СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(28.08–12.09)

2017 № 15

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(28.08–12.09)
№ 15

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 2017

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

28.08.2017
YouTube запускает раздел со «Срочными новостями»

YouTube уже давно перестал быть простым «хранилищем видео». Сегодня эта платформа воспринимается как эффективный способ продвижения, современный «телевизор» и место работы тысяч блоггеров. Но Google хочет большего (InternetUA).

Разработчики занялись тестирование нового раздела «Срочные новости», который будет перекликаться с «Рекомендованными видео». Вместо отображение видеороликов, соответствующих интересам конкретного пользователя, в «Срочные новости» будут попадать видео, связанные с актуальными новостями из мира политики, технологий, медицины и т.д.

Представители Google пока не раскрывают алгоритм подбора новостей — делается ли это вручную или компания использует специальные рейтинги. Неясно, станет ли раздел постоянным, либо его активация будет связана лишь с выходом «громких» новостей.

***

29.08.2017
Приложение Facebook Messenger Lite скачали более 50 млн раз

В октябре прошлого года компания Facebook выпустила приложение Facebook Messenger Lite, которое является уменьшенной версией оригинального Messenger с ограниченной функциональностью (InternetUA).

Приложение Facebook Messenger Lite предназначено для старых смартфонов, работающих под управлением ОС Android 2.3 Gingerbread (и более новых версий), а также для регионов с низкой скоростью подключения к сети Интернет.

Согласно последним данным, приложение Messenger Lite App уже скачано более 50 млн раз. Несмотря на популярность приложения, компания не планирует позиционировать его как альтернативу полноценному Messenger в развитых странах.

***

28.08.2017
Топ-10 приложений, без которых миллениалы не могут жить

Более трети пользователей в возрасте от 18 до 34 лет не могут жить без Amazon. Такие выводы нового исследования comScore. Gmail и Facebook заняли второе и третье место.

Докладніше

***

30.08.2017

Skype представил функцию «Интервью» для технических работников. Там можно писать и проверять код

Дмитрий Демченко

Skype представил функцию «Интервью». С ее помощью рекрутеры могут проводить технические интервью и проверять навыки программирования кандидатов, не покидая пределы сервиса.

Докладніше

***

30.08.2017

YouTube запустил новый дизайн для десктопов и новые функции для мобильных

Ольга Карпенко

Популярный видеосервис YouTube 29 августа выкатил большое обновление своей десктоп-версии, а также представил ряд новых функций для мобильного приложения.

Докладніше

***

31.08.2017

Эпоха квадратных снимков в Instagram окончательно ушла в прошлое

В феврале этого года обновление Instagram позволило пользователям публиковать до 10 фотографий и видеозаписей в одной публикации, но лишь в квадратных пропорциях. Теперь это ограничение снято (IGate).

Новое обновление открывает путь для фото и видео в различных пропорциях, однако внутри публикации весь материал будет одинаков. Загрузив видео в 16:9, последующие снимки тоже будут иметь это соотношение сторон.

В обновлении улучшили и интерфейс приложения: он стал просторнее, шрифт – тоньше и изящнее, а меню выбора аккаунта переехало в нижнюю часть экрана. А вот фильтры, отображаемые теперь с эффектом размытия, смотрятся спорно. Обновление будет распространяться волнами и уже в ближайшие дни станет доступно всем пользователям социальной сети.

***

1.09.2017

Instagram Stories запускают в мобильной веб-версии
Павел Красномовец

Instagram обновил веб-версию приложения, добавив формат Stories, скопированный у Snapchat. Начиная с 1 сентября и в ближайшие недели в мобильной браузере можно будет только смотреть истории друзей. Но в течение нескольких месяцев в мобильной веб-версии станет доступна и загрузка своих Stories (AIN).

Как и в приложении, «Истории» в браузере находятся наверху страницы. Чтобы просмотреть историю, нужно на нее кликнуть, а затем навигация осуществляется кликам по боковым стрелкам.

Социальная сеть Facebook скопировал у Snapchat много функций, но реализация Stories именно в Instagram показала лучшие результаты. К годовщине запуска формата в начале августа «Истории» достигли показателя в 250 млн пользователей в день. У Snapchat же всего 173 млн активных дневных пользователей.

***

5.09.2017

Сооснователь украинской соцсети Ukrainians сообщила о закрытии проекта

Дмитрий Демченко

Украинская социальная сеть Ukrainians прекращает работу. Об этом сообщила ее сооснователь Александра Струмчинская на своей странице в Facebook (AIN).

«Меня поставили перед фактом, что разработка украинской социальной сети прекращается. Мне очень жаль. И я откровенно прошу прощения и благодарю всех пользователей, которые вместе со мной искренне верили в реализацию и успех этого проекта», – заявила Струмчинская.

Она отметила, что ее голоса не хватило, чтобы самостоятельно продолжать реализацию проекта. Руководство компании StartupSoft, которая также является сооснователем соцсети и ее разработчиком, отказалось не только от самостоятельного развития проекта, но и от возможности передать его любой другой стороне, подчеркнула Струмчинская.

Украинская соцсеть Ukrainians была запущена в середине мая. На момент закрытия проекта в ней было зарегистрировано более 390 000 аккаунтов. Информации о том, насколько активными были эти пользователи, нет.

***

5.09.2017

В Telegram переработали систему ответов и добавили раздел с избранными стикерами

Мессенджер Telegram приобретает всё большую популярность, а вместе с этим обретает все большее количество возможностей.

Докладніше

***

6.09.2017

На YouTube можно будет стримить экран iPhone

Google анонсировала обновление сервиса YouTube Live. Теперь пользователи смогут стримить экран своего iOS-устройства. (IGate).

Пользователи смогут напрямую транслировать экран своего устройства на iOS. Также будет возможность записывать видео через фронтальную камеру и звук через микрофон, чтобы давать комментарии происходящему.

Google также поработала над модерированием комментариев в «живом» чате – стало проще скрывать сообщения и блокировать пользователей. Уменьшили и время задержки стрима, что поможет во взаимодействии со зрителями в режиме реального времени.

***

7.09.2017

Искусственный интеллект Facebook научится распознавать выражения лиц пользователей

Команда по разработке искусственного интеллекта Facebook решила научить ботов соцсети не только распознавать человеческую речь, но и выражения лиц пользователей. Согласно уведомлению разработчиков, они пытаются научить бота понимать мимику живых людей на примере записей разговоров по Skype.

Докладніше

***

7.09.2017

Facebook запустила тестирование комментариев с цветным фоном

Facebook тестирует функцию добавления цветного фона под текст комментария. Новую возможность заметил пользователь соцсети Эверт Грут (Evert Groot) (IGate).

Груту удалось оставить в Facebook комментарий с цветным фоном, соцсеть предложила на выбор несколько однотонных фонов и градиентов.

В декабре 2016 года Facebook разрешила пользователям добавлять цветной фон к текстовым публикациям без фото, видео или ссылок на посторонние сайты.

***

8.09.2017

Twitter добавил ночной режим в десктопную версию сервиса

Twitter объявил о запуске ночного режима (Night Mode) в десктопной версии сервиса. Ранее он был доступен только в приложениях для iOS и Android (IGate).

По словам представителя компании, большинство пользователей начали видеть новую опцию 6 сентября, остальные получат доступ к ней в ближайшие недели.

Чтобы включить ночной режим, нужно нажать на картинку профиля в правом верхнем углу экрана и в появившемся меню выбрать соответствующий пункт.

***

8.2017

Facebook почав тестувати сервіс для зустрічей

У месенджері Facebook з'явилася нова функція, яка дозволяє призначити зустріч з друзями користувача. Як відзначає Motherboard, інтерфейс нової функції дуже нагадує додаток для знайомств Tinder (ZN.UA).

Мобільний додаток Facebook надсилає користувачеві повідомлення про те, що він міг би зустрітися з кимось зі своїх друзів. При натисканні на посилання відкривається фотографія одного з друзів з питанням «чи хочете ви призначити зустріч на цьому тижні?». Якщо обидва користувача дадуть ствердну відповідь, додаток дозволить влаштувати зустріч, якщо ж один з них відмовиться, другий про це не дізнається.

Як зазначає видання, на даний момент функція проходить період бета-тестування і доступна користувачам у США та Канаді.

***

10.09.2017

Facebook вложит $1 млрд в производство собственных шоу в 2018 году // *Facebook делает ставку на собственный видеоконтент*

Facebook планирует потратить $1 млрд на создание собственного контента для собственной видеоплатформы Watch. Об этом пишет The Wall Street Journal (IGate).

Такое вложение станет для Facebook самой дорогой инвестицией в видеоконтент, уточняет Techcrunch.

Facebook представила платформу для просмотра видео Watch в августе 2017 года. Сервис позволяет подписываться на контент от других пользователей, искать ролики по категориям и загружать свои видео.

Свои шоу и трансляции на платформе запустят Major League Baseball, National Geographic, NASA, Billboard и другие компании. 5 сентября 2017 года сайт и приложения Watch стали доступны на территории США.

***

11.09.2017

«ВКонтакте» все еще пользуется популярностью среди пользователей Украины

Исследование, которое проводила компания Factum Group Ukraine в августе, показало, что сайт «ВКонтакте» – четвертый по популярности среди украинских пользователей, сообщает Интернет Ассоциация Украины. Первое место в рейтинге с большим отрывом занимают сайты Google, 68 % всех украинских пользователей интернета посещали в августе эти сайты. На втором месте с небольшим отрывом – Youtube. Замыкает тройку сайт facebook.com, который в августе посетила почти половина украинских пользователей – 49 %. Также в исследовании отмечается, что российский сайт mail.ru опустился с 10 на 11 место в рейтинге, поменявшись местами с сайтом sinoptik.ua. Это единственное изменение в ТОП-10 в августе по сравнению с июлем. В то же время, по данным другого исследования, которое провела компания Gemius, российская соцсеть «ВКонтакте «занимает пятое место среди самых популярных сайтов. При этом тройка лидеров в двух исследованиях совпадает, а вот на четвертом месте у Gemius расположился сайт Приватбанка. Согласно данным исследования Gemius, в августе 22,1 миллиона украинцев пользовались интернетом. В среднем за месяц пользователь тратит 25 часов своего времени на сеть (Marketing Media Review).

***

12.09.2017

Смогут ли украинские соцсети конкурировать с Facebook

Ukrainians, Nimses, а теперь еще Woolik и Psyball. Удастся ли им потеснить Facebook и Instagram? После блокировки российских «ВКонтакте» и «Одноклассники» в Украине появляются новые социальные сети.

Докладніше

***

12.09.2017

Разработчики Ukrainians объявили о создании новой соцсети

Она будет называться ЄСВОЄ. Как сообщает издание LIGA.net, часть команды разработчиков социальной сети Ukrainians, которая прекратила свое существование в начале сентября, объявила о создании новой соцсети ЄСВОЄ (Marketing Media Review).

Об этом сообщила соучредитель Александра Струмчинская в Facebook. В посте она пишет, что именно в Украине появился инновационный продукт, который они продемонстрируют всему миру: «Уже в сентябре начнет работу новая, инновационная социальная сеть ЄСВОЄ, которая объединит не только украинцев, а и граждан других государств».

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

1.09.2017

Этот день войдет в историю: соцсети бурно отреагировали на введение Украиной биометрического контроля для россиян

В сети бурно отреагировали на новость о том, что с 1 января 2018 года Украина будет проводить фиксацию биометрических данных всех россиян, пересекающих границы Украины (Апрострофф).

Об этом пишут пользователи Facebook.

«Да! Да! Да! Свершилось! Этот день войдет в учебники истории! Украина с 1 января 2018-го фактически разрывает соглашение о безвизовом режиме пересечения границы Украины гражданами России! Очередная историческая веха, равнозначная безвизовому режиму с Евросоюзом», – отмечает на своей странице журналист Юрий Бутусов.

***

6.09.2017

«За доступне розмитнення»: Соцмережі відреагували на акцію водіїв авто на єврономерах

У середу, 6 вересня, у центрі Києва проходила акція автовласників під назвою «За доступне розмитнення авто». Її учасники вимагаюли від депутатів Верховної Ради спростити реєстрацію в Україні транспортних засобів на іноземних номерах. Мітингувальники також готові були штурмувати Кабінет міністрів України.

На своїх сторінках в соціальних мережах українці висловили свою думку щодо цієї акції, а ми зібрали найцікавіші їх висловлювання (Народна правда).

***

5.09.2017

Капітуляція Путіна, акт перший: соцмережі відреагували на заяву про миротворців на Донбасі

У вівторок, 5 вересня, президент Російської Федерації Володимир Путін зробив несподівану заяву щодо введення на Донбас миротворчих військ Організації об'єднаних націй. Однак голова Кремля зазначив, що це має відбутися тільки на його умовах, тому доручив представникам МЗС РФ направити відповідний документ в Радбез ООН (World News).

В Україні різко відповіли на послання Путіна щодо миротворців. За словами першого першого віце-спікера Верховної Ради України Ірини Геращенко, Путін має намір спотворити ідею українського керівництва та перевернути все з ніг на голову, інформує видання «Народна Правда».

Українці в соціальних мережах також запідозрили недобре. Одні впевнені, що цим кроком президент РФ хоче підкреслити «громадянську війну» в Україні, а інші вважають, що Кремль хоче «офіційно» направити на Донбас ЗС РФ у вигляді миротворчих сил.

Окремі українці пропонують направити миротворців ООН на територію Російської Федерації, а також на анексований Кримський півострів.

***

11.09.2017

Це сором! Програли всі, – соцмережі про прорив Саакашвілі

Прорив 10 вересня українсько-польського кордону у пункті пропуску «Краковець» екс-президентом Грузії, екс-головою Одеської ОДА Міхеїлом Саакашвілі сколихнув соцмережі. Події стали приводом для створення фотожаб і колажів, які розлітаються інтернетом.

Докладніше

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

28.08.2017

Три месяца без «ВКонтакте»: выигравшие и проигравшие от бойкота российских соцсетей

Прошло три месяца с тех пор, как президент Петр Порошенко своим указом заблокировал ряд российских интернет-ресурсов, в число которых попали и популярные в Украине социальные сети «Одноклассники» и «ВКонтакте». Кто выиграл, а кто проиграл от социального бойкота?

Докладніше

***

30.08.2017

Франция и Германия хотят добиться более справедливых налогов от интернет-гигантов

Франция и Германия намерены подготовить совместный проект по налогообложению американских интернет-гигантов с тем, чтобы сделать более «справедливыми» выплаты таких компании, как Google, Apple, Facebook и Amazon – передает агентство France-Press со ссылкой на заявление министра финансов Франции Брюно Ле Мэра (Bruno Le Maire).

Докладніше

***

29.08.2017

Facebook объединяет подразделения по выпуску потребительской электроники

Facebook объединяет в одно подразделения, занимающиеся разработкой потребительской электроники. Созданную структуру возглавил исполнительный директор Facebook Эндрю Босуорт (Andrew Bosworth), сообщает издание Business Insider (InternetUA).

Компания объединила подразделения Oculus (создание шлемов виртуальной реальности) и лабораторию Building 8. Последняя специализируется на разработке потребительских гаджетов.

По данным Business Insider, в Building 8 сейчас разрабатывается домашний планшет под кодовым именем Aloha. Презентация продукта стоимостью 500 долларов намечена на май 2018 года, впрочем, планы еще могут измениться.

Дело в том, что Facebook все еще не определилась с тем, каким должно быть будущее устройство. Из-за скандалов, связанных с утечками конфиденциальных данных, компания думает над тем, чтобы позиционировать Aloha в качестве средства для пожилых людей, при помощи которого они без лишних проблем смогут связываться с родными и близкими, отмечает источник.

***

4.09.2017

Facebook вимагає у російської платіжної системи домен facebook.ru

Facebook Inc. вимагає передати їй безоплатно домен facebook.ru, який займає російська платіжна система «Золота корона». Про це пише видання «Коммерсант». (Espreso.tv).

Американська корпорація дала російській компанії термін до 30 вересня, щоб вирішити питання.

Нині з домену facebook.ru йде автоматична переадресація на сайт російської платіжної системи «Золота корона». Корпорація в своєму зверненні до платіжної системи зазначила, що Facebook Inc. була заснована в 2004 році, є власником однойменної соціальної мережі і правовласником товарного знака

facebook в різних написаннях. З листа випливає, що доменне ім'я facebook.ru відтворює зареєстрований товарний знак, що є неприйнятним для американської корпорації.

Керівництво Facebook посилається на ст. 1515 Цивільного кодексу Росії, яка передбачає накладення відповідальності за використання чужого товарного знаку та покарання у вигляді компенсації до 5 млн руб. або подвійної суми вартості ліцензії на товарний знак.

***

1.09.2017

Facebook оказывает большее влияние на покупки, чем Snapchat и Instagram.

Исследование CivicScience обнаружило, что реклама на таких платформах, как Facebook и Instagram слабо конвертирует пользователей в покупателей. (MMR - Marketing).

В опросе 1900 американских потребителей только 1 % респондентов в возрасте от 13 лет совершил покупку благодаря рекламе в Snapchat, и только 4 % купили что-то, увидев рекламу в Instagram. 45 % отметили, что никогда не совершали покупок после просмотра рекламы на социальных площадках, а более трети вообще не пользуется социальными медиа. Facebook оказался самой влиятельной сетью для совершения покупательского поведения: 16 % потребителей купили продукт, увидев рекламу в Facebook.

***

1.09.2017

Facebook отберет у You Tube часть рекламного «пирога»

Дмитрий Малышко

Новый сервис Watch от Facebook может отнять у You Tube большую аудиторию любителей он-лайн видео. Однако речь идет, прежде всего, о прибыли от рекламы.

Докладніше

***

2.09.2017

Facebook назвал 17 запрещенных рекламных форматов

В своем блоге компания объяснила, что этот шаг продиктован стремлением повысить ценность самых эффективных рекламных форматов и помочь рекламодателям найти решения для достижения целей. Новые правила вступят в силу с 15 сентября (InternetUA).

Среди запрещенной рекламы сообщения с поддержкой политиков, продвижение статуса о просмотре ТВ передачи, спортивного ивента и так далее:

– Поддержка шеринга продуктов из магазина
– Поддержка шеринга поста о продаже
– Поддержка чекинов на карте, в ресторане или в городе
– Поддержка шеринга заметки
– Поддержка шеринга опроса
– Поддержка рекомендации места
– Поддержка шеринга культурных моментов
– Поддержка шеринга комментариев
– Поддержка смены фото профиля
– Поддержка загрузки файла или шеринга
– Поддержка спортивного ивента
– Поддержка загруженного видео или фото с помощью камеры Facebook
– Поддержка посещения мероприятия
– Поддержка шеринга плейлиста
– Поддержка статуса просмотра ТВ-шоу, фильма или программы
– Поддержка поста из приложения, размещенного в ленте страницы
– Поддержка сообщений политиков

***

11.09.2017

YouTube запустил первую рекламную кампанию, чтобы вернуть бренды

Платформа создала серию роликов, чтобы проинформировать потенциальных рекламодателей о влиянии своей рекламной сети. Обо всех преимуществах платформы активность расскажет на YouTube, Twitter и LinkedIn. В кампании от R/GA, Anomaly, Kornhaber Brown и C42D снялись лидеры мнений, включая Джеки Айну, Джиджи Горджес и Тома Флетчера. Их цель представить разные типы аудитории YouTube, включая спортивных фанатов, геймеров и молодых родителей. Решение запустить кампанию, нацеленную на рекламодателей, было вызвано тем, что бренды массово начали удалять рекламу с YouTube после того, как она появилась рядом с сомнительным контентом (Marketing Media Review).

***

11.09.2017

К 2019 году медийная реклама составит более 50 % расходов на онлайн-рекламу

Инновационные рекламные форматы, такие как видео, платный контент, нативная реклама и реклама в ленте в сетях, будут стимулировать 14 % рост

глобальной медийной рекламы между 2016 и 2019 годами, отмечает новое исследование Zenith (Marketing Media Review).

Если коротко, то медийная реклама составит 50,4 % всех расходов на онлайн-рекламу к 2019 году. Реклама в социальных сетях будет расти на 20 % в год, а видео – на 21 %. Рост платного поиска составит 10 %, так как формат захватила медийная реклама в 2015 году. Отчет отметил, что граница между ТВ и видео стала стираться, так как смарт-ТВ и другие девайсы начали переходить эти границы. Компаниям нет смысла планировать ТВ и онлайн-видео отдельно, так как они друг друга не заменяют, а дополняют. Глобальные расходы на рекламу вырастут на 4 % к 2018 году и составят $558 млрд: компания понизила июньский прогноз 2016 года, который предсказывал рост в 4,2 %. 90 % основных игроков отрасли в Европе отметили, что бренды больше тратили бы на digital-каналы, если бы кросс-медийные возможности измерений были улучшены.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

8.09.2017

Отклики в соцсетях оказывают сильное влияние на психику человека

Эксперты представляющие международную исследовательскую компанию YouGov провели исследование на тему как пользователи относятся к комментариям и лайкам своих заметок и фотографий в соцсетях. Оказалось, каждый четвертый человек очень расстраивается если читает негативные отклики на свои записи.

