих мыслях вы друг друга не разделяете. Вы вполне можете выкладывать в социальные сети свои селфи и рассказывать, как вас растрогала недавно вышедшая мелодрама, искренне считая, что в этом нет ничего дурного. Но ваш партнер может вовсе не разделять вашего взгляда на это, так что ни за что и никогда не выкладывайте в сеть без его разрешения любую информацию, которую можно считать личной. Некоторые люди предпочитают, чтобы их личная жизнь оставалась как можно более личной. Уважайте их предпочтения.

Клинический сексолог и эксперт по личным отношениям доктор Дон Майкл пишет об этом следующее: «Если вы хотите, то, конечно, можете

выкладывать в интернет личную информацию, но не делайте того же с личной информацией вашей второй половинки, так как это является вторжением в их личное пространство».

3. Вы вовсе не обязаны оповещать о своих ссорах весь мир.

Пожалуй, это один из самых важных пунктов. Вы никогда и ни за что не должны позволять себе оповещать о ваших ссорах весь интернет. Ваши разногласия и проблемы личного характера должны разрешаться между вами двумя.

Поделиться в социальной сети подобной информацией – все равно что пригласить в свой дом и спальню толпу совершенно незнакомых людей, разрешив им комментировать все, что они увидят.

4. Личные фото вашего партнера без его разрешения не должны уходить в сеть.

Фотографии вашего партнера, которые лично вы считаете забавными, милыми и смешными – настолько, что вам захочется поделиться ими со всем миром – могут показаться вашему партнеру слишком личными или даже оскорбительными.

Не выкладывайте в интернет фотографии вашего партнера, если только у вас нет на это его четкого и недвусмысленного разрешения. Поверьте, никто не хочет, пролистывая новостную ленту социальной сети, наткнуться на фото, на которой он пускает слюни на подушку во время сна. Лучше наступите на горло своей песне.

5. Не подшучивайте над вашим партнером в сети.

Понимаете… дело в том, что тон и смысл вашего сообщения вовсе не обязательно будет воспринят вашими читателями (и вашим партнером!) так, как вы надеялись. Да, с глазу на глаз вы можете доброжелательно посмеиваться над недостатками вашего партнера, использовать шутки «ниже пояса». Это не будет сочтено оскорбительным, так как он знает, что вы думаете о нем на самом деле, да и тон вашей речи будет четко говорить о том, что это шутка.

Но вот социальные сети… Обезличенная шутка, переведенная в текстовый формат, может превратиться из доброжелательного сарказма в злобный и оскорбительный удар в самое больное место.

Как считает Аарон Андерсон, семейный психолог: «Когда вы выкладываете ошибки и оплошности вашего партнера в социальные сети, учтите, что там они оказываются вырванными из контекста, и вы не можете ограничить круг людей, которые их увидят».

6. Воздержитесь от пассивно-агрессивных комментариев о вашем партнере в интернете.

Если в вашем партнере вас что-то не устраивает, лучшее, что вы можете сделать – это поговорить с ним на эту тему и совместно найти решение проблемы, если она действительно существует. Если же вы поделитесь этим в социальных сетях, вы не только не решите проблему, но и подольете бензина в огонь.

Не давайте никому влезать в проблемы ваших отношений, и побольше общайтесь с вашим партнером – желательно, лично и с глазу на глаз.

7. Хватит стремиться к чужому вниманию и одобрению с помощью сомнительных сообщений.

Да, все мы любим видеть обновления статуса наших друзей и новые сообщения от них. Но есть люди, которые видят в этом чуть ли не смысл своей жизни. Они настолько «подсели» на свои учетные записи в социальных сетях, что их мысли практически полностью занимает вопрос, сколько раз просмотрели или «лайкнули» их сообщения. Почему? Да потому что чем больше эти показатели и чем больше людей на них подписалось, тем более «востребованными» они себя чувствуют.

Но как при всем этом найти время на своего партнера и личные отношения?

8. Хватит унижать себя, перемывая кости «бывшим» вашего партнера.

Неважно, насколько плохо закончились прошлые личные отношения вашего партнера, и насколько сильно вам хочется этим поделиться, воздержитесь от этого. Пусть эти грязные тайны останутся там, где им место – в небытии. Сделайте это из уважения к своему партнеру, да и к себе тоже.

Эксперт по личным отношениям Нили Штейнберг считает: «Хотя у вас может возникнуть большой соблазн написать несколько едких комментариев в адрес «бывших» вашего партнера – особенно если он или она лезет в ваши отношения – но когда вы жалуетесь на это в социальных сетях, это выглядит жалко».

Хватит унижать себя рассказами на Facebook о том, какой этот человек плохой. Все, кого это касается, включая вашего партнера и его «бывшего», и так об этом знают. Лучше поговорите с ним о том, что вас беспокоит, и добейтесь разрешения смущающей и беспокоящей вас ситуации.

Будьте благодарны за то, что ваш партнер выбрал именно вас… и отпустите прошлое.

(вгору)

Додаток 12

3.01.2019

Ирина Фоменко

Через ваш аккаунт в Twitter могут распространять исламистскую пропаганду

Хакеры взламывают и используют бездействующие аккаунты Twitter для распространения террористической пропаганды. Об этом сообщает TechCrunch (InternetUA).

Твиты с измененным стилем написания или языком говорят о взломанном аккаунте – иногда достаточно даже одной публикации на арабском языке, восхваляющей Аллаха, или ретвит такой пропаганды.

Хакеры взломали неподтвержденные по электронной почте учетные записи. Адреса электронной почты, использовавшиеся для создания аккаунта, либо уже не существуют, либо ими давно не пользуются. Таким образом, многие старые аккаунты можно легко взломать через создание нового почтового ящика.

«Эта проблема была известна давно, но никто не воспользовался ею. Теперь у нас есть сторонники Исламского государства, которые это выяснили», – заявил хакер и исследователь безопасности, известный как WauchulaGhost. – «Адрес электронной почты легко определить – обычно это логин пользователя с @hotmail.com или @yahoo.com. У некоторых учетных записей были десятки тысяч подписчиков».

Большинство взломанных аккаунтов имели публикации с видео на арабском языке боевиков Исламского государства с оружием. В других твитах – просто текст, также на арабском языке, восхваляющий насилие, или просто ретвиты подобных постов.

В одном твите использовался хештег Исламского государства: «…со своими машинами, собирайте чемоданы, бомбите, делайте это любым путем». Другой аккаунт призывал мусульман «убивать этих христиан везде, где бы вы ни были, найдите их». Еще один твит сообщал о превращении рождественских праздников в «горе и ужас».

«Повторное использование адресов электронной почты таким образом не является новой проблемой для Twitter или других онлайн-сервисов. Со своей стороны, наши команды осведомлены и работают над поиском решений, которые могут помочь обеспечить безопасность учетных записей», – заявил представитель Twitter.

