СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(1.03–14.03)

2017 № 5

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(1.03-14.03)
№ 5

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

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

2.03.2017
Ірина Коркішко
Facebook буде виявляти та попереджати суїцидальні настрої у Мережі

Соціальна мережа Facebook розробила алгоритми, що виявляють повідомлення з суїцидним вмістом. Про це повідомляє BBC (Watcher).

Сервіс почав використовувати штучний інтелект для визначення користувачів, які можуть перебувати у зоні ризику самогубства. Алгоритми Facebook виявляють ознаки до самогубства в постах користувачів і коментарях їхніх друзів. Наприклад, такі пости можуть містити опис болю, страждань або приречення. Серед коментарів друзів алгоритм визначає слова стурбованості та питання про те, чи все з другом гаразд. Якщо команда працівників Facebook підтвердила зроблене програмою припущення, компанія виходить на зв'язок з користувачем і пропонує допомогу.

Поки що алгоритм працює тільки для США. Перед тим, як поширювати програму на інші країни, Facebook планує заручитися підтримкою організацій охорони здоров'я та організацій, що займаються психологічною підтримкою людей.

У майбутньому соціальна мережа передбачає розширення сфер застосування програми на виявлення постів від терористів.

***

7.03.2017
Александра Захарова
Стоит ли русским бояться «красной метки» Facebook. Как это работает

Facebook объявил войну фейковым новостям, но они останутся доступными интернет-пользователям (Укррудпром).

Соцсеть обещала начать борьбу с фальшивками еще в декабре 2016 г., но только сейчас придумала способ. Теперь под сомнительным постом с неправдивой информацией в ленте будет появляться значок Defused («спорный»). Чтобы поспособствовать его появлению, пользователь должен будет отметить любую область новости, которая кажется ему ложной. После этого новость проверит саппорт и решит, ставить на нее «красную метку» или нет.

«Facebook слишком осторожен»

Идея бороться с фейками появилась после обвинений Facebook в том, что именно неправдивая информация повлияла на исход президентских выборов в США (справедливости ради, частичной причиной стали алгоритмы, которые не позволили сторонникам Д. Трампа и Х. Клинтон оценить масштабы поддержки

оппонента). Проверять сами новости собираются совместно с ABC News, FactCheck.org, AP, Сноупс и PolitiFact.

Пока функция украинцам недоступна, не смогли мы ее увидеть, и зайдя в Facebook через TOR-браузер (выбирает IP-адрес произвольной страны). Вероятнее всего, доступ частично есть в США. Техподдержка Facebook на запрос о функции отвечает, что она доступна не всем, но не конкретизирует охват аудитории.

Тем не менее, пользователи в Twitter уже поделились первыми скриншотами о сомнительных новостях.

Удалять фальшивые новости никто не собирается, что вызвало различные мнения пользователей. «Facebook слишком осторожно подходит к проблеме. “Спорная” метка выглядит скорее как повод к дискуссии, чем как маркировка фейковой новости», пишут иностранные СМИ. SMM-специалисты соглашаются, что ноу-хау скорее станет поводом для конфликтов и споров вокруг темы новости, что даже добавит ей видимости в ленте, но вряд ли поспособствует очищению соцсети от лжи. Что касается метки, она может как отпугнуть, так и привлечь читателя. А значит, сайты с неправдивой информацией могут получить еще больше аудитории, по крайней мере, поначалу.

СМИ боятся цензуры

Противоположное опасение, которое вызывает новая функция в связи с этим, – то, что решения о сомнительных новостях будут необъективными. Впрочем, первыми забили в набат российские СМИ. «Борьба с поддельными новостями выглядит как план обуздать альтернативные СМИ», – считает, например, RT. Последствием практики сомнительных новостей может стать наступление на свободу слова, опасаются отдельные медийщики. Жалобы на новостные сайты могут стать проблемой в том смысле, что с ними могут сотрудничать как объективные журналисты, так и люди, занимающиеся пропагандой.

Сами же пользователи будут помечать посты, исходя из своих личных предпочтений, а не экспертного умения отсеивать ложь, что может закончиться массовыми «атаками» на неугодные страницы и посты, где под видом борьбы с оскорблениями или фейком могут скрываться абсолютно личные интересы. Примером могут быть случаи блокировки аккаунтов украинских Facebook-пользователей после массовых жалоб от российских. В то же время при завуалированных, но очевидных угрозах и оскорблениях поддержка соцсети может и не усмотреть проблемы.

Что касается борьбы с пропагандой, инициатива тут вряд ли поможет. Качественная пропаганда – это, как правило, правда, искусно завернутая в манипуляции, претензии в которой сформулировать сложно.

Анализируя новые функции в соцсетях, стоит понимать, что Facebook не настолько вникает в вопросы этики, а лишь следует ряду правил, пытаясь сохранять площадку для общения, работы и знакомств. Как будет решаться вопрос со СМИ, каким образом миллионы постов, на которые поступят

жалобы, рассмотрят всемирно известные медиа, пользователям сознательно не объясняют. С другой стороны, если бы кто-то знал все алгоритмы Facebook, он давно бы там работал.

Наши IT-специалисты считают идею неплохой. Правда, по их мнению, она нескоро у нас заработает адекватно и поначалу породит много конфликтов и споров. Но если со временем лента начнет предупреждать тебя – осторожнее, этот сайт пишет неправду, это поможет в нашем глобальном мире быстрее выбрать себе контент. С другой стороны, у нас и так все знают, какие СМИ и на кого работают, но любые идеи закрыть сайты с «легким налетом сепаратизма» и «руки Москвы» вызывают все те же споры о свободе слова.

***

6.03.2017

Количество пользователей Snapchat превысило 500 миллионов

Количество пользователей приложения Snapchat (главная фишка – сообщения с самоуничтожением) превысило 500 млн на Android. К сожалению, точное количество подсчитать не получится – в Play Store указывается цифра от 500 млн до 1 млрд (InternetUA).

Кстати, на первых после IPO торгах (2 марта) на Нью-Йоркской бирже акции компании Snap, владеющей Snapchat, возросли на 47 %. На данный момент они торгуются на уровне 27 долл. за акцию.

***

6.03.2017

Facebook тестирует кнопку «Не нравится» в Messenger

В Messenger появится то, что все так ждут в Facebook (IGate).

Компания Facebook начала тестирование реакций в собственном сервисе быстрых сообщений Messenger. Помимо знакомых всем пользователям социальной сети смайлов в Messenger опробуют и новую кнопку – «дизлайк».

Издание TechCrunch рассказывает, что при наведении курсора на полученное сообщение всплывает кнопка в виде смайла. Нажав на нее, пользователю предлагается выбрать подходящую реакцию, включая «Не нравится».

Каждый участник переписки будет видеть, как часто использовалась та или иная реакция, и кто ее оставил.

«Мы всегда находимся в писке новых способов сделать Messenger более вовлекающим и удобным. Данное тестирование проводится в ограниченном масштабе. Оно позволит людям поделиться смайлами, которые лучше всего выражают их мнение о сообщении», – рассказали представители Facebook.

Если нововведение будет принято хорошо, его запустят для всех без исключения пользователей приложения.

***

7.03.2017

Facebook хочет запустить путеводитель

Facebook запустила тестирование путеводителя City Guides в своем мобильном приложении («КОММЕНТАРИИ»).

С помощью путеводителя, как отмечает издание, пользователи смогут посмотреть города, в которых побывали их друзья, а также список рекомендованных к посещению мест и мероприятий, сообщает «РБК-Украина».

При выборе конкретного города можно узнать, кто из друзей в нем был, а также какие места он посещал. В путеводителе будет отдельный раздел, который будет содержать список мест, посещаемых местными жителями. Информация в нем будет основана на отзывах пользователей из этого города.

Все понравившиеся города, места и мероприятия можно заносить в избранное.

На данный момент функция тестируется в ограниченном масштабе и пока не известно, когда будет доступна всем пользователям.

***

7.03.2017

Инфографика: мобильные тренды потребления YouTube

Недавно YouTube назвал удивительную цифру – зрители смотрят миллиард часов контента в день на платформе. В Facebook, к примеру, пользователи потребляют 100 млн часов видео-контента в день. Кроме того, YouTube стал частью интерактивного процесса – поиск на платформе так же распространен как и в Google. Лидерство платформы предполагает, что любой бренд, планирующий видео контент-стратегию, должен включить YouTube в этот микс. А по данным новой инфографики от comScore, 70 % всего времени, проведенного на YouTube, приходится на мобильные девайсы (Marketing Media Review).

***

7.03.2017

Китайские социальные сети привлекают пользователей со всего мира

«Это Билл Гейтс, добро пожаловать в мой аккаунт WeChat!». 11 февраля основатель корпорации Microsoft Б. Гейтс записал 30-секундное видеообращение, в котором на китайском языке приветствовал китайских интернет-пользователей и выразил надежду, что сможет делиться с китайскими подписчиками «впечатлениями от повстречавшихся людей, прочитанных книг и полученных уроков». Спустя недолгое время, это сообщение было прочитано более 100 тыс. раз (МИА «Вектор Ньюз»).

Помимо Б. Гейтса, все больше мировых знаменитостей вступают в китайские социальные сети, включая политиков, бизнес-лидеров, знаменитостей культуры и спорта и т. д. Президент Европейского Совета Д. Туск, президент Международного валютного фонда К. Лагард, генеральный директор компании Apple Т. Кук – все они давно пользуются микроблогом «Вэйбо». ООН, МВФ и многие посольства также имеют официальные микроблоги.

Основатель маркетинговой компании Kepios С. Кемп в 2016 г. опубликовал ежегодный доклад о глобальном «оцифровывании», в котором указано, что в мировом рейтинге социальных медиа, QQ и WeChat заняли третье и шестое места по ежемесячной активности пользователей. Как показывают данные Tencent, ежедневное количество активных приложении WeChat уже достигло 768 млн аккаунтов по всему миру.

«Внешняя граница» китайских социальных сетей постоянно укрепляется, во-первых, благодаря непрерывному росту китайской экономики, а также благодаря вниманию международных организаций и знаменитостей политических и бизнес-кругов к международному влиянию Китая, все они хотят стать ближе к китайским интернет-пользователям. Бизнес-структурам необходимо осуществлять продажи при помощи социальных сетей, взаимодействовать с китайскими пользователями.

Во-вторых, китайские платформы социальных сетей делают акцент на удобство, постоянно расширяют зарубежные рынки, повышается количество пользователей. WeChat, QQ, «Вэйбо» имеют международные версии. WeChat уже имеет 20 версий на иностранных языках, поддерживает оплату в долларах, евро, иенах и других иностранных валютах.

Вслед за бурным развитием Интернета, все более заметным становится совокупный эффект платформ социальных сетей, все больше иностранцев вступают с социальные медиа Китая, WeChat и «Вэйбо» становятся для всего мира важным окном в Китай.

***

8.03.2017

Як Facebook збирає дані – і що саме знає про нас Цукерберг

Більшість користувачів усвідомлює той факт, що соціальна мережа Facebook збирає дані про нашу активність, аналізує та використовує їх для рекламних чи аналітичних цілей. Однак, мало хто розуміє, як саме працює механізм накопичення користувацької інформації (InternetUA).

Саме для цього програмісти створили розширення Data Selfie для браузеру Chrome. Програма з відкритим кодом допомагає зрозуміти, як алгоритми машинного навчання збирають та аналізують Facebook-дії користувача, створюючи персональний профіль онлайн-звичок.

***

10.03.2017
«ВКонтакте» блокуватиме сторінки з суїцидальним контентом

«Ми провели зустріч з керівниками найпоширенішої мережі в Росії "ВКонтакте". Було ухвалене рішення про технічні заходи із блокування сторінок із суїцидальним контентом у пріоритетному порядку», – цитує слова омбудсмена агенція РІА (Незалежне Бюро Новин).

***

9.03.2017
Facebook випускатиме власні короткометражки

У Facebook вирішили випускати кожного тижня короткі ролики на актуальні тематики (Знай.ua).

«Соціальна мережа вперше випускатиме власний контент, при цьому не рекламного типу», – повідомляє сайт Wall Street Journal.

Кожного тижня виходитимуть нові ролики про спорт, науку відеоігри, музику та соціальне життя.

Формат роликів буде подібний до серіалів і телепередач.

Відомо, що одним із авторів проекту є Рік Ван Він – один із засновників розважального сервісу CollegeHumor.