Докладніше

***

11.09.2017

Ученые обнаружили, что соцсети вредны для здоровья

Исследователи из американского университета Регика выяснили, что пребывание в Facebook повышает уровень стресса у человека и вызывает тревожность. В результате увеличивается вероятность заболевания инфекциями верхних дыхательных путей (ООО "Центр информационной безопасности").

Большое количество информации, которое потребляют пользователи Facebook, отрицательно влияет на иммунную систему человека. Потребление данных вызывает тревожность и хронический стресс, что становится причиной заболевания различными инфекциями. Показательно, что особо высокому риску подвержены те, у кого больше «друзей».

Чтобы изучить последствия регулярного использования Facebook, исследователи в течение 10 недель наблюдали примерно за 90 студентами. Результаты опубликованы в журнале Computers in Human Behavior.

***

12.09.2017

В Індії заблокували «ВКонтакте» через групи смерті та «Синього кита»

В Індії деякі провайдери повністю заблокували доступ до соціальної мережі «ВКонтакте».

Вони вчинили так через загрозу життю дітей, повідомляє The Times of India (Espreso.tv).

Зокрема, мова йде про групи смерті і гру «Синій кит», яка прийшла в Індію саме через російську соцмережу.

Тепер при спробі зайти в соцмережу деякі користувачі бачать повідомлення, що сайт заблокований за рішенням влади країни.

За словами представника міністерства інформаційних технологій Аджая Кумара, зараз чиновники намагаються з'ясувати, скільки людей користуються «ВКонтакте» для гри. Він уточнив, що соцмережу заблокували після зустрічі з інтернет-компаніями.

Точне число інцидентів, пов'язаних з «Синім китом» в Індії невідомо. NDTV повідомляє про зростання їх числа, не називаючи конкретних цифр. Як передає телеканал, в декількох регіонах школярам почали читати лекції про небезпеку гри. Багато індійських ЗМІ почали публікувати докладні статті про «Синього кита» і створювати інструкції для батьків.

Наразі відомо про суїцид 14-річного жителя Мумбаї, який стався наприкінці серпня. 12 вересня повідомлялося, що вдалося врятувати 17-річного підлітка, який перебував у депресії.

Маніпулятивні технології

28.08.2017

В Facebook президента Украины нашли 1,5 тыс. «плодовитых» ботов

Боты написали каждый шестой комментарий на странице Петра Порошенко в соцсети. К такому выводу пришли эксперты интернет-ресурс

Voxukraine и компании TheRespo, проанализировав один из самых многочисленных аккаунтов страны.

Докладніше

***

30.08.2017

Російські та європейські комуністи створять ЗМІ для пропаганди сепаратистів

Російська комуністична партія дала розпорядження своїм представникам на окупованому Донбасі розпочати створення низки ЗМІ разом з комуністами з ЄС, для пропаганди в країнах Європи.

Про це повідомив координатор групи «Інформаційний спротив», народний депутат України від «Народного фронту» Дмитро Тимчук на своїй сторінці в Facebook (Espreso).

«За вказівкою керівництва КПРФ, представниками комуністичних партій "ЛДНР" розпочато інформаційний проект спільно з функціонерами Німецької комуністичної партії (DKP) і італійськими "антифашистами". Йдеться про створення т.зв. "Міжнародного комуністичного інформаційного центру"», – пише Тимчук.

Зазначається, що мова йде про створення інформаційних ресурсів в мережі.

«Першочерговими завданнями даного центру є збільшення кількості прихильників діяльності "ЛДНР" серед громадян європейських країн», – пише координатор групи «Інформаційний спротив».

Так, планується проведення заходів щодо визнання «ЛНР» та «ДНР» в країнах ЄС, формування негативного іміджу України.

Фінансувати зазначені інформаційні заходи буде «Комуністична партія Російської Федерації».

***

1.09.2017

Майже всі твіти російською про НАТО у Балтії пишуть боти

Два з трьох користувачів Twitter, які пишуть російською мовою про присутність НАТО в Східній Європі – це так звані боти.

Про це йдеться у доповіді Центру стратегічних комунікацій НАТО (STRATCOM) під назвою Robotrolling.

Докладніше

***

4.09.2017

Нейросеть научили писать убедительные поддельные клиентские отзывы

Разработчики из Чикагского университета обучили нейронную сеть писать убедительные и почти ничем не отличающиеся от реальных поддельные клиентские отзывы на услуги, рестораны и гостиницы.

Докладніше

***

5.09.2017

Национальный научный фонд США выдал грант на создание технологии, распознающей фейковые новости в Сети

Национальный научный фонд США, независимое федеральное агентство при американском правительстве, созданное конгрессом еще в 1950 году «для развития научных исследований, национального здравоохранения, благосостояния и для обеспечения национальной обороны», выдал грант на создание технологии, которая должна позволить цифровым устройствам распознавать в Сети фейковые новости.

Докладніше

***

7.09.2017

Facebook заявив, що Росія купувала політичну рекламу під час виборів в США

Екаунти у соціальній мережі Facebook, пов'язані з Росією, два роки купували політичну рекламу, яка могла вплинути на ситуацію в США під час президентських виборів – повідомляє Facebook (Watcher).

З червня 2015 року по травень 2017 року 470 недостовірних екаунтів і сторінок заплатили за рекламні повідомлення близько $100 тисяч, розповів директор служби безпеки Facebook Алекс Стамос. Вони купили близько трьох тисяч повідомлень, які зачіпали соціальні та політичні питання, від ЛГБТ до мігрантів і прав на зброю. В повідомленнях використовували слова «патріот» і «біженець».

Велика частина повідомлень мала дуже чіткий географічний таргетинг.

У соцмережі вважають, що сторінки були пов'язані між собою і управлялися з Росії. Соцмережа вже видалила всі ці сторінки.

Facebook знайшов ще 2,2 тисячі рекламних повідомлень, на які витратили $50 тисяч і які потенційно мали відношення до політики і до Росії. Інформацію передали владі США, яка розслідує можливе втручання Росії у вибори американського президента.

***

12.09.2017

В ЄС створили сайт, який протидіятиме російській пропаганді

В Євросоюзі запустили новий сайт euvsdisinfo.eu для протидії російської дезінформації. Про це повідомляється на самому сайті (Espreso.tv).

Ресурс є частиною кампанії ЄС для кращого прогнозування та реакції на дезінформацію з Кремля.

На сайті публікуватимуть інтерактивну статистику та контент англійською, російською та німецькою мовами.

«Відповідаючи на неодноразові запити від дослідників, журналістів та державних службовців, ми створили нову функцію єдиної комплексної бази даних, що дозволяє вам шукати в нашому реєстрі понад 3300 випадків дезінформації за ключовими словами», – повідомляється на сайті.

Зазначається, що він є частиною кампанії ЄС для кращого прогнозування та реакції на дезінформацію з Кремля.

Цю кампанію веде оперативна група зі стратегічних комунікацій, яка створила зовнішньополітична служба ЄС.

Спецслужби і технології «соціального контролю»

28.08.2017

СБУ задержала сепаратистов из соцсетей «ВКонтакте» и «Одноклассники»

Сотрудники Службы безопасности Украины в течение августа прекратили деятельность нескольких администраторов, которые поддерживали антиукраинские сообщества в запрещенных в Украине социальных сетях «ВКонтакте» и «Одноклассники».

Докладніше

***

29.08.2017

В Китае запретили анонимность в Интернете

В преддверии 19-го съезда компартии Китай ужесточил правила пользования Интернетом, введя обязательную регистрацию реальных имен пользователей у провайдеров. Анонимные посты на форумах и других ресурсах будут удаляться интернет-цензурой.

Докладніше

***

31.08.2017

Порошенко ввів у дію рішення РНБО щодо кардинального посилення заходів кібербезпеки держави

Згідно з Указом, Уряд у тримісячний строк має врегулювати питання щодо заборони державним органам та підприємствам державної форми власності закуповувати послуги з доступу до Інтернету у операторів телекомунікацій, у яких відсутні документи про підтвердження відповідності системи захисту інформації встановленим вимогам у сфері захисту інформації.

Докладніше

***

3.09.2017

Спецслужби Росії намагаються стежити за користувачами соцмереж

Олена Матусова

Російські спецслужби посилюють контроль над Інтернетом. Незабаром вони можуть отримати усі особисті дані на користувачів мереж «ВКонтакте», «Одноклассники» та інших, які вирішили залишитися працювати в Росії. Відповідний наказ розробляє Міністерство комунікацій та зв'язку Росії.

Докладніше

***

5.09.2017

Кибербезопасность или диктатура: что сулит нам Указ Президента

Владимир Кондрашов

В конце августа был опубликован Указ Президента Украины, которым Петр Порошенко ввел в действие решение СНБО по укреплению кибербезопасности государства. Документ активно обсуждается в телекомсообществе.

Докладніше

***

12.09.2017

Китайская соцсеть Weibo дала неделю пользователям, чтобы указать настоящие имена

Пользователям Sina Weibo, популярного в Китае сервиса микроблогов, дали неделю, чтобы указать в своих аккаунтах настоящие имена. «Закручивание гаек» производится в целях соблюдения новых директив властей Китая, ограничивающих анонимное онлайн-общение (InternetUA).

Аналогичные правила действуют в Китае с 2011 года, но социальная сеть их не выполняла, так как проще продекларировать устранение анонимности в Сети, чем это сделать. Многие пользователи скорее покинут социальную сеть, где сейчас общаются под разными псевдонимами, чем укажут в аккаунте свои настоящие имена.

Все это связано с усилением цензуры со стороны китайского правительства, которое в дополнение к выпуску директивы о необходимости указания реального имени начало в прошлом месяце борьбу с использованием VPN-сервисов, а также занялось дальнейшим сокращением возможностей онлайн-дискуссий и ограничением публикаций зарубежного контента.

Введение требования указания настоящего имени может привести к упадку Weibo, аналога Twitter в Китае, продолжающей функционировать, несмотря на усиливающуюся цензуру и давление со стороны властей. Если Weibo действительно начнёт удалять аккаунты тех, кто не предоставляет достоверную информацию о себе, она может потерять миллионы пользователей, которых сейчас насчитывается 340 млн.

***

12.09.2017

Суд на Днепропетровщине вынес приговор Интернет-сепаратисту

1 сентября Павлоградский горрайонный суд Днепропетровской области приговорил уроженца села Вербки Павлоградского района, администратора группы «Столиця Западного Донбасса!!» в соцсети «ВКонтакте», к двум годам ограничения свободы с испытательным сроком в один год за размещение в упомянутой группе информации с призывами к насильственному изменению и свержению конституционного строя и захвату государственной власти Украины (InternetUA).

Суд установил, что в период с марта по май 2017 года (3 марта в 03:57 и 04:05, а также 4 мая в 11:15), в неустановленном месте, разделяя преступные намерения незаконных объединений сепаратистского и террористического толка, так называемых «Донецкая Народная Республика» и «Луганская Народная Республика», у него возник умысел на распространение в сети Интернет с помощью социальной сети «ВКонтакте» материалов с публичными призывами к насильственному изменению, свержению конституцийного строя и к захвату государственной власти Украины.

Он размещал информацию со своего мобильного телефона «Lenovo» в социальной сети «ВКонтанте» в группе «Столиця Западного Донбасса!!», в которой был администратором.

Симпатик сепаратистов полностью признал свою вину.

Проблема захисту даних. DDOS та вірусні атаки

28.08.2017

Dr.Web первым обнаружил загрузчик троянца для «умных» Linux-устройств

Ассортимент современных вредоносных программ для устройств под управлением Linux чрезвычайно широк. Одним из широко распространенных троянцев для данной ОС является Linux.Hajime, несколько загрузчиков детектировал только Антивирус Dr.Web.

Докладніше

***

28.08.2017

Кому вы нужны. Как мошенники используют слитые базы данных и информацию о вас из соцсетей

Сегодня трудно представить человека, который бы не пользовался социальными сетями. Однако зачастую открытого профиля достаточно, чтобы стать добычей ловцов данных и жертвой навязчивого внимания такси. Нарушение правил использования персональных данных для Украины – обычное дело. Государство не спешит защищать приватность своих граждан.

Докладніше

***

29.08.2017

Киберпреступная схема «вымогатель как услуга» набирает популярность

Исследование, проведённое компанией Positive Technologies, показало, что во втором квартале текущего года продолжили набирать популярность сервисы «вымогатели как услуга» по сдаче троянов в аренду. США и Россия стали наиболее частыми жертвами атак, хотя больше четверти (28 %) киберкампаний были масштабными и затронули одновременно десятки стран.

29.08.2017

Киберпреступная схема «вымогатель как услуга» набирает популярность

Исследование, проведённое компанией Positive Technologies, показало, что во втором квартале текущего года продолжили набирать популярность сервисы «вымогатели как услуга» по сдаче троянов в аренду. США и Россия стали наиболее частыми жертвами атак, хотя больше четверти (28 %) киберкампаний были масштабными и затронули одновременно десятки стран (InternetUA).

Схема работы зловредов-вымогателей сводится к следующему. Проникнув на устройство жертвы, вредоносная программа шифрует файлы распространённых форматов. Далее на экран выводится сообщение с

требованием выкупа за восстановление доступа к данным. Обычно жертве предлагается заплатить некую сумму в криптовалюте.

По статистике Positive Technologies, 67 % атак шифровальщиков во втором квартале текущего года были совершены с целью получения прямой финансовой выгоды. Так, нашумевшая эпидемия вируса-вымогателя WannaCry принесла злоумышленникам около $130 тыс., а ущерб компаний составил более миллиарда долларов.

Киберпреступники всё чаще сдают вредоносное ПО с функциями шифрования в аренду. Так, дистрибьютор Petya или Mischa получает от 25 % до 85 % от суммы платежей жертв, а троян-шифровальщик Karmen продаётся на чёрном рынке за $175.

Аналитики отмечают появление новых нестандартных цепочек проникновения в целевую систему. Например, группировка Cobalt использовала произвольные уязвимые сайты в качестве хостинга для вредоносного ПО. Члены группировки APT10 в ходе целевых атак сначала получали доступ в корпоративные сети провайдеров облачных сервисов, а затем по доверенным каналам проникали в сеть организаций-жертв.

***

28.08.2017

Онлайн-шпигуни. Як за вами стежать Facebook, Google та Microsoft

Анастасія Пашинська

Ми всі боїмося бути зламаними хакерами, але велика загроза конфіденційності в інтернеті – це сайти і додатки, з якими ми співпрацюємо щодня. Як за нами стежать Facebook, WhatsApp, Microsoft, Google.

Докладніше

***

29.08.2017

ФРГ опасается хакерских атак со стороны российских спецслужб

Спецслужбы ФРГ опасаются кибератак со стороны России во время предстоящих парламентских выборов, запланированных на 24 сентября. Об этом немецкому изданию «Die Welt» сообщил в эксклюзивном интервью президент Федеральной службы защиты конституции Германии Ханс-Георг Маасен (Hans-Georg Maaßen) (InternetUA).

По словам чиновника, в ведомстве ожидают массивную пропагандисткую кампанию со стороны спецслужб РФ в преддверье выборов в бундестаг. В то же время, политик не уверен, что Кремль пойдет на подобный шаг и воздействие на выборы в Германии является «актуальным политическим курсом Кремля». Маасен считает маловероятным желание России значительно ухудшить отношения между двумя государствами.

Контразведка Германии не способна предоставить какие-либо доказательства осуществления кибератак со стороны спецслужб РФ. Однако, ведомство, подконтрольное Маасену, считает причастность РФ весьма вероятной.

Выборы в бундестаг запланированы на 24 сентября текущего года.

***

29.08.2017

Кража средств с помощью WAP-биллинга набирает обороты

Исследование, проведённое «Лабораторией Касперского», показало, что киберпреступники всё чаще используют вредоносные программы для кражи денег посредством WAP-биллинга.

Докладніше

***

29.08.2017

300 Android-приложений оказались вредоносными программами

Зловредные приложения для Android создали свою сеть и наносили массированные удары по популярным сайтам России и Азии. Команда специалистов смогла обезвредить ботнет – армию зараженных мобильных телефонов под управлением ОС Android от Google, – сообщает Fortune.

Докладніше

***

30.08.2017

Набравший популярность анонимный мессенджер Sarahah похищает данные пользователей

В последние недели приложение Sarahah, созданное разработчиком из Саудовской Аравии Зейном аль-Абидин Тофиком (Zain al-Abidin Tawfiq) возглавляет рейтинги App Store и Google Play, набрав миллионы пользователей. Независимый ИБ-специалист Закари Джулиан (Zachary Julian) предупреждает, что анонимный мессенджер не так уж анонимен.

Докладніше

***

30.08.2017

Растет число фирм, предлагающих услуги по слежке за телефонами по всему миру

Отслеживание телефонов по всему миру постепенно становится привлекательной нишей для ведения бизнеса, сулящей большие доходы. В

связи с этим в последнее время стремительно растет число компаний, предлагающих технологии для удаленной слежки за мобильными устройствами невзирая на государственные границы.

Докладніше

***

29.08.2017

Бразильский университет собирал данные о пользователях Tor

Ретрансляционный узел Tor команды исследователей из Бразильского университета Кампинас в Сан-Паулу заблокировали, поскольку он был замечен в сборе информации об onion-адресах пользователей (InternetUA).

Команда настроила узел Tor для сбора конкретных данных о скрытых сервисах. Исследователи пояснили, что собранные данные не могут использоваться, чтобы деанонимизировать пользователя или найти определенный сервер, на котором запущен сервис.

По словам администраторов Tor, деятельность, проводимая исследователями, является нарушением этических принципов Tor Project.

Маркус Родригес (Marcus Rodrigues), младший научный сотрудник Бразильского университета, объяснил, что он и его коллеги работали над разработкой инструмента, который мог бы идентифицировать вредоносные луковичные сервисы.

Исследователи признали свою вину, но оправдывают свои действия сугубо научными целями. Решение собрать адреса .onion и получить их содержимое было принято для упорядочивания сервиса и в целях безопасности.

«Мои исследования, в частности, касаются вредоносных скрытых сервисов. Я разрабатываю метод автоматической категоризации вредоносной скрытой службы по ее контенту, например, сайт по продаже наркотиков, распространению вредоносного ПО и.т. д.», – сообщил Родригес порталу The Register.

Родригес не смог восстановить свой узел Tor, но заявил, что исследование будет продолжаться в любом случае с использованием альтернативных технологий.

***

3.09.2017

Хакеры получили доступ к номерам телефонов и почте 6 млн пользователей Instagram. И выставили их на продажу

Илья Кабачинский

Как сообщает издание The Verge, неизвестные хакеры обошли защиту Instagram, получив доступ к личным контактным данным порядка 6 млн человек. Среди них есть как обычные пользователи, так и знаменитости. Теперь эти данные пытаются продавать (AIN).

По данным The Verge, сразу после взлома в сети появилась база Doxagram, которую пытались продавать по $10 за 1000 аккаунтов. Хакеры обещали, что в каждой из таких подборок есть и данные знаменитостей. Правда, уже через несколько часов база исчезла из сети – появились предположения, что теперь информация распространяется через дарквеб.

Есть сведения, что в базе присутствуют данные таких пользователей: Эммы Уотсон, Эмилии Кларк, Зака Эфрон, Леонардо ДиКаприо, Виктории Бэкхем, Бейонсе, Тейлор Свифт, Адель, Леди Гага, Неймара, Зидана и многих других.

В Instagram особо много комментировать не стали, заявив лишь, что баг в системе, из-за которого удалось получить доступ к личной информации, уже закрыт. Пользователям также посоветовали сменить адрес электронной почты и телефон, который привязан к аккаунту.

***

3.09.2017

3 способа проверить Android-устройство на наличие вредоносных приложений

Беспокоитесь о надёжности программ в мобильном устройстве? Инструмент от Google позволит убедиться в том, вы не загрузили какие-либо подозрительные Android-приложения. Предлагаем детальную инструкцию, как это проверять.

Докладніше

***

4.09.2017

Загрузчики Android от крупных производителей подвержены уязвимостям

В загрузчиках ОС Android от пяти производителей процессоров для мобильных устройств обнаружены уязвимости, нарушающие процесс доверенной загрузки и ставящие под угрозу безопасность пользователей.

Докладніше

***

5.09.2017

Новая масштабная спам-кампания распространяет вымогатель Locky

Недавно была зафиксирована новая кампания по распространению по электронной почте приложения-вымогателя Locky среди миллионов пользователей. Работающая в сфере веб-безопасности компания AppRiver утверждает, что в конце августа за сутки было отправлено более 23 млн. писем

с вредоносным вложением. Эта кампания названа одной из самых крупных в нынешнем году (InternetUA).