(вгору)

Додаток 13

2.01.2019
Соцмережі розчиняють науку та перетворюють її на «клікбейт»
Євген Корольов

Сьогодні соцмережі є головним джерелом інформації у світі – майже 28 % користувачів отримують свіжі відомості саме звідти, а 23 % дізнаються там «гарячі» новини раніше, ніж ті з’являться в офіційних каналах. Це потужні інструменти, які, на відміну від традиційних медіа, не мають проміжної ланки – редакторів та журналістів. Що породжує одну з головних проблем соцмереж – фейкові новини. І дуже часто такими неправдивими матеріалами є публікації про різноманітні наукові відкриття та факти, в яких головне завдання – не донести правду, а розчинити справжню науку до рівня «клікбейту» – гучного заголовка, на який «клюне» читач (techtoday).

Наукові новини дуже складно передавати звичайним людям. Труднощі відчувають навіть традиційні ЗМІ, які часто не повністю передають усі

особливості наукового дослідження, неправильно тлумачать його результати та акцентують увагу не на тому, про що розповідають вчені.

Потрапляючи в соцмережі, ці вже спотворені публікації починають ще більше деформуватися, втрачаючи важливі факти на користь кричущого заголовка та утримання уваги читачів.

Розчинення науки в «клікбейтних» постах соцмереж не є просто прикрою ознакою сучасності. Це явище несе безпосередню загрозу кожному. Учені лабораторії Emerging Media Studies Університету Бостона дослідили, як соціальні медіа спотворюють інформацію про стійкість мікробів до антимікробних засобів. Виявилося, що користувачі соцмереж отримували з цих медіа таку інформацію, яка призводила до неправильного використання антибіотиків. Останнє веде до зростання стійкості мікробів – це актуальна проблема, а від таких супербактерій уже гинуть люди.

Дослідження показує, що головним критерієм віри в написаний пост є його автор. Читачі швидше сприймуть його як правдивий, якщо вони отримають його від друзів чи близьких членів родини.

Ще однією проблемою постів у соцмережах є надмірне спрощення задля більшої привабливості посту. При цьому правдиві факти та історії про наукове дослідження зводять до такого стану, що пост втрачає правдивість. З подібними публікаціями зустрічався кожен: «червоне вино дорівнює годині в спортзалі», «поїдання шоколаду дозволяє скидати вагу» тощо.

Ще одним загрозливим фактором розчинення науки в «клікбейтних» постах є відсутність ввічливості. Причому написані на мобільних гаджетах коментарі несуть більше грубості, ніж відправлені з інших девайсів. Неприємний тренд, зважаючи, що інтернет стає дедалі більш мобільним, а ПК перетворюється на нішевий інструмент.

Відсутність ввічливості призводить до поляризації думок, особливо в галузі усвідомлення ризиків тих чи інших наукових відкриттів. Також це спонукає деяких користувачів мовчати, щоб не вплутуватися в брудні віртуальні суперечки.

Разом усі перераховані фактори виявляється дуже складно побороти, навіть якщо вчені безпосередньо та активно беруть участь в обговоренні в соцмережах.

(вгору)

Додаток 14

16.01.2019

Facebook ужесточает правила размещения политической рекламы для Украины

Компания Facebook расширит некоторые из своих правил политической рекламы и инструменты для сдерживания вмешательства в выборы на Украину, Индию, Нигерию и Европейский Союз (InternetUA).

Изменения в Facebook должны ввести до выборов в этих странах. Ранее компания усилила контроль над политической рекламой на своей площадке.

Сообщают, что в Нигерии на этой неделе только рекламодатели, которые находятся непосредственно в стране, смогут запускать политическую рекламу по выборам.

Такие же правила будут введены в Украине в феврале, заявили в Facebook. Президентские выборы в Нигерии пройдут 16 февраля, в Украине президентские выборы назначены на 31 марта.

В Индии, которая проголосует за парламент этой весной, Facebook разместит предвыборную рекламу в онлайновой библиотеке с возможностью поиска, начиная со следующего месяца, сказал Роб Лезерн, директор по управлению продуктами Facebook.

Индийский архив будет содержать контактную информацию некоторых покупателей рекламы или их официальные документы. Для тех, кто покупает политическую рекламу, Facebook заявил, что их имя будет соответствовать выданным правительством документам.

«Мы учимся в каждой стране», – сказал Лезерн. «Мы знаем, что мы не будем совершенны, но наша цель – это постоянное улучшение», – добавил представитель Facebook.

Facebook считает, что хранение рекламы в библиотеке в течение семи лет является ключевым элементом борьбы с попытками повлиять на выборы. Такая библиотека будет напоминать архивы, введенные в США, Бразилии и Великобритании в прошлом году.

По словам Лезерна, Евросоюз получит версию этой системы разрешений и прозрачности в преддверии парламентских выборов в мае.

Новая политика прозрачности Facebook вызвала одобрение и критику. К примеру, не все эксперты довольны тем, что Facebook позволяет рекламодателям в США скрывать свою личность.

(вгору)

Додаток 15

4.01.2019

Свыше 5 млн. пользователей Google Play установили в декабре ПО с рекламными троянцами

Компания «Доктор Веб» представила обзор вирусной активности для мобильных устройств в декабре 2018 г. В начале декабря вирусные аналитики исследовали банковского троянца Android.BankBot.495.origin, атаковавшего клиентов бразильских кредитных учреждений. Эта вредоносная программа пыталась получить доступ к специальным возможностям (Accessibility Service) ОС Android, с использованием которых она самостоятельно управляла банковскими программами, считывала содержимое их окон и передавала злоумышленникам конфиденциальную информацию. Кроме того, Android.BankBot.495.origin показывал фишинговые окна поверх приложений и

обманом получал от жертв пароли, логины, данные банковских карт и другие секретные сведения (Компьютерное Обозрение).

В течение месяца в Google Play было выявлено множество вредоносных и нежелательных программ. Среди них – рекламные троянцы Android.HiddenAds.343.origin и Android.HiddenAds.847, распространявшиеся под видом игр и полезных приложений. После запуска они скрывали свой значок с главного экрана и начинали показывать рекламу.

Также были выявлены программы со встроенными нежелательными модулями Adware.Patacore и Adware.HiddenAds. Они демонстрировали рекламу даже тогда, когда содержащее их ПО не было запущено. В общей сложности такие программы установили свыше 5300000 пользователей.

Злоумышленники вновь распространяли мошеннические приложения. В вирусную базу Dr.Web были добавлены записи для детектирования троянцев Android.FakeApp.149, Android.FakeApp.151 и Android.FakeApp.152. Эти вредоносные программы загружали веб-страницы, на которых потенциальным жертвам предлагалось за вознаграждение ответить на вопросы. Для получения «оплаты» от пользователя требовалось выполнить проверочный платеж, однако после перевода средств киберпреступникам владельцы зараженных устройств не получали ничего.

Кроме того, вирусные аналитики обнаружили троянца Android.Proxy.4.origin, которого вирусописатели использовали для перенаправления трафика через смартфоны и планшеты их владельцев. Android.Proxy.4.origin скрывался в безобидных на первый взгляд играх.