Також із В. Віном над проектом працюють М. Лефівре (у минулому топ-менеджер музканалу MTV), колишній директор музикального співтовариства YouTube і Google Play Т. Хрівнак.

На один ролик Facebook виділятиме півмільйона доларів.

***

10.03.2017
Google разделила Hangouts на два отдельных сервиса

В 2016 г. Google запустил мессенджер Allo и сервис для видеоконференций Duo, а также объявил о том, что Hangouts превратится в кроссплатформенный инструмент связи для корпоративных клиентов. С тех пор никаких существенных изменений в работе Hangouts не происходило, однако недавно был представлен новый сервис для онлайн-конференций Meet by Google Hangouts. Теперь же компания официально объявила, что Hangouts был разделен на два отдельных сервиса: Hangouts Meet, который предназначен для проведения конференций, и Hangouts Chat – для рабочей переписки (IGate).

Hangouts Meet позволяет создавать видеоконференции с участием до 30 пользователей. Подключение к онлайн-встрече происходит по специальному коду. При этом необязательно, чтобы участники были в списке контактов друг друга. Сервис позволяет планировать будущие встречи с синхронизацией времени собеседников и прочих параметров.

Hangouts Chat в свою очередь напоминает такие сервисы как Slack и Microsoft Teams. Он поддерживает несколько виртуальных комнат для обсуждения тем, многопоточные разговоры, а также интеграцию с другими службами G Suite. Как и Slack, Hangouts Chat поддерживает интеграцию с другими службами и ботами.

Какое будущее ожидает нынешнюю версию Hangouts, доступную в виде приложений для Android и iOS, а также расширения для Chrome – пока не сообщается.

***

10.03.2017
Ірина Коркішко
Facebook запустить нову функцію зі зникаючими статусами

Facebook запускає нову функцію для свого Месенджера – Messenger Day. Це фото і відеостатуси, що можна поширювати для друзів або обмеженої групи просто в Месенджері. Кожен статус буде активним протягом 24 годин, після чого зникатиме (Watcher).

Facebook взяли за основу механізм, що уже існував у Snapchat і Stories.

***

12.03.2017
Telegram начал тестировать функцию звонков

Мессенджер Telegram начал тестировать функцию аудиозвонков. Об этом сообщается в канале Telegram info (@tginfo) 12 марта (InternetUA).

Как отмечается, звонки защищены end-to-end шифрованием. «Возможно ограничить список контактов, которые смогут вам позвонить, или полностью запретить», – говорится в сообщении.

Протестировать функцию может любой желающий, у кого установлена бета-версия мессенджера. Канал также опубликовал инструкцию для решивших сделать звонок. В ней отмечается, что пока это возможно сделать лишь на специальном сервере, для чего придется пройти повторную регистрацию.

***

14.03.2017
Facebook захистить користувачів від спецслужб

Керівництво наймасштабнішої соцмережі Facebook заборонило розробникам використовувати інформацію про користувачів з метою стеження. Таким чином компанія нагадує про їх політику щодо конфіденційності (Знай.ua).

Про це повідомляє BBC.

«Розробники не можуть використовувати зібрану інформацію, щоб створювати інструменти для стеження», – заявили в адміністрації Facebook.

Таке рішення компанія прийняла після минулорічного скандалу, коли Американський союз захисту громадських свобод поскаржився на те, що Facebook разом з популярною нині мережею Instagram передавали дані компанії Geofeedia, що займається обробкою інформації та співпрацює з правоохоронними органами.

***

13.03.2017

Facebook создало приложение для просмотра сферического контента

Facebook всё больше внимания уделяет 360-градусному контенту и виртуальной реальности («КОММЕНТАРИИ»).

Поддержка такого контента появилась в социальной сети в 2015 г., и с тех пор в ней было опубликовано более миллиона 360-градусных видео и более 25 млн 360-градусных фотографий, однако порой отыскать их в сервисе довольно трудно, сообщает «3Dnews».

Чтобы устранить эту проблему, компания выпустила новое приложение под названием Facebook 360, позволяющее через шлем виртуальной реальности Samsung Gear VR с лёгкостью искать и просматривать публичный 360-градусный контент. Это первое брендированное VR-приложение Facebook, появившееся на рынке.

Продукт доступен через приложение Oculus на любом совместимом с Gear VR устройстве.

На смартфонах и компьютерах также присутствует возможность просмотра 360-градусного контента, однако эти устройства не обеспечивают такой глубины погружения, как шлемы виртуальной реальности.

Через Facebook 360 можно не только просматривать контент от компаний и пользователей социальной сети, но и подписываться на их страницы. Фото и видео можно сохранять для отложенного просмотра, также ими можно делиться на своей странице в социальной сети.

Через Gear VR можно просматривать свой собственный 360-градусный контент. Компания встроила в приложение поддержку реакций, а вскоре пообещала оснастить его и другими социальными функциями.

В январе Samsung сообщила, что продала уже более пяти миллионов шлемов Gear VR, и Facebook заинтересована в том, чтобы устройство компании так же хорошо продавалось и дальше.

Gear VR работает именно на базе технологии Oculus, которой владеет Facebook, причём компания помогла разработать последнюю версию шлема с ручным контроллером.

***

13.03.2017

Viber запустил секретные чаты

Функция секретных чатов полезна в тех случаях, когда необходимо предпринять дополнительные меры безопасности помимо шифрования (Finance.Ua).

Компания Viber в рамках обновления до версии 6.7 представляет новую функцию секретных чатов со сквозным шифрованием текстовых сообщений и звонков.

Что такое функция секретных чатов:

В секретных чатах можно установить таймер самоуничтожения для всех сообщений, отправляемых в чат.

В секретных чатах отключена функция пересылки сообщений.

Если один из участников попытается сделать скриншот переписки, эта функция будет либо полностью недоступна, либо остальные участники немедленно получат сообщение об этом прямо в окне чата.

В то же время любая коммуникация пользователей по-прежнему защищена по технологии сквозного шифрования Viber и недоступна третьим лицам.

Мессенджер позволяет вести одновременно два чата с одним и тем же собеседником или группой, при этом один из чатов будет обычным, а второй – секретным. Пользователи смогут узнать, какой из этих двух чатов является секретным, по значку замка на иконке чата. Начало секретного чата из уже существующего обычного чата не приведет к удалению или замене обычного чата, а просто создаст отдельный чат.

В обычных чатах Viber существует таймер самоуничтожения для отдельных сообщений, содержащих фотографии или видео, тогда как в секретных чатах предусмотрена возможность применить таймер самоуничтожения ко всем сообщениям, отправляемым в чат.

Пользователи могут скрыть свои секретные чаты и вновь обращаться к ним позднее, указав PIN-код. Для этого после создания секретного чата необходимо найти его в списке чатов, сделать свайп влево и нажать на кнопку «Скрыть».

***

12.03.2017

Исследование: каждый второй пользователь Facebook делится видео

Несколько лет назад социальная сеть взяла курс на популяризацию видеоконтента, вступив тем самым в конкуренцию с YouTube. В 2015 г. разница была колоссальной: совокупно американцы провели на YouTube 8061 год, тогда как на Facebook просмотр роликов занял «всего» 713 лет. Согласно исследованию компании Quintly, за последние два года ситуация кардинально изменилась (AIN.UA).

В рамках исследования сотрудники Quintly изучили более 6 млн постов от 162 000 пользователей. Полученные данные показали – видео в Facebook все больше становится нативным и виральным контентом для пользователей соцсети. Причин тому несколько. Например, ролики в Facebook запускаются автоматически, а еще они органично вписаны в ленту, пользователю нет необходимости делать никаких лишних движений.

Как результат, на 53 % исследуемых профайлах было зашерено видео: люди не просто смотрят видео в своей ленте, они охотно делятся ими с друзьями, что лишь добавляет роликам виральности. А имея для этого удобный инструмент (кнопка «Поделиться»), так называемый Share Rate на Facebook на 1055 % выше, чем на YouTube. Более того, порядка 90 % пользователей сами записывают видео, что легко делается после запуска прямых трансляций. Исключением не стали и популярные страницы с число подписчиков в более чем 10 млн человек: за последний год число создаваемых видео для Facebook выросло на 35 %.

Очевидно, что популярность YouTube не падает: не так давно представители сервиса заявили, что каждый день люди просматривают там 1 млрд часов контента. Но М. Цукерберг активно работает над тем, чтобы сделать Facebook новым телевидением. Например, было выпущено приложение для Smart TV, а внутри компании есть большой многомиллионый фонд для финансирования съемки роликов звезд и инфлюенсеров.

***

13.03.2017

«ВКонтакте» даст пользователям маски

Уже в следующем месяце у пользователей «ВКонтакте» появится возможность создавать маски для себя и других. Как поясняют «Известия», дополненная реальность позволит пририсовать к лицу пользователя новые детали, которые сможет создать любой пользователь. А после модерации эта маска станет доступна всем пользователям социальной сети (Grifonsoft).

«ВКонтакте» планирует использовать маски в запущенном в конце прошлого года сервисе «Истории». Последний представляет собой фото и короткие видео, самоуничтожающиеся через 24 часа. И маски можно будет использовать как в статичных фотографиях, так и в видеороликах. Причем в последнем случае маска будет менять положение при движении изображения.

Маски будут создаваться как командой разработчиков «ВКонтакте», так и самими пользователями, которые смогут сделать их общедоступными, отправив свои творения специальному боту через сообщения в сообществе VK Masks. Правда, для создания даже самой простой маски понадобятся хорошие навыки работы с графическими редакторами. А в случае с 3D-масками вы не сможете обойтись без специальных знаний в области анимации.

«Мы хотим создать целую экосистему, в которой будет постоянно появляться что-то новое, – прокомментировал разработчик “ВКонтакте” О.

Илларионов, ответственный за “маски”. – Чтобы постоянно появлялись инфоповоды, рождались новые мемы, платформа должна быть открытой для всех пользователей. Маски будут разной степени сложности – от совсем простых до сложных анимированных».

***

13.03.2017
Прасковья Быстрицкая
Соцсеть «Одноклассники» запустила службу онлайн поддержки

При возникновении проблем использования социальной сети «Одноклассники», пользователи имеют возможность получить помощь сотрудника сервиса в онлайн чате. О нововведении сообщили в пресс-службе сервиса (HiTech-News.ru).

Время устранения неполадок в соцсети «Одноклассники» сократилось в несколько раз. Если раньше проблема решалась при помощи сообщений по e-mail, то сейчас выйти на связь и решить проблему можно отправив СМС-сообщение. При этом создается чат, посредством которого пользователь общается с сотрудником сервиса.

В основном, удобство оценили пользователи системы денежных переводов «Одноклассников». В целом, дополнительный сервис положительно оценили 90 % участников соцсети. Разработчики сервиса планируют создать приложения для ОС iOS и Android.

***

14.03.2017
Facebook тестирует новую функцию

Facebook тестирует функцию, которая напоминает пользователю о необходимости досмотреть видео («КОММЕНТАРИИ»).

Пользователям высвечивается напоминание «продолжить просмотр» видеороликов, если пользователь начал, но не закончил их смотреть, сообщает «РБК-Украина».

Напоминание будет появляться в верхней части ленты новостей некоторых пользователей и доступно только в веб-версии Facebook.

Ранее соцсеть вводила ряд функций, связанных с просмотром видео, с целью дальнейшей монетизации этого вида контента.

***

14.03.2017
Ольга Карпенко
Сотрудники Google запустили сервис для совместного просмотра YouTube

В компании Google сотрудники официально могут 20 % рабочего времени тратить на свои собственные проекты, для этого в компании даже создали специальный инкубатор Area 120. Один из таких проектов – свежее приложение Uptime, созданное специально для YouTube-вечеринок по сети. Пока что оно доступно только для владельцев iPhone и только по инвайтам, но в Twitter проекта регулярно публикуются инвайт-коды (можете использовать слово PIZZA) (AIN.UA).

Uptime создано, прежде всего, чтобы во время просмотра видео можно было делиться своими реакциями с друзьями в реальном времени. Здесь можно логиниться с помощью Google-аккаунта, фолловить друзей и видеть, какие ролики они сейчас смотрят.

Во время просмотра видео можно его комментить, а также реагировать на него разными эмоджи, в целом, эта функция работает похоже на то, как пользователи реагируют на онлайн-трансляции в Facebook. Все эти смайлики и комментарии могут просматривать и другие зрители, которые будут смотреть видео позже. Записывать или стримить собственные видео здесь нельзя.