Письма содержат заголовки вроде please print, photo, documents и images. Вложение доставляется в виде архива ZIP, внутри содержится файл Visual Basic Script (VBS). При его запуске начинается скачивание последней версии вредоносного приложения Locky.

Когда процесс шифрования пользовательских файлов завершён, к ним добавляется расширение .lukitus. За возврат файлов вымогатель требует 0,5 биткоина. Такая большая сумма может объясняться малым процентом инфицирования; злоумышленники рассчитывают, что среди жертв попадутся платёжеспособные обладатели ценных файлов.

Пока нет метода разблокировать зашифрованные файлы бесплатно. Пользователям рекомендуется выполнять резервное копирование и внимательно относиться к вложенным файлам и ссылкам в интернете, особенно при работе на Windows.

***

5.09.2017

Вирус Cerber проник на сайт правительства США и вымогал биткоины

В августе 2017 года на веб-сайте Национальной координационной группы по лесным пожарам (NWCG) в США был обнаружен вирус-вымогатель. Первым его идентифицировал Анкит Анубхав, исследователь из компании NewSkySecurity.

Докладніше

***

5.09.2017

Данные 4 миллионов пользователей Time Warner Cable утекли в Сеть

Исследователи из компании Kromtech обнаружили данные более четырех миллионов пользователей приложения MyTWC, от провайдера кабельного телевидения Time Warner Cable. Данные были размещены на незащищенном сервере Amazon (InternetUA).

Файлы, общим размером более 600 гигабайт, содержащие конфиденциальную информацию, такую как идентификаторы транзакций, имена, MAC-адреса, серийные номера и номера счетов были обнаружены 24 августа исследователями из Kromtech.

Компания Charter Communications Inc (CHTR.O), владелец Time Warner Cable, подтвердила факт утечки некоторых нефинансовых данных клиентов, которые использовали устаревшее мобильное приложение MyTWC.

Информация была удалена сразу после обнаружения, также было инициировано внутреннее расследование утечки.

***

6.09.2017

Google Drive превращается в крупный распространитель пиратского контента

Пока правообладатели боролись с пиратскими ресурсами, такими как KickassTorrents и TorrentHound, а «ветеран разбоя» The Pirate Bay менял адреса, у торрент-трекеров появилась альтернатива – Google Drive (IGate).

Голливудские студии и прочие владельцы авторских прав завалили компанию из Маунтин-Вью почти пятью тысячами запросов на удаление незаконных материалов, размещенных в облачном хранилище за последние 30 дней. Google Drive стал столь же популярным пиратским ресурсом, как и The Pirate Bay: каждая ссылка, обработанная сервисом удаления Lumen Database, имеет десяток дубликатов, ведущих в Drive.

Несмотря на то, что в начале 2017 Google ввела хеш-проверку всех загружаемых файлов для борьбы с нарушениями, пираты придумали способы обхода защиты: они обмениваются ссылками на файлы через Drive, встраивают в них видео с YouTube. Для минимизации риска быть обнаруженными, информацию об украденном контенте публикуют в малоизвестных группах в Facebook и на досках объявлений.

Dropbox и OneDrive в 25 раз менее «популярны», чем детище Google. Причина сложившейся ситуации – преимущества Google Drive перед конкурентами: интеграция с другими сервисами и больший объем предоставляемого хранилища – целых 15 Гбайт без платной подписки. Полюбился пиратам и другой продукт компании – My Maps. В редакторе карт нет систем проверки, а возможность создавать личные ссылки открывает новые пути распространения нелицензионного контента.

***

6.09.2017

Vodafone предложил Zillya! для смартфонов

Vodafone Украина в сотрудничестве с украинскими разработчиками запустил услугу «Антивирус Zillya!». Услуга защищает пользовательское устройство от вирусов, перехода на вредоносные сайты, навязчивых контактов и потери личной информации. Услуга также поможет оптимизировать и ускорить работу смартфона или планшета (ITnews).

«Антивирус Zillya!» предлагает следующие функции: антивирус, антивор, который обеспечивает защиту данных на смартфоне в случае кражи или утери устройства, WEB-фильтр, блокирующий доступ к фишинговым и другим

вредоносным сайтам, черный список, оптимизация, ускорение и родительский контроль.

Для того чтобы уберечь юных пользователей от сомнительной информации и нежелательных действий в интернете, в услуге реализован модуль «Родительский контроль». Работа модуля построена на принципе блокировки нежелательных для посещения сайтов по установленным категориям. Родительский контроль способен блокировать онлайн шопинг, сайты служб знакомств, азартных игр, торренты и социальные сети, а также сайты с контентом для взрослых.

По сравнению с бесплатными версиями антивирусных программ услуга «Антивирус Zillya!» обладает расширенным функционалом средств защиты устройства от киберугроз и возможностью профессиональной настройки системы безопасности.

Воспользоваться услугой могут все обладатели смартфонов с OS Android 4.2 и выше. Подключиться к «Антивирус Zillya!» можно, отправив SMS на номер 7227 с цифрой 1 в тексте, в ответ абонент получит SMS со ссылкой на приложение. Абоненты Vodafone могут бесплатно протестировать услугу в течение 14 дней.

***

11.09.2017

ФБР начало расследование против Uber из-за программы для слежки за водителями Lyft

ФБР начало расследование в связи с информацией об использовании компанией Uber программы Hell для слежки за водителями сервиса-конкурента Lyft. Об этом сообщает Bloomberg (IGate).

Власти подозревают Uber в незаконном вмешательстве в работу конкурента с помощью специального программного обеспечения. Расследование началось после ухода из компании руководителя глобального отдела по правовому соответствию Джозефа Шпиглера.

Пресс-секретарь Uber Мэтт Каллман заявил, что компания сотрудничает с властями в рамках расследования, а программа Hell больше не используется. Представители ФБР и действующего прокурора США в боро Манхэттен Джона Кима отказались от комментариев.

В апреле 2017 года издание The Information сообщило, что Uber использовал Hell в период с 2014 по 2016 год. Система создавала поддельные аккаунты пассажиров сервиса Lyft, чтобы изучать расположение машин конкурента, а также анализировать действия работающих на оба сервиса водителей. По информации издания, как минимум 60% водителей Lyft параллельно работали с Uber.

В конце апреля 2017 года водитель Михаэль Гонзалес подал в суд на компанию из-за Hell. Истец потребовал $5 млн в рамках группового иска.

В мае Минюст США открыл расследование в отношении Uber за использование программы для обмана чиновников и полиции Greyball.

***

11.09.2017

Facebook оштрафували за використання даних користувачів для реклами

В Іспанії соціальну мережу Facebook оштрафували за незаконне використання даних користувачів. Загальна сума штрафу становить 1,2 млн євро (Espreso.tv).

Соціальна мережа збирала особисту інформацію користувачів, але не попереджала, на які саме цілі. Ще одним порушенням стало те, що дані продовжували зберігатися після того, як їх уже використовували у відповідних ситуаціях.

Крім цього, Facebook збирав дані про запити користувачів поза соцмережею, а також інформацію про дії незареєстрованих користувачів.

У Facebook заявили, що лише показували користувачам рекламу, яка могла бути їм корисною.

«Користувачі самі вибирають, яку інформацію хочуть додати в свій профіль, включаючи дані про релігійні переконання. Ми не використовуємо цю інформацію для рекламного таргетування», – запевнили в компанії.

***

11.09.2017

Хакеры используют CDN-серверы Facebook для обхода антивирусов

Группа злоумышленников эксплуатирует CDN-серверы Facebook для хранения вредоносных файлов, которые затем используются для инфицирования систем пользователей банковскими троянами.

Докладніше

***

11.09.2017

Антивирус Касперского выводят из свободной продажи в США

Крупнейший продавец электроники и продуктов программного обеспечения в США компания Best Buy выводит из продажи продукцию виртуальной безопасности «Лаборатория Касперского» как в магазинах, так и в интернете из-за опасения, что московская фирма может находиться под контролем российского правительства (InternetUA).

Об этом сообщило американское информагентство Reuters.

«Best Buy считает, что осталось без ответов слишком много вопросов и поэтому решила прекратить продажу антивирусных продуктов», – пишет

агентство со ссылкой на местные СМИ, которые в свою очередь цитируют источники.

Позже пресс-секретарь Best Buy подтвердила этот факт, зато отказалась предоставлять дополнительную информацию.

В июле этого года группа американских конгрессменов обратилась к правительственным учреждениям США с просьбой поделиться документами по «Лаборатории Касперского», заявив, что ее продукты могут использоваться для «негативных действий против Соединенных Штатов».

Как сообщалось, тогда администрация США исключила продукцию Касперского из списков утвержденных поставщиков для правительственных учреждений США.

***

11.09.2017
Банковский троян Emotet вернулся и распространяется через спам

Исследователи из TrendMicro сообщили о новой вредоносной кампании, в рамках которой злоумышленики распостраняют банковский троян Emotet. Впервые вредоносное ПО Emotet было обнаружено в 2014 году.

Докладніше

***

12.09.2017
Хакеры похитили данные половины жителей США

В США разгорается громкий скандал из-за крупнейшей утечки данных, произошедшей в Equifax, одном из трех ведущих бюро кредитных историй в США. В результате масштабного взлома хакеры получили сведения о примерно 143 миллионах американцев, то есть почти о половине населения Соединенных Штатов.

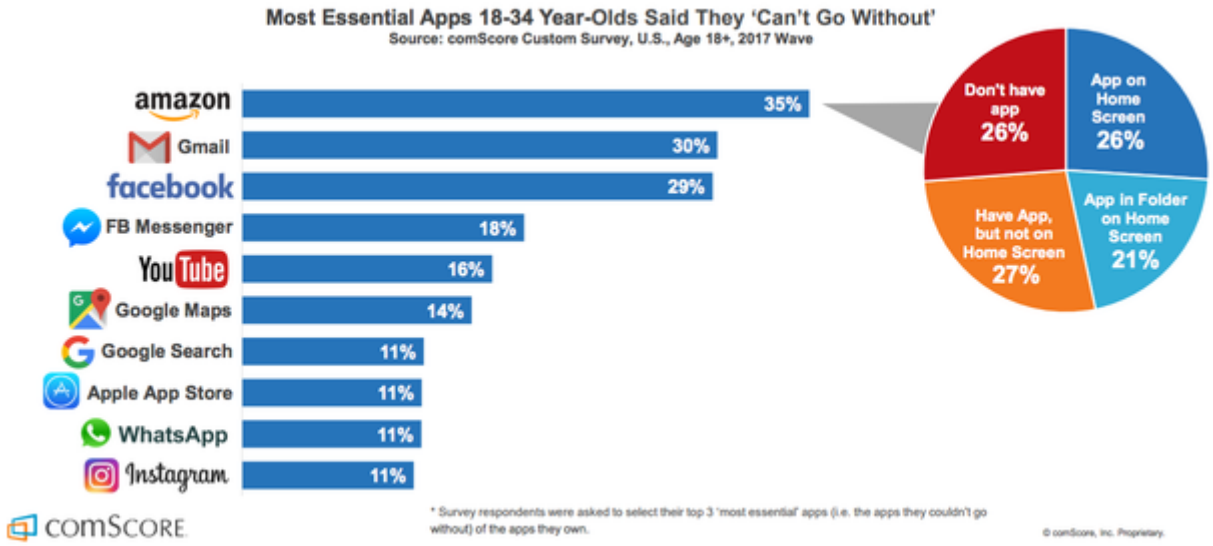
Докладніше

ДОДАТКИ

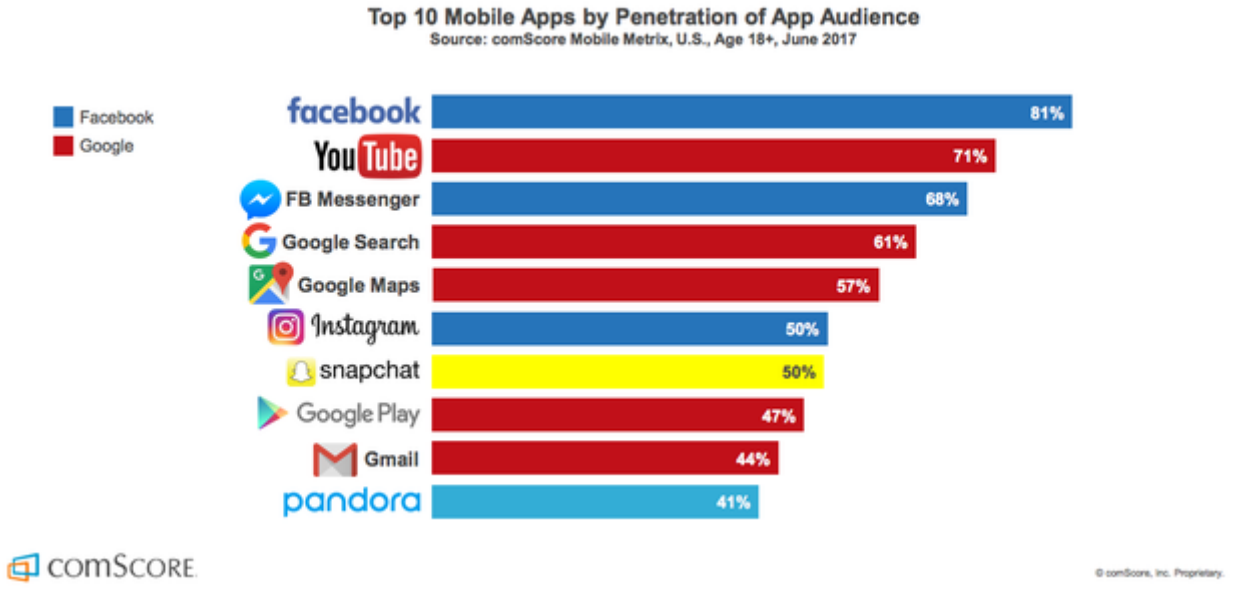
Додаток 1

28.08.2017
Топ-10 приложений, без которых миллениалы не могут жить

Более трети пользователей в возрасте от 18 до 34 лет не могут жить без Amazon. Такие выводы нового исследования comScore.



Gmail и Facebook заняли второе и третье место. Snapchat, к удивлению, не вошел в число самых необходимых приложений для этой категории. Кроме того, Facebook и Google вместе составили восемь приложений из десяти среди всех возрастных групп. Snapchat удерживает прочную позицию среди молодых миллениалов до 24 лет, и занимает шестую позицию среди пользователей в возрасте от 25 до 34 лет, вслед за Instagram, но отсутствует в рейтинге приложений для аудитории старше 35 лет. Instagram занял седьмую позицию среди аудитории в возрасте от 35 до 54 лет. YouTube и Facebook занимают топ позиции среди всех возрастных групп.



Snapchat удерживает прочную позицию среди молодых миллениалов до 24 лет, и занимает шестую позицию среди пользователей в возрасте от 25 до 34 лет, вслед за Instagram, но отсутствует в рейтинге приложений для аудитории старше 35 лет. Instagram занял седьмую позицию среди аудитории в возрасте от 35 до 54 лет. YouTube и Facebook занимают топ позиции среди всех возрастных групп (Marketing Media Review).

(вгору)

Додаток 2

30.08.2017

Skype представил функцию «Интервью» для технических работников. Там можно писать и проверять код

Дмитрий Демченко

Skype представил функцию «Интервью». С ее помощью рекрутеры могут проводить технические интервью и проверять навыки программирования кандидатов, не покидая пределы сервиса. На новинку обратило внимание издание TechCrunch (AIN).

Новая функция позволяет пользователям писать код, проверять результат, а также делать пометки в режиме реального времени для того, чтобы обращать внимание собеседника на ошибки.

Сейчас функция «Интервью» работает в режиме предварительного просмотра и доступна в веб-версии Skype в браузерах Microsoft Edge и Chrome (версия 32+). Для запуска нужно изменить язык браузера на английский и зайти на Skype.com. Устанавливать приложение сервиса или дополнительные плагины не нужно.

Вместо этого на сайте нужно выбрать раздел «Интервью» и нажать на кнопку «Начать интервью». После этого пользователь получит ссылку, которую нужно отправить своему собеседнику. При запуске функция поддерживает семь популярных языков программирования, включая C, C ++, C #, Java, JavaScript, Python и Ruby.

TechCrunch отмечает, что на рынке уже присутствуют сервисы для технических собеседований, среди которых HackerRank, Codility, Interview Zen, CoderPad, Remoteinterview.io, CodeVue и другие. «Но преимущество в использовании Skype – это вездесущность платформы, что делает ее

распространенным инструментом для видеозвонков любого типа. Внедрение подобной функции в сервис может ускорить процесс собеседования, так как собеседникам не придется переключаться на другие инструменты для завершения технического тестирования», – добавляет издание.

(вгору)

Додаток 3

30.08.2017

YouTube запустил новый дизайн для десктопов и новые функции для мобильных

Ольга Карпенко

Популярный видеосервис YouTube 29 августа выкатил большое обновление своей десктоп-версии, а также представил ряд новых функций для мобильного приложения (AIN). Среди новостей для пользователей смартфонов:

– Обновленный дизайн приложения.

– Управление видео свайпом: свайп влево, чтобы просмотреть предыдущее видео, вправо – чтобы просмотреть последующее, правда, эта функция будет доступна для смартфонов не прямо сейчас, а в ближайшие месяцы.

– Управление скоростью проигрывания видео. Сейчас для видео на YouTube можно задать темп: проигрывать его в 1,5 раза быстрее, в 2 раза медленней и т. д. – его можно выбрать в настройках видео. Сейчас эту функцию включают и для видео на мобильных.

– Скоро YouTube-плеер будет адаптироваться под любой видеоформат, который сейчас просматривает пользователь, по форме, будь-то вертикальное видео, квадратное и т. д. Так что настал конец эре вертикальных видео, снятых со смартфонов, с черными полосами по краям.

– Список рекомендованных видео можно будет просматривать прямо из полноэкранного режима.

Для дизайна десктопа изменения более глобальные. Этот дизайн долгое время тестировали, и поскольку он получил положительные отзывы, выкатили его по всему миру. Как мы уже сообщали ранее, он привносит во внешний вид YouTube черты material-дизайна. У сервиса изменился интерфейс, добавились новые функции. Среди основных изменений:

– Немного изменили логотип и иконку сервиса.

– Добавили Dark Theme – ночной режим, который позволяет включить черный фон, чтобы ничего не отвлекало от просмотра видео. Его можно включить, кликнув по иконке профиля.

– Из интерфейса убрали визуальные элементы, которые отвлекают от контента.

Новый дизайн десктопной версии привели в соответствие дизайну приложения на других устройствах.

Если вам не нравится новый дизайн, пока что можно откатить его к старой версии, кликнув по иконке профиля и выбрав соответствующий пункт.

(вгору)

Додаток 4

5.09.2017

В Telegram переработали систему ответов и добавили раздел с избранными стикерами

Мессенджер Telegram приобретает всё большую популярность, а вместе с этим «обрастает» большим количеством возможностей. Разработчики представили функцию ответов ещё в 2015 году, но с тех пор максимальной количество групп выросло в 50 раз – от 200 до 10000 пользователей. При таком числе людей поток сообщений иногда бывает слишком большим, поэтому очень просто пропустить сообщение, адресованное вам. Поэтому в версии 4.3 разработчики переработали систему ответов (InternetUA).

Если вы были упомянуты в переписке или кто-то ответил на ваше сообщение, то в списке чатов помимо количества новых уведомлений вы увидите соответствующую иконку – «@». Затем уже в самом чате можно нажать на эту иконку, чтобы сразу перейти к сообщениям, адресованным именно вам.

Стикеры стали неотъемлемой частью общения в Telegram. Пользователям доступны тысячи наборов стикеров. Но в большинстве случаев целый набор держится только из-за одного конкретного стикера. Теперь если вам понравился какой-то стикер, то можно нажать на него и добавить в список избранных. Все отмеченные стикеры будут отображаться в специальном разделе.

Также в Telegram 4.3 появилась возможность выбрать официальный стикер для групп с не менее чем сотней членов. Данный стикер будет виден и доступен всем участникам переписки без необходимости добавлять его в свой список.

Ещё одно важное изменение – переработанный раздел «Invite Friends». Если кого-то из вашего списка контактов ещё нет в Telegram, но его друзья уже есть в этом сервисе, то такие пользователи будут показываться в самом верху списка.

Также в новой версии появилась поддержка воспроизведения роликов с Twitch, при голосовом вызове теперь отображается индикатор уровня сигнала, пользователи iOS могут отредактировать любую фотографию, вставленную из буфера обмена перед отправкой, а на Android сообщение можно переслать сразу нескольким контактам.

(вгору)

Додаток 5

7.09.2017

Искусственный интеллект Facebook научится распознавать выражения лиц пользователей

Команда по разработке искусственного интеллекта Facebook решила научить ботов соцсети не только распознавать человеческую речь, но и выражения лиц пользователей (IGate).