Среди выявленных в декабре потенциально опасных программ оказалась новая версия коммерческого шпиона Program.Spyzie.1.origin, который позволяет следить за пользователями Android-устройств. Он перехватывает содержимое SMS и сообщений электронной почты, отслеживает телефонные звонки, историю посещений веб-браузера, координаты зараженного смартфона или планшета, получает доступ к переписке в популярных программах для онлайн-общения, а также крадет другую информацию.

(вгору)

Додаток 16

6.01.2019

Шахраї придумали нову аферу з номерами телефонів та соцмережами

На ваш номер за декілька днів надходять десятки дзвінків із різних номерів. Нібито звертаються за неіснуючим оголошенням або просто «помиляються». Комусь ви передзвонюєте, якісь дзвінки залишаються без відповіді. А через декілька годин ваша сім-картка заблокована, акаунти в соціальних мережах зламані, а з банківського рахунку зникли всі гроші (BusinessUA).

Про нову схему шахрайства розповіли в прес-службі поліції. Зловмисники телефонують оператору, називають номер телефону «жертви» і

кажуть, що втратили телефон із карткою. Називають співробітнику компанії останні контакти. Після цього ваш номер опиняється «в руках» злочинців. За його допомогою можуть зламати пошту, акаунти в соціальних мережах і навіть банківський рахунок.

Як крадуть номери українців і чим це загрожує.

Продаю номери. Дешево

Зателефонувавши в службу таксі, залишивши свій номер телефону у відкритій формі на будь-якому із сайтів, ви ризикуєте потрапити у бази даних шахраїв. Згодом ці списки продають по 2-20 коп. за номер. Бази продаються в інтернеті. Телефони «Нової пошти», великих банків, служби таксі – всі вони потрапляють на «відкритий ринок». Офіційно кожна зі згаданих компаній декларує: номери зберігають, як зіницю ока, а інформація захищена. Насправді ж уся інформація продається.

Покупців таких баз умовно можна поділити на дві групи. Перша – маркетологи. Вони займаються СМС-розсилками. У таких СМС найчастіше інформують про акції, розіграші, спеціальні пропозиції. Якщо магазин, який проводить розіграш, розташований у Києві, за 5 коп. можна купити тисячі номерів жителів столиці.

Друга група – ті, хто використовує інформацію для більшої наживи. Шахраї, які телефонують вам із інформацією про «блокування рахунку», або переконують, що ваш родич порушив закон і потрібно заплатити хабар, також найчастіше черпають інформацію із відкритих джерел. Один із способів шахрайства детальніше розглянемо в цьому матеріалі.

Завдання шахрая, який купив ваш номер телефону – домогтися вашого дзвінка. Якщо співробітник мобільного оператора, перед відновленням номера телефону, запитає, куди ви телефонували, шахрай із легкістю зможе назвати його. Але тільки за умови, що ви «клюнули» на вудку і передзвонили.

Журналісти задля експерименту спробували відновити випадковий номер телефону Vodafone. Оператор поставила нам три запитання: два номери, на які ви найчастіше дзвонили, сума останнього поповнення, сума на рахунку. Пройти перевірку не вдалося. Правда, варто враховувати, що номери, з якими найчастіше спілкується клієнт втраченого номера, ми назвали практично випадково. Якщо шахрай телефонував вам із завидною регулярністю і приблизно назве суму на вашому рахунку, цілком можливо, що «відновити» номер телефону йому вдасться.

Крім того, враховуючи, що в поліції заявляють про почастішання подібних випадків, це більш ніж імовірно. Мешканка Дніпра Юлія Устименко розповідає: після того, як вона залишала свій номер телефону в оголошеннях на сайті OLX, їй почали приходити СМС із підозрілим вмістом, проте дівчина на них не відповідала.

«Я помітила, якщо довго не продавати, а потім розмістити свій номер, приходить СМС: “Ви виграли – передзвоніть”, або “Ваш номер може бути заблокований – передзвоніть”. Я не знаю, з якою метою, ніколи не

передзвонювала. Можливо, що найлегше просто скопіювати номер телефону з OLX і продати комусь за ці 5-20 коп.», – розповіла OBOZREVATEL дівчина.

До речі, якщо перейти на контракт, то відновити картку шахраям буде не так легко. Знадобляться дані паспорта. Також якщо ви вже відновлювали свою карту, в відділенні залишаються ваші дані, які не зможуть підтвердити шахраї.

Як не потрапити на гачок

Експерт у сфері кібербезпеки Максі Очкун радить: щоб не попастися на гачок шахраїв, необхідно завести окремий «фінансовий номер». До нього варто прикріпити банківську карту і акаунти в найважливіших соціальних мережах. Наприклад, якщо ви активно розвиваєте свій Instagram, до «фінансового номеру» також можна прикріпити цей акаунт.

Водночас «звичайний» номер телефону можна залишати колегам, друзям і клієнтам. Якщо ж використовувати один номер, цілком можливо, що в якийсь момент вам зателефонують шахраї.

Як захистити себе від шахраїв:

– Не передзвонювати, якщо вам телефонували з незнайомих номерів;

– Завести окремий «фінансовий» номер для банку і важливих соціальних мереж;

– Про підозрілі СМС одразу повідомляти своєму оператору для того, щоб ваш номер без вашого відома не «відновлювали».

«Якщо послухати операторів, зараз номери так захищені, що взагалі нереально їх зламати. Але ми задля експерименту пробували із декількома колегами. Зламати номер простіше, ніж дістати пошту з поштової скриньки сусіда. Те, що точно можу стверджувати: складно зламати той номер телефону, який мало хто знає. Тому, якщо ви дійсно цінуєте його, то не роздавайте усім підряд свої персональні дані», – радить Максим Очкун.

(вгору)

Додаток 17

8.01.2019

Новая атака через побочный канал опасна для любого ПК с Windows и Linux

В работе, опубликованной 7 января на сервере arXiv, пять специалистов в информатике и компьютерной безопасности описали новую атаку по побочным каналам (Side-Channel Attack, SCA), эффективную против операционных систем, таких как Windows и Linux, а возможно и macOS (она выходила за рамки данного исследования) (Компьютерное Обозрение).

От известных прежде SCA эта отличается тем, что не использует конструкционные недостатки микропроцессоров и других компонентов компьютера, то есть, сохраняет действенность независимо от аппаратного обеспечения ПК.

Целью новой атаки являются «страничные кэши», часть памяти, куда операционная система загружает код (исполняемые файлы, библиотеки и

пользовательские данные), необходимый одному или нескольким открытым приложениям. Такие кэши организованы чисто программным способом и управляются на уровне операционной системы. Это отличает их от классической аппаратной кэш-памяти, применяемой вместе с центральным процессором для ускорения вычислений.

«Некоторые из этих (страничных) кэшей имеют очень специфические сценарии использования, например, кэш браузера, хранящий содержимое веб-сайта; другие являются более универсальными, например страничный кэш, в котором размещается большая часть используемых кода и данных», – поясняют исследователи в своей статье.