Перед тем, как пользователь просмотрит свое первое видео на Uptime, от него потребуется согласие на то, чтобы показывать его реакции на просмотренные видео другим пользователям. Ведь в YouTube никто не знает, какое видео вы смотрите на данный момент, а здесь это можно проверить.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

6.03.2017

В Днепре состоится флешмоб «Трезубец – это Украина»

С целью популяризации украинских государственных символов за рубежом, общественность Днепропетровщины совместно с Днепропетровской областной государственной администрацией инициирует проведение флешмоба «Трезубец – это Украина». Об этом сообщает Интернет-издание «ДНЕПР. ГЛАВНОЕ» со ссылкой на организаторов мероприятия (ДНЕПР. ГЛАВНОЕ).

***

4.03.2017

Учні однієї з сільських шкіл на Тернопільщині оголосили антисуїцидний флешмоб // *Діти самотужки записали відеоролик, в якому показали, чому треба жити і радіти життю*

Учні сільської школи з Тернопільщини оголосили бій «групам смерті» у соцмережах, передає Depo.Хмельницький з посиланням на ТСН (depo.ua).

Діти з Ягільниці започаткували флешмоб «Чому варто жити». Тринадцятирічні та старші учні поміркували над сенсом життя та поділилися власними переконаннями на відео. Естафету передали учням сусіднього села та всій Україні.

Основний посил відео, яке записали діти, – тебе люблять, заради тебе хтось живе на цьому світі. Життя – прекрасне.

***

14.03.2017

«Не засмічувати стрічку»: у Facebook ширится флешмоб проти чайлдхейтерів #моїдіти

Дописувачі українського Facebook ініціювали флешмоб #моїдіти та масово постять світлини своїх дітей (ZIK).

Це сталося у відповідь на пост журналістки і голови програмної ради «Громадського телебачення» Н. Гуменюк, яка обурилася публікацією у ЗМІ новин про те, як діти увірвалися в прямий ефір ВВС, пише «Українська правда. Життя».

Нагадаємо, професор Р. Келлі погодився поспілкуватися з журналістами з дому через відеозв'язок. Він коментував ситуацію у Південній Кореї, коли до кімнати забігли спочатку його донька, потім немовля на ходунках, а потім жінка, яка почала їх забирати з кімнати.

Коментуючи публікації у ЗМІ Н. Гуменюк, зокрема, написала, що її дратують пости батьків у соцмережі про дітей.

«Гірше людей, які засмічують стрічку постами про власних дітей, нав'язуючи іншим історії, які цікавлять тільки самих батьків у силу генетичної спорідненості, є тільки люди, які засмічують стрічку постами про те, як чужі діти з'явилися в телевізорі», – написала вона.

Хоча пост був виключно для друзів, він отримав більше як сотню коментарів.

Багато дописувачів обурилися та придумали навіть хештеги #генетичнесміття та #засмічуюСтрічку.

Однією з перших, хто написав пост #моїдіти, була виконавчий директор «Громадського телебачення» К. Горчинська. Вона розповіла про двох своїх синів, та повідомила, що пост Наталки від 10 березня стане предметом розгляду Редакційної ради «Громадського» 14 березня.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

10.03.2017

Соцсеть Pinterest купила поисковую систему Jelly

Социальная сеть Pinterest объявила о приобретении поисковой системы Jelly (Finance.Ua).

Сумма сделки не раскрывается. Как отмечает издание, поисковик был создан четыре года назад соучредителем Twitter Б. Стоуном и позиционировался как социальная сеть вопросов и ответов.

Однако проект был неуспешным, в частности в 2014 г. его создатели отказались от его поддержки в пользу другого приложения. Как полагает издание, Jelly была приобретена скорее из-за команды, которая его разрабатывала.

Так, команда продолжит работу в Pinterest и усилит поисковые возможности самой соцсети. В частности, Б. Стоун стал акционером Pinterest. Сам же проект Jelly, скорее всего, будет закрыт.

***

12.03.2017

WhatsApp тестирует систему общения предприятий с клиентами

WhatsApp, находящийся в распоряжении Facebook мессенджер более чем с миллиардом пользователей по всему миру, тестирует систему, которая позволит компаниям напрямую общаться со своими клиентами. Тестирование проводится среди нескольких стартапов, являющихся частью бизнес-инкубатора Y Combinator. Таким образом WhatsApp планирует обзавестись ещё одним источником дохода: через три года после приобретения компанией Facebook за 19 млрд долл. Мессенджер так и не разработал никакой чёткой бизнес-модели (InternetUA).

Появление WhatsApp на рынке значительно улучшило процесс использования мобильных устройств, позволив пользователям бесплатно отправлять друзьям сообщения и звонить им. Среди сильнейших конкурентом Мессенджера – WeChat, подразделение китайского гиганта Tencent.

Один из потенциальных источников дохода WhatsApp – взымать с предприятий плату за общение через Мессенджер со своими клиентами. Судя по документу, к которому получил доступ сайт Reuters, компания тщательно работает над тем, чтобы у неё не возникало никаких проблем со спамом. Также WhatsApp начала опрашивать пользователей о том, насколько часто они общаются с предприятиями и получали ли они когда-либо нежелательные сообщения рекламного характера.

В прошлом месяце WhatsApp заключила соглашение с Y Combinator, предоставляющим обучение и поддержку демонстрирующим потенциал стартапам. В рамках этого соглашения небольшое число компаний получило ранний доступ к новой возможности Мессенджера для предприятий.

Президент бизнес-инкубатора С. Альтман (Sam Altman) сообщил в письме Reuters, что не знал о проводимом WhatsApp тестировании, но сказал, что многие компании изъявляют желание протестировать свои продукты с помощью Y Combinator.

Проект находится в зачаточной стадии, сообщил У. Ильяс (Umer Ilyas), сооснователь Cowlar – одного из стартапов, принимающих участие в тестировании. По его словам, релиз системы очень ожидаем в отдалённых местах, где WhatsApp особенно популярен.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

6.03.2017

Американские психологи выяснили, что соцсети усиливают чувство одиночества

Социальные сети – в том числе Twitter, Facebook и Pinterest – усиливают у людей чувство одиночества, говорится в докладе американских психологов. Как отмечают специалисты, если человек ежедневно проводит в соцсетях более двух часов, у него удваивается риск развития социальной изоляции (ЧАС.UA).

По данным исследования, идеализированный образ людей на страницах соцсетей может заставить человека чувствовать зависть.

К числу таких сайтов эксперты также отнесли Instagram и такие платформы, как Snapchat и Tumblr.

«Мы пока точно не знаем, что происходит раньше – использование соцсетей или ощущение социальной изоляции», – поясняет соавтор исследования, профессор Питтсбургского университета Э. Миллер.

«Возможно, молодые люди, которые изначально чувствовали социальную изоляцию, обращаются к соцсетям. Или же частое использование соцсетей каким-то образом вызывает чувство изоляции от реального мира», – добавляет она.

По данным исследования, чем больше времени человек проводит в Интернете, тем меньше времени у него остается для общения в реальном мире.

В опросе для исследования приняли участие 2 тыс. человек в возрасте от 19 до 32 лет.

Как отмечает профессор Питтсбургского университета Б. Примак, современные технологии во многом усложняют общение, а не упрощают его.

«Хотя на первый взгляд кажется, что соцсети дают возможность заполнить эту социальную пустоту, это исследование говорит о том, что они

могут быть не тем решением проблемы, которое люди надеялись получить», – говорит Б. Примак.

***

7.03.2017

Стало известно число участников групп смерти в Украине

Работники департамента киберполиции Украины обнаружили 434 группы «самоубийств» в социальных сетях. В них зарегестрировано около 35 тыс. участников (InternetUA).

Об этом сообщает интернет-издание «Информат» со ссылкой на пресс-службу Нацполиции.

По состоянию на 27 февраля этого года 102 группы были заблокированы.

***

6.03.2017

Ученые связали активность в социальных сетях с чувством изоляции

Ученые заявили о том, что частое использование социальных сетей повышает риск субъективного переживания социальной изоляции. Выводы ученых были опубликованы в The American Journal of Preventive Medicine (Зеркало недели. Украина).

Социальная изоляция проявляется в отторжении индивида или группы от других индивидов или групп из-за прекращения контактов. Феномен включает в себя два аспекта: объективный (физическая изоляция) и субъективный (переживание изоляции), которые могут выражаться автономно и не всегда взаимосвязаны.

Стоит отметить, что общение в социальных сетях упрощает поиск поддержки для тех, кто испытывает трудности в установлении контактов. Вместе с тем злоупотребление социальными сетями повышает риск ухода от «живого» общения. Большое же количество «идеализированных» профилей вызывает у некоторых пользователей ощущение того, что другие живут лучше, что также повышает риск развития изоляции и депрессии.

В ходе исследования ученые опросили 1787 американцев в возрасте от 19 до 35 лет. Участники заполняли шкалу социальной изоляции, целью которой было оценить, насколько часто они испытывали чувства, ассоциирующиеся у них с изоляцией (например, незаинтересованность окружающих), за последние семь дней. Также добровольцы заполнили опросник, в котором указывали время и частоту использования 11 социальных сетей, в том числе Reddit, Snapchat и Vine, в неделю.

В результате было установлено, что низкий, средний и высокий уровни субъективной социальной изоляции были характерны для 42, 31 и 27 % испытуемых соответственно. В среднем участники посещали социальные сети 30 раз в неделю, только 3,2 % сообщили, что не пользуются подобными

сервисами. При этом частота посещения соцсетей коррелировала с риском переживания изоляции: так, те, кто пользовался ими более 121 минуты в день, были вдвое больше подвержены чувству изоляции, чем те, кто тратил на соцсети менее получаса в день. Втрое чаще изоляцию чувствовали те, кто посещал социальные сети свыше 58 раз в неделю, по сравнению с теми, чей показатель составил менее 9 раз в неделю.

***

8.03.2017

В город Николаев заплыл «синий кит» // В социальных сетях таится реальная угроза жизни подростков

В Украине в соцсетях появились группы, в которых подростков подталкивают к суициду (Николаевские новости).

Увы, эта напасть не обошла стороной и Николаев. Как сообщил на своей странице в социальных сетях общественник П. Казарьян, в одной из николаевских школ выявили 15 учеников, которые играли в «Синего кита».

«У одного малыша порезаны руки. Проверьте своих детей! В большей степени подвержены игре дети 12-17 лет, особенно девочки переходного возраста», – написал П. Казарьян.

Фанаты таких сообществ называют себя китами, потому что эти животные ассоциируются у них со свободой, могут «летать» и являются одним из немногих видов млекопитающих, которые могут добровольно свести счеты с жизнью. Поэтому у всех поклонников «моря китов» и «тихих домов» на личных страницах изображены видео или рисунки с летящими китами.

Чтобы подростки не попали в такие группы, полицейские советуют родителям уделять больше внимания психологическому состоянию ребенка.

Кроме этого, среди подростков набирает популярность игра «Беги или умри», суть которой заключается в том, чтобы перебежать проезжую часть перед автомобилем, который движется. Подростки подходят к дороге и по команде начинают пересекать ее, набирая таким образом себе «баллы».

Как сообщили в Департамент екоммуникации Национальной полиции, оперативники киберполиции установили в Украине около двухсот профилей детей в социальных сетях, которые входили в так называемые «группы смерти». Проведены обыски у нескольких администраторов интернет-ловушек «синий кит». Обнаружена информация, которая существенно поможет в расследовании.

Тем временем, 1 марта полиция нашла двух подростков, которые покинули дом и были участниками интернет-сообщества «синий кит». В Харькове мальчик ушел из дома, оставив записку тревожного содержания. Полицейским удалось найти его и вернуть родителям. В Тернополе правоохранители нашли девушку, которая накануне также оставила записку и ушла. Сейчас с детьми и их родителями работают психологи.

Известно, что для вступления в «группу смерти», требуют подать заявку и написать определенный текст у себя на странице. Если «администрация» группы утвердит кандидатуру, то в приватном чате проводят психологическое изучение его личности и готовность к самоубийству.

Судя по общению в чатах «китовых» сообществ, некоторые дети сами ищут «кураторов», которые помогли бы им попасть в опасную игру. В сообщества дети могут попадать и из-за банального любопытства либо желания получить подарок. Участников могут завлекать какими-то розыгрышами, обещаниями. Есть группа «китов», где якобы разыгрывали современные гаджеты.