Согласно уведомлению разработчиков, они пытаются научить бота понимать мимику живых людей на примере записей разговоров по Skype. Для этого используются видеозаписи, на которых отчетливо видно лица собеседников, и бот учится распознавать эмоции.

При этом создатели учат систему понимать не абстрактные выражения, такие как грустное, или счастливое лицо, а распознавать определенные изменения в мимике, присущие отдельным эмоциям. Эти, так называемые, «мимические узоры» являются одинаковыми для всех, независимо от того, насколько могут отличаться выражения тех или других эмоций у отдельных людей. Изучая подобные шаблоны, система может предсказывать, какое из выражений будет наиболее похожим на человеческую эмоцию.

Для тестирования новой возможности были приглашены сторонние люди. Им предлагали рассмотреть несколько выражений бота и высказать свое мнение на счет того, насколько правдоподобно искусственный интеллект передает человеческие эмоции.

Разработчики не вдавались в подробности метода, используемого для обучения ИИ. Они также не сообщили, для каких целей проводятся подобные исследования. Вполне вероятно, что распознавание ботами человеческих эмоций в дальнейшем будет реализовано в разработках, касающихся виртуальной реальности.

(вгору)

Додаток 6

12.09.2017

Смогут ли украинские соцсети конкурировать с Facebook

Ukrainians, Nimses, а теперь еще Woolik и Psyball. Удастся ли им потеснить Facebook и Instagram?

После блокировки российских «ВКонтакте» и «Одноклассники» в Украине, как грибы, появляются новые социальные сети. Но взлеты и падения пока происходят очень часто (InternetUA).

Команда тернопольского проекта Ukrainians недавно объявила о его закрытии. Партнер – канадский акселератор StartupSoft – оказался недоволен темпами развития. В соцсети менее чем за три месяца зарегистрировалось около 400000 пользователей, но, как рассказала mc.today основательница проекта Александра Струмчинская, ежедневно сервисом пользовались только 20000.

Данные SimilarWeb показывают, что пик посещаемости ресурса пришелся на июнь. За этот месяц было зарегистрировано 4,8 млн уникальных визитов. После чего трафик просел и по итогам августа снизился до 3,3 млн.

То есть, несмотря на рост общего числа регистраций, активных пользователей соцсети становилось меньше.

С каждым месяцем падает посещаемость и у нашумевшей в начале лета соцсети Nimses. Согласно данным SimilarWeb, больше всего посещений было в июне – 5,9 млн. В июле – 1,8 млн, по итогам августа – 620 000.

«Нас не интересует посещаемость сайта, тем более в СНГ. Он не несет функциональной нагрузки для пользователей, а является лишь лендингом для перехода в AppStore и Google Play Market», – объясняет CMO Nimses Андрей Сирченко. По его словам, проект переключается на глобальный рынок. Как недавно сообщалось, Nimses уже установили себе 4 млн пользователей в 70 странах.

Они не заканчиваются

Новые соцсети продолжают появляться. Буквально на днях произошел запуск еще одного украинского проекта Woolik. Правда, его сайт сразу же начал испытывать технологические сложности. На страничке проекта в Facebook объяснили медленную работу серверов большим интересом к ресурсу со стороны как украинцев, так и иностранцев. «У нас регистрируются люди со всего мира – Украина, Польша, Россия, Беларусь, Израиль», – написал журналисту LIGA.net представитель проекта со странички Woolik в Facebook. По его словам, команда стартапа состоит из 11 человек, базируется преимущественно в Киеве. Основатели – граждане Украины, которые пока предпочитают оставаться непубличными. «Пример Ukrainians показал, что десятки интервью на телеканалах и радиостанциях необязательно приводят владельцев сети к успеху. Слава мимолетна», – пишет представитель Woolik.

В соцсети уже зарегистрировалось более 100 000, отмечает представитель Woolik. По его словам, из-за такого наплыва проекту уже пришлось переехать на серверы, которые «в 12 раз мощнее предыдущих, но спрос такой, что, скорее всего, придется в ближайшие пару дней опять переезжать». Объем инвестиций команда пока также не разглашает. Цели до конца года выглядят амбициозными: 2,5-3,5 млн пользователей. То есть в разы больше, чем за три месяца привлекла Ukrainians.

Что не имеет смысла?

Эксперты отзываются о новых украинских социальных проектах крайне скептично. «Главное условие существования соцсети – критическая масса пользователей. Для этого какая-то аудитория должна перестать пользоваться имеющейся соцсетью, чтобы перейти к новой. Я не вижу никакого стимула для этого», – говорит управляющий партнер PlusOne Максим Саваневский. Причина тому – копирование уже существующего у других соцсетей функционала.

«Мы вынуждены признать, что Facebook, Instagram, VK и Одноклассники не оставляют на рынке ниши для еще одной социальной сети», – признала в своем последнем сообщении команда Ukrainians.

«Если кому-то удастся придумать что-то новое, why not? Правда, я пока не видел ничего интересного из того, что запускалось или запускается», – подчеркивает Саваневский.

Woolik скепсисом не остановить. «Своим дизайном мы уже опередили время, YouTube обновился до похожего дизайна не до, а после нас», – пишет представитель проекта.

Как считает Максим Саваневский, больше шансов у проектов, которые не будут стараться подменить собой проект Цукерберга, а создадут социально полезные сервисы. «Человек просто раз в неделю/месяц будет заходить на такой сайт, чтобы решить имеющуюся проблему», – считает эксперт.

Что такое социальные сервисы?

Такие соцсервисы в Украине тоже начинают появляться. Например, на следующей неделе планирует заявить о себе стартап Psyball.com.

«Это нечто похожее на социальную сеть для занятий спортом и активного досуга. Psyball помогает подобрать команду или партнеров для спорта рядом, организовать людей и найти место для встречи», – рассказывает основатель проекта Сергей Якимчук. Он соглашается с тезисом, что замахиваться на нишу гигантов наподобие Facebook не стоит. «Делать то же самое, но “с перламутровыми кнопками”, я смысла не вижу», – говорит стартапер.

Как рассказал Якимчук, его проект совмещает некоторые функции Facebook, Meetup, Google Maps, Booking.com. «И плюс к этому у нас есть уникальные ноу-хау из области big data. Мы умеем искать соответствие между желающими найти партнеров для спорта/тренера и организаторами встреч, которым недостает участников», – подчеркивает основатель.

Ядро команды – 4 человека, а в общей сложности к работе над проектом уже привлекалось по разным задачам около 15 человек. «Разработка распределена между Прагой, Мукачево и Киевом», – говорит Якимчук. За четыре года на проект уже потратили около $400 000. «Наша цель в Украине, чтобы при помощи Psyball организовывали свой активный досуг как минимум 2 млн людей», – делится планами стартапер.

Вместо резюме

Пока украинские социальные команды и сервисы лишь собираются покорять рынок интернет-коммуникаций, глобальные соцсети быстро его завоевывают. Так, с момента блокировки в Украине российских соцсетей количество пользователей Facebook в нашей стране выросло с 6,5 до 8,9 млн, а Instagram – с 3,7 до 6,1 млн. Зарубежные гиганты, расширив аудиторию, заметно усилили свои позиции на украинском рекламном рынке. Места для локальных проектов стало еще меньше.

(вгору)

Додаток 7

11.09.2017

Це сором! Програли всі, – соцмережі про прорив Саакашвілі

Прорив 10 вересня українсько-польського кордону у пункті пропуску «Краковець» екс-президентом Грузії, екс-головою Одеської ОДА Міхеїлом Саакашвілі сколихнув соцмережі (ZIK).

Події стали приводом для створення фотожаб і колажів, які розлітаються інтернетом.

Письменниця Ірен Роздобудько також відреагувала на вчорашні події, пов'язані із Саакашвішлі.

«…Як на мене, це ганебне шоу. Як для України – черговий скандал, який нам не на користь.

…Співчуваю тим, хто буде розгрібати всю цю кашу з громадянством, порушенням закону, зберігати реноме країни перед іншими країнами. Марудна робота. Ганебне шоу…

Ну і співчуття людям, котрі безневинно застряглі в потязі. План вдався.

А нам… своє робить», – написала Ірен Роздобудько.

Директор Інституту практичної політики Богдана Бабич у Facebook написала таке:

«Цугцванг Порошенко

Програє, якщо піде на переговори з Саакашвілі й заплющить очі на «прорив кордону». Якщо почне кримінальне переслідування всіх учасників прориву на кордоні – програє ще більше.

Не можна руйнувати правове поле, бо тоді право приймати рішення переходить в руки натовпу, суспільство радикалізується, а державні інститути втрачають легітимність».

Журналіст, редактор «Історичної правди» Вахтанг Кіпіані наголошує, що від цих подій програли всі.

«Держава програла. Програли громадяни. Програв весь політикум, який взяв участь у цих подіях, і, зокрема, «правитель слабый и лукавый». Як невимовно сумно. Бо це не ураган «Ірма». Цієї ганьби могло і не бути. Від слова взагалі. Все можна було вирішити тихо і навіть з видимістю законності від Печерського суду. І ще сумно, що у всій владі не знайшлося того, хто сказав просте слово «ні»», – йдеться у його дописі на Facebook.

Фінансовий експерт Сергій Фурса у Facebook наголошує, що людям, які допомагали Саакашвілі на кордоні, пишатися нічим.

(вгору)

Додаток 8

28.08.2017

Три месяца без «ВКонтакте»: выигравшие и проигравшие от бойкота российских соцсетей

Прошло три месяца с тех пор, как президент Петр Порошенко своим указом заблокировал ряд российских интернет-ресурсов, в число которых попали и популярные в Украине социальные сети «Одноклассники» и «ВКонтакте». Кто выиграл, а кто проиграл от социального бойкота?

По данным исследования Интернет ассоциации Украины (ИнАУ), месячный охват (ранжирование по среднедневной доле) соцсети «ВКонтакте» в Украине сократился с 68 % в мае до 35 % в июле, «Одноклассников» – с 48 % в мае до 22 % в июле. Таковы итоги трех месяцев блокирования в Украине российских интернет-ресурсов, которое было введено указом президента Украины в конце мая 2017 года (InternetUA).

«Российские сервисы и соцсети потеряли от 55 % до 65 % украинской аудитории», – констатирует руководитель практики Digital Influence агентства SPN Communication Ukraine Даниэль Лурье.

По его словам, в дальнейшем эта тенденция продолжится, несмотря на то, что большая часть украинских пользователей научилась обходить блокировки. «Кто-то сменит компьютер/телефон и не захочет вновь заниматься настройками обхода блокировок. Кто-то просто откажется от “ВКонтакте” и “Одноклассников”, заметив, что все окружение ушло из российских сетей. Причины будут разные, но аудитория продолжит отказываться от российских сетей», – прогнозирует Даниэль Лурье.

Кто в выигрыше

Если где-то убывает, то где-то непременно прибывает. Одним из главных бенефициаров закрытия российских соцсетей в Украине стал Facebook. «Аудитория Facebook за последние три месяца существенно выросла, ведь как минимум 45 % пользователей “ВКонтакте” и “Одноклассников” уже имеют там аккаунты. По данным самой соцсети, в июле ресурсом пользовались 11 млн украинцев по сравнению с около 7,5 млн в мае», – отмечает руководитель SMM & Context Department диджитал-агентства Liquid 7 Герман Севальнев.

Эксперты предполагают, что в дальнейшем рост украинской аудитории Facebook будет продолжаться и к концу этого года достигнет 12 млн пользователей.

При этом нишевые соцсети – Twitter, Instagram, Linkedin – практически не ощутили притока аудитории из Украины. «Как большинство людей про них не слышали/не пользовались, так и продолжают не пользоваться», – подчеркивает эксперт.

В то же время часть украинской аудитории начала перетекать в мессенджеры. Наибольший приток пользователей ощутили на себе Facebook Messenger, Telegram и Viber.

Последствия для бизнеса

Как и прогнозировалось экспертами ранее, крупные украинские компании практически не пострадали от запрета соцсетей. Так, часть из них, не желая рисковать, просто закрыли свои официальные аккаунты в запрещенных соцсетях и продолжили вести свои страницы на других площадках. «Крупный бизнес ничего не потерял, поскольку в основном страницы в социальных сетях

ведутся больше для имиджа компании, в отличие от малого и среднего бизнеса, где акцент делается на прямых продажах через соцсети», – отмечает руководитель проекта «Киевское публичное Агентство коммуникаций/PR» Инна Ковальчук.

В частности перераспределение трафика между социальными сетями у крупных компаний после указа президента увеличилось в пользу Facebook. Это можно проследить на примере компании Rozetka.ua, у которой ранее была самая большая среди украинских компаний группа во «ВКонтакте» (более 824 тыс. на момент закрытия, 814 тыс. – по состоянию на конец августа – ред.) Так, на момент выхода указа о блокировке соцсети около 45 % трафика из соцсетей на Rozetka.ua приходилось на «ВКонтакте», тогда как на Facebook только 21,14 %. Сейчас же соотношение составляет 48,62 % и 34,3 % в пользу детища Цукерберга. При этом страница компании во «ВКонтакте» фактически не активна, на ней только время от времени появляются призывы подписываться на страницы в других соцсетях.

Как отмечают эксперты, на данный момент прирост подписчиков страниц крупных брендов в Facebook хотя и наблюдается, однако о массовой миграции пользователей речь не идет. Так, новые пользователи Facebook не стремятся подписаться на те же страницы, что были у них во «ВКонтакте». «Они выстраивают свое медиа-окружение заново и для брендов это прекрасная возможность привлечь новых подписчиков, клиентов и потребителей. Люди готовы рассматривать новое и выбирать», – отмечает Даниэль Лурье.

Сложнее предпринимателям, особенно тем, которые занимались торговлей исключительно через соцсети. «Первый месяц был провальным для малого/среднего бизнеса, который занимался активными продажами через “ВКонтакте”. Целевая аудитория такого бизнеса в основном молодые люди до 25 лет. Параллельно предприниматели начали создавать страницы в других социальных сетях, таких как Facebook/Instagram, но быстро компенсировать потери сложно», – рассказывает Инна Ковальчук.

Нарастить аудиторию, подобную той, которая была во «ВКонтакте», за столь короткое время малому и среднему бизнесу не удалось. В частности аудитория одной из крупнейших подобных групп «Женская обувь. Сороконожка» в соцсети Facebook за три последних месяца выросла с чуть более 400 пользователей до порядка 1,6 тысяч, тогда как во «ВКонтакте» она на момент закрытия российских соцсетей превышала 170 тыс.

По мнению Инны Ковальчук, сейчас ситуация для предпринимателей несколько улучшилась. «Блокирование российских соцсетей многих заставило мыслить масштабнее и применять новые каналы сбыта своей продукции», – отмечает эксперт.

Так, примечательно, что за три месяца группа «Женская обувь. Сороконожка» продолжает активно работать во «ВКонтакте», нарастив свою аудиторию до более 200 тыс. пользователей (при этом время от времени напоминая о своей странице в Facebook), но при этом открыла несколько офлайновых точек продажи.

А что рекламодатели?

А какая же ситуация с рекламодателями? Как отметил Герман Севальнев, больше всего пострадали те рекламодатели, которые не проводили диверсификацию своей аудитории и ограничивались продвижением только в заблокированных соцсетях. Сохранить же свои позиции смогли только те бренды, которые параллельно обеспечивали свое присутствие на других площадках.

В целом же рекламодатели сейчас скорее находятся на перепутье и активно следят за тем, куда будет мигрировать аудитория. «Мы видим, что у рекламодателей еще существует непонимание, как дальше строить отношения с аудиторией в digital-среде. Куда мигрирует эта аудитория? Как работать с новыми площадками? Не всем удалось найти ответы на эти вопросы. Отсюда и массовое увеличение количества украинских рекламодателей в Facebook – происходит банальный переброс бюджетов из “ВКонтакте” и “Одноклассников”», — подчеркивает Герман Севальнев.

Все это, по мнению эксперта, приведет к большей конкуренции за внимание украинцев и, как следствие, к удорожанию контакта. По словам Даниэля Лурье, каких-либо заметных скачков рекламных ставок не наблюдалось, при этом сейчас идет сезон активной подготовки осенних рекламных кампаний. «И это ожидаемо приведет к росту рекламных цен в социальных и рекламных сетях. Но это происходит каждый год, никаких неожиданностей не будет», – добавляет Даниэль Лурье.

(вгору)

Додаток 9

30.08.2017

Франция и Германия хотят добиться более справедливых налогов от интернет-гигантов

Франция и Германия намерены подготовить совместный проект по налогообложению американских интернет-гигантов с тем, чтобы сделать более «справедливыми» выплаты таких компании, как Google, Apple, Facebook и Amazon – передает агентство France-Press со ссылкой на заявление министра финансов Франции Брюно Ле Мэра (Bruno Le Maire) (InternetUA).

На страницах соцсети Facebook он сообщил, что на следующей встрече министров финансов, которая состоится в середине сентября в Таллине, Франция совместно с Германией представит новый план по налогообложению Google, Apple, Facebook и Amazon.

«Мы предлагаем взять за точку отсчета выручку этих крупных компаний, и исходя из нее, определять уровень налогообложения. Таким образом компании будут выплачивать надлежащие суммы в казну каждой страны, где они зарабатывают деньги», – написал Ле Мэр.

В то же время министр финансов Франции отметил, что подобные предложения уже делались на уровне Евросоюза и стран Организации европейского экономического сотрудничества (ОЭСР), однако безрезультатно.

«На сегодняшний день переговоры по этому поводу застопорились», – признал Ле Мэр.

Американские интернет-гиганты подвергаются в Европе резкой критике за использование лазеек в сложных механизмах налогообложения с целью снижения выплат. В частности, компании стараются декларировать свои доходы в странах ЕС с наименьшей ставкой налога, хотя большую часть средств зарабатывают в других государствах европейского альянса.

(вгору)

Додаток 10

1.09.2017
Facebook отберет у You Tube часть рекламного «пирога»
Дмитрий Малышко

Новый сервис Watch от Facebook может отнять у You Tube большую аудиторию любителей он-лайн видео. Однако речь идет, прежде всего, о прибыли от рекламы (InternetUA).

31 августа мировая соцсеть №1 открыла новый сервис Watch и планирует, что каждый сможет добавить свое шоу для всеобщего просмотра. Таким образом, Facebook призывает помериться силами с You Tube за право получать больше прибыли от рекламы на онлайн-видео, – сообщает Fortune.

Такое решение не удивительно, ведь согласно данным компании eMarketer, занимающейся изучением цифровой коммерции, американцы тратят более 73 минут в день на просмотр видео в интернете, что на 7 % больше, чем в прошлом году. А вот время просмотра телевизора наоборот – уменьшилось на 2 % по сравнению с прошлым годом – до 244 минут в день.

Благодаря Watch, который Facebook начал тестировать еще в первых числах августа, более 2 миллиардов пользователей смогут увидеть сотни шоу от таких компаний, как Vox, Buzzfeed, Discovery Communications, ABC от Walt Disney, а также спортивные соревнования, проводимые, например Главной Бейсбольной Лигой.

Если вспомнить про украинцев, то согласно данным Opinion Software Media © – проекта медиаисследований интернет-аудитории Украины по заказу ИнАУ, в июле этого года You Tube значительно обошел Facebook как по охвату, так и средней доле посещений. Так, You Tube охватил 62 % серфирующей украинской аудитории, в то время, как Facebook – всего лишь 46 %. Средняя доля «Трубы» от посещений всех оцениваемых сайтов составила 48 %, а Фейсбука – только 31 %. Однако, творению Цукерберга есть чем гордиться – его посетили почти на 10 % больше интернет-пользователей, чем запрещенный VKontakte. Стоит отметить, что количество респондентов,

принимавших участие в исследовании – 5000. Оценивались сайты с аудиторией не менее 50 панелистов.

(вгору)

Додаток 11

8.09.2017

Отклики в соцсетях оказывают сильное влияние на психику человека

Эксперты представляющие международную исследовательскую компанию YouGov провели исследование на тему как пользователи относятся к комментариям и лайкам своих заметок и фотографий в соцсетях. Оказалось, каждый четвертый человек очень расстраивается если читает негативные отклики на свои записи (SunDayNews).

Эксперты проанализировали реакцию людей на комментарии и лайки в социальны сетях и определили, что отклики и комментарии к записям оказывают сильное влияние на весь день для 61 % людей. Для 10 % пользователей они важны крайне сильно, а остальных они почти не волнуют.

Выяснилось, что 44 % испытуемых чувствуют себя гораздо лучше, если видят положительные комментарии к своим публикациям, а 26 % признались, что плохие комментарии в прямом смысле слова могут разрушить весь день.

Психологи в свою очередь поясняют, что даже одно нелицеприятное замечание, а тем более несколько атак с критикой, с большой долей вероятности оставят неприятный осадок, несмотря даже на то, что они оставлены в цифровом виде.