Описываемая атака работает, взламывая механизмы ОС, с помощью которых разработчик или приложение проверяет наличие страницы памяти в страничном кэше. В Linux эту функцию выполняет системный вызов mincore, а в Windows – QueryWorkingSetEx.

После этого, с помощью запущенного в системе вредоносного процесса, исследователи создавали вытесняющие состояния, которые высвобождают старые страницы памяти из кэша страниц ОС. При записи высвобожденных данных на диск система страничных кэшей генерирует различные ошибки, а также загружает в кэш новые страницы. Авторы утверждают, что анализируя эту активность, можно определить содержимое страничного кэша, даже если оно использовалось другими процессами/приложениями.

Большинство SCA работают очень медленно и поэтому представляют главным образом теоретический интерес, однако новый метод позволяет извлекать большие объёмы данных за один раз, что делает его оптимальным для использования в реальной обстановке.

Авторы пишут, что их побочная атака «обеспечивает непривилегированный мониторинг некоторых обращений к памяти других процессов с пространственным разрешением 4 кБ и временным разрешением 2 мкс в Linux (ограничено 6,7 измерениями в секунду) и 466 нс в Windows (ограничено 223 измерениями в секунду)».

Эта атака позволяет обходить «песочницы» систем безопасности. Она также может быть адаптирована к сценарию удалённого применения, но в этом случае утрачивает аппаратную независимость.

Microsoft уже закрыла эту уязвимость в сборке для Windows Insiders, ведётся и активная работа над соответствующим патчем для Linux.

«Мы не проверяли macOS, – сообщил в электронном письме один из исследователей этой проблемы, Дэниел Грусс (Daniel Gruss). – Но, конечно же, раз они используют страничный кеш, то также будут уязвимы…».

(вгору)

Додаток 18

8.01.2019

Google Chrome для Android стал оружием в руках злоумышленников

Google Chrome для Android в течение длительного времени мог быть причиной утечки приватной информации о пользователях, выяснили исследователи в области информационной безопасности компании Nightwatch. Как оказалось, веб-браузер раскрывал данные о модели устройства, версии операционной системы, а также предоставлял сторонним приложениям сводку об установленных обновлениях безопасности. Таким образом создавался риск нарушения конфиденциальности, а также заражения вредоносным ПО (InternetUA).

Сведения, которыми Google Chrome делился со сторонними приложениями, представляли серьезную опасность для безопасности пользователей и работоспособности их устройств. Обладая данными о текущей версии прошивки, на базе которой работает аппарат, злоумышленники могли эксплуатировать уязвимости, устанавливать слежку за пользователями и действиями, которые они совершали со своим устройств. Как следствие – украденные пароли от учетных записей и отсутствие средств на банковских счетах.

По словам Джейкоба Шафрановича, исследователя компании Nightwatch, уязвимость, о которой идет речь, существует в Google Chrome с 2015 года. Несмотря на то, что эксперты неоднократно информировали Google о данной бреши, разработчики поискового гиганта не спешили устранять ее, предложив исправление только сейчас. Впрочем, даже текущая версия апдейта с баг-фиксом оказалось полумерой, поскольку запретила браузеру делиться информацией только о прошивке, но не о модели устройства.

Ранее в Google Chrome появилась функция сокращения URL-адресов. Несмотря на стремление Google сделать серфинг удобнее, эксперты нашли нововведение чрезвычайно опасным для рядовых пользователей. Оказалось, что, используя функцию сокращения, состоящей в удалении из адреса дополнительных букв и символов, злоумышленники могли бы подменять легитимные веб-сайты фишинговыми, чтобы таким образом получать учетные данные от банковских аккаунтов и т. п.

(вгору)

Додаток 19

8.01.2019

Ирина Фоменко

Google Play опять «грузит» пользователей Android вредоносным софтом

В Google Play в очередной раз обнаружили вредоносные приложения. Об этом сообщает TechCrunch (InternetUA).

Исследователи из Trend Micro обнаружили десятки приложений, популярные утилиты и игры, у которых есть масса обманчиво отображаемой рекламы (чтобы выжать как можно больше денег из ничего не подозревающих пользователей Android), в том числе – полноэкранной, скрытой и фоновой.

Так, 85 приложений «продвигают» рекламное ПО, что в общей сложности затрагивает не менее 9 миллионов пользователей.

У одного универсального телевизионного приложения для Android было более пяти миллионов пользователей, несмотря на множество негативных отзывов и жалоб на «скрытую рекламу и объявления в фоновом режиме». Другие пользователи заявили, что «было так много рекламы, что они даже не могли его использовать».

Исследователи протестировали все приложения и обнаружили, что большинство из них используют один и тот же или похожий код, и часто имеют одинаковые названия. При каждом клике приложение будет показывать рекламу – таким образом приложение генерирует деньги для разработчика.

Приложения с рекламным ПО могут и не выглядеть, как программы с вредоносным ПО или скрытыми функциями (устанавливающими данные с другого сервера после установки). Заработок на мошеннической рекламе может достигать до нескольких тысяч долларов еженедельно.

Некоторые объявления могут содержать скрытый код, который пытается обманом заставить пользователей установить вредоносное ПО на свои телефоны или компьютеры. Некоторые из них: A/C Air Conditioner Remote, Police Chase Extreme City 3D Game, Easy Universal TV Remote, Garage Door Remote Control, Prado Parking City 3D Game.

Несмотря на все усилия Google по сканированию приложений до того, как они появятся в Google Play, вредоносные программы представляют собой одну из самых больших и распространенных угроз для пользователей Android. Google только за последний год удалил из Google Play более 700000 вредоносных приложений и постарался улучшить свой бекенд, чтобы в первую очередь предотвратить появление вредоносных приложений в Google Play.

Тем не менее, поисковый и мобильный гигант продолжает борьбу с мошенническими и вредоносными приложениями, допустив появление в Google Play по меньшей мере 13 вредоносных программ только в ноябре.

(вгору)

Додаток 20

9.01.2019

Експертка з інформаційної безпеки: Додати друга у соцмережі – все одно, що пустити незнайомця додому

Катерина Баркалова

Чого не можна робити в мережі, чим небезпечні фейки про маніяків, що викрадають дітей та чому тест «Який ти сир?» потрібно оминати десятою дорогою (vn.depo.ua).

Війна з Росією триває п’ятий рік, але інформаційна війна розпочалася значно раніше. Про те, які форми вона набуває, як уберегти свої персональні дані та нервову систему від ворожих агентів і звичайних шахраїв, Depo.Вінниця

розповіла координаторка проекту «Вижити в мережі. Інформаційна безпека в час гібридної війни» Лариса Полулях.

Як гадаєте, скільки десятиліть тому мав місце початок інформаційної війни проти України?

– Напевне, гібридна війна проти України розпочалася ще задовго до розвалу Радянського Союзу. Згадайте радянські фільми: якщо боєць говорить українською, це означає, що він падлюка й десь має стати зрадником. Наших східних сусідів і так від слова «Бандера» завжди тіпало, і тому мода створювати відповідний образ українця існувала давно.