Специалисты говорят, что спровоцировать мысли о суициде у подростка могут два фактора – кризисный период полового созревания, когда и тело, и разум адаптируются к измененному гормональному уровню, и социальное давление родителей и сверстников.

«Увеличивают напряжение в сознании ребенка завышенные требования. Порой желание сделать ребенку “как лучше” может вызывать у него яркое нежелание жить», – говорит кандидат психологических наук Б. Хомуленко. Психолог советует обращать внимание на поведение отпрыска. Насторожить должна внезапная замкнутость и желание быть в одиночестве, отсутствие увлечений и интереса к происходящему. Это могут быть первые звоночки, свидетельствующие, что подростка посещают суицидальные мысли...

***

8.03.2017

«Синіми китами» керував росіянин: Студент з Миколаєва викрив куратора «групи смерті», зімітувавши самогубство

У поліції заявили, що допомога небайдужих добровольців значно підвищить ефективність боротьби із кіберзлочинцями (Украинские реалии).

У Миколаєві студент зімітував самогубство, аби виявити одного з кураторів групи смерті «Сині кити». Хлопець разом з друзями вирішив «боротися» з людьми, які через соцмережі доводять дітей до самогубства. Так, 18-річний студент-програміст І. Бондар кілька днів нібито виконував завдання куратора, – повідомляють «Українські реалії» з посиланням на Патріоти України.

Він малював рани на руках і ногах олівцем та фарбами, а фотозвіти кожного етапу відправляв керівнику групи. За три дні хлопець виконав усі 50 завдань. Останнім наказом було самогубство. Як зазначається, у процесі листування було з’ясовано IP-адресу куратора. Він виявився із Росії.

Усю зібрану інформацію хлопці передали до кіберполіції, де її перевіряють. У поліції заявили, що допомога таких людей значно підвищить ефективність боротьби із «Синіми китами».

***

9.03.2017

Почему люди делятся информацией в соцсетях

Ученые из Университета Пенсильвании решили узнать, от каких критериев зависит раскрученность того или иного материала, опубликованных в соцсетях (Экономические известия).

Исследователи следили за активностью мозга людей во время чтения заголовков и отрывков из 80 статей о здоровье в The New York Times, информирует news.eizvestia.com.

После этого добровольцев спросили, какова вероятность того, что они захотят поделиться прочитанной информацией.

Выяснилось, что люди готовы распространять тот контент, который мог бы улучшить качество их отношений с другими людьми.

К тому же, делясь той или иной информацией, индивиды хотят показаться умнее в глазах других.

В итоге ученые пришли к выводу, что внутренние ощущения и социальные отношения находятся в непосредственной связи друг с другом.

***

10.03.2017

Instagram схибнувся на слизу та піску

Серед користувачів Instagram з кожним днем дедалі більшої популярності набирає новий тренд: звуки, які видає слиз і пісок, якщо їх м’яти і розрізати (Знай.ua).

Автори відеороликів використовують прозорі загусники з додаванням блискіток і починають м’яти цю суміш або беруть кінетичний пісок, який зазвичай купують для дітей для розвитку дрібної моторики, і починають робити невеликі надрізи. Суть тут не в логіці дії, основна мета – звуки, які при цьому видаються. Усі подібні відео публікуються з хештегом #satisfyingsounds (звуки, які приносять задоволення).

Користувачі соцмереж вважають, що ці звуки ефективно розслаблюють і умиротворяють глядачів. Уже зараз опубліковано 125 тис. відео зі шматуванням кінетичного піску і 2 млн – з розминанням і розтягуванням блискучою слизу. Як не дивно, подібні роботи збирають неймовірну кількість лайків і коментарів.

***

13.03.2017

«Синій кит». Восьмикласник намагався викинутися з даху дев’ятиповерхівки на Львівщині

На Львівщині врятували 13-річного хлопця, який намагався скоїти суїцид. Про це, 13 березня на брифінгу повідомив головний поліцейський Львівщини

В. Середа, передає Львівський портал з посиланням на прес-службу ГУ НП у області (Львівський портал).

У Дрогобицький відділ поліції 13 березня близько 12:00 надійшло повідомлення про те, що в місті Стебник школяр піднявся на дах дев'ятиповерхового будинку і намагається скоїти самогубство.

На місце події виїхали працівники поліції, психолог, а також представники інших служб. Правоохоронці встановили, що покінчити життя самогубством намагається 13-річний мешканець міста Стебник, який навчається у восьмому класі однієї з місцевих шкіл.

«Хлопець поводився агресивно, нікого до себе не підпускав. Нам допомогла дівчинка, яка приятелювала з хлопцем. Вона піднялася до нього на дах і після тривалого спілкувалася врешті переконала його відійти від краю будинку, після чого правоохоронцям спільно з рятувальниками вдалося зняти його з даху», – розповів В. Середа.

Хлопець неушкоджений, перебуває під наглядом лікарів, з ним працюють психологи. Наразі правоохоронці встановлюють, що стало причиною вчинку школяра, вирішується питання про відкриття кримінального провадження.

Водночас активісти спільноти «Галицька Варта – Галицькі новини» пов'язали цей інцидент із небезпечною грою «Синій кит».

***

13.03.2017

Психолог рассказал, кто подвержен влиянию «групп смерти» в Интернете

Необходимо понимать, что не все дети могут стать жертвами «групп смерти» в Интернете (InternetUA).

Об этом корреспонденту ГолосUA сообщила социальный психолог Е. Мельникова.

«Главной аудиторией суицидальных групп в Интернете являются дети из неблагополучных семей, а также не социализированные подростки. Это связанно в первую очередь с тем, что дети этих двух категорий чувствуют себя изгоями в обществе, невероятно сильно нуждаются в принятии и понимании», – отмечает эксперт.

По словам психолога, подростки без друзей в реальной жизни, зачастую ищут поддержки в Интернете, поскольку в 13-16 лет приходить за советом к родителям, детям кажется неправильным и неестественным.

«Если ваш ребенок, трудно идет на контакт, постоянно проводит время в Интернете, становится замкнутым, у него меняется режим дня, а также он перестает волноваться о "подростковых проблемах" – вам стоит начать беспокоиться», – подчеркивает Е. Мельникова.

«Подростковые проблемы» – зачастую кажутся взрослым глупыми и надуманными, однако для ребенка они невероятно важны: страх быть высмеянным, первая влюбленность, поиск собственного пути в жизни. Все это

для подростка является демонстрацией желания жить и быть успешным. Однако, если эти «проблемы» в один миг пропадают, то можно говорить о том, что будущее для вашего чада становиться призрачным и не очень важным.

Маніпулятивні технології

9.03.2017

Війна і пропаганда. Як працюють війська інформаційних операцій Росії? // Тетяна Попова, Радіо Свобода

На засіданні Державної думи Російської Федерації 22 лютого в «годину уряду» міністр оборони Росії С. Шойгу проінформував депутатів про основні напрями діяльності свого відомства. Він відкрито підтвердив існування у збройних силах Росії військ інформаційних операцій (АРАТТА. Український національний портал).

Хоча заяву російського міністра про війська інформаційних операцій слід розуміти лише як чергове і далеко не перше оприлюднення факту їхнього реального існування та активних дій проти України.

Витік такої цікавої інформації спровокувало запитання депутата В. Жириновського, який запропонував відтворити так зване сьоме управління Генштабу: «Потрібна спецпропаганда, щоб не тільки знати армію противника, але і підготуватися до роботи з населенням».

На це, за інформацією з російських ЗМІ, С. Шойгу відповів: «За цей час створені війська інформаційних операцій, що набагато ефективніше і сильніше від усього того, що раніше ми створювали в напрямі, який називався контрпропагандою... Пропаганда повинна бути розумною, грамотною та ефективною».

Неназване «джерело» російського агентства «РБК» у Держдумі пояснило, що міністр мав на увазі структурний підрозділ у Міністерстві оборони, який займається відбиттям хакерських атак, контрпропагандою як усередині країни, так і за її межами, в Інтернеті, у ЗМІ тощо.

Голова комітету Держдуми з питань оборони В. Шаманов також заявив, що нові війська зможуть вирішувати проблеми кібератак: «Сьогодні ряд викликів перенесені у так звану кіберсферу, і, по суті, сьогодні йде інформаційне протиборство як складова частина загального протиборства».

Але давайте читати та розуміти офіційну інформацію правильно. Міністр оборони Росії та інші спікери оголосили не про початок створення військ інформаційних операцій, а лише підтвердили факт їхньої наявності та функціонування.

Справа в тому, що російська сторона ніколи не залишала інформаційний простір поза межами своєї уваги.

Зокрема, в «Доктрине информационной безопасности Российской Федерации», яка була затверджена президентом Росії 9 вересня 2000 р. зазначалося: «Источником внешней угрозы информационной безопасности Российской Федерации является разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним».

Ще в 2011 р. Міністерство оборони Росії оприлюднило документ під назвою «Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве». Зрозуміло, що це була лише відкрита та «вилизана» частина з закритих документах більш високого рівня. Наведемо кілька цитат з цього джерела:

«Наряду с сухопутным, морским, воздушным и космическим пространством, информационное пространство в армиях наиболее развитых стран стало активно использоваться для решения широкого круга военных задач…. Одним из приоритетных направлений противодействия данной угрозе является решение задач совершенствования приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника. Кроме того, в последнее время вследствие широкого применения в системах управления войсками и оружием компьютерной техники, этот перечень дополнился задачей защиты информационной инфраструктуры Вооруженных Сил Российской Федерации от различного рода компьютерных атак...

...Вооруженные Силы Российской Федерации в своей практической деятельности… развивают систему обеспечения информационной безопасности Вооруженных сил Российской Федерации, предназначенную для сдерживания и разрешения военных конфликтов в информационном пространстве.

В условиях эскалации конфликта в информационном пространстве и перехода его в кризисную фазу… воспользоваться правом на индивидуальную или коллективную самооборону с применением любых избранных способов и средств…»

Як ми бачимо, ще задовго до подій 2014–2017 рр. в Україні російська сторона офіційно визнала наявність та розвиток «системы обеспечения информационной безопасности ВС РФ».

Кінець 2016 р. також став визначальним, бо 5 грудня російський президент В. Путін своїм указом затвердив «Доктрину информационной безопасности Российской Федерации», яка замінила аналогічний нормативний акт 2010 р. Заслуговує уваги зміст 20-21 статей цього нормативного акту:

«Статья 20. Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз,

связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Статья 21. В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

а) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;

б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;

в) прогнозирование, обнаружение и оценки информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере;

г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере;

д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества».

Тобто чогось несподіваного для нас у недавній заяві російського міністра оборони ми не побачили. Є факт нормативного регулювання діяльності російських військових в інформаційному просторі у відкритих документах. Деталізацію ми можемо знайти в тих документах та планах, оприлюднення яких поки не на часі.

А для отримання можливостей здійснювати практичні заходи інформаційного впливу російське керівництво створило і активно розвиває ті структури, про які йшлося у недавньому виступі російського міністра оборони С. Шойгу перед парламентаріями. У цьому контексті недавня заява С. Шойгу є далеко не першою. Структури інформаційного протиборства традиційно були у складі збройних сил (далі – ЗС) Росії і раніше. Наприклад, на початку російської анексії Криму в складі Чорноморського флоту Росії в Севастополі дислокувалася окрема військова частина – група психологічних операцій, яка мала можливості випускати свої матеріали інформаційного впливу, поширювати інформацію в позавідомчих джерелах, організовувала та координувала відповідну «роботу» серед місцевих ЗМІ, громадських організацій тощо. З початком захоплення Криму окупанти активно пропонували українським військовослужбовцям з військової частини інформаційно-психологічних операцій ВМС ЗС України перейти на російську

сторону з обіцянкою створити для них аналогічну структуру у складі Чорноморського флоту.

Сьогодні підрозділи «інформаційних бійців» російської армії присутні у складі всіх угруповань військ, які розгорнуті вздовж кордонів України, в тому числі й на східному напрямку в складі Центру територіальних військ Південного військового округу, у складі Чорноморського флоту (включаючи підрозділи, які дислоковані на тимчасово окупованій території Криму), а також у Придністров'ї.