Данное явление очень распространено в Сети, и оно имеет определение как онлайн-ненависть. Такое проявление агрессии наносит моральный ущерб большинству людей, поэтому следует принять меры для ограничения доступа таких людей к вашей странице.

(вгору)

Додаток 12

28.08.2017

В Facebook президента Украины нашли 1,5 тыс. «плодовитых» ботов

Боты написали каждый шестой комментарий на странице Петра Порошенко в соцсети (InternetUA).

К такому выводу пришли эксперты интернет-ресурс Voxukraine и компании TheRespo, проанализировав один из самых многочисленных аккаунтов страны.

Так, например, банальная фраза на странице президента «Поздравляю с Днем независимости Украины! Желаю мира и единства. Слава Украине!» набрала более 500 комментариев, почти 1,4 тыс. репост и 10 тыс. лайков. При

этом, 21 % комментариев под сообщением, а это 111 шт., оставлены именно ботами.

Как подсчитали эксперты, за время президентства Порошенко (с июня 2014 по май 2017 года) более 79 тыс. уникальных Facebook-пользователей написали хотя бы один комментарий на его официальной странице, сделав в совокупности около 176 тыс. сообщений. Исследования показали, что 98 % комментаторов (или 77,5 тыс.) – это реальные люди.

Однако остальные – 2 % аккаунтов, или 1,5 тыс. ботов – были значительно более продуктивными. Они оставили около 15 % от всех сообщений, а это 26 тыс. комментариев.

«То есть каждый шестой комментарий под постами президента оставлен ботами», – пишет Voxukraine.

В рамках исследования определили три группы ботов «президента»: негативные, позитивные и нейтральные.

К негативным отнесли ботов, которые агрегируют преимущественно или исключительно эмоции «злость» или «грусть». Таких 29 %. Им больше всего «понравились» сообщения Порошенко об освобождении Романа Сущенко, о транше из США и альбоме, посвященному МН-17.

Для «положительных ботов» характерна эмоция всех комментов «радость». Таких ботов 27 %. Они больше оставили комментариев под приветствием Порошенко с Днем рождения его жены, Марины. Там с 680 комментариев каждый десятый оставлен ботами. Много положительных ботов также набрал пост, в котором Порошенко выражает сочувствие и скорбь из-за гибели мужа Татьяны Чорновил. На третьем месте пост, в котором Порошенко говорит о беседе с Меркель об агрессии РФ на Донбассе.

Нейтральные боты примерно одинаково использовали в своих комментариях на странице Порошенко отрицательные и положительные эмоции. Таких ботов оказалось 44 %.

Бот – это аккаунт в соцсети, который оставляет комментарии, для дальнейшего определенного влияния на точку зрения реальных пользователей.

Боты делятся на два вида: к созданному аккаунту подсоединяется алгоритм, который оставляет заданный комментарий под заданным сообщением, или же аккаунт под определенным именем используется реальными людьми, которые получают денежное вознаграждение за комментарии от его имени под определенными сообщениями других лиц.

По стоимости предоставленных услуг боты делятся на три вида:

– Эконом-вариант. Без друзей или с их минимальным количеством.

– Спам-боты. Распространяют контент через друзей, которых у них обычно более 1 тыс.

– Хорошо замаскированные боты. Количество друзей имеет такое же распределение, как и у обычных людей – от 100-1000 друзей. Это самые дорогие и наиболее часто используемые в политических баталиях боты.

(вгору)

Додаток 13

1.09.2017

Майже всі твіти російською про НАТО у Балтії пишуть боти

Два з трьох користувачів Twitter, які пишуть російською мовою про присутність НАТО в Східній Європі – це так звані боти.

Про це йдеться у доповіді Центру стратегічних комунікацій НАТО (STRATCOM) під назвою Robotrolling (Espreso.tv).

У НАТО підрахували, що ці бот-акаунти загалом створюють 84 % російськомовних повідомлень. В англомовному просторі також існує сильна присутність росіян: кожен четвертий активний акаунт є роботом і загалом вони видають 46 % всього англомовного контенту.

З чотирьох країн – Естонія, Латвія, Литва та Польща – Естонія найчастіше є мішенню бот-повідомлень. Тоді як в Польщі та Литві спостерігали найменше діяльності автоматизованих акаунтів.

Експерти аналізували твіти, написані в період з 1 березня по 30 серпня 2017 року, в яких згадувалися НАТО та Естонія, Латвія, Литва чи Польща.

Зазначається, що переважна більшість повідомлень ботів – аполітичний спам. Загальна кількість твітів склала близько 32 тисяч, з яких кожен третій був написаний російською.

Кількість активних користувачів – 11600, з них кожен четвертий писав російською. Таким чином, російськомовні користувачі в середньому вдвічі активніші за англомовних ботів.

«На нашу думку, Twitter в російськомовному сегменті контролюється не так ефективно, як в англомовному. Незважаючи на високу присутність автоматизованої діяльності, у розглянутий період не зафіксовано масштабних скоординованих бот-кампаній», – йдеться у звіті.

Відзначається, що сплеск російськомовних повідомлень досяг максимуму в травні/на початку червня під час найбільших навчань НАТО, тоді як англомовні повідомлення активно поширювалися у березні та квітні, коли західні війська прибули до Балтії.

Російськомовний контент стосувався в основному новин про військові навчання, розгортання військ та незначні інциденти, в яких брали участь військові.

Англомовний контент більше стосувався внутрішніх та зовнішньополітичних проблем США, зокрема коментарів Дональда Трампа про Альянс і його візит до Польщі на початку липня.

(вгору)

Додаток 14

4.09.2017

Нейросеть научили писать убедительные поддельные клиентские отзывы

Разработчики из Чикагского университета обучили нейронную сеть писать убедительные и почти ничем не отличающиеся от реальных поддельные клиентские отзывы на услуги, рестораны и гостиницы (InternetUA).

Как пишет The Verge, искусственный интеллект не копирует уже существующие отзывы, а самостоятельно пишет рецензии на основе миллионов существующих в Сети мнений клиентов, оставленных на сервисах Amazon, Yelp и TripAdvisor.

В октябре 2017 года новая разработка будет представлена на ежегодной международной конференции по компьютерной и информационной безопасности.

Один из создателей проекта Бен Джао заявил, что тексты, созданные искусственным интеллектом, уже сейчас практически не отличимы от реальных, написанных человеком. А в дальнейшем подобная технология сможет создавать не только отзывы и рецензии, но и вообще любые тексты, !серьезно изменив нашу уверенность в том, что реально, а что нет!.

Таким образом, отзывы на Yelp и Amazon, созданные искусственным интеллектом, могут стать началом новой «фейковой эры» в Сети вкупе с разработками специалистов Вашингтонского университета, которые на примере фейкового видео с Бараком Обамой показали возможности нейросети превращать аудиозаписи голосов в реалистичное видео, совмещая движения губ говорящего с произносимым текстом. К примеру, эти технологии могут легко фальсифицировать видео выступлений политиков, стать причиной политических и экономических кризисов.

(вгору)

Додаток 15

5.09.2017

Национальный научный фонд США выдал грант на создание технологии, распознающей фейковые новости в Сети

Национальный научный фонд США, независимое федеральное агентство при американском правительстве, созданное конгрессом еще в 1950 году «для развития научных исследований, национального здравоохранения, благосостояния и для обеспечения национальной обороны», выдал грант на создание технологии, которая должна позволить цифровым устройствам распознавать в Сети фейковые новости (InternetUA).

Финансирование в размере 300 тысяч долларов на разработку получили два преподавателя Государственного университета Пенсильвании, который уже вплотную занимается этой проблемой.

Профессор информатики Донгун Ли и профессор кафедры информационно-коммуникационных технологий Шьям Сундар отмечают, что поддельные новости существуют уже долгие десятилетия, однако развитие интернета и социальных сетей упростило их распространение, превратив в опасный инструмент влияния на общественное мнение.

Ученые планируют исследовать «характерные индикаторы поддельных новостей» и предложить математическое решение, которое позволит цифровым устройствам распознавать эти индикаторы, передает Yahoo News со ссылкой на AP.

Отметим, специалисты систем компьютерной безопасности относят фейковые новости к одной из самых серьезных киберугроз. Постоянно растущее число поддельных новостей в соцсетях создают угрозу усиления киберпропаганды.

Появление в Сети ложных новостей и их влияние на мнение читателей стало отчасти причиной исхода голосования на президентских выборах в США, приведших к победе Дональда Трампа.

Активно бороться с фейковыми публикациями призывают главы высокотехнологичных компаний и правительства разных стран. Разработкой инструментов, применение которых позволило бы снизить количество таких новостей, уже занимаются многие крупные корпорации.

Facebook в конце 2016 года запустила в США механизм, который позволяет сторонним организациям по жалобам пользователей проверять достоверность информации, содержащейся в подозрительных публикациях. Позднее этот инструмент был запущен в предвыборный период в Германии и Франции.

В середине января в США был анонсирован проект под названием Facebook Journalism Project, включающий в себя три основных направления: сотрудничество со СМИ в области разработки новых продуктов и форматов, обучение журналистов работе с сервисами и инструментами Facebook, а также повышение новостной грамотности пользователей соцсети.

Сервис микроблогов Twitter намерен внедрить функцию, которая позволит пользователям помечать твиты, которые, по их мнению, содержат ложную или опасную информацию.

В последнее время обвинения в распространении подложных новостей все чаще адресованы России. Спецкомитеты по разведке в сенате и палате представителей конгресса США, которые ведут разбирательства в отношении попыток российских властей повлиять на выборы американского президента в 2016 году, обратились в Facebook с требованием раскрыть информацию о том, сотрудничал ли предвыборный штаб Трампа с представителями РФ с целью публикации в соцсети недостоверных новостей, которые могли способствовать победе республиканца на выборах. Москву же обвинили в том, что она стояла за публикацией в интернете новостей, порочащих репутацию кандидата в президенты и экс-госсекретаря Хиллари Клинтон.

Во Франции новый президент Республики Эммануэль Макрон во время совместной пресс-конференции по итогам переговоров с президентом России Владимиром Путиным, состоявшейся в мае этого года, назвал российский телеканал Russia Today и информационное агентство Sputnik «органами лживой пропаганды», обвинив их в распространении во Франции ложной информации и клеветы.

Спецслужбы Германии, где в сентябре предстоят выборы в парламент страны (Бундестаг), предупреждают об опасности кибератак со стороны российских хакеров и массовой пропаганды в Сети в интересах РФ. В июне коалиция нынешнего канцлера ФРГ Ангелы Меркель провела через парламент «Акт о соблюдении правопорядка сетями», согласно которому соцсети будут штрафовать не менее чем на 50 млн долларов, если они не удалят немедленно «незаконный контент», под который подпадают пропаганда и фейковые сообщения.

В Евросоюзе уже создано ведомство по опровержению фейковых новостей и российской пропаганды. В Чехии учреждено полицейское агентство, которое прочесывает соцсети в поисках дезинформации и других «гибридных угроз».

Министры обороны Швеции и Дании Петер Хультквист и Клаус Йорт Фредериксен заявили о необходимости стран Евросоюза совместно противостоять российской пропаганде в Сети, отметив, что так называемая гибридная война включает в себя не только кибератаки, но и распространение дезинформации и фейковых новостей, влияющих на мнение общества.

Все эти шаги указывают на серьезные опасения, что инструменты политического саботажа настолько усовершенствовались, что могут стать угрозой для западных демократий.

(вгору)

Додаток 16

28.08.2017

СБУ задержала сепаратистов из соцсетей «ВКонтакте» и «Одноклассники»

Сотрудники Службы безопасности Украины в течение августа прекратили деятельность нескольких администраторов, которые поддерживали антиукраинские сообщества в запрещенных в Украине социальных сетях «ВКонтакте» и «Одноклассники» (InternetUA).

Об этом сообщает Украинская правда со ссылкой на пресс-службу СБУ.

По данным правоохранителей, пропагандисты работали в девяти областях Украины – в Киевской, Львовской, Черкасской, Хмельницкой, Харьковской, Черниговской, Ивано-Франковской, Днепропетровской и Сумской областях. Сейчас все они задержаны.

Одного из них задержали на столичном железнодорожном вокзале, во время возвращения из очередного инструктажа в Москве. Оперативники спецслужбы установили, что это был житель города Ватутино, Черкасской области. На собственных страницах в соцсетях он распространял антиукраинские материалы.

Кроме того, в Киеве так называемый пресс-секретарь и активный участник антиукраинской сепаратистской организации создал ряд ресурсов в

соцсетях. Там он призывал к свержению государственного строя и продвигал идеи для создания так называемой «новороссии».

Подобные действия совершали и другие пропагандисты на своих антиукраинских ресурсах. Они создавали десятки веб-страниц и сообществ в соцсетях и активно распространяли украино-ненавистнические и сепаратистские материалы.

Например, пропагандист из Хмельницкой, руководствуясь указаниями координаторов из России, распространял призывы к свержению государственного строя в стране, оправдывал агрессию РФ и преступные действия террористических формирований ЛНР / ДНР. В одной из групп он разместил фото погибших и раненых участников АТО с циничными комментариями.

Оперативники СБ Украины задокументировали, что агитаторы получили задание от российских спецслужб активизировать антиукраинскую пропаганду как раз накануне Дня Независимости.

«Основной задачей кремлевских информационных наемников было создание картинки неприятия центральной власти в нескольких регионах страны. Злоумышленники, по указанию российских кураторов, в частности, публиковали призывы к свержению конституционного строя, государственной власти и нарушения территориальной целостности в стране», – говорится в сообщении СБУ.

Во время обысков изъяты компьютеры и мобильные телефоны пропагандистов с доказательствами получения заданий от российских кураторов и размещения антиукраинских материалов.

По выявленным фактам открыт ряд уголовных производств по ст. 109 (действия, направленные на насильственное изменение или свержение конституционного строя или на захват государственной власти), ст. 110 (посягательство на территориальную целостность и неприкосновенность Украины), 258-3 (создание террористической группы или террористической организации) и ст. 436-1 (изготовление, распространение коммунистической, нацистской символики и пропаганда коммунистического и национал-социалистического (нацистского) тоталитарных режимов) Уголовного кодекса Украины.

Продолжается досудебное следствие.

(вгору)

Додаток 17

29.08.2017

В Китае запретили анонимность в Интернете

В преддверии 19-го съезда компартии Китай ужесточил правила пользования Интернетом, введя обязательную регистрацию реальных имен пользователей у провайдеров. Анонимные посты на форумах и других ресурсах будут удаляться интернет-цензурой (InternetUA).

Новые правила

В Китае утверждены новые правила пользования интернетом, направленные на борьбу с анонимными сообщениями, которые пользователи оставляют на форумах и других площадках. С 1 октября 2017 г. все такие сообщения будут удаляться государственной интернет-цензурой. Выполнение нормы обеспечит Администрация киберпространства Китая.

По новым правилам, провайдеры интернета и сервисов обязаны запрашивать и верифицировать реальные имена пользователей в процессе регистрации. В том случае, если пользователь размещает какой-либо незаконный контент, компания должна сообщить об этом властям.

Ужесточение правил использования интернета связано с тем, что осенью в Китае должен состояться 19-й Национальный конгресс Коммунистической партии, на котором ожидается назначение новых людей на некоторые ключевые должности, пишет ресурс TechCrunch. В связи с этим, крупные китайские интернет-компании, в том числе Baidu, Alibaba и Tencent, находятся сейчас под большим давлением со стороны правительства.

Напомним, в Южной Корее система регистрации реальных имен пользователей для сайтов с аудиторией более 100 тыс. человек в день была введена в 2007 г., а в 2009 г. были запрещены анонимные посты. В 2012 г. корейский суд признал эту систему противоречащей конституции в той части, которая гарантирует свободу слова.

Какой контент считается незаконным

Сообщив об утверждении новых норм, Администрация киберпространства Китая одновременно напомнила, какой контент считается в стране незаконным. Согласно статье 15 Правил администрирования информационных служб интернета, поставщики интернет-услуг не должны создавать, воспроизводить, публиковать или распространять контент, который содержит противодействие основным принципам конституции, подвергает опасности национальную безопасность или наносит ущерб национальной чести и интересам.

Также запрещено размещать материалы, которые подстрекают национальную ненависть, этническую дискриминацию и подрывают национальное единство, или же подрывают национальную религиозную политику и пропагандируют культы. Кроме того, в интернете запрещено распространение слухов, нарушение общественного порядка и разрушение социальной стабильности, равно как и распространение порнографии, пропаганда азартных игр, насилия, убийства, террора или подстрекательство к преступлению. Запрещено также оскорбление или клевета на других лиц и ущемление их достоинства.

Запрет VPN

В июле 2017 г. стало известно, что китайское правительство приказало всем телеком-провайдерам страны заблокировать пользователям доступ к виртуальным частным сетям (VPN). Распоряжение должно быть выполнено до 1 февраля 2018 г. После этого китайские пользователи не смогут посещать

через VPN иностранные ресурсы, заблокированные на территории Китая. В настоящий момент VPN используются в стране как лазейка в «Великом китайском файерволе» – системе блокировки зарубежных сайтов, начиная от соцсетей вроде Twitter и Facebook и заканчивая новостными изданиями типа New York Times.

Через несколько дней власти Китая заявили, что не собираются закрывать те VPN-сервисы, которые прошли государственную регистрацию. VPN будут доступны в первую очередь мультинациональным компаниям, работающим в Китае.

Чтобы взять под контроль использование VPN на мобильных устройствах, в Китае с начала 2017 г. была введена обязательная регистрация SIM-карт, с присвоением каждой собственного идентификационного номера. С помощью этой системы можно отследить использование VPN на смартфонах, удаленно заблокировать SIM-карту или вызвать пользователя в полицию, где его обяжут удалить VPN-приложение.

Проект «Золотой щит»

Проект «Золотой щит», неофициально известный как «Великий китайский файервол», начал действовать в 2003 г. В рамках проекта была создана система специальных серверов между китайскими провайдерами и глобальными сетями. Этот «щит» блокирует доступ к ряду иностранных ресурсов, а также не дает китайским сайтам ссылаться на зарубежные источники без предварительного разрешения. Также «щит» проводит фильтрацию иностранного контента по ключевым словам, относящимся к сфере госбезопасности.

«Золотой щит» является частью усилий председателя Си Цзиньпина (Xi Jinping) по установлению «киберсуверенитета» Китая. Той же цели служит «расплывчатый» закон о кибербезопасности, принятый в ноябре 2016 г., который обязывает интернет-провайдеров сотрудничать с правительством в расследовании преступлений и дел, относящихся к национальной безопасности. Также закон вводит обязательное тестирование и сертификацию ИТ-оборудования и дает властям неограниченный доступ к данным компаний, попавших под подозрение.

Кроме того, закон ввел ограничение на хранение данных за рубежом: любая информация о китайских гражданах, собранная внутри Китая, должна храниться на его территории. На хранение данных за рубежом требуется специальное разрешение. Закон вступил в силу 1 июня 2017 г.

(вгору)

Додаток 18

31.08.2017

Порошенко ввів у дію рішення РНБО щодо кардинального посилення заходів кібербезпеки держави

Президент Петро Порошенко підписав Указ №254/2017, яким увів у дію рішення Ради національної безпеки і оборони України від 10 липня 2017 року щодо суттєвого посилення заходів кібербезпеки держави (Watcher).

Згідно з Указом, Уряд у тримісячний строк має врегулювати питання щодо заборони державним органам та підприємствам державної форми власності закуповувати послуги з доступу до Інтернету у операторів телекомунікацій, у яких відсутні документи про підтвердження відповідності системи захисту інформації встановленим вимогам у сфері захисту інформації.

Також Кабінет міністрів має запровадити в рамках розвитку державно-приватного партнерства механізм залучення фізичних і юридичних осіб на умовах аутсорсингу до виконання завдань кіберзахисту державних електронних інформаційних ресурсів.

СБУ має підготувати та подати на розгляд парламенту законопроект щодо розмежування кримінальної відповідальності за злочини у сфері використання комп'ютерів і комп'ютерних мереж, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідного розмежування підслідності.

Держспецзв'язку разом із Нацполіцією мають невідкладно активізувати співпрацю із зарубіжними партнерами щодо протидії кібератакам на критичну інформаційну інфраструктуру, проведення розслідувань таких кібератак, установлення причин і умов, що сприяли їх вчиненню, а також щодо залучення міжнародної технічної допомоги для забезпечення кіберзахисту державних електронних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури.

Протягом 2017 року Уряд має забезпечити фінансування видатків на проектування захищеного центру обробки даних для розміщення державних електронних інформаційних ресурсів; вжити заходів щодо створення Національного центру оперативно-технічного управління мережами телекомунікацій України та забезпечення його функціонування; забезпечити безумовне виконання державними органами законодавства у сфері технічного захисту інформації, а також оперативно реагувати в установленому порядку на виявлені порушення.