Перша помітна інформаційна атака мала місце у період Помаранчевої революції. Яких тем найбільше стосувалися маніпуляції?

– «Ющенко – американський шпигун» (це почалося ще до Помаранчевого Майдана), «Україна – Схід та Захід», був навіть безумний ролик, у якому йшлося, що помаранчевий колір є неприродним і погано впливає на психіку. Тобто були маніпуляції, спрямовані на розкол України на Схід та Захід, на агентів Держдепу та гарних прихильників Кремля.

Чи розвивалась така активність після Ющенка?

– Був період затишшя. А потім, коли вже починався Майдан, я побачила на сторінці свого приятеля з Луганської області, абсолютно нормальної та поміркованої людини, дуже багато перепостів російських пропагандистів на кшталт Дугіна. Я почала дивитися в інших українських користувачів, своїх та його друзів, і побачила, що ці перепости з'явилися й там. Коли вже почався Євромайдан, цей мій знайомий почав робити великі скріни про «наколоті апельсини» та тому подібне. Я пропонувала йому купити квиток, приїхати до Києва та побачити все на власні очі, але моя пропозиція викликала у нього дику лють. Це був абсолютний блок: «Ні, ви там людей їсте».

Що Ви побачили з початком війни?

– Сучасна війна досить гібридна і впливати на людей можна не лише зброєю, а й формуючи їхню думку. Дуже яскравий приклад – події 7 травня 2014 року, коли Вінницю охопила паніка у зв'язку із захопленням, яке ніби має відбутися. Того дня я написала багато дурнуватих постів про ніби то захоплення Вінниці, багато людей їх перепостило і всі ми думали, що ця паніка – жарт. Але коли ми з колегами з інших міст України звірили карти, виявилося, що в багатьох із них розганялась аналогічна інформація: до Харкова їде група диверсантів на катамаранах, у Чернівцях теж щось подібне. Мабуть, то був пробний шар, аби з'ясувати, наскільки ми піддаємось паніці, перевірка на істеричність.

Наскільки Вінниця пройшла цю перевірку?

– Нормально. Ніхто нікого не вбив, ніхто не кинувся скуповувати продукти. Вінничани просто посміялися над цим. Але іноді хочеться якихось безпекових заходів, щоб люди знали, чого не можна робити в мережі, аби не потрапити у неприємну ситуацію. Адже ми часто легковажимо, не усвідомлюючи небезпеку, на яку наражаємося.

Чого конкретно не можна робити в мережі?

– Наприклад, є тести «Який ти сир» чи «Яка ти принцеса». Сайт, який пропонує їх, одразу попереджає, що ми погоджуємося на скачування своїх персональних даних.

Але люди чомусь все одно натискають та з'ясовують, який вони сир чи принцеса…

– Тому що цю небезпеку не можна помацати руками. Хоча ця дія одного порядку з передачею комусь ключів від власної квартири або пін-коду від своєї карти. Бо персональні дані – це й номер телефона, який прив'язаний до Фейсбука та банківської картки або електронних скриньок, це контакти твого оточення, це й твоя родина, якщо вона є на Фейсбуці, наприклад, діти або чоловік, який наразі проходить військову службу. І виходить, що, клацнувши раз, ти здаєш всіх. І коли кажуть: «Я не носій державної таємниці» – так, але ти носій своєї банківської картки, ти носій паніки або недостовірної інформації, яку можеш розповсюдити.

Так само ми вчиняємо, коли необачно набираємо собі друзів у Фейсбук. Є, наприклад, сторінка екскурсовода Вінницького краєзнавчого музею, яку активно додавали й вінницькі журналісти, й вінницькі активісти. Але якщо ви зателефонуєте до краєзнавчого музею, ви дізнаєтесь, що там немає посади екскурсовода, вже не кажучи про те, що ця пані там не працює. А додати друга у соцмережі – це все одно, що запросити незнайому людину до себе додому. А потім ця людина скаже, що твою дитину викрали або у воді завівся якийсь хробак. І тебе охоплює паніка.

Хто є найбільш вразливим, коли йдеться про інформаційну небезпеку?

– Згадайте квітень-травень, коли мережею поширилася інформація про маніяка-педофіла. Ми відслідковували батьківські групи у Фейсбуці, які постили його фото, яке виявилося фотографією Захара Прилепіна. Так, вони казали: «Попереджений – значить озброєний». Але таким чином створюється та сама паніка, нервозність та істерія. Ми знайшли сторінку пані, яка почала поширювати цей фейк, вона виявилася випускницею однієї з вінницьких шкіл. Але інші випускники її не знали, а її Фейсбук-друзі не знали її в реалі. Але при цьому були багатотисячні перепости.

Але діти та їхня небезпека – це дуже болюча тема для всіх батьків…

– Ми не кажемо дитині про завідомо безпечні речі, що вони несуть загрозу. І це відповідальність батьків та взагалі будь-якої дорослої людини – не створювати небезпеку там, де її реально немає. Тому що коли з'явиться реальна загроза, ми на неї можемо не зреагувати. Це як у казці про хлопчика, який постійно кричав «Вовк!».

Чи можна сказати, що це і є основна мета створення паніки?

– Можливо. Це створення втоми для людей, які постійно живуть у стресі й потім вже не помічають, що несе реальну небезпеку. Вони закручують у цей вир і себе, й своїх близьких, а потім будь-яка інформація сприймається як негативна та тривожна. Таких людей легше підбурити на будь-що або, навпаки, увігнати в депресію.

Що потрібно зробити, аби люди, перш ніж панікувати, почали «вмикати мізки»?

– Спасіння потопаючих – справа рук самих потопаючих. Так само, як ми маємо самі дбати про свої зуби, ми маємо дбати про інформаційну гігієну. І аби не підхопити той інформаційний «трипер», потрібно дотримуватися правил поводження у мережі: не додавати у друзі незнайомців, перевіряти інформацію перш ніж поширити її, не давати геолокацію тощо. Одна моя знайома, чинна військовослужбовиця, переконувала, що це примарна небезпека. Але коли їй за два тижні змогли зробити висновок, у який час можна пограбувати її квартиру, у якій школі навчається її дитина, вона все зрозуміла. Ця інформація, яку ми самі про себе надаємо, нікуди не зникає. Тому й у результатах тестів, про які я говорила, все більше співпадінь. Одна пані виставила результат: «У тебе народиться хтось». А вона й справді вагітна. Хоча починалися усі ці тести із маркетингу. Інформація збиралася для того, аби запропонувати людині, що їй потрібно. Але чому б памперси, які створювалися для космонавтів, не використати для діточок? Чому б метод, який довів свою ефективність у маркетингу, не використати, наприклад, у політиці, під час виборів для промивки мізків?

До речі, про вибори. До чого в інформаційному плані нам варто бути готовими?