Українська розвідка неодноразово оприлюднювала інформацію про діяльність Управління інформаційного протиборства (у ряді джерел ця структура називається також Центром інформаційного протиборства, але від цього його сутність не змінюється) Центру територіальних військ Південного військового округу ЗС Росії.

Організаційно-штатна структура управління:

Зазначену структуру було створено з єдиною метою – підвищення ефективності проведення заходів інформаційної війни проти України в межах зони відповідальності зазначеного центру територіальних військ, включаючи тимчасово окуповані райони Донецької та Луганської області.

Дані щодо особового складу російського підрозділу також оприлюднило Головне управління розвідки Міноборони України.

Цілком очевидно, що сидячи лише в місті Новочеркаськ Ростовської області, проводити активні інформаційні заходи впливу важко. Тому, у складі штабів 1-го та 2-го армійських корпусів угруповань «ДНР/ЛНР» (давайте говорити відверто – російської армії) сформовані відповідні підрозділи – групи інформаційного протиборства та оперативного маскування. А на більш нижчому рівні – безпосередньо в «полі» або з реалізації конкретних проектів впливу – діють тимчасові оперативні групи фахівців, у тому числі від зазначеного центру інформаційного протиборства.

У відкритих джерелах вдалося знайти інформацію про певні результати діяльності таких «фахівців»:

– підготовка матеріалів інформаційно-психологічного впливу на визначені цільові аудиторії, їхнє розміщення на підконтрольних інформаційних ресурсах РФ і так званих «ДНР/ЛНР»;

– поширення відповідної інформації антиукраїнського спрямування в соціальних мережах, адресна робота серед українських громадян і представників сил АТО через мережу Інтернет;

– підготовка матеріалів впливу в проросійській інтерпретації про події на Сході України та їхня передача іншими інформаційним структурам для подальшого поширення в російських та іноземних ЗМІ;

– організація теле- та радіомовлення, підготовка та організація розсилання з використанням мобільного зв'язку СМС-повідомлень відповідного змісту військовослужбовцям сил АТО і населенню поблизу лінії зіткнення сторін;

– інформаційні заходи серед особового складу 1-го та 2-го армійських корпусів військ агресора;

– сприяння розбудові інформаційної інфраструктури так званих «ДНР/ЛНР»;

– проведення заходів щодо «керованого надання інформації» представникам міжнародних організацій та ЗМІ безпосередньо в районі АТО;

– нарощування власних можливостей інформаційного впливу через залучення до співпраці окремих громадян із антиукраїнськими настроями, формування їхніх відповідних мереж, у тому числі на інтернет-ресурсах;

– сприяння ватажкам угруповань «ДНР/ЛНР» щодо створення та діяльності власних структур інформаційного впливу (починаючи від так званих «міністерств інформації», «незалежних» ЗМІ тощо), їхня координація.

Можна навести кілька типових прикладів діяльності Центру інформаційного протиборства.

Зокрема, 29 липня 2016 р. українська розвідка виявила спробу російських «інформаційних бійців» із залученням підконтрольних ЗМІ зробити постановочні відеорепортажі на окупованій частині Донбасу на позиціях «7-ї окремої мотострілецької бригади» (Дебальцеве) та «6-го окремого мотострілецького полку» (Стаханов) про нібито обстріли силами АТО знімальних груп російських та іноземних телеканалів.

Схожа ситуація з підготовкою «фейкових» репортажів була виявлена на позиціях «11 окремого мотострілецького полку» (Донецьк).

До речі, російське командування постійно здійснює заходи щодо розширення технічних спроможностей зазначеного підрозділу інформаційного протиборства. Зокрема, у березні 2016 р. з метою обмеження доступу населення тимчасово окупованих територій до українських джерел в мережі Інтернет у Донецьк було направлено програмно-апаратний комплекс для проведення розподілених кібератак типу «відмова в обслуговуванні (DDoS)».

Керівництво угруповань «ДНР/ЛНР», які визнані в України терористичними, за сприяння російських кураторів активно розвиває «власні» структури інформаційного впливу та інформаційної інфраструктури: органи

«влади» на кшталт «міністерства інформації ДНР», підконтрольні ЗМІ, власних операторів мобільного зв'язку (наприклад «Фенікс») та інших телекомунікаційних послуг, інтернет-провайдерів тощо. В усіх цих проектах неприкрито стирчать «вуха» фахівців Центру інформаційного протиборства та інших силових структур Росії, які активно діють на тимчасово окупованих територіях України.

Скажемо відверто, що ЗС Росії порівняно з нами працювати легше, бо, окрім можливостей оборонного відомства та інших силових структур, у Росії функціонує загальнодержавна система активного інформаційного впливу. Зокрема, недавно у відкритому нормативному документі РФ офіційно включила інформаційні агентства «RT» («Россия сегодня») та «ТАСС», а також «Всероссийскую государственную телевизионную и радиовещательную компанию» («ВГТРК») (телеканали «Россия 1», «Россия 24», «РТР Планета» тощо) та телецентр «Останкино» у список федеральних державних унітарних підприємств, які мають «существенное значение для обеспечения прав и законных интересов граждан РФ, обороноспособности и безопасности государства».

В узагальненому вигляді Росія реалізує заходи, які дуже схожі на те, що ми спостерігаємо у західних країнах щодо набуття спроможностей ведення збройного протиборства в інформаційному домені. Водночас ці підходи мають своє, власне, «національне забарвлення», з огляду на внутрішні та зовнішні умови, в яких перебуває Росія.

«Національні особливості» визначаються тим, що, окрім ЗС РФ, на російські правоохоронні органи та спецслужби покладено також значний перелік завдань, які вони називають «обеспечением информационной безопасности в области государственной и общественной безопасности».

Іншою особливістю є наявність значних і потужних державних ресурсів для теле- і радіомовлення, присутності в Інтернеті, у тому числі за кордоном, які Росія активно розвиває протягом багатьох років.

Також важливо зазначити, що існують механізми чіткої централізації дій в інформаційному просторі на загальнодержавному рівні та координації їхньої діяльності з боку російського президента та його оточення.

Про українські варіанти реагування на наведені вище заходи російських військових, у тому числі щодо створення власних структур для дій в інформаційному просторі поговоримо в наступній публікації. Але вже сьогодні українці можуть привітати один одного з невеликою, але все ж таки перемогою. Вважається, що під час війни краща оцінка твоїх дій – це оцінка з боку противника. Очевидно, що ЗС РФ змушені були створити свої війська інформаційних операцій як відповідь на заходи протидії російській інформаційній агресії з боку України. І це означає, що всі бійці інформаційного фронту Української держави протягом 2014–2016 рр. показали таку ефективність своїх дій, що в своїй сукупності змусили противника переглянути свої попередні підходи та приступити до чергового перезавантаження.

***

14.03.2017

Около 48 миллионов аккаунтов в Twitter могут быть ботами

Как выяснилось, значительная доля лайков и ретвитов в Twitter исходит совсем не от людей. Согласно новому исследованию Университета Южной Калифорнии, до 15 % аккаунтов в сервисе – это боты, а не живые пользователи. Для Twitter, изо всех сил пытающейся расширить свою пользовательскую базу на фоне растущей конкуренции со стороны Facebook, Instagram, Snapchat и других сервисов, эта новость может оказаться довольно тревожной (InternetUA).

Исследователи университета воспользовались более чем тысячей функций для идентификации ботов в Twitter – учитывались пользователи в списках друзей таких аккаунтов, контент в твитах и их настроение, а также периодичность публикаций. С помощью специального фреймворка исследователи выяснили, что «от 9 до 15 % активных аккаунтов в Twitter являются ботами».

Поскольку в сервисе сегодня насчитывается 319 млн активных пользователей, число ботов в нём может равняться приблизительно 48 млн. В отчёте при этом говорится, что некоторые сложные боты могут демонстрировать поведение, близкое к человеческому, из чего можно сделать предположение, что 15 % – показатель как минимум слегка заниженный.

Стоит отметить, что по оценкам самой Twitter число ботов в сервисе значительно ниже. В поданной в Комиссию по ценным бумагам и биржам США заявке компания отметила, что до 8,5 % всех активных аккаунтов обращались к серверам Twitter «без каких-либо заметных дополнительных действий, инициированных пользователем».

Если подсчёты Университета Южной Калифорнии верны, то ботов в сервисе примерно на 20 млн больше, чем предполагает Twitter. И в свете обеспокоенности аналитиков касательно роста числа пользователей это может стать для компании серьёзной проблемой.

Представитель компании написал, что в то время как боты зачастую оказывают на сервис негативное влияние, «многие аккаунты-боты чрезвычайно полезны, вроде тех, которые автоматически предупреждают людей о стихийных бедствиях». Исследователи университета также отмечают полезность некоторых ботов.

В отчёте, тем не менее, упоминается и другая их сторона – в частности, отмечается, что в сервисе растёт число вредоносных ботов. Некоторые из них, имитируя человеческое поведение, способны оказывать политическую поддержку и содействовать террористической пропаганде и вербовке.

Спецслужби і технології «соціального контролю»

5.03.2017

Китайский чиновник выступил за ослабление интернет-цензуры

Заместитель председателя Народного политического консультативного совета КНР Л. Фухэ заявил, что интернет-цензура в Китае вредит развитию экономики и науки страны, сообщает The Guardian (InternetUA).

По его словам, запреты в Интернете также уменьшили энтузиазм иностранных инвесторов по вложению средств в КНР. Л. Фуэх считает возможным ослабить интернет-цензуру и отменить ее в отношении всего, что не касается высказываний по политике страны.

Отмечается, что это очень редкий критический выпад в сторону цензуры в КНР, которая лишь усилилась с момента, как председателем КНР в 2012 г. стал С. Цзиньпин.

В середине 2015 г. сообщалось, что китайское правительство намерено блокировать доступ к Интернету в случае массовых волнений и беспорядков в стране.

В Китае действует одна из самых строгих и сложных систем цензуры Интернета под названием «Великий фаервол»: она полностью блокирует многие зарубежные сайты вроде Google, Twitter, Facebook, Instagram и YouTube.

***

6.03.2017

Папиев: Любую критику власти «закатает в асфальт» Доктрина информационной безопасности

Доктрина информационной безопасности не просто угрожает свободе слова – это прямой путь к тоталитаризму. Такое мнение высказал народный депутат от Оппозиционного блока М. Папиев, комментируя введение в действие решения СНБОУ «О Доктрине информационной безопасности Украины», передает Украинские Новости. По мнению политика, доктрина «информационной безопасности» станет одним из орудий власти по сведению счетов с инакомыслием (From-UA Новости Украины).

«Доктрина информационной безопасности “закатает в асфальт” любую критику власти. Ее суть состоит не в защите информационного поля, а в “закручивании гаек” на фоне тотального недовольства властью», – отметил М. Папиев.

По его словам, любая критика власти отныне будет расцениваться как угроза национальной безопасности.

«Кабмин уже получил указание разработать ряд законов, которые позволят оперативно блокировать все неугодные интернет-ресурсы. То есть, власть на свое усмотрение будет решать, какой ресурс представляет для нее угрозу, а какой нет», – добавил оппозиционер.

М. Папиев обратил внимание на то, что против доктрины информационной безопасности выступил ряд международных правозащитных организаций, в том числе – Amnesty International.

Кроме того, по словам политика, украинские власти не получили позитивных выводов европейских экспертов на доктрину, а предыдущую версию документа резко раскритиковали медиаэксперты Совета Европы.

«В 2015 г. Совет Европы делал анализ проекта концепции информационной безопасности Украины и рекомендовал не утверждать его, поскольку он содержал положения, которые могут ограничивать свободу слова. В этот раз мнением Совета Европы украинская власть решила вообще пренебречь», – подчеркнул оппозиционер.

Народный депутат также привел данные организации «Репортеры без границ», согласно которым практика блокирования неугодных интернет-ресурсов успешно практикуется в Алжире, Бахрейне, Зимбабве, Иране, Киргизии, Пакистане, России, Китае, Сирии и Северной Корее.

«Учитывая уровень недовольства властью и рост напряжения в украинском обществе, обвинить в “угрозе национальным интересам” можно любой информационный ресурс. Таким образом, доктрина информационной безопасности не просто угрожает свободе слова и демократии, а ведет страну к диктатуре», – подчеркнул М. Папиев.

По его словам, действующую «информационную доктрину» необходимо немедленно отменить. При этом Верховная Рада должна начать работу над альтернативным документом с привлечением экспертов Совета Европы.