Також рекомендовано НБУ за участю Держспецзв'язку та СБУ невідкладно вжити заходів, спрямованих на удосконалення кіберзахисту системно важливих банків України.

Уряд також повинен опрацювати питання щодо визначення Держспецзвя'зку органом, відповідальним за збереження резервних копій інформації та відомостей державних електронних інформресурсів, а також щодо встановлення порядку передачі, збереження і доступу до цих копій.

(вгору)

Додаток 19

3.09.2017

Спецслужби Росії намагаються стежити за користувачами соцмереж
Олена Матусова

Російські спецслужби посилюють контроль над Інтернетом. Незабаром вони можуть отримати усі особисті дані на користувачів мереж «ВКонтакте», «Одноклассники» та інших, які вирішили залишитися працювати в Росії. Відповідний наказ розробляє Міністерство комунікацій та зв'язку Росії. Посилення контролю над користувачами Інтернету відбулося вже невдовзі після того, як українська Рада національної безпеки і оборони фактично заборонила роботу в Україні популярних російських соціальних мереж. Попри це, згідно з одним з опитувань, третина українських користувачів, продовжує ними користуватися (PRportal).

Російські чиновники розробили і подали на громадське обговорення проект наказу, в якому вказується, які дані інтернет-сервіси повинні передавати до ФСБ Росії в рамках проведення оперативно-розшукових заходів. Наказ описує вимоги до програмно-технічних засобів і обладнання, які повинні будуть встановити «організатори поширення інформації», що увійшли до спеціального реєстру.

Список даних про користувачів таких мереж, як «ВКонтакте», «Одноклассники», «Яндекс», Rambler, Mail.ru, Snapchat, Telegram та інших популярних російських соцмереж вражає: вони будуть мусити встановити тотальне стеження за своїми користувачами.

До розпорядження спецслужб надійдуть всі особисті дані – псевдонім та справжнє ім'я, паспортні, дані, адреса, імена друзів та родичів, все листування в мережі, і так далі.

Нічого неможливого

Заступник головного редактора сайту «Агентура.ру» і співавтор книги «Битва за рунет» Ірина Бороган вважає, що запропонований проект наказу набуде чинності.

«Це проект наказу Мінзв'язку, який поки ще не ухвалений, але, напевно, буде ухвалений, і він стосується того, що організатор поширення інформації – це всі соцмережі, можуть бути будь-які сайти, месенджери й інше, повинні забезпечити для російських правоохоронних органів і спецслужб можливість на перехоплення інформації і її зберігання протягом півроку або метаданих до одного року. Це означає, що все, що передається – відео, розмови, чати, всі комунікації, які йдуть через соціальні мережі, сайти, месенджери, форуми, всі ті, кого вважають за законом організаторами поширення інформації – все це повинно перехоплюватися за допомогою засобів легального перехоплення. У Росії це так званий СОРМ», – каже Бороган.

Пакет Ярової

Проект наказу російського Мінкомзв'язку підготовлений в рамках виконання антитерористичного закону, більш відомого як «пакет Ярової». У чинній редакції «закон Ярової» з 1 липня 2018 року зобов'язує інтернет-компанії зберігати інформацію про факти прийому і передачі даних не менше

від одного року, а операторів зв'язку – три роки. Зміст повідомлень, включаючи текст, голос і відео, компанії повинні будуть зберігати до шести місяців.

Закон Ярової, який має офіційну назву «Про внесення змін до Кримінального кодексу Росії і Кримінально-процесуальний кодекс Росії в частині встановлення додаткових заходів протидії тероризму і забезпечення громадської безпеки» викликав чимало критики і пересічних громадян, і фахівців у сфері зв'язку, але втілюється в життя.

Вимоги або побажання

На думку інтернет-експерта, журналіста Олександра Плющева, далеко не всі пропозиції доходять до ухвалених документів, тож ініціатива Мінзв'язку може бути ще одним непрацюючим законом.

«Справа в тому, що це поки вимоги ФСБ або, скажімо так, побажання ФСБ до нового законодавства, яке ще не ухвалено. В якому вигляді це законодавство дійде до готових законів, в якому вигляді ці побажання дійдуть до готових законів, які в результаті ухвалить Держдума, Рада Федерації і підпише президент, досить важко сказати. Як правило, судячи з практики, найодіозніші якісь положення відкидаються ще на першому читанні, потім ще щось, і в результаті дуже неприємний зазвичай закон, але не такий страшний, який був спочатку. З іншого боку, не зовсім зрозуміло, яким чином це буде здійснюватися. Швидше за все, це ще один непрацюючий закон», зазначив експерт.

Контроль без контролю

Останнім часом російська держава і спецслужби під будь-яким приводом все більше втручаються в життя громадян. Неможливість суспільства контролювати цей процес, на думку Ірини Бороган, є однією з головних проблем.

«У Росії суспільство і навіть парламент не мають ніякої можливості контролювати спецслужби. Немає ніякої можливості контролювати ось це легальне перехоплення. Формально спецслужби зобов'язані отримувати ордер в суді, що вони, я так вважаю, і роблять, – на прослуховування і на перехоплення будь-якої інформації. Але оскільки ця процедура секретна, вона не контролюється ніким, крім вищого начальника, того офіцера, який отримує цей ордер, то ми не маємо уявлення, як вони використовують цю можливість. Формально офіцерська служба, яка займається перехопленням, має можливість зі свого пульта, зі свого комп'ютера перехопити всю цю інформацію, яку я перерахувала без ордера, з ордером, як завгодно. Ми цього не знаємо. Ми не можемо це контролювати, тому що важелів контролю немає. Вони не передбачені російським законодавством ніяк», – зауважує Ірина Бороган.

Заборона не перешкода

Президент України Петро Порошенко в травні підписав указ про блокування на Україні найбільших російських інтернет-ресурсів. Після запровадження заборони українська аудиторія російських сайтів скоротилася на 50-60 %, але зараз почала компенсувати втрати. Олександр Плющев вважає, що в сучасних умовах для інтернет-аудиторії заборона – це не перешкода для

користувачів. І якогось вражаючого падіння відвідання російських сайтів помічено не було.

«Напевно, якоїсь шкоди їм було завдано, особливо в перші дні і тижні дії цієї заборони, – каже він. – "Яндекс" називав цифру, якщо не помиляюся, мінус 25 % українського трафіку. Але, по-перше, з часом і самі соцмережі і сайти навчилися надавати своїм користувачам можливості обходу навіть без втручання з їхнього боку. Також самі користувачі швидко опановують інструменти типу VPN, анонімайзерів або спеціальних інших сервісів і в результаті втрати можна оцінювати максимум в 15 відсотків українського трафіку. Але треба розуміти, що український трафік для російських соцмереж дійсно, має потужну складову, з одного боку. А з іншого боку, все-таки його не зрівняти з російським, якщо враховувати ще й закордонний. Ця частка не така вже й велика, хоча абсолютне число цього трафіку, напевно, може бути, вражаючим».

Заборона на російські сайти і соцмережі в Україні випередила проект наказу Мінкомзв'язку Росії на кілька місяців. На думку інтернет-експерта Олександра Плющева, навіть якби російські сайти продовжували працювати на території України, особистим даним користувачів все одно б нічого не загрожувало, бо, на його думку, наказ буде ухвалений у набагато м'якшому вигляді, ніж він запропонований.

Тим часом в рейтингах 10 топовий сайтів, які відвідують українські користувачі, не залишилось жодного російського. Перші три рядки займають Google, YouTube та Facebook.

(вгору)

Додаток 20

5.09.2017

Кибербезопасность или диктатура: что сулит нам Указ Президента

Владимир Кондрашов

На прошлой неделе был опубликован Указ Президента Украины, которым Петр Порошенко ввел в действие решение СНБО по укреплению кибербезопасности государства.

Документ активно обсуждается в телекомсообществе и отзывы на него, мягко говоря, неоднозначные (InternetUA).

– По сути, это некая «дорожная карта», список дальнейших действий в сфере кибербезопасности для ряда госструктур, – комментирует заместитель Главы правления ИнАУ Николай Крылов.

InternetUA разбирался в нюансах президентского Указа.

Пути решения от Президента

В «дорожной карте» регулируется ряд вопросов киберзащиты – обозначаются основные шаги и назначаются ответственные за их проработку и исполнение.

Партнер практики TMT АО «Юскутум» Юрий Котляров считает, что активность государства в сфере кибербезопасности в текущих условиях является логичной и ожидаемой:

– Решение СНБО Украины, по сути, определяет направления, в которых со стороны КМУ, регулятора и других органов будут разработаны соответствующие механизмы. И такие механизмы, безусловно, не должны противоречить действующим законам, – считает Котляров.

По словам юриста, фактически, уже сейчас можно говорить о четких тенденциях:

– Государство пытается усилить борьбу с уязвимостями и защиту информации прежде всего в государственном секторе, что является адекватной мерой;

– Для достижения этой цели распределяются ключевые роли между государственными органами;

– Государство усиливает функцию мониторинга информационных ресурсов и стремится повысить технические возможности для реализации блокировки (ограничения) доступа к информационным ресурсам.

Последняя тенденция, говорит Котляров, – одна из болезненных тем для общества.

Детальный разбор подписанного Президентом Указа на своей странице в Facebook опубликовал Глава Правления Интернет Ассоциации Украины Александр Федиенко, подчеркнув, что это исключительно его мнение, а не позиция ИнАУ.

Предоставьте справку

Согласно Указу Правительство в трехмесячный срок должно урегулировать вопрос о запрете государственным органам, предприятиям, учреждениям и организациям государственной формы собственности закупать услуги (заключать договоры) по доступу к сети Интернет у операторов (провайдеров) телекоммуникаций, в которых отсутствуют документы о подтверждении соответствия системы защиты информации установленным требованиям в области защиты информации.

– То есть, речь идет именно о государственном учреждении, на которое будет распространяться действие Закона о защите информации в информационно-телекоммуникационных системах, – комментирует Указ Александр Федиенко. – Таким образом, я могу сделать вывод, что если речь идет о государственном учреждении, что является владельцем системы, в которой обрабатываются государственные информационные ресурсы или информация с ограниченным доступом, то в дальнейшем доступ такого учреждения в сети Интернет осуществляются в соответствии с требованиями в области защиты информации.

Александр Павлович считает, что первоочередное, что нужно сделать, – это донести до государственных органов, предприятий, и учреждений: если они не являются производителями, распорядителями и владельцами систем, которые обрабатывают / производят государственные информационные

ресурсы, или информацию с ограниченным доступом, то такие предприятия могут и дальше пользоваться услугами своих операторов/провайдеров по доступу к сети Интернет.

Уже сейчас непонимание особенностей Указа в некоторых моментах доходит до абсурда.

– Некоторые руководители школ звонили операторам и требовали от них уже справки о наличии соответствующего документа по защите их сетей, ссылаясь на указ Президента, – пишет Федиенко. – Я скажу больше: то, что мне говорили операторы, имеет все признаки будущей коррупции. Эти «государственные» дельцы, намекают оператору, что другие операторы уже пообещали, что они такую справку сделают, и «поэтому мы к ним переключимся, но если вы сделаете нам дешевле и справку, то мы подумаем, чтобы остаться с вами».

Навязывание цен

Возникают вопросы и по поводу цен на услуги доступа к Интернет, которые будут предоставляться госструктурам. Как только оператор начинает работать согласно действующих нормативно-правовых актов, он тут же подпадает под действие регуляторного акта относительно стоимости Интернет-услуг, считает Александр Федиенко.

В таком случае, согласно с третьим пунктом «Предельных тарифов на услуги конфиденциальной связи», стоимость предоставления услуги безлимитного защищенного доступа к сети Интернет на скорости 1 Мб/с будет составлять 286,71 грн, на скорости 50 Мб/с – более 7 тысяч гривен, а от за скорость от 100 Мб/с – от 11 тысяч гривен в месяц.

– Вопрос цен для государственных структур теперь будет регулироваться. Это важный момент, ведь тогда уходит понятие «рыночной цены» и цены просто навяжут, – уточнил Александр Павлович в комментарии для нашего издания. – Кроме того, такие цены создадут дополнительную финансовую нагрузку на госпредприятия и бюджет.

Украинский СОРМ-3/Ревизор

Одним из пунктов Указа Президента, о котором в пресс-службе Главы Государства забыли упомянуть, дается указание Администрации Государственной службы специальной связи и защиты информации Украины вместе с СБУ разработать в месячный срок требования к техническим средствам, применяемым для мониторинга блокировки (ограничения) доступа к информационным ресурсам и / или информационным сервисам. Администрация Госспецсвязи вместе с СБУ также должны провести расчеты по потребности в таких средствах и в установленном порядке внести предложения относительно финансирования их закупки.

– Государство продолжает свой путь к будущему контролю и цензуре в сети интернет, вроде российского СОРМ-3 /Ревизор, – считает Федиенко.

Напомним, российский комплекс СОРМ-3/Ревизор фактически является инструментом цензуры и слежки за пользователями в сети Интернет. «Ревизор» в автоматическом режиме проверяет операторов связи на предмет блокировки

сайтов, внесенных в реестр запрещенных ресурсов Роскомнадзора, а СОРМ-3 собирает данные о пользователях интернет-коммуникаций и позволяет хранить полную запись трафика сетевых взаимодействий за определенный период.

«Нецарское дело»?

В общем и целом, несмотря на коррупционные риски и вопросы цензуры, операторы и провайдеры, хотят они того или нет, выполнят президентский Указ. Но, считает Александр Федиенко, правильнее было бы иметь в фундаменте закон.

– Я не могу понять, почему этими вопросами в виде указов президента занимается президент, а не занимаются соответствующие профильные учреждения, не принимаются профильные законы депутатами, не отслеживается тот пласт действующего законодательства, который даже на уровне терминов уже невозможно между собой связать, – пишет Федиенко.

Александр Федиенко также отмечает, что «эта слойка-пирог, постановлений, указов, законов и т.д.» плохо коррелируются между собой, как по срокам, так даже и по существующим названиям некоторых государственных учреждений.

– Это все нужно объединить в новом законе об электронных коммуникациях и кибербезопасности, что, кстати, было бы логичным. На мой взгляд, для того мы и выбирали депутатов и нанимали чиновников на наши налоги, – считает Александр Павлович. – Существует и второй вариант, который уже стал нормой в нашем государстве, – через указ президента как-то совместить (указы, законы, постановления и т.д. – В.К.) хотя бы в терминах и институтах.

(вгору)

Додаток 21

28.08.2017

Dr.Web первым обнаружил загрузчик троянца для «умных» Linux-устройств

Ассортимент современных вредоносных программ для устройств под управлением Linux чрезвычайно широк (ITnews).

Одним из широко распространенных троянцев для данной ОС является Linux.Hajime, несколько загрузчиков детектировал только Антивирус Dr.Web.

Троянцы семейства Linux.Hajime известны вирусным аналитикам с конца 2016 года. Это сетевые черви для Linux, распространяющиеся с использованием протокола Telnet. После успешной авторизации путем подбора пароля плагин-инфектор сохраняет на устройство хранящийся в нем загрузчик, написанный на ассемблере. С компьютера, с которого осуществлялась атака, тот загружает основной модуль троянца. В свою очередь вредоносная программа включает инфицированное устройство в децентрализованный P2P-ботнет. Linux.Hajime способен заражать объекты с аппаратной архитектурой ARM, MIPS и MIPSEL.

Помимо вредоносного загрузчика для ARM-устройств в «дикой природе» уже более полугода распространяются аналогичные по своим функциям модули для устройств с архитектурой MIPS и MIPSEL. Первый из них получил наименование Linux.DownLoader.506, второй – Linux.DownLoader.356. На момент подготовки этой статьи они оба детектировались только продуктами Dr.Web. Кроме того, вирусные аналитики «Доктор Веб» установили, что помимо использования троянцев-загрузчиков злоумышленники осуществляют заражение и при помощи стандартных утилит, например, скачивают Linux.Hajime посредством wget. А начиная с 11 июля 2017 года киберпреступники стали загружать троянца на атакуемое устройство с помощью утилиты tftp.

Собранная специалистами «Доктор Веб» статистика показывает, что на первом месте среди стран, к которым относятся IP-адреса зараженных Linux.Hajime устройств, находится Мексика. Также в тройку входят Турция и Бразилия.

Компания «Доктор Веб» напоминает: одним из наиболее надежных способов предотвращения атак на Linux-устройства является своевременная смена установленных по умолчанию логина и пароля. Кроме того, рекомендуется ограничивать возможность подключения к устройству извне по протоколам Telnet и SSH и своевременно обновлять прошивку. Антивирус Dr.Web для Linux определяет и удаляет все упомянутые версии загрузчиков Linux.Hajime, а также позволяет выполнить дистанционное сканирование устройств.

(вгору)

Додаток 22

28.08.2017

Кому вы нужны. Как мошенники используют слитые базы данных и информацию о вас из соцсетей

Сегодня трудно представить человека, который бы не пользовался социальными сетями. Однако зачастую открытого профиля достаточно, чтобы стать добычей ловцов данных и жертвой навязчивого внимания такси. Нарушение правил использования персональных данных для Украины – обычное дело. Государство не спешит защищать приватность своих граждан.

В самый неподходящий момент из телефона раздаётся писк – пришла СМС с предложением воспользоваться услугами очередной службы такси. Через час всё повторяется, но теперь предлагают купить шубу на распродаже в непонятном магазине. Не успели вы успокоиться, как Viber оповещает о месте, в котором можно недорого приобрести натяжные потолки (InternetUA).

У большинства украинцев получение нежелательных сообщений с рекламой вызывает негодование. Однако юристы говорят, что в этом случае человек может пенять только на себя. «Для успешной защиты своих персональных данных их надо самому надёжно хранить – только тогда в случае

их разглашения и/или несанкционированного использования третьими лицами у вас будет возможность не только наказать нарушителя, но и получить компенсацию за “неудобство”, – говорит юрист компании «Ильяшев и Партнёры» Ирина Кириченко.

На острие ножа

Сегодня трудно представить человека, который бы не пользовался социальными сетями. Однако зачастую открытого профиля достаточно, чтобы стать добычей ловцов данных и жертвой навязчивого внимания такси.

Специалисты по массовым рассылкам используют специальные сканирующие программы – парсеры, которые шерстят социальные сети на предмет наличия подходящей целевой аудитории. «С помощью такой программы можно прицельно собирать информацию. К примеру, меня интересуют люди 1990–1995 годов рождения, проживающие в Киеве и имеющие доступный номер телефона. Информация автоматически собирается, и формируется база данных», – говорит SMM-эксперт Роман Русанов.

Но такие базы «открытых» данных далеко не всегда используются для вполне безобидных рекламных рассылок. В Нацполиции говорят, что хоть и реже, чем в 2013–2015 годах, но и сегодня бывают случаи, когда звонят людям и говорят, что, к примеру, их ребёнок напал на полицейского и тот находится в реанимации, поэтому срочно нужны деньги на лечение. Иначе, мол, сына посадят за убийство. «Такие данные в большинстве случаев собираются мошенниками по пересечениям слитых баз данных социальных сетей (например, VK за 2014 год) и самих страничек социальных сетей с данными родственников, которые очень распространены в даркнете», – рассказывает руководитель киберполиции Сергей Демедюк.

3 млн записей с личными данными людей злоумышленники крадут каждый день по всему миру.

Часто промышляют таким «хулиганством», по словам Демедюка, заключённые или же недавно освободившиеся. Нередко подобные звонки поступают с территории ОРДЛО.

Помимо этого, сбором и последующей продажей баз данных зачастую подрабатывают вполне пристойные ресурсы, например, поисковики дешёвых билетов. «Вы оставляете минимальные данные о себе, к примеру, e-mail, телефон, делаете какие-то действия внутри сайта. Система запоминает, чем вы интересуетесь», – поясняет, как это работает, Роман Русанов и добавляет, что таким образом к данным, оставленным клиентом, прибавляется описание его профиля.

Такие базы данных интересны в первую очередь для рекламных целей, в частности для точечной таргетированной рекламы. Спрос на услуги специалистов, которые занимаются обработкой больших массивов данных, достаточно большой. Одна из самых востребованных и хорошо оплачиваемых профессий – аналитик bigdata, зарплата таких специалистов на украинском рынке начинается от $1 тыс.

Для компаний же, ориентированных на массовые рассылки, есть вполне легальные сервисы от мобильных операторов. Стоимость одного СМС-сообщения в таких программах около 20 копеек. Как неоднократно поясняли мобильные операторы, если клиент им напрямую не запретил присылать рекламные СМС, у них нет оснований прекращать рассылку. Впрочем, как показывает практика, даже в случае обращения клиента операторы закрывают рассылки крайне неохотно.