– Подивіться на досвід американських виборів. У дуже багатьох джерелах описано, як використовувалися соцмережі на користь того чи іншого кандидата, як використовували комерційні вподобання людей. Приблизно те ж саме буде у нас, тільки з розрахунку на наш менталітет. І будуть використовувати дуже адресний вплив. Коли у нас тільки оголосили воєнний стан, моя сестра, яка живе в Ізраїлі, надіслала мені абсолютно безглуздий російський текст, де фігурують назви російських служб, про те, що за нами будуть слідкувати так, що просто жах. Виявилось, це надіслала її подруга з Вінниці, яка зараз живе у Бєлгороді в Росії. Вона працює в інтернет-магазині, і це їй дали такий додатковий заробіток: надсилати інформацію своїм знайомим та друзям, яких вони добре знають, щоб попередити і зробити гарну справу. Щоправда, полінувались цей текст, який був згенерований десь у 2008 році, підправити для України. А люди не надто думають. Ну й що, що там написано «федеральний»? Головне, що будуть слухати твої телефони.

Це єдина новація?

– Є ще українські дівчата з Таїланду, які нещодавно наводнили мережі, «IloveUkraine». В українських віночках, щоправда, у павлово-посадських платках. Вже більше 200 аккаунтів з'явилося. Люди зайшли, подивилися, яка гарна дівчинка і клацнули – нехай у друзях буде. А не подивилися, що до оголошення воєнного стану у неї друзі були тільки в Таїланді чи Тайвані.

Така нерозбірливість у додаванні друзів онлайн – це від наївності та довірливості?

– Це називається «Поки грім не гряне». У нас п'ятий рік триває війна, а більшість ще не вміє надавати первинну медичну допомогу. В Ізраїлі кожна

дитина знає, що не можна підбирати іграшку, яка валяється на землі. У нас про це не знають навіть дорослі. Згадайте історію з гумовими каченятами, які розкидали у Вінниці і які люди збирали, бо халява. Так, ті іграшки не були небезпечними. Але, можливо, то був якийсь тест.

Звідки таке ігнорування потенційної небезпеки?

– Ми дуже інфантильні, навіть попри війну. І це питання до загальнодержавної політики та власної відповідальності. Як би держава не стукала тобі по голові та не нагадувала, що у нас війна, поки ти сам впевнишся, що тебе це не стосується, сенсу у цьому стуканні не буде. Можливо, це треба перерости й взяти відповідальність на себе. Так, у нас держава не ідеальна, та звинувачуючи її, ми забуваємо, що цей інформаційний «трипер» ми підхопили самі й не лікуємося.

(вгору)

Додаток 21

10.01.2019

Владимир Кондрашов

В Украине ищут интернет-мошенников, которые вымогали деньги от имени МВД Беларуси

Украинская полиция помогает правоохранителям Республики Беларусь в расследовании случая компьютерного саботажа. Интернет-злоумышленники вымогали деньги от имени Министерства внутренних дел Республики Беларусь за разблокировку браузера пользователя. Следы мошенников ведут в Украину (InternetUA).

Об этом пишет InternetUA со ссылкой на определение Суворовского районного суда города Одесса.

Речь идет о весьма популярном способе интернет-вымогательства – блокировке устройства от имени правоохранительных органов за якобы просмотр порнографии с дальнейшим вымогательством денег (якобы штрафа) за разблокировку.

Согласно материалам дела, 11 мая 2018 года неизвестное лицо «через глобальную сеть Интернет осуществило блокировку браузера «Google Chrome», установленного на мобильном устройстве «Xiaomi Redmi 4», который принадлежит жителю Беларуси: на экран его смартфона неустановленное лицо установило диалоговое окно с информацией от имени МВД Республики Беларусь о том, что пользователь посетил порнографические сайты и просмотрел соответствующие материалы, в связи с чем мобильный телефон заблокирован. Для разблокировки устройства мошенники требовали оплатить сумму 70 рублей (около 900 гривен) на электронный кошелек платежной системой «WebMoney».

Как выяснили белорусские правоохранители, электронный кошелек МВД Республики Беларусь зарегистрирован 24.10.2017 на гражданина Украины, а доступ к кошельку в разное время осуществлялся с технических устройств,

которым присваивались IP адреса, принадлежащие провайдерам Украины и, в частности, Одессы.

В Республике Беларусь уголовное производство открыто по признакам нарушения, предусмотренного частью 1 статьи 351 УК РБ («Компьютерный саботаж»). Санкция статьи предусматривает наказание в виде штрафа, или лишения права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от одного года до пяти лет.

(вгору)

Додаток 22

10.01.2019

В Сети выложен простой инструмент для преодоления двухфакторной защиты

Новое средство тестирования проникновения, опубликованное на GitHub в начале года, позволяет автоматизировать фишинговые атаки и даже преодолевать двухфакторную аутентификацию (2FA). Оно представляет собой так называемый обратный прокси-сервер, модифицированный для работы с трафиком для страниц входа и фишинговых операций (Компьютерное Обозрение).

Он располагается между пользователем и целевым веб-сайтом, например, Gmail, Yahoo! или ProtonMail. Жертва получает подлинный контент от подлинного сайта, однако весь трафик и все взаимодействия жертвы с сайтом проходят через сервер злоумышленников.

Обратный прокси регистрирует все вводимые пользователем пароли, а если конфигурация эккаунта предусматривает двухфакторную аутентификацию – то и токены 2FA. Владелец сервера может в реальном времени применять эти токены для загрузки в эккаунт жертвы и открытии новых законных сессий на защищённом сайте.

Польский разработчик этого инструмента, Пиотр Душински (Piotr Duszyński), считает, что появление подобного простого в использовании средства способно в корне изменить ситуацию в сфере сетевой безопасности. Доверие к двухфакторной аутентификации серьёзно пошатнулось в декабре прошлого года, когда организация Amnesty International опубликовала отчёт, показав в нем, что пользующиеся государственной поддержкой преступники уже начали применять фишинговые схемы, способные обходить 2FA.

Обратный прокси, получивший название Modlishka (по-польски – хищное насекомое богомол), может автоматизировать преодоление проверок 2FA, основанных на SMS и одноразовых кодах, однако неэффективен против схем U2F, предполагающих использование аппаратных ключей безопасности.

(вгору)

Додаток 23

10.01.2019

Пользователи обнаружили в инстаграме ссылки на детскую порнографию

Война хештегов развернулась между пользователями, которые распространяли ссылки на детскую порнографию, и подростками, намеренными это остановить (Главное).

В начале недели стало известно, что некоторые пользователи ставят определенные хештеги в инстаграме для поиска и обмена фотографиями несовершеннолетних. Об этом сообщает The Atlantic. Хештег #dropboxlinks был одним из самых популярных, хотя встречались и другие варианты – для тех, кто ищет мальчиков, геев или определенную возрастную группу. Все, что было нужно, – это отыскать хештеги. Затем беседа якобы переходила в личные сообщения, где пользователям присылали ссылки на папки Dropbox, содержащие незаконные изображения.