***

10.03.2017
Тимур Чмерук
Інтернет-цензура – крок у майбутнє?

Чи є необхідність впроваджувати обмеження в Інтернеті і чому цією проблемою активно займається влада?

Про цензуру в політиці і в публічному просторі українські політики нового призову не полюбляють говорити відверто й чесно. Проте готові «діяти» і боротися з уявним ворогом за допомогою механізмів, які, по суті, мають тональність і форму цензури в Інтернеті. За великим рахунком, цензура в Інтернеті – це, по-перше, контроль та припинення доступу до інформації у глобальній мережі («Главком»).

«Зрада» чи «перемога»?

Кінець 2016 р. був вельми «продуктивним» для українського політикуму на «цікаві» закони, ініціативи та пропозиції. Зокрема, П. Порошенко ввів у дію рішення РНБО від 29 грудня 2016 р. «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» – відповідний указ від 13 лютого опубліковано на сайті Президента. Згідно з документом, який передбачає «запровадження механізму використання в кримінальному процесі доказів в

електронній формі», Кабміну в тримісячний строк доручено внести на розгляд парламенту законопроекти щодо імплементації положень Конвенції про кіберзлочинність. Вони повинні «передбачити запровадження блокування (обмеження) за рішенням суду операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (сервісу)». Безумовно, рішення неоднозначне. І логічно, що цілком виправданою є реакція громадськості. Ідеться про позицію Інтернет-асоціації України. За її оцінками, справжня мета рішення РНБО – блокування інформації, що є запровадженням політичної цензури. Крім того, введення технічного механізму блокування доступу до Інтернету поставить Україну в один ряд з такими країнами, де цей механізм існує, – Китаєм, Іраном, Росією.

Водночас країни західної цивілізації з розвинутою демократією, до яких Україна прагне належати, такого механізму принципово не мають. Тож українським високопосадовцям доведеться вирішувати: свобода слова, думки є для них фейком чи реальною політичною метою? Якщо можновладці схиляться до першого, то очевидним результатом стане не лише обмеження політичних свобод громадян країни, а й значні збитки для економіки.

Так, уряд має передбачити «встановлення вимог щодо надання операторам та провайдерам телекомунікацій на вимогу правоохоронних органів інформації, необхідної для ідентифікації постачальників послуг і маршруту, яким було передано інформацію». При цьому правоохоронним органам мають бути надані повноваження щодо внесення обов'язкових до виконання приписів власникам комп'ютерних даних, необхідних для розкриття злочину, на строк до 90 днів із можливістю продовження такого строку до трьох років.

Інтернет-цензура для громадян?

РНБО, політики від коаліції переконують: «Усе добре, це для вашого блага». Очевидно, на їхню думку, це має заспокоїти представників інтернет-провайдерів і громадян. Але, щоб щось контролювати, потрібно чітко знати, для чого це потрібно і які ризики та наслідки можуть мати ці дії.

Якщо послухати народних депутатів від коаліції, жодного негативу від рішення РНБО від 26 грудня 2016 р. немає. Контроль над сайтами, на яких міститься інформація, наприклад, як самотужки виготовити бомбу або якими методами пограбувати банкомат, справді зрозумілий аргумент для громадян.

Непокоїть депутатів і питання різноманітних «груп смерті», які націлені на деструктивний психологічний вплив на дітей. Адже, якщо проаналізувати наслідки діяльності цих груп у Росії, дійсно стає зрозумілим, що їм треба протидіяти.

Так, інтернет-цензура достатньо складна, але цілком здійсненна. Її можливо реалізувати за допомогою ряду заходів.

Перше. Зосередження в руках держави управління мережевими комунікаціями, важелів впливу на компанії, у віданні яких перебувають Мережі.

Друге. Надання права доступу до інтернет-ресурсів компаніям, готовим контролювати вміст ресурсів, видаляючи або редагуючи повідомлення. Це так чи інакше підпадає під цензуру.

Третє. Також уряди мають можливість контролювати зміст деяких інтернет-ресурсів через підставні фірми, «неурядові організації» або приватних осіб, які під різними приводами цензурують інформацію.

У Росії, приміром, було створено Єдиний реєстр заборонених сайтів, який оновлюється і до якого додаються потенційно небезпечні інтернет-ресурси.

Як і в кожної монети тут є зворотній бік – не лише плюси, а й мінуси.

Інший же бік цієї проблеми – значні втрати, як матеріальні так і репутаційні, для приватного бізнесу. Цензура Інтернету матиме опосередкований вплив на сферу інтернет-провайдингу, на ті компанії, які інвестують у якісне надання послуг, натомість якщо кількість цих клієнтів зменшуватиметься, кампанії будуть змушені переорієнтовуватись на інші ринки та зменшувати кількість спеціалістів, обмежувати можливість доступу до надання якісного інтернет-провайдингу.

У сучасних умовах, коли, з одного боку, з'явилися нові можливості отримувати вигоду від ІТ, а з іншого – у багатьох компаній виникла необхідність оптимізації витрат на ІТ, інтернет-провайдери розробляють пропозиції, що враховують ці потреби. Чи розуміють можновладці, політикум шкоду для інтернет-бізнесу, коли допускають імовірність упровадження поступової цензури? Повною мірою, вочевидь, ні.

Є, звичайно, методи подолання інтернет-цензури, як-от можливість доступу до заблокованих ресурсів через дозволені ресурси. Такими ресурсами є веб-проксі, проксі-сервер, анонімні мережі, веб-сервіси перекладу вмісту веб-сторінок за вказівкою адреси сторінки (наприклад, Google Translate).

***

10.03.2017

Украинские интернет-провайдеры опасаются, что власти заставят их «фильтровать» контент

Потенциальные риски нарушения конституционных прав украинских граждан содержатся в одобренной недавно президентом доктрине информбезопасности СНБО. Такой посыл дает крупнейшее отраслевое объединение Интернет Ассоциация Украины (ИнАУ) в своем письме главе СНБО А. Турчинову, премьер-министру В. Гройсману, главе СБУ В. Грицаку и руководителям других ведомств, – передает ЛІГАБізнесІнформ (ОстроВ).

В доктрине написано, что на законодательном уровне должен появиться механизм фиксации, блокировки и удаления из украинского сегмента сети Интернет информации, которая угрожает жизни, здоровью граждан, пропагандирует войну, вражду, изменение конституционного строя насильственным путем или угрожает суверенитету.

В ИнАУ считают, что при выполнении указанного требования доктрины государство должно гарантировать гражданам право на свободу слова, как это прописано в Конституции. Кроме этого, ассоциации непонятно ни с юридической, ни с технологической точки зрения, кто именно и как должен удалять информацию из УАнета. Ведь по закону о телекоммуникациях операторы и провайдеры не несут ответственности за содержание информации, передаваемой их сетями. Поэтому в ИнАУ убеждены, что государственные меры должны быть направлены в первую очередь на выявление и наказание лица, угрожающего информбезопасности, а не на создание препятствий в ведении телеком-бизнеса.

«Мы опасаемся злоупотреблений со стороны властей», – рассказывает глава ИнАУ А. Федиенко. По его словам, если бы в стране доверие общества к правительству было на высоком уровне, то изложенные в доктрине идеи не вызывали бы ни у кого вопросов. «Но у нас государство неоднократно хотело регулировать доступ к информации в сетях провайдеров. Поэтому мы считаем, что единственный правильный способ блокировки контента в Интернете – через суд», – подчеркивает он.

А. Федиенко говорит, что запрет на доступ к информации не самый действенный метод. По его словам, не запрет, а контрпропаганда – это наиболее эффективный путь и для Украины. «Нашу страну нельзя изолировать от мирового информпространства. Нельзя отключить Интернет. Поэтому противостоять можно, создавая собственный разъясняющий контент», – добавляет он.

Впрочем, управляющий партнер ЮК Jurimex Ю. Крайняк считает, что ИнАУ торопится паниковать, так как сама доктрина имеет лишь декларативный характер. А непосредственные нормы вводятся только через изменения в закон. «Вы же знаете, как принимаются законы, и что это процесс непредсказуемый и слабо поддающийся контролю?» – отмечает он.

Как считает Ю. Крайняк, лучшее, что могла бы сделать ИнАУ в данной ситуации, – это самостоятельно подготовить законодательные изменения по информбезопасности в таком виде, в каком их видят члены Ассоциации. «Если ты не хочешь сделать сам, как хочешь ты, тогда это сделает кто-то другой, как хочет он», – резюмирует юрист.

***

10.03.2017

У Прилуках затримали антиукраїнського інтернет-агітатора

«Правоохоронці зафіксували, що чоловік регулярно розміщував на персональних сторінках пропагандистські матеріали, що закликають до зміни державного кордону України і популяризують терористичні організації “ДНР/ЛНР”. Інформацію агітатор отримував від куратора тимчасово окупованих бойовиками територій», – йдеться в повідомленні (Незалежне Бюро Новин).

Під час обшуку за місцем проживання зловмисника співробітники спецслужби вилучили комп'ютерну техніку з доказами протиправної діяльності.

У рамках кримінального провадження, відкритого за ч. 1 ст. 110 (посягання на територіальну цілісність і недоторканність України) Кримінального кодексу України, агітатору оголошено про підозру у вчиненні злочину.

Триває досудове слідство.

***

9.03.2017

Касперская: Компьютерное оружие ЦРУ может проникнуть в незащищенные устройства каждого

Наталья Касперская, глава InfoWatch и соосновательница «Лаборатории Касперского» заявила, что компьютерное оружие ЦРУ способно проникнуть в устройства каждого. Предприниматель рассказала об угрозах и последствиях утечки WikiLeaks, сообщает Царьград (Grifonsoft).

По словам Н. Касперской, спустя некоторое время появятся программы, способные защищать компьютерные устройства от влияния разных опасных приложений. По мнению предпринимателя, подобные вирусы могут поражать систему мобильных устройств, работающих на разных операционных устройствах. На портале организации WikiLeaks появилась информация, что хакеры смогут в дальнейшем дистанционно осуществлять взлом больничных систем жизнедеятельности. Н. Касперская считает, что средства защиты существенно отстают от выпускаемых программ.

Как заявила Н. Касперская, Интернет вещей является очень опасным явлением, так как он усугубляет проблему отсутствия защиты на множество устройств и приложений. По мнению предпринимателя, государство должно контролировать процесс защиты данных пользователей от хакеров и определять границы поступления личной информации населения. Руководитель InfoWatch полагает, что должна быть организована специальная служба, сотрудники которой проверяли бы, куда поступают личные данные пользователей соцсети.

***

9.03.2017

Ассанж звинуватив спецслужби в некомпетентності, яка дозволила отримати доступ до даних про кібершпіонаж

Організація WikiLeaks вирішила надати технологічним компаніям ексклюзивний доступ до файлів про хакерські операції ЦРУ, щоб вони могли розробити захисні механізми проти вразливостей, якими користувалася спецслужба. Про це заявив засновник WikiLeaks Дж. Ассанж на прес-конференції з посольства Еквадору в Лондоні 9 березня (Корреспондент.net).

«Ми вирішили працювати з ними, надати їм ексклюзивний доступ до окремих технічних деталей, які у нас є», – розповів Дж. Ассанж.

Він нагадав, що опубліковані на сайті організації документи і файли були відредаговані, щоб у відкритий доступ не потрапили безпосередньо хакерські методи ЦРУ.

Ассанж вважає, що ЦРУ втратило контроль над усім арсеналом своєї кіберзброї, який необачно зберігався в одному місці і був недостатньо захищений. У підсумку до нього отримало доступ велике коло неавторизованих осіб.

Навіть більше, зважаючи на дані ЗМІ, спецслужби знали ще кілька місяців тому, що дані про кіберможливості ЦРУ потрапили в широкий доступ, однак не вжили нічого, щоб попередити про це громадськість або технологічні компанії.

Раніше Wikileaks опублікував новий витік даних під назвою Vault 7. У ньому міститься понад 8 тис. документів ЦРУ, які говорять про існування систем кіберслідкування, про розробку вірусних програм і спроби зламати антивірусне програмне забезпечення.

***

9.03.2017

Павел Дуров объяснил, каким образом ЦРУ получает доступ к перепискам пользователей Мессенджеров

7 марта, известный портал WikiLeaks опубликовал официальные документы ЦРУ, повествующие о взломе устройств на операционных системах iOS и Android, а также Smart TV. Служба безопасности использовала уязвимости операционных систем, чтобы получить доступ к любой переписке пользователя. П. Дуров объяснил, каким образом ЦРУ получает доступ к перепискам пользователей Мессенджеров, в том числе и в Telegram (InternetUA).