Нелегальные добытчики

Впрочем, можно найти и немало примеров откровенно незаконного использования персонализированной информации. Наиболее часто «сливают» информацию о клиентах медики. «К врачам скорой помощи регулярно подходят сотрудники похоронных бюро, оставляют визитки и просят сообщать им телефоны и имена родственников умерших на вызове пациентов», – на условиях анонимности рассказывает один из врачей столичной скорой. Как поясняет наш собеседник, в случае смерти близкого родственники дезориентированы. Поэтому обычно соглашаются на услуги первого же позвонившего им агента. Именно врачи скорой и патологоанатомы в моргах сообщают о большей части клиентов в похоронные бюро. Среди ритуальных агентств конкуренция за лояльность медиков достаточно высока.

Врачу за помощь в поиске клиентов дают около 200 грн. Немного, но при нищенских зарплатах украинских врачей неплохое подспорье к жалованью. По словам нашего собеседника, точно такая же ситуация и в моргах. Только «ставки» у патологоанатомов выше. Естественно, официально передача телефонов третьим лицам запрещена, но наш визави не помнит случаев, чтобы из-за этого у него или его коллег возникали проблемы.

Кроме того, как поясняет врач одной из киевских больниц, в некоторых случаях персонал передаёт посредникам контакты пациентов, нуждающихся в незарегистрированных в стране лекарствах, которые можно купить только на чёрном рынке.

По частоте злоупотреблений использования персональных данных за пальму первенства с медиками борются таксисты. «На рынке еженедельно открываются и умирают десятки таксопарков, они могут продавать оборудование вместе с какой-то базой», – говорит директор по маркетингу сервиса Uklon Даниил Ваховский.

«На жаргоне таксистов, “диспетчерские” службы, которые вам шлют спам, называются “жлоб-такси”», – рассказывает столичный извозчик Василий, получающий заказы через Uber. Как утверждает таксист, среди его коллег всегда есть люди, недовольные высокими комиссиями, которые взимают с таксистов крупные сервисы вызова такси. ЭВот он ездит и думает: “И зачем мне Uber или “Яндекс.Такси”, четвёртую часть заработка отдавать? Жена всё равно ничего не делает, скинусь с друзьями на мини-АТС и базу данных, пусть заказы принимает”», – поясняет наш собеседник логику спамеров. В итоге такой человек покупает за 3–5 тыс. грн на чёрном рынке базу номеров клиентов других служб такси и рассылает спам. Однако уже спустя пару дней

выясняется, что такой метод «маркетинга» не работает, и незадачливый предприниматель ищет, кому бы дальше перепродать мини-АТС и базу данных…

Да и в целом сегодня в интернете можно найти базы данных любого объёма и наполнения: авто, паспортные данные, коммерческая информация о деятельности компаний. Более того, десятки компаний предлагают сформировать базу под заказ. Расценки варьируются в зависимости от сложности и актуальности базы – от пары сотен гривен до $5–10 тыс.

Можно без проблем найти и базы данных номеров и платёжных карт, которые незадачливые пользователи оставляют на маскирующихся под сервисы пополнения мобильных фишинговых сайтах или во время покупок в интернет-магазинах с сомнительной репутацией. «По банковским картам рынок баз данных довольно большой. В даркнете выставлены на продажу данные где-то по 5 тыс. выпущенных украинскими банками карт. С каждым днём актуальность базы падает, так как данные по картам меняются. Поэтому базы всегда востребованы. Правда, структура списания средств с карт очень сложная. Занимаются таким вещами, как правило, международные группы хакеров», – рассказывает Роман Русанов.

Масштабы незаконного использования персональной информации поражают. Сергей Демедюк говорит, что нелегальный рынок баз данных представлен как данными, ворованными из государственных ресурсов (в том числе Государственной фискальной службы, Пенсионного фонда, Государственной миграционной службы, реестра персональных идентификационных кодов физических лиц, реестра пересечения товаров государственной границы таможенной службы, реестра транспортных средств, реестра информации о преступлениях и событиях подразделений Национальной полиции Украины, реестра земельного кадастра Украины, реестров избирателей), так и частных компаний кредитно-финансовой сферы (база данных неблагонадёжных кредиторов), перевозчиков (база данных заказчиков доставки), операторов мобильной связи (база данных номеров и их пользователей), и здесь перечислены только большие базы данных с количеством записей более 10 млн. Если перечислять мелкие базы, то нужно создавать отдельную базу только с названиями.

Слишком мелко

Несанкционированное использование персональных данных – глобальная проблема. Однако в нашей стране её масштабы особенно велики. По мнению старшего партнёра адвокатской компании «Кравец и Партнёры» Ростислава Кравца, это происходит по причине того, что хоть действующее законодательство формально защищает персональные данные граждан Украины, но по факту государство не препятствует их незаконному распространению. В Украине никто не боится ответственности за продажу личных данных. «Компенсация пострадавшим от подобных нарушений в Украине будет мизерной. Можно лишь требовать возмещения морального

ущерба, а украинские суды моральный ущерб возмещают в суммах не более 5 тыс. грн. При этом в судах придётся провести не менее года», – говорит Кравец.

Из-за этого украинцы не спешат преследовать лиц, незаконно использующих их данные. Как подсчитали в юридической фирме «Ильяшев и Партнёры», в Едином государственном реестре судебных решений можно найти не более 4 тыс. дел касательно защиты персональных данных.

Характерный пример. В Днепропетровской области был случай, когда истец выиграл дело против компании «Экология Украины», которая незаконно получила и использовала персональные данные. В частности, истцу звонили по ночам и напоминали о задолженности. В результате ему присудили 1 тыс. грн в качестве возмещения морального ущерба.

Теоретически можно отстоять свои права и подав жалобу в офис омбудсмена, Уполномоченного Верховной Рады по правам человека. Как сообщили Фокусу в секретариате омбудсмена, в 2016 году граждане и юрлица подали 1,3 тыс. жалоб по этому поводу. Главным образом обращения касались обработки персональных данных банками, коллекторскими компаниями, медучреждениями, ЖЭКами, Пенсионным фондом и органами соцзащиты. Заявители сообщали о неправомерном распространении персональных данных, блокировке доступа к ним или же сборе слишком большого объёма данных для незначительных целей. Однако по всем этим заявлениям офис Лутковской составил всего 45 админпротоколов.

В Украине, по словам Сергея Демедюка, наиболее активно использует украденные базы данных бизнес с большим потоком потенциально опасных клиентов (банки, кредитно-финансовая сфера), на втором месте – бизнес с большим потоком кадров (производство, торговля), на третьем – детективные агентства, чья работа связана с постоянным анализом информации.

«Если же говорить о тех, кто халатно относится к хранению вверенных им баз данных, то всё зависит от уровня оплаты труда администраторов и их связей в среде потенциальных заказчиков», – добавляет Демедюк. По его словам, руководство частных и государственных компаний, как правило, обеспечено на должном уровне и не занимается сливами баз. «Ни одного такого случая мы не задокументировали», – говорит он.

Помимо нерадивых администраторов, «сливают» базы и пользователи, которым халатно предоставили бесконтрольный доступ со значительно преувеличенными привилегиями. Или же базы данных получают через несанкционированный доступ путём взлома, с использованием брешей в системах информационной безопасности. «Есть базы данных, преимущественно государственные дампы (резервные копии. – Фокус), которые сливают каждый квартал или полгода, но в большей степени сливы ситуативны», – поясняет Сергей Демедюк.

В Нацполиции предлагают несколько вариантов борьбы с незаконным распространением баз данных. Для этого стоит обеспечить достойную оплату администраторам баз данных, максимально ограничить привилегии пользователей, тщательно логировать действия пользователей, использовать

систему глубокого анализа передаваемых сетью пакетов, постоянный контроль состояния защищённости инфраструктуры, на законодательном уровне усилить ответственность за такого рода злодеяния, дабы у правоохранителей появилась возможность по ходу документирования использовать весь арсенал гласных и негласных средств. Но пока это всё лишь прожекты. По факту в вопросе защиты персональных данных стоит полагаться только на себя. Чтобы избежать негативных последствий, делиться информацией необходимо ответственно.

(вгору)

Додаток 23

28.08.2017

Онлайн-шпигуни. Як за вами стежать Facebook, Google та Microsoft

Анастасія Пашинська

Ми всі боїмося бути зламаними хакерами, але велика загроза конфіденційності в інтернеті – це сайти і додатки, з якими ми співпрацюємо щодня. Як за нами стежать Facebook, WhatsApp, Microsoft, Google (Еспресо).

Facebook стежить за третиною населення Землі

Чим більше часу Facebook тримає користувачів на сайті, тим більше даних він може зібрати на кожного з нас. Ці дані збираються для рекламодавців, які поповнюють бюджет Facebook. Щоб збільшити шанси на взаємодію користувача з рекламою, Facebook сортує своїх користувачів за різними групами.

І якщо ви ніколи не замислювалися, чому в стрічці Facebook ви бачите саме цю рекламу, а ваш знайомий бачить іншу – вся справа в таргетуванні. Наприклад, у вашої мами в Харкові скоро День народження, тоді у вас у стрічці з'являється реклама харківських флористів та доставки квітів.

Як вас бачить Facebook можна дізнатися у розділі «ваші категорії». Ви також можете видалити свої категорії, але від цього Facebook не перестане показувати рекламу або збирати про вас інформацію. Це призведе до того, що реклама в стрічці стане випадковою.

Це лише частина інформації, яку Facebook «знайшов» на вас і не посоромився поділитися. Подібне сортування з'являється за рахунок уподобаних вам сторінок, статусу, ваших друзів, місця розташування, кар'єри і навіть того, як ви взаємодієте з іншими обліковими записами або оголошеннями за межами Facebook.

Якщо ви авторизовані в Facebook, то соціальна мережа здатна відстежувати сайти, які ви відвідуєте. Навіть коли ви виходите з системи, Facebook знає багато з вашого браузера. Він отримує інформацію кожен раз, коли ви завантажуєте сторінку з кнопкою «Like» (Подобається) або «Share» (Поділитися).

Washington Post опублікував 98 видів персональних даних, які збирає Facebook. Серед них усі дані: від віку, до кількості кредитних карт, якими користується людина.

Також Facebook співпрацює з правоохоронними органами. І за запитом може надати все: від IP адреси до особистих повідомлень користувача.

Секретні агенти Facebook

Також Facebook знає, що мільйони людей роблять на своїх телефонах, навіть якщо вони не використовують соціальну мережу, стверджує Wall Street Journal.

Усе завдяки сторонньому додатку Onavo Protect, який компанія Facebook придбала ще 2013 року. «Подбайте про те, як ви використовуєте мобільні дані і захистіть свою особисту інформацію», – йдеться в описі програми на Google Play і Apple Store.

Додаток повідомляє, якщо сторонні додатки збирають інформацію на вашому пристрої, блокує їх, а також захищає інтернет-з'єднання за допомогою VPN.

І, як виявилося, всю зібрану інформацію відсилає своїй материнській компанії – Facebook Inc. Звісно про цю функцію в описі замовчується. Onavo Protect збирало дані про відвідувані сайти, встановлені програми, інформацію про кількість часу, який проводить користувач на різних ресурсах. Таким чином Facebook дізнавався про звички користувача і поліпшував свій продукт.

Facebook придбав Onavo Protect саме перед покупкою популярного месенджера What'sApp. Тоді сервіс показав, що месенджер встановлено на 99 % пристроїв у Іспанії. Можливо саме цих даних було досить, щоб придбати месенджер за $19 мільярдів.

Додаток Onavo Protect було встановлено понад 24 мільйонів разів як на систему Android, так і на iOS.

Крім цього, Facebook належить Instagram, WhatsApp і ще 7 компаній, тому додаткові дані підтягуються з цих додатків.

Чи чує нас Facebook

Минулого року професор Університету Південної Флориди Келлі Бренсон припустила, що соціальна мережа підслуховує своїх користувачів через мікрофон пристрою. Вона зробила цей висновок виходячи з активності свого мікрофона під час користування програмою.

Щоб протестувати свою теорію, Бренсон кілька разів говорила про теми, які жодного разу не шукала або не обговорювала на своєму смартфоні. І в рекламі Facebook відразу з'явилися елементи, які обговорювала Бренсон неподалік від смартфона.

Однак представники Facebook спростували ці чутки. Вони також зазначили, що використовують мікрофон тільки якщо користувач дозволив його використання. Мікрофон потрібен для функції «розпізнавання» в Facebook.

Наприклад, коли ви пишете статус у соціальній мережі, вона «прислухається» до оточуючих звуків, і може визначити яке шоу ви дивитеся, або яка пісня зараз грає. Усе це можна додати в статус.

Як заблокувати. Однак, якщо ви параноїк, і не хочете, щоб Facebook слухав усе, що ви говорите в будь-який час, ви можете відключити доступ

програми до вашого мікрофона. В iOS перейдіть на панель «Налаштування», знайдіть «Facebook» і зніміть опцію «мікрофон».

На Android перейдіть у розділ «Політика конфіденційності» в розділі «Налаштування», знайдіть розділ мікрофона під панеллю дозволів, і вимкніть доступ до Facebook.

WhatsApp

Месенджер і так належить компанії Facebook, яка вже є гігантською базою даних на кожного користувача. Ми відправляємо 10 мільярдів повідомлень Facebook на день, натискаємо кнопку «Подобається» 4,5 мільярда раз і завантажуємо 350 мільйонів нових фотографій кожного дня. На Facebook розміщено 17 мільярдів геолокацій і близько 250 мільярдів фотографій.

Уся ця інформація означає, що Facebook знає, як ми виглядаємо, хто наші друзі, якими є наші погляди на більшість речей, коли наш день народження, незалежно від того, знаходимося ми в стосунках чи ні, де ми знаходимося, що нам подобається і не подобається і багато іншого. Це дуже багато інформації в руках однієї комерційної компанії.

Навіщо ж Facebook ще один сервіс, такий як WhatsApp? WhatsApp дійсно не вписується в бізнес-модель Facebook, тому що на ньому немає і не буде реклами. І якщо раніше, щоб користуватися WhatsApp необхідна була платна підписка, то зараз її повністю скасували. Як тоді Facebook отримає дохід від своїх витрачених на месенджер $19 мільярдів?

Офіційної відповіді на це питання немає, однак WhatsApp також збирає інформацію: телефонну книгу, фотографії, відео. На липень 2017 року у WhatsApp 1,7 мільярда користувачів, а за день відсилається близько 42 мільярдів повідомлень.

Компанія WhatsApp отримує доступ до вашого номера телефону, адресної і телефонної книги, динаміка, дані про запущені додатки на тому ж пристрої, визначає кому і коли ви телефонуєте (або коли телефонують вам), точну геолокацію.

Також WhatsApp має дозвіл на запис аудіо через мікрофон без повідомлення користувача про це. Теж саме стосується запису відео та фото – додаток може все це робити в будь-який час, без вашої згоди або повідомлення. А ще додаток отримує інформацію про всі облікові записи (Google, Facebook та інші) на пристрої. Також додаток може відправляти і читати ваші смс-повідомлення.

І ця інформація не якась там таємниця, ви самі приймаєте угоду користувача. Усе це ви можете прочитати в налаштуваннях вашого смартфона, в розділі програми.

Як заблокувати. Однак можна заблокувати доступ додатки до мікрофона і камери. Робиться це так само як і в Facebook. В iOS перейдіть на панель «Налаштування», знайдіть WhatsApp і відключіть доступ до мікрофона і камери.

На Android перейдіть у розділ «Політика конфіденційності» в розділі «Налаштування», знайдіть розділ мікрофона під панеллю дозволів, і вимкніть

доступ до WhatsApp. Або зайдіть в «настройки», виберіть «додатки», знайдіть там WhatsApp і відключіть мікрофон та камеру.

Що знає Google

Практично те ж саме, що і Facebook. Тут вони змагаються в кількості зібраної інформації, хоча використовують схожі методи.

Коли ви використовуєте Google, ви йдете на угоду. Можете безкоштовно користуватися такими сервісами, як Gmail, Google-диск, пошуковик, YouTube і Карти Google в обмін на надання інформації про себе.

Всього у компанії Google близько 70 продуктів (включаючи систему Android), кожен з яких збирає про вас інформацію. Google навіть докладно пише про те, яку інформацію компанія отримує.

Google використовує безліч методів, щоб дізнатися про вас. Також компанія відстежує будь-яку взаємодію з системою: подорожі, веб-пошук, локації, номери телефонів і навіть записує голосовий пошук.

Однак і тут є можливість очистити журнал та інформацію про себе. Але як і з Facebook, це не означає, що система перестане збирати про вас інформацію або показувати рекламу.

Windows – король серед шпигунів

Від моменту запуску Windows 10 Microsoft звинувачують в тому, що нова система дозволяє Microsoft контролювати все, що ви робите. Навіть якщо ви просто натискаєте клавіші на клавіатурі.

Виконавчий віце-президент Microsoft Террі Майерсон пояснив, що, хоча компанія і збирає інформацію, користувачі самі можуть вибирати, якими даними хочуть поділитися з корпорацією. Але за замовчуванням система збирає всі дані.

Крім того, що компанія Microsoft збирає дані про ваш пристрій, щоб поліпшити роботу системи, вона збирає будь-яку інформацію, яку ви вводите на пристрої з Windows 10.

Однак віце-президент запевнив, що ці дані не використовують для ідентифікації користувачів, а також що їх зашифровано на серверах Microsoft.

«Зверніть увагу, що з новими функціями, такими як Cortana (голосовий помічник WIndows – ред.) для яких потрібно більше особистої інформації, вас запитують, чи хочете ви включити їх і отримали додаткові параметри налаштування конфіденційності», – написав Майерсон у повідомленні в блозі.

Майерсон також пояснив, що Windows 10 не виконує сканування ваших файлів та електронних листів, щоб краще зорієнтувати рекламу під вас.

Щоб заборонити Windows стежити за вами, при установці системи ніколи не вибирайте «швидку» установку. Прочитайте всі положення і приберіть галочки там, де система дозволяє собі відсилати ваші персональні дані.

Усі у змові

Ще наприкінці 2015 року дослідники з Массачусетського технологічного інституту (MIT), Гарварда і університетів Карнегі-Меллона вивчили найпопулярніші 110 додатків, доступних у Google Play і Apple App Store. Як

з’ясувалося, більшість додатків ділиться конфіденціальною інформацією про користувача, не попереджаючи його про це.

У своєму дослідженні «Хто що про мене знає?» вони виявили, що 73 % програм на Android розкривали поштові адреси та імена своїх користувачів. А 47 % додатків для iOS відсилали третім особам геолокацію користувачів.

Куди ж відсилалися ці дані? Велика частина інформації, а саме 36 % (40 додатків зі 110) відсилалася за адресою Google.com, ще 18 % інформації йшло на Googleapis.com. Сайт Apple.com отримував інформацію від 17 % досліджуваних програм, а соціальна мережа Facebook.com – від 14 % додатків.

Дослідження також показало, що 93 % тестованих додатків Android підключені до загадкового домену safemovedm.com. Найцікавіше, що дані на цей домен передаються у фоновому режимі, навіть коли немає запущених додатків. Компанія Google (як власник системи Android) не прокоментувала призначення домену.

Також було проаналізовано 30 медичних та фітнес-додатків. З них 3 додатки відсилали інформацію третім особам. Наприклад, популярний додаток Android Health Drugs.com, який працює як медичний довідник, надсилав інформацію за пошуковими запитами 5 різним доменам. Тож якщо людина шукала інформацію про «герпес» про це тут же дізнавався один з сервісів Google і велика компанія цифрової реклами DoubleClick.

Рекордсменом з розсилки особистої інформації в Android виявився додаток «Text Free», за допомогою якого користувачі можуть обмінюватися безкоштовними смс і телефонними дзвінками. Його було завантажено 50 мільйонів разів. Ця програма відсилає особисту інформацію 11 стороннім компаніям.

Найбільш «проблемним» додатком на iOS став «Localscope» – спеціальний браузер, за допомогою якого користувачі дізнаються про найцікавіші місця поблизу. Ця програма надсилала інформацію 17 стороннім компаніям.

Не секрет, що більшість додатків окупається за рахунок реклами, яка в них міститься. Однак якщо додаток без реклами, але безкоштовний (як, наприклад, WhatsApp), слід насторожитися: швидше за все він краде ваші особисті дані.

(вгору)

Додаток 24

29.08.2017

Кража средств с помощью WAP-биллинга набирает обороты

Исследование, проведённое «Лабораторией Касперского», показало, что киберпреступники всё чаще используют вредоносные программы для кражи денег посредством WAP-биллинга (InternetUA).

Услуга WAP-биллинга – это вид мобильных платежей, предусматривающий списание средств напрямую с баланса лицевого счёта

мобильного телефона без необходимости регистрации банковской карты или создания имени пользователя и пароля. Этот механизм схож с оплатой с помощью Premium SMS, но в данном случае отправлять какие-либо SMS-сообщения не нужно. Более распространённое название услуги – WAP-подписки.

С точки зрения пользователя, страница, использующая оплату посредством WAP-подписок, ничем не отличается от других. Как правило, такие страницы содержат полную информацию о платеже и кнопку. После нажатия на неё пользователь перенаправляется на сервер оператора сотовой связи, на котором может быть указана дополнительная информация и который может запросить окончательное подтверждение платежа, попросив пользователя нажать на очередную кнопку.