Вирусная кампания с мемами началась, когда 16-летний Джек под ником ZZtails загрузил видео на ютьюб, в котором рассказал об учетной записи с откровенными фотографиями детей. Джек обнаружил, что ее можно найти по хештегу #dropboxlinks. После этого он и другие подростки стали загружать мемы с таким хештегом, чтобы тем, кто ищет ссылки, было сложнее найти запрещенный контент. «Мои ровесники не должны видеть ничего, связанного с детской порнографией, даже людей, предлагающих продать ее, – говорит Джек. – Никто не должен иметь доступа к таким материалам».

Седьмого января, соцсеть удалила хештеги #dropboxlinks и #tradedropbox. «Безопасность детей и подростков очень важна для нас, – сказал представитель Instagram. – У нас запрещен контент, который подвергает опасности детей, поэтому мы заблокировали эти хештеги». Пресс-секретарь Dropbox также заявил в комментарии The Atlantic, что платформа уже сотрудничает с Instagram и другими сайтами, чтобы удалить такой контент как можно скорее.

(вгору)

Додаток 24

11.01.2019

Китайское приложение для смартфонов украло данные 10 миллионов пользователей со всего мира

Как стало известно, китайский производитель бытовой электроники TCL собирал данные с мобильных телефонов, не спрашивая разрешения пользователей. Получение информации производилось с помощью бесплатного приложения для смартфонов с прогнозом погоды, которое с момента его выпуска в декабре 2016 года было загружено пользователями со всего мира более 10 миллионов раз (InternetUA).

Компания TCL зарегистрирована на фондовых биржах Гонконга и Шэньчжэня. Это международный конгломерат по производству электроники,

продукция которого включает телевизоры, кондиционеры, стиральные машины, холодильники и мобильные телефоны.

Одним из ключевых предприятий холдинга TCL является компания TCL Communication Technology Holdings, которая производит интеллектуальные устройства и разрабатывает мобильные приложения. TCL Communication также владеет французским производителем телефонов Alcatel и канадским телефонным брендом Blackberry. В 2016 году её объём продаж составил 68,77 миллиона мобильных телефонов в 160 странах и регионах.

И вот, как сообщило 2 января издание Wall Street Journal, лондонское охранное предприятие Upstream Systems обнаружило, что погодное приложение TCL несанкционированно собирает пользовательские данные.

Приложение, о котором идёт речь, называется Weather Forecast – World Weather Accurate Radar («Прогноз погоды – всемирный точный метеорологический радар»). Разработано оно для системы Android от Google и доступно для бесплатной загрузки в Google Play. Приложение показывает прогноз погоды на 21 день, предоставляя оценки по конкретным параметрам, таким как влажность, скорость ветра и видимость.

По данным компании App Annie, которая занимается аналитикой и проводит маркетинговые исследования в области приложений для смартфонов, примерно в 30 странах, включая Великобританию и Канаду, продукт TCL принадлежит пятёрке лучших в своей сфере. В США он входит в топ-20.

Как удалось обнаружить Upstream Systems, приложение TCL собирает данные о географическом местоположении пользователей и об адресах электронной почты, а также о международном идентификаторе мобильного оборудования, уникальной метке, присваиваемой каждому аутентифицированному сотовому телефону. Полученная информация хранится на серверах TCL в Китае.

Кроме того, было замечено, что приложение погоды незаметно подключило платные сервисы пользователям недорогих смартфонов Alcatel в Бразилии, Малайзии, Нигерии и других развивающихся странах. Эта автоматическая подписка затронула 100 тысяч телефонов Alcatel и, не вскройся эта ситуация, совокупно обошлась бы их владельцам в 1,5 миллиона долларов.

После того, как Wall Street Journal отправил в TCL запросы, в ноябре прошедшего года компания обновила погодное приложение. На сегодняшний день, по данным Upstream, приложение прекратило автоматическую подписку пользователей, но сбор данных продолжается.

Китайские приложения могут представлять опасность

Надо отметить, это уже не первый случай, когда продукты TCL несут риск для пользователей.

В ноябре 2017 года Alcatel было обновлено приложение для редактирования фотографий под названием Gallery (позже переименованное в Candy Gallery), которое также можно загрузить в Google Play. В отличие от предыдущей версии, в которой запрашивалось разрешение на доступ только к файлам на смартфоне, обновленная версия стремится получить информацию об

идентификаторе устройства, подключении Wi-Fi, доступ к текстовым сообщениям SMS и другим данным, не связанным с редактированием фотографий.

В июне 2017 года беспокойство по поводу вопросов безопасности побудило американскую организацию Inseego расторгнуть соглашение о продаже TCL своей компании по разработке решений для мобильного интернета Novatel Wireless. Это произошло после того, как на сделку обратил внимание Комитет по иностранным инвестициям в США, межведомственная правительственная организация, которая рассматривает деловые соглашения на предмет потенциальных рисков национальной безопасности.

В декабре 2018 года Google приостановила использование двух китайских приложений для смартфонов после проведения внутреннего расследования. Согласно данным Wall Street Journal, эти приложения – CM File Manager от Cheetah Mobile Inc. и Keyboard от Kika Tech Inc. – предположительно использовали полученные от пользователей разрешения для построения мошеннической схемы, связанной с рекламой.

В декабре 2017 года издание Indian Times сообщило, что правительство Индии обратилось ко всем военным с просьбой удалить со своих смартфонов 42 китайских приложения, если они их ранее устанавливали. По данным индийских спецслужб, приложения, доступные для систем Android и iOS (iPhone), собирали пользовательские данные и отсылали их в Китай. Приложения также располагают потенциалом для проведения кибератак против индийцев.

(вгору)

Додаток 25

15.01.2019

Google избавила Google Play от сотни вредоносных программ для Android

За последние два месяца Google удалила из Google Play более сотни вредоносных и потенциально опасных приложений. Об этом рассказали официальные представители компании. Как показала практика, программные алгоритмы, анализирующие ПО, попадающее в каталоге, справляются далеко не всегда. Поэтому регулярные чистки – единственный способ избавить Google Play от злонамеренного программного обеспечения и тем самым обезопасить пользователей устройств под управлением Android (InternetUA).

«Несмотря на то, что большинство разработчиков заботятся о своей аудитории, некоторые злонамеренные создатели [ПО] все-таки пытаются обойти системы безопасности и проникнуть в Google Play, подвергая опасности многих людей и их устройства, – комментирует чистку представитель Google. – Причина, по которой разработчики вредоносного ПО стремятся в Google Play, состоит в колоссальной аудитории пользователей, которую охватывает каталог».

Google Play Protect

Несмотря на то, что Google Play все-таки нуждается в периодической чистке, Google регулярно совершенствует системы безопасности, стоящие на страже каталога. Только в 2017 году из магазина приложений за нарушение правил антивирус Google Play Protect удалил более 700 тысяч программ, часть из которых содержала вредоносный код, а часть оказывала негативное влияние на автономность и быстродействие инфицированных устройств.

Вредоносные приложения из Google Play

По статистике большинство потенциально опасных приложений, попадающих в Google Play, не содержат вредоносного кода. Как правило, они принадлежат к типу рекламных программ (adware), которые в фоновом режиме запускают браузер и занимаются тем, что переходят по ссылкам и кликают по баннерной рекламе, принося деньги своим создателям. Эти действия неизменно приводят к преждевременной разрядке зараженных смартфонов и планшетов и потере интернет-трафика.