Представительство Telegram утверждает, что шифрование в приложениях не имеет никакого значения, если существуют инструменты для взлома операционных систем. ЦРУ не взламывали шифрование Мессенджеров, таких как Telegram, WhatsApp или Signal, а использовали уязвимости операционных систем iOS и Android. Решение вопросов безопасности полностью лежит на таких компаниях, как Apple, Google и Samsung.

«Замок – это безопасное приложение для обмена сообщениями. Устройство и операционная система – это гора. Замок может быть крепким, но если гора под ним – это действующий вулкан, то разработчики ничего не смогут с этим поделать.

Неважно, каким Мессенджером вы пользуетесь, приложение не может запретить вашей клавиатуре считывать информацию о том, на какие кнопки вы нажимаете. Никакое приложение не скроет от системы информацию о том, что

демонстрируется на экране. Всё это не является проблемой приложений», – говорит П. Дуров.

В данном случае, гора полна тайных туннелей и проходов. Теперь, когда производители получили её карту, они могут начать исправлять все уязвимости системы. Для этого потребуется много часов работы и много обновлений безопасности для устройств, но в конце концов они должны исправить все существующие проблемы.

В Telegram считают, что их пользователей проблема не должна волновать: «Если за вами не гонится ЦРУ, то вам не о чем беспокоиться», а также дали несколько советов по защите личных данных:

– не используйте кастомизированные версии прошивок;

– не устанавливайте приложения из небезопасных источников;

– всегда устанавливайте актуальную версию операционной системы и все патчи безопасности, приходящие на устройство.

***

13.03.2017

Китай закликав США припинити стеження і кібератаки

«Китай виступає проти будь-яких форм кібератак, ми закликаємо США зупинити прослуховування, спостереження, стеження, кібератаки і т. д. щодо Китаю й інших країн», – про це на прес-конференції 9 березня заявив прес-секретар Міністерства закордонних справ Китаю Г. Шуан, відповідаючи на запитання про кібератаки ЦРУ на Китай, повідомляє кореспондент газети «Женьмінь жибао» Х. Цзес (LB.ua).

7 березня на сайті Wikileaks було опубліковано майже 9000 секретних документів, що, ймовірно, належать ЦРУ, з яких видно, що інформаційний інтернет-центр ЦРУ налічує понад 5000 співробітників, сукупно було створено понад 1000 хакерських інструментів. Документи показують, що ЦРУ використовувало слабкі місця персональних електронних пристроїв і операційних систем; за допомогою розроблених тисяч програмних вірусів, троянських програм та інших хакерських інструментів втручалося в життя звичайних людей, наприклад, інтелектуальний телевізор Samsung може після хакерської атаки перетворитися на записувальний пристрій, пише журналіст.

Уряд США 8 березня порушив кримінальну справу за фактом витоку інформації. Прес-секретар Білого дому Ш. Спайсер на черговій прес-конференції цього дня відмовився підтвердити справжність цих документів, але підкреслив, що американців у цій ситуації повинен хвилювати витік секретної інформації.

«Китай буде твердо стояти на захисті своєї кібербезпеки, зміцнювати діалог і співпрацю з міжнародною спільнотою, у рамках ООН розробляти загальноприйняті міжнародні правила поведінки в кіберпросторі, а також спільно сприяти зміцненню мирного, безпечного, відкритого й упорядкованого мережевого простору», – підкреслив Г. Шуан.

1 березня китайський уряд випустив Стратегію міжнародного співробітництва в кіберпросторі. У цій стратегії наголошено, що необхідно сприяти розвитку міжнародного співробітництва на основі чотирьох базових принципів – миру, суверенітету, спільного управління та повсюдної вигоди.

У червні 2013 р. колишній співробітник Агентства національної безпеки США Е. Сноуден надав німецькій газеті Der Spiegel інформацію про те, що США здійснюють масштабні мережеві атаки проти Китаю, мішенями також є китайські лідери, компанія Хуавей та ін. Мішені атак включали Міністерство комерції, Міністерство закордонних справ, банки, телекомунікаційні компанії та ін. Der Spiegel зазначила, що спостереження США також поширюється на колишніх китайських лідерів і багато урядових структур і банків. З тих пір Китайський інформаційний інтернет-центр випустив Записи глобального прослуховування США, де зазначено, що відповідні китайські відомства протягом декількох місяців провели перевірки і виявили, що знахідки про дії проти Китаю загалом відповідають дійсності.

***

9.03.2017

Кремль звинуватив спецслужби США у прослуховуванні російських чиновників

«Спецслужби США давно прослуховують російських чиновників», – заявив офіційний представник Кремля Д. Пєсков (Інформаційна агенція «Вголос»).

Про це він сказав у коментарі про матеріали Wikileaks, які, як стверджують їхні автори, розкривають хакерський інструментарій американських спецслужб, повідомляє ВВС.

«У Вашингтоні, власне, і не приховують, що вони активно прослуховують російських офіційних осіб – і нашого посла [у США Сергія] Кисляка і т. д., – сказав він. – Там цього ніхто і не приховує, тому тут можна Wikileaks і не розкривати – можна здогадатися».

***

13.03. 2017

Кабмін почав готувати законопроект про блокування сайтів

Уряд доручив МВС, Нацполіції і СБУ до кінця квітня підготувати пропозиції до законопроекту про блокування доступу до інформаційних ресурсів на підставі рішення суду (LB.ua).

Про це йдеться в Розпорядженні уряду № 155 від 10 березня, яким затверджено план заходів щодо реалізації стратегії кібербезпеки України на 2017 р.

***

13.03.2017

Росіянам увімкнуть сповільнювач Інтернету

Уряд Росії обговорює ідею закону про обмеження швидкості доступу до сайтів іноземних компаній, які не виконують рішення російських судів (Знай.ua).

Про це пишуть російські ЗМІ, з посиланням на чиновників.

Водночас прес-секретар президента країни-агресора В. Путіна Д. Пєсков заявив, що нічого не чув про цей законопроект.

Ідея виникла після того, як Google відмовився виконувати вимоги Федеральної антимонопольної служби (ФАС) про попереднє встановлення додатків на Android. Тоді глава відомства І. Артем'єв заявив, що жодна держава не потерпить того, щоб рішення її судів не виконувалися. І пообіцяв Google «багато цікавого».

Варіант уповільнити доступ, а не повністю відключити ресурси, обрали тому, що блокування популярних сайтів недоцільне в передвиборчий період.

Водночас, за словами джерел, це і більш складний варіант. Особливо важко сповільнювати швидкість для операторів фіксованого зв'язку.

***

14.03.2017

Рішення РНБО щодо блокування інформації – це політична цензура, – Інтернет асоціація України

Рішення РНБО щодо блокування інформації в Інтернет і прийнятий на підставі нього указ Президента П. Порошенко, це спроба ввести в Україні політичну цензуру, вважають в Інтернет Асоціації України (ІнАУ). Про це повідомляє sprotiv.org. (Громадський спротив України).

«ІнАУ схиляється до висновку, що справжні цілі впровадження Рішенням РНБО блокування інформації є суто створення політичної цензури», – сказано в тексті відкритого листа Асоціації на ім'я Президента, прем'єра і глави служби спецзв'язку і захисту інформації України.

Фахівці звертають увагу, що впровадження технічного механізму блокування доступу до Інтернету поставить Україну в один ряд з такими країнами, де цей механізм існує: Китаєм, Іраном, Росією.

Водночас, як відзначають в ІнАУ, країни західної цивілізації з розвинутою демократією, до яких Україна декларує прагнення належати, такого механізму принципово не мають, наприклад Швеція, Фінляндія, США.

При цьому фахівці вказують на ряд положень указу, які можуть призвести не тільки до обмеження політичних свобод громадян країни, а й до багатомільярдних збитків для економіки.

Проблема захисту даних. DDOS та вірусні атаки

6.03.2017
Для приложения-вымогателя Dharma выпустили дешифратор

Пользователи пострадавших от приложения-вымогателя Dharma компьютеров получили радостную весть, поскольку смогут вернуть свои зашифрованные файлы бесплатно. Исследователи создали инструмент дешифрования для этого семейства вымогателей после того, как в сеть недавно попали ключи дешифрования (InternetUA).

Вымогатель Dharma появился в прошлом ноябре и основан на более старом вымогателе Crysis. Его можно узнать по расширению зашифрованных файлов: .[email].dharma, где email является адресом электронной почты для связи со злоумышленниками для переговоров по выкупу файлов.

Пользователь gektar опубликовал на форуме BleepingComputer.com ссылку на пост в Pastebin. По ней содержатся ключи дешифрования для всех вариантов Dharma. В ноябре то же самое произошло с ключами для Crysis.

Неизвестно, кто такой gektar и откуда взяты ключи. Есть предположение, что у него был доступ к исходному коду вымогателя. Главное, что ключи настоящие, что подтвердили лаборатория Касперского и компания ESET. Они обновили свои инструменты для дешифрования Crysis, приложения Kaspersky RakhniDecryptor и ESET CrysisDecryptor, теперь они могут расшифровывать и Dharma.

Это ещё раз напоминает о том, что пользователи должны сохранять зашифрованные файлы на случай, если возможность вернуть доступ к ним появится в будущем. Специалисты могут найти уязвимости в коде приложений или получить доступ к командным серверам и за счёт этого к ключам шифрования. Также следует искать инструменты дешифрования на портале NoMoreRansom.org.

***

6.03.2017
Uber годами следила за чиновниками по всему миру

Компания Uber в течение нескольких лет обманывала правительства государств, где ее работе препятствовали правоохранительные органы или где сервис был запрещен. Как сообщает New York Times, с помощью инструмента Greyball компания использовала данные с приложения Uber и другие техники для идентификации и обмана чиновников, пытавшихся закрыть сервис. В частности компании удалось перехитрить власти Бостона, Лас-Вегаса, Парижа, а также правительства Австралии, Китая и Южной Кореи (InternetUA).

Greyball является частью программы под названием VTOS, сокращенно от «violation of terms of service» – «нарушение условий использования».

Кампания была запущена в начале 2014 г. и затрагивает преимущественно цели за пределами США. Примечательно, программа и в частности Greyball были одобрены юристами Uber.

VTOS работает следующим образом. При запуске сервиса в новом городе назначается ответственный за его работу региональный менеджер. Одной из его обязанностей является обнаружение сотрудников правоохранительных органов, способных помешать работе Uber. В частности на цифровой карте города вокруг правительственных учреждений помечаются геозоны. Далее компания фиксирует, кто в отмеченных геозонах регулярно открывает и закрывает приложение.

Другие техники слежения включают обнаружение связей между введенными в приложение данными кредитных карт и правоохранительными органами. Для поиска дополнительных сведений сотрудники Uber анализируют учетные записи в социальных сетях.

***

6.03.2017

Россия продолжает кибератаки на американские серверы

Хакеры из России продолжают осуществлять кибератаки на серверы в США. Они взламывают серверы «либеральных групп» для получения компромата и вымогательства денег, сообщает Bloomberg (InternetUA).

Сообщается, что среди атакованных организаций – Arabella Advisors (занимается консультацией либеральных активистов) и Центр прогресса США (призывал расследовать связи президента США Д. Трампа с Россией).

Источники информагентства информируют, что с попытками вымогательства в период выборов в США столкнулись не менее 12 таких групп. Требования варьировались от 30 тыс. до 150 тыс. долл. в биткоинах. По данным агентства, методы, используемые хакерами, походят на методы работы группы Cozy Bear. В США ее называют ответственной за взлом серверов Национального комитета Демократической партии и связывают с российскими властями.

***

5.03.2017

NYT: США проводят кибератаки против серверов КНДР

Вашингтон в течение последних трех лет проводит серию кибератак на серверы Северной Кореи с целью дестабилизировать ракетную программу КНДР, пишет The New York Times (InternetUA).

Отмечается, что экс-президент США Б. Обама во время своего президентства поручил создать специальную программу по кибератакам против Пхеньяна, чтобы срывать тестовые запуски баллистических ракет, проводимых государством.

В результате этой политики Вашингтона число неудачных ракетных пусков Северной Кореи значительно возросло: ракеты стали чаще взрываться, отклоняться от курса и падать в море.