«Лаборатория Касперского» обнаружила сразу несколько зловредов, эксплуатирующих систему WAP-биллинга. Такие трояны сначала отключают Wi-Fi и включают мобильную передачу данных, поскольку WAP-подписки возможны только при подключении к Интернету через мобильное подключение. Затем открывается ссылка, которая перенаправляет жертву на веб-страницу WAP-биллинга. Обычно такие трояны загружают веб-страницы и нажимают кнопки при помощи файлов JavaScript (JS). После этого они удаляют входящие SMS-сообщения от сотового оператора, содержащие информацию о подписках.

Сообщается, что обнаруженные зловреды созданы различными группами злоумышленников.

(вгору)

Додаток 25

29.08.2017

300 Android-приложений оказались вредоносными программами

Зловредные приложения для Android создали свою сеть и наносили массированные удары по популярным сайтам России и Азии (InternetUA).

Команда специалистов смогла обезвредить ботнет – армию зараженных мобильных телефонов под управлением ОС Android от Google, – сообщает Fortune.

В этих телефонах были запущены сотни вредоносных приложений, которые этим летом просочились в магазин приложений Google Play. Многие из них маскировались под медиа- и видеоплееры, рингтоны или инструменты для менеджеров хранилищ и магазинов приложений и в основном загружались на рынки России, Китая и других азиатских стран.

Все началось с того, что вредоносные программы осуществляли показы всплывающей рекламы и их создатели зарабатывали деньги на кликах от пользователей.

Эта мошенническая схема, собственно, не нова. Пользователи, в том числе и в Украине, неоднократно устанавливали безобидные программы, а в нагрузку получали кучу всплывающей рекламы.

Однако со временем этот ботнет, который эксперты окрестили WireX, создал своеобразную систему артилерии для DDoS-атак – одновременных атак со множества устройств на определенный сайт с целью довести его до прекращения работы.

Google выявил и заблокировал 300 приложений, которые вызвали эту проблему.

Всего было инфицированно 120,000 гаджетов. Пик атак пришелся на начало августа, когда ботнет отправлял на страницу сайта-мишени 20 000 запросов страниц в секунду. Сейчас ботнет все еще активен, но его деятельность пошла на спад.

На борьбу с ботнетом были брошены силы экспертов в сфере сетей доставки контента Akamai и Cloudflare, компании-исследователя киберугроз Flashpoint, разработчиков инфраструктуры интернета из Oracle, экспертов по кибербезопасности из RiskIQ и Team Cymru, а также ФБР.

«Это первый случай когда мы увидели очень большую сеть мобильных телефонов Android, используемых для запуска DDoS-атак», – говорит Мэтью Принс, генеральный директор и соучредитель Cloudflare.

Однако, это не самый мощный ботнет из существоваших. Первенство пренадлежит все-таки Mirai, который вызвал перебои в работе Интернета на восточном побережье США. Он отправлял сотни миллионов запросов в секунду.

Однако в этот раз опасность состоит в том, что приложения действовали тайно, – они атаковали сайты даже когда мобильные устройства-носители «спали».

(вгору)

Додаток 26

30.08.2017

Набравший популярность анонимный мессенджер Sarahah похищает данные пользователей

В последние недели приложение Sarahah, созданное разработчиком из Саудовской Аравии Зейном аль-Абидин Тофиком (Zain al-Abidin Tawfiq) возглавляет рейтинги App Store и Google Play, набрав миллионы пользователей. Слово «sarahah» переводится с арабского как «искренность», и приложение позволяет пользователям получать анонимный фидбек, причем ответить на такие послания пользователь не может, лишь настроить фильтры, к примеру, чтобы отфильтровывать самые очевидные оскорбления (InternetUA).

Независимый ИБ-специалист Закари Джулиан (Zachary Julian) предупреждает, что анонимный мессенджер не так уж анонимен. Исследователь рассказал журналистам The Intercept, что Android и iOS версии

приложения передают список контактов пользователя (номера телефонов и email-адреса из адресной книги) на удаленный сервер, сразу же, как только пользователь устанавливает Sarahah.

Хотя приложения часто запрашивают разрешение на доступ к списку контактов и работают с ними, но это не значит, что все контакты пользователей тут же «утекают» в неизвестном направлении. Более того, Sarahah на данный момент вообще не имеет никаких связанных с контактами функций, по сути, приложение просто похищает данные пользователей, загружая их на удаленный сервер.

Разработчик Sarahah Зейн аль-Абидин Тофик объясняет, что функции, чья работа связана со списком контактов, обязательно появятся в приложении чуть позже (скорее всего, это будет некая форма списка друзей). И якобы именно с этим связана утечка пользовательских данных. Автор приложения заверил, что сбор информации прекратится, как только выйдет следующая версия Sarahah, а также заявил, что компания не хранит полученные от пользователей списки контактов, что, увы, никак невозможно проверить.

(вгору)

Додаток 27

30.08.2017

Растет число фирм, предлагающих услуги по слежке за телефонами по всему миру

Отслеживание телефонов по всему миру постепенно становится привлекательной нишей для ведения бизнеса, сулящей большие доходы. В связи с этим в последнее время стремительно растет число компаний, предлагающих технологии для удаленной слежки за мобильными устройствами невзирая на государственные границы (InternetUA).

Как только объект слежения включает свой смартфон, его местоположение сразу же фиксируется без необходимости взламывать само устройство. Куда бы ни направилась жертва, за ее перемещениями будет вестись непрерывная слежка даже за десятки тысяч километров в другой стране. Большое количество частных фирм предлагают подобные услуги правоохранительным органам и спецслужбам.

Как сообщает The Daily Beast, шпионские технологии эксплуатируют уязвимости в сетях сотовой связи – стандартная услуга, предлагаемая спецслужбам частными компаниями. Речь идет об уязвимости в наборе протоколов ОКС-7 (SS7), позволяющей любому, у кого есть доступ к нему, подменять сообщения. ОКС-7 «верит» всему, что ему скажут, и не проверяет источник сообщения.

ОКС-7 – набор сигнальных телефонных протоколов, используемых для настройки большинства телефонных станций по всему миру на основе сетей с канальным разделением по времени. В основе ОКС-7 лежит использование

аналоговых или цифровых каналов для передачи данных и соответствующей управляющей информации.

Издание The Daily Beast представило обзор ряда частных фирм, предлагающих шпионские технологии для слежки за абонентами мобильных операторов. К примеру, немецкая компания Wolf Intelligence предлагает ПО для взлома смартфонов, средств радиоэлектронного подавления и защищенных телефонов. Среди ее услуг также указана возможность «отслеживания местоположения конкретного телефона в любой точке мира в радиусе действия ближайшей антенны».

Похожий инструмент под названием Observer предлагает компания Almenta Group, чьи офисы находятся в Гонконге и Болгарии. Продукт представлен на сайте Milipol – постоянно действующей выставке-продаже военных и шпионских технологий. По словам компании, Observer способен определять и указывать на Картах Google местоположение жертвы по одному лишь номеру телефона.

Израильская компания Picsix предлагает продукт P6-GEO, «позволяющий оперативникам виртуально определять местонахождение, отслеживать и тайно манипулировать абонентами GSM и UMTS по всему миру, в том числе в роуминге».

Большинство компаний, с которыми пытались связаться журналисты The Daily Beast, так и не дали ответа. Согласно указанной на их сайтах информации, фирмы предоставляют свои услуги только правоохранительным органам для поимки террористов, наркоторговцев и других опасных преступников. Если верить израильской компании Rayzone Group, ее технологии предназначены для использования исключительно правительственными службами и только в рамках лицензии Министерства обороны.

Среди других компаний, предлагающих слежку за абонентами операторов связи по всему миру, издание также отмечает Circles (Болгария), Cleversig, Proximus (Украина), Intercept Monitoring Systems (Россия) и Trovicor (Пакистан).

(вгору)

Додаток 28

3.09.2017

3 способа проверить Android-устройство на наличие вредоносных приложений

Беспокоитесь о надёжности программ в мобильном устройстве? Инструмент от Google позволит убедиться в том, вы не загрузили какие-либо подозрительные Android-приложения. Предлагаем детальную инструкцию, как это проверять (InternetUA).

Google Play Protect – новейший инструмент компании, призванный помочь владельцам Android-устройств избегать любых небезопасных приложений. Сервис постоянно сканирует смартфон или планшет Android и

извещает пользователя в том случае, если обнаруживает какие-нибудь проблемы. Имейте в виду: Play Protect создан для сканирования и обнаружения вредоносных приложений в онлайн-магазине Play Store, а не на сторонних сайтах, на которых размещаются мобильные программы. Самый простой способ защитить своё устройство – загружать приложения только из Play Store.

Существует несколько способов проверить, одобрено ли приложение Play Protect:

Последние сведения о сканировании

Чтобы просмотреть текущее состояние сканирования и убедиться в том, что Play Protect включён, зайдите в Настройки>Google>Безопасность>Google Play Protect. Здесь можно найти список последних загруженных приложений, текущие вредоносные программы и опцию включения и выключения сервиса.

Вскоре после того, как был анонсирован новый сервис, Play Protect стал доступен для всех пользователей, но в разделах отзывов и на форумах появлялись сведения о том, что на некоторых устройствах эта функция недоступна (например, на Galaxy S8). Поэтому стоит перепроверить своё устройство.

На странице приложения Play Store

Когда Google завершит внедрение Play Protect на рынок, вы увидите значок подтверждения на странице непосредственно самого приложения в Play Store. Это быстрый и простой способ убедиться в том, что программа безопасна, не дожидаясь её установки и сканирования Play Protect.

Перед обновлением приложений

То, что приложение безопасно при первичной загрузке из Play Store не означает, что злоумышленники не будут пытаться в будущем «втиснуть» что-то компрометирующее в программу. Специалисты Google предусмотрели и это: после окончательного выпуска Play Protect появится ещё одна функция – подтверждение того, что обновления приложений, которые вы собираетесь загружать, являются безопасными. В верхней части списка обновлений появится сообщение о том, что никаких угроз не найдено с указанием последнего времени сканирования.

(вгору)

Додаток 29

4.09.2017

Загрузчики Android от крупных производителей подвержены уязвимостям

В загрузчиках ОС Android от пяти производителей процессоров для мобильных устройств обнаружены уязвимости, нарушающие процесс доверенной загрузки и ставящие под угрозу безопасность пользователей (InternetUA).

Проблемы были обнаружены командой исследователей Калифорнийского университета в ходе изучения аппаратных загрузчиков Android. Эти

компоненты привлекли внимание исследователей, поскольку провести их анализ крайне сложно из-за отсутствия привычных метаданных и закрытого исходного кода.

Целью исследования являлось создание инструмента BootStomp для тестирования и анализа загрузчиков. С его помощью ученые обнаружили семь уязвимостей – шесть ранее неизвестных и одну известную (CVE-2014-9798). Из шести новых уязвимостей производители подтвердили пять. Некоторые из них позволяют выполнить код в процессе загрузки или вызывать постоянный отказ в обслуживании. Эксплуатируя еще две уязвимости, злоумышленник с привилегиями суперпользователя на ОС может разблокировать устройство и нарушить процесс доверенной загрузки.

Уязвимости затрагивают следующие продукты:

– Чипсет Huawei / HiSilicon (используется в устройствах Huawei P8 ALE-L23);

– Чипсет NVIDIA Tegra (используется в устройствах Nexus 9);

– Чипсет MediaTek ((используется в устройствах Sony Xperia XA);

– Новый загрузчик Qualcomm LK; Старый загрузчик Qualcomm LK.

– Доверенная загрузка – загрузка операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и аппаратной идентификации/аутентификации пользователя.

(вгору)

Додаток 30

5.09.2017

Вирус Cerber проник на сайт правительства США и вымогал биткоины

В августе 2017 года на веб-сайте Национальной координационной группы по лесным пожарам (NWCG) в США был обнаружен вирус-вымогатель. Первым его идентифицировал Анкит Анубхав, исследователь из компании NewSkySecurity (InternetUA).

Неясно, как долго вирус был на официальном сайте правительства, и смог ли он кому-нибудь навредить.

Несмотря на то, что файл уже удален, тот факт, что он смог проникнуть в официальный домен .gov, вызывает немалое беспокойство. Большинство таких доменов аккредитованы, а значит, любая загрузка, сделанная с этих сайтов в целом безопасна.

По словам исследователей, вредоносный файл размещал загрузчик вируса-вымогателя Cerber. Подобно большинству вымогателей, он шифрует файлы на зараженном устройстве и делает их недоступными до тех пор, пока владелец не согласится заплатить выкуп в виде биткоинов.

Cerber существует уже более года и даже продается как услуга, которую может заказать любой пользователь на форумах даркнета. Он также был обнаружен в спам-кампаниях и атаках бот-сетей.

По словам аналитика вредоносных программ Мариано Паломо Вильяфранка из компании Telefonica, загрузчик Cerber происходит из популярного вредоносного домена.

Пока непонятно, как загрузчик Cerber смог проникнуть на веб-сайт NWCG. Анубхав предположил, что сайт взломали или файл был отправлен в письме государственному чиновнику, которое вместе с вредоносным загрузчиком было заархивировано и сохранено на сайте.

NWCG в свою очередь не сделал публичное заявление и не предоставил дополнительную информацию об обнаружении и удалении вредоносного файла.

В прошлом году число подобных атак увеличилось, а их целью стали политики, университеты и даже частные компании. Хотя мотивы нападений шифровальщика Cerber до сих пор неизвестны, очевидно, что государственным органам следует принять меры по усилению кибербезопасности. А согласно недавним исследованиям, уязвимыми оказались 65 процентов банков США, которые провалили тесты на безопасность.

(вгору)

Додаток 31

11.09.2017

Хакеры используют CDN-серверы Facebook для обхода антивирусов

Группа злоумышленников эксплуатирует CDN-серверы Facebook для хранения вредоносных файлов, которые затем используются для инфицирования систем пользователей банковскими троянами. В последние две недели исследователи в области безопасности заметили несколько подобных кампаний. Предположительно, их организатором является та же группировка, ранее эксплуатировавшая облачные сервисы Dropbox и Google для хранения и распространения вредоносного ПО (ООО "Центр информационной безопасности").

Новая вредоносная кампания была замечена экспертом в области безопасности, известным в Сети как MalwareHunter. Злоумышленники используют CDN-серверы Facebook, поскольку домену Facebook «доверяет» большинство защитных решений, пояснил исследователь.

Процесс заражения проходит в несколько этапов. На первом жертва получает спам-письмо якобы от местных властей, содержащее ссылку, которая ведет на CDN-сервер Facebook. Атакующие загружают вредоносные файлы на страницы различных групп в соцсети либо в другие публичные разделы ресурса, а затем добавляют соответствующие ссылки в спам-письма.

После того, как пользователь перейдет по ссылке, на его компьютер загрузится .rar или .zip архив, включающий ссылку на файл. Нажатие на ссылку

приводит к запуску интерфейса командной строки или PowerShell и исполнению зашифрованного скрипта PowerShell. Данная техника, предполагающая использование легитимных приложений для сокрытия вредоносных операций, называется Squiblydoo и применяется для обхода защитных решений.

Далее скрипт PowerShell загружает и исполняет дополнительный скрипт PowerShell, выполняющий ряд операций. Он загружает DLL-библиотеку, которая, в свою очередь, загружает EXE-файл и вторую вредоносную DLL-библиотеку. Эта библиотека загружает и устанавливает на компьютеры жертв банковский троян Win32/Spy.Banker.ADYV.

По словам исследователя, злоумышленники проверяют местоположение пользователя по его IP-адресу. Если жертва находится не в целевой стране (в данном случае в Бразилии), все операции прекращаются.

В настоящий момент активность кампании значительно снизилась, однако эксперты предполагают, что в ближайшем будущем злоумышленники вновь запустят ее с некоторыми изменениями. Администрация Facebook уже проинформирована о проблеме.

Сеть доставки (и дистрибуции) содержимого – географически распределенная сетевая инфраструктура, позволяющая оптимизировать доставку и распространение контента конечным пользователям в сети Интернет.

(вгору)

Додаток 32

11.09.2017

Банковский троян Emotet вернулся и распространяется через спам

Исследователи из TrendMicro сообщили о новой вредоносной кампании, в рамках которой злоумышленики распостраняют банковский троян Emotet. Впервые вредоносное ПО Emotet было обнаружено в 2014 году. Затем оно исчезло из поля зрения, но в августе 2017 года была зафиксирована повышенная активность новых разновидностей вредоноса (TSPY_EMOTET.AUSJLA, TSPY_EMOTET.SMD3, TSPY_EMOTET.AUSJKW, TSPY_EMOTET.AUSJKV), способных загружать различные типы вредоносных модулей на целевую систему (InternetUA).

В качестве возможных причин возвращения Emotet исследователи называют заинтересованность злоумышленников в новых регионах и отраслях. Хотя предыдущие варианты Emotet были нацелены преимущественно на банковский сектор, в этот раз авторы вредоносного ПО расширили поле деятельности. Злоумышленники атаковали компании из различных отраслей, включая обрабатывающую, пищевую промышленность и область здравоохранения.

Основными целевыми регионами являются США, Великобритания и Канада. При этом в США было зафиксировано 58 % всех обнаруженных

случаев заражения, на долю Великобритании и Канады пришлось 12 % и 8 % соответственно.

Троян распространяется несколькими способами, в основном через спам-рассылку, замаскированную под счета или уведомления о подтверждении оплаты. В теле письма содержится вредоносная ссылка, при переходе по которой загружается документ с вредоносным макросом. После активации макрос исполняет команду Powershell, загружающую троян Emotet.

Оказавшись на системе, Emotet загружает свои копии в системные папки и регистрируется как системная служба. Он также добавляет записи в реестр Windows для обеспечения автоматического исполнения при каждой загрузке системы. Затем вредоносное ПО приступает к сбору информации о системе и данных банковских учетных записей, обновляется до последней версии и загружает дополнительное вредоносное ПО.

(вгору)

Додаток 33

12.09.2017

Хакеры похитили данные половины жителей США

В США разгорается громкий скандал из-за крупнейшей утечки данных, произошедшей в Equifax, одном из трех ведущих бюро кредитных историй в США (Украинский телекоммуникационный портал).

В результате масштабного взлома хакеры получили сведения о примерно 143 миллионах американцев, то есть почти о половине населения Соединенных Штатов. В руки киберзлоумышленников попали имена, номера социального страхования, даты рождения, адреса и в ряде случаев номера водительских удостоверений. Кроме того, похищены номера банковских карт 209 тысяч клиентов Equifax, документы о претензиях на 182 тысячи человек, сообщает CNN.

Также в Equifax признали, что хакерская атака, произошедшая в мае-июне 2017 года, затронула клиентов из Великобритании и Канады, но о точном количестве пострадавших в этих странах не сообщается.

Об утечке руководство Equifax узнало еще в конце июля 2017 года, однако с официальным заявлением компания выступила только 8 сентября. Также скандал усугубляется тем, что спустя три дня после того, как стало известно о взломе, три топ-менеджера Equifax, в том числе финансовый директор, продали акции компании стоимостью почти 1,8 миллиона долларов.

Согласно отчётным документам Equifax, направленным в Комиссию по ценным бумагам и биржам США (SEC), 1 августа 2017 года финдиректор компании Джон Гэмбл (John Gamble) и Джозеф Лафран (Joseph Loughran), занимающий пост президента Equifax по информационным решениям в США, продали акции на сумму более 946 тысяч и 584 тысяч долларов, сообщает Bloomberg. На следующий день, 2 августа, их коллега Родольфо Плодер

(Rodolfo Ploder), возглавляющий подразделение Workforce Solutions, продал акции на 250 тысяч долларов.

В Equifax заверяют, что высокопоставленные сотрудники выставили на торги лишь небольшой процент принадлежащих им ценных бумаг, и что на момент продажи они не знали о взломе. Тем не менее, 8 сентября котировки компании рухнули более чем на 13 процентов, что стало крупнейшим падением почти за 20 лет.

По данным Bloomberg, топ-менеджеры продали примерно 13, девять и четыре процента своих акций. Джефф Мейлер, аналитик Robert W. Baird & Co, в интервью агентству отметил, что руководители Equifax действительно могли быть не в курсе утечки, так как согласно заявлению Equifax, о ней стало известно в субботу, 29 июля.

Специалисты сходятся во мнении, что кража данных Equifax – очень серьёзное происшествие.

«Если оценивать по шкале от 1 до 10, то это 10 баллов. Инцидент затрагивает всю систему кредитной отчётности США, ведь исправить ничего нельзя, все пользуются одной и той же информацией» – прокомментировал в интервью «Рейтер» аналитик Gartner Авива Литан (Avivah Litan), следящий за происшествиями, связанными с хищением личных данных и мошенничеством.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

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