(вгору)

Додаток 26

15.01.2019

Распространяемый через торренты поддельный видеофайл подменяет результаты поиска в Google

Распространяемое через The Pirate Bay и замаскированное под видеофайл вредоносное ПО заражает компьютеры под управлением Windows и выполняет ряд вредоносных функций. К примеру, вредонос способен внедрять подготовленный злоумышленником контент на такие популярные сайты, как Википедия, Google или Яндекс (InternetUA).

Киберпреступники часто распространяют вредоносное ПО через The Pirate Bay, однако в данном случае интерес вызывает необычный способ заражения компьютеров и большое разнообразие вредоносной активности.

Все началось с того, что исследователь безопасности 0xffff0800 скачал с The Pirate Bay фильм «Девушка, которая застряла в паутине». Однако вместо видеофайла он получил файл .LNK, выполнявший команды PowerShell.

Исследователя заинтересовала иконка файла, и он пропустил его через VirusTotal. Как показало сканирование, файл представлял собой вредоносное ПО CozyBear, используемое одноименной APT-группой, также известной как APT29 и CozyDuke. Тем не менее, этот результат оказался ошибочным. По словам Ника Каппа (Nick Carr) из FireEye Advanced Practices Team, вредоносные .LNK – частое явление в сфере интернет-пиратства.

0xffff0800 опубликовал скачанный файл .LNK, и как показал быстрый анализ Лоуренса Абрамса (Lawrence Abrams) из Bleeping Computer, он представляет собой нечто большее, чем просто инжектор рекламы для страницы поиска Google. Помимо внедрения контента на множество сайтов,

вредонос отслеживает страницы кошельков Bitcoin и Ethereum и заменяет их другими, принадлежащими киберпреступникам.

Чтобы проделать все вышеописанное, вредонос модифицирует ключи реестра для отключения Windows Defender. ПО также принудительно устанавливает в Firefox расширение Firefox Protection и взламывает расширение для Chrome под названием Chrome Media Router, заменяя ID на «pkedcjkdefgpdelpbcmbmeomcjbeemfm».

Сразу после запуска браузера вредоносное расширение подключается к базе данных Firebase и извлекает оттуда множество настроек, в том числе JavaScript-код для внедрения в различные web-страницы.

В страницу поисковой выдачи Google вредонос внедряет нужные злоумышленнику результаты поиска (к примеру, сайты, предлагающие подозрительное антивирусное ПО). То же самое происходит и с другими поисковиками. Например, на странице Википедии отображается поддельный баннер с просьбой оказать финансовую поддержку в виде криптовалюты.

(вгору)

Додаток 27

15.01.2019

«Умные» телевизоры дешевеют, продавая информацию о пользователях

Благодаря таким компаниям, как американская Vizio и китайская TCL, огромные телевизоры с тонкими рамками, отличным качеством изображения и встроенными службами потокового вещания стали доступны широким слоям населения. В сезон рождественских праздников в США были проданы миллионы телевизоров с поддержкой 4K и HDR. Стоимость такой модели, которая останется актуальной ещё много лет, с диагональю экрана 65" составляла порядка $500 (InternetUA).

Но такая низкая цена связана с оговоркой, на которую большинство людей не обращают внимания: некоторые производители собирают данные о пользователях, а затем продают их третьим сторонам. Они могут включать тип и время просматриваемой передачи, реакцию на рекламу, приблизительное местоположение и многое другое. В недавнем интервью The Verge с техническим директором Vizio Биллом Бакстером (Bill Baxter) прозвучало много любопытных подробностей.

Интерфейс платформы Roku на «умном» телевизоре TCL с видным расположением рекламы на домашнем экране

«Это беспощадная отрасль. Это отрасль с прибыльностью в 6 %. Но более эффективная стратегия заключается в том, что мне в действительности не нужно зарабатывать на самом телевизоре. Я должен лишь покрыть свои издержки», – пояснил господин Бакстер. Подобный подход можно наблюдать в продвижении популярных игровых консолей, владельцы экосистем которых готовы отдавать устройство по себестоимости, а порой и ниже. Это очень

удобно для потребителей, получающих столь передовое устройство дешевле и не предвидящих своих будущих расходов на игры. Но в широких масштабах – со стороны компаний – всё это поддаётся анализу и прогнозу.

Хотя TCL с Roku TV предлагает пользователям ограничить объём сбора данных, лимит устанавливает сам производитель

Vizio тоже готова продавать свои телевизоры без особой наценки, получая прибыль с помощью сбора данных, рекламы и продажи развлечений для потребителей. И к этим действиям пользователи уже не столь благожелательны. «Речь идет не только о сборе данных. Речь идет о монетизации ТВ после покупки. Вы продаете определённые фильмы, какие-то телевизионные шоу, некие рекламные объявления, знаете ли. На самом деле это не так уж и отличается от веб-сайта The Verge», – последовала ремарка от Билла Бакстера.

Именно эти дополнительные формы заработка помогают компаниям вроде Vizio и TCL делать большие, красивые и «умные» телевизоры такими доступными. По словам технического директора Vizio, без этого подхода потребителям придётся платить больше: «Мы бы взимали немного большую плату в рознице, чтобы компенсировать расходы».

(вгору)

Додаток 28

15.01.2019

США звинуватили українця у зламі бази даних Комісії з цінних паперів

США висунули звинувачення українському хакеру і ще кільком особам через проникнення в базу даних Комісії з цінних паперів і бірж США (SEC). Про це повідомляє Reuters, передає Європейська правда (Еспресо).

У вересні 2017 року Комісія заявила про виявлення зламу своєї корпоративної бази даних Edgar, яку використовують компанії, які керують капіталами.

Влада заявила, що 27-річний Олександр Єременко з Києва та інші його спільники отримали тисячі документів, в тому числі приблизно 157 оголошень про доходи, зламавши Edgar через литовський сервер, а потім поділилися ними з мережею трейдерів.

За даними SEC, ці трейдери, що складаються з восьми чоловік і компаній в США, Росії та Україні, потім отримали незаконний прибуток у розмірі понад $4,1 млн, торгуючи зламаною інформацією в період з травня по жовтень 2016 року.

В обвинувальному акті з 16 пунктів, поданому до окружного суду США в Ньюарку, штат Нью-Джерсі, Міністерство юстиції США звинуватило Єременка та Артема Радченка, ще одного українського громадянина, який, за його словами, залучав трейдерів до незаконної діяльності, в комп'ютерному шахрайстві та інших злочинах.

SEC подала відповідні цивільні обвинувачення проти Єременка і ще восьми підозрюваних.

Згідно з судовими документами, Єременко знаходиться на волі з моменту пред'явлення йому в 2015 році кримінального звинувачення в крадіжці понад 150000 закритих корпоративних прес-релізів від дистриб'юторів Business Wire, Marketwired і PR Newswire.

(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.