При этом издание отмечает, что последние успешные пуски ракет Пхеньяна демонстрируют снижение эффективности воздействия со стороны американских спецслужб.

***

7.03.2017

Ольга Карпенко

Киберполиция закрыла 67 фейковых автосайтов: они выманивали деньги на «выигрышные авто»

Киберполиция на днях отчиталась о закрытии 67 сайтов, с помощью которых мошенники выманивали у пользователей деньги. Закрыли также и хостинг, который обеспечивал работу сайтов (название не уточняется) (AIN.UA).

Были закрыты сайты autolife.co.ua, evro-drive.info, kiamotor-ua.info, comfort-m.info и многие другие (полный список есть на сайте ведомства). Сейчас они недоступны онлайн, но в кеше Google можно проверить, что на подобных сайтах размещались правила акции, где призами якобы были автомобили различных марок. Официальные представительства и дилеры еще в прошлом году заявляли, что не имеют отношения к этим сайтам и их акциям.

Как сообщает ведомство, призов на самом деле не было и акций никаких не проводилось, мошенники действовали по довольно старой схеме: просто рассылали пользователям СМС про якобы выигранные авто. Чтобы получить такой приз, пользователю предлагали уплатить некоторый процент налога от стоимости авто или требовали с него другой платеж.

6 марта Киберполиция с представителями следственного управления полиции Харькова и прокуратуры задержала участников группы: 3 основных организаторов и 11 членов группы. При обыске и задержании оперативники изъяли компьютеры, GSM-шлюз для рассылки сообщений и около 1500 использованных SIM-карт различных операторов, которые использовались для массовых рассылок.

Киберполиция также опубликовала номера карточных счетов, которые использовались для присвоения средств.

***

5.03.2017

Из телефонов Samsung сделали устройства для кражи денег с карт

Специалист по информационной безопасности Б. Кребс (Brian Krebs) продемонстрировал новый вид скиммеров (устройств для кражи денег с карт),

имитирующих переднюю панель банковского терминала. Об этом сообщает TechCrunch (InternetUA).

По словам Б. Кребса, злоумышленники изготовили скиммеры из офисных телефонов Samsung, снабдив их полностью рабочей клавиатурой. Они устанавливаются на POS-терминалы для безналичной оплаты Ingenico и воруют как пароли от карт, так и данные с NFC-чипов бесконтактной оплаты. Полученная информация по Bluetooth передается на смартфон преступников.

Владельцы супермаркета, в котором были установлены скиммеры, случайно обнаружили их, решив починить плохо работавшие банковские терминалы.

***

6.03.2017

«Доктор Веб»: приложение с агрессивной рекламой загрузили более 50 млн раз

Рекламные модули, которое встраиваются в Android-приложения для их монетизации, получили широкое распространение (ITnews).

Многие из этих плагинов действуют агрессивно: создают ненужные ярлыки, показывают баннеры и всплывающие окна. Вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play программу с одним из таких модулей. Ее установили свыше 50 000 000 пользователей.

Исследованное специалистами «Доктор Веб» приложение представляет собой экранную клавиатуру под названием TouchPal, которую владельцы мобильных устройств могут использовать вместо стандартной. Оно действительно предоставляет заявленный функционал, однако содержит нежелательный рекламный модуль, по классификации Dr.Web получивший имя Adware.Cootek.1.origin.

Этот плагин способен показывать рекламу нескольких типов. Например, он создает на домашнем экране виджеты, которые не удаляются до тех пор, пока владелец устройства не нажмет на них. При нажатии на виджет Adware.Cootek.1.origin показывает интерактивное окно с небольшой игрой, в которой пользователь всегда побеждает и получает в качестве «приза» рекламу. Помимо «игры» модуль может отображать окно с новостными публикациями, которые сопровождаются баннерами.

Кроме того, Adware.Cootek.1.origin встраивает рекламу в экран блокировки, а также показывает баннеры непосредственно после разблокирования мобильного устройства.

Несмотря на то, что сама по себе программа TouchPal не является вредоносной, применяемый в ней нежелательный модуль Adware.Cootek.1.origin фактически мешает пользоваться мобильным устройством из-за постоянно всплывающих уведомлений и неудаляемых виджетов. Поскольку этот плагин встроен непосредственно в ПО TouchPal, удалить его можно лишь вместе с основным приложением. Запись об

Adware.Cootek.1.origin добавлена в вирусную базу, поэтому антивирусные продукты Dr.Web для Android успешно детектируют его во всех программах.

***

6.03.2017

В 2016 г. число приложений-вымогателей возросло на 752 %

Компания Trend Micro Inc провела исследования, в рамках которых изучила число киберугроз в 2016 г. (iLenta.com).

По результатам исследований стало известно, что суммарное число киберугроз в 2016 г. стало рекордным за всю историю развития технологий.

Эксперты рассказали, что больше всех от киберпреступлений страдали крупные корпорации, а общий ущерб от кибератак в 2016 г. превысил 1 млрд долл.

Наибольший ущерб нанесло мошенничество посредством электронной почти. Убытки от этого вида киберпреступлений составили 140 млн долл. Примечательно, что количество курсирующих в Сети приложений-вымогателей в 2016 г. возросло на 752 %.

Что до наиболее крупного киберпреступления за 2016 г., Trend Micro Inc выделяет нападение на аккаунты пользователей сервиса Yahoo! Чтобы получить доступ к данным и паролям граждан злоумышленники порядка года создавали фальшивые cookie-файлы.

***

9.03.2017

Поддельное приложение Facebook Lite содержит троян

Версия приложения Facebook Lite из сторонних магазинов мобильных приложений оказалась заражена трояном Spy FakePlay. Это приложение в реальности создано не компанией Facebook, а кем-то из Китая. Исследователи из компании Malwarebytes Labs говорят, что эта версия популярного мобильного приложения, которое расходует меньше трафика (InternetUA).

Приложение работает как и должно, но за кулисами происходит дополнительная вредоносная деятельность. Используется вредоносный приёмник (com.google.update.LaunchReceiver) и сервис (com.google.update.GetInst), чтобы выдать себя за обновление Google Update.

com.google.update.LaunchReceiver загружается при включении устройства, после чего запускается приёмник com.google.update.GetInst. Последний содержит вредоносный код для кражи персональной информации пользователей и установки других вредоносных программ. Собираются данные о номере ID устройства, версии операционной системы, Mac-адрес, операторе сотовой связи и т. д.

Китайское происхождение этого варианта Facebook Lite удалось установить по некоторым символам в коде. В Китае доступ к официальному

магазину приложений Google Play закрыт, потому программа распространяется в сторонних магазинах. Без механизма сканирования Google эти магазины представляют собой не самое безопасное место. При наличии доступа в Google Play Store рекомендуется ставить программы только оттуда, хотя периодически вирусы проникают и в него.

***

8.03.2017

В сетевых накопителях WD My Cloud обнаружено 85 уязвимостей

Исследователь безопасности, известный под псевдонимом Zenofex, обнаружил в общей сложности 85 уязвимостей разной степени опасности, включая критические, в сетевых устройствах серии MyCloud производства компании Western Digital (InternetUA).

По данным эксперта, проблемы затрагивают следующие модели: My Cloud, My Cloud Gen 2, My Cloud Mirror, My Cloud PR2100, My Cloud PR4100, My Cloud EX2 Ultra, My Cloud EX2, My Cloud EX4, My Cloud EX2100, My Cloud EX4100, My Cloud DL2100 и My Cloud DL4100.

Некоторые из выявленных проблем позволяют удаленно выполнить код на целевом устройстве, а также получить доступ к данным пользователей.

Значительное количество обнаруженных уязвимостей могут быть проэксплуатированы путем изменения значений файлов cookie или внедрения shell-команд в параметры cookie. Более сложные атаки предполагают внедрение вредоносного кода в теги изображений на сайтах, посещаемых владельцами уязвимых устройств WD My Cloud. В результате злоумышленник может получить контроль над устройством.

По словам Zenofex, наиболее опасную уязвимость, позволяющую обойти механизм аутентификации, проще всего проэксплуатировать. Для этого нужно всего лишь модифицировать параметры cookie сессии.

Исследователь решил не информировать Western Digital о найденных им уязвимостях после того, как пообщался с другими специалистами на конференции Black Hat USA 2016, которые неоднократно жаловались на то, что WD постоянно игнорирует сообщения об уязвимостях.

«Из-за игнорирования этих проблем уязвимые устройства дольше будут оставаться онлайн. Мы хотим обратить внимание сообщества на уязвимости и надеемся, что пользователи ограничат общественный доступ к своим сетям там, где это возможно», – говорит Zenofex.

Исследователь опубликовал PoC-код к 48 уязвимостям, а также представил видео с демонстрацией эксплуатации ряда проблем.

***

8.03.2017

Apple уверяет, что закрыла в iOS большинство уязвимостей, которыми пользовались спецслужбы США

Apple уже закрыла значительную часть уязвимостей, которые, согласно данным WikiLeaks, использовались американскими спецслужбами для доступа к iPhone интересующих их лиц. Об этом говорится в заявлении калифорнийского гиганта (InternetUA).

Представитель Apple заявил, что компания продолжит работать над безопасностью операционной системы iOS и просит пользователей своевременно устанавливать обновления. В Купертино добавили, что пока только поверхностно ознакомились с материалами, которые опубликовал WikiLeaks.

Накануне WikiLeaks выложило первую порцию утечек из центра киберразведки ЦРУ, включающую свыше 8700 документов и файлов. Обнародованные данные, в частности, указывают на существование глобальной программы для взлома разного рода смартфонов и планшетов, включая iPhone, iPad, Android-устройства и даже телевизоры Samsung.

Отдел разведывательного управления, отвечающий за мобильные гаджеты, разрабатывал различные методы «для удаленного взлома и управления популярными смартфонами». «Зараженным» телефонам могла быть дана команда отправлять в ЦРУ данные о местонахождении пользователя, включать камеру, также открывался доступ к разговорам, текстовой переписке.

«Документы Wikileaks, если они достоверны, содержат таблицы с уязвимостями iOS, которые позволяли ЦРУ следить за пользователями iPhone и в отдельных случаях управлять их устройствами. Некоторые эксплоиты были разработаны спецслужбой, некоторые покупались или скачивались из неправительственных источников», – отмечает Techcrunch.

Хотя продукция Apple не является самой распространенной в мире, она весьма популярна среди «общественных деятелей, политической, дипломатической и бизнес-элиты», подчеркнули в WikiLeaks. По данным издания, консульство США в немецком Франкфурте-на-Майне является «тайной хакерской базой» ЦРУ для организации кибератак по всему миру.

Подлинность документов WikiLeaks уже подтвердил бывший сотрудник Агентства национальной безопасности США Э. Сноуден. На своей странице в Twitter он написал, что все еще продолжает анализировать обнародованные документы, но уже может отметить важность опубликованных данных.

***

8.03.2017

В Сеть «утекла» спамерская база из 1,4 миллиарда почтовых адресов

В Интернет попала база данных, состоящая из более чем 1,4 млрд адресов электронной почты. Как сообщил эксперт в области информационной безопасности, сотрудник компании MacKeeper К. Викери, огромный архив содержит реальные имена пользователей, а также их физические и IP-адреса (InternetUA).

Как оказалось, утечку по ошибке допустила River City Media (RCM) – американская фирма, которая официально занимается сетевым маркетингом, но на деле ежедневно рассылает миллионы спам-сообщений. В ходе одного из исследований К. Викери случайно обнаружил незапароленный архив RCM, содержащий чат-логи, переписку и, что важно, крупнейшую базу рассылок рекламных писем. По-видимому, она оказалась в Сети в результате неудачного создания резервной копии.

По словам К. Викери, архив также содержит статистику рассылок RCM и обсуждения изощренных спамерских техник. Например, компания успешно обходила спам-фильтры Google, отправляя «разогревочные письма» на собственные серверы в Gmail. А поскольку жалоб на такие сообщения поступало, почта Google переставала считать их назойливыми.

«Они разработали тонну софта для сокрытия своих почтовых адресов, что позволяло им выдавать себя за обычных людей и подменять адреса», – сказал исследователь. Он подчеркнул, что RCM использовала более 2,2 тыс. IP-адресов, а ее услугами (не напрямую, а при посредничестве других законных маркетинговых фирм) пользовались такие бренды, как Nike, Gillette, Victoria's Secret, Covergirl и AT&T.

***

9.03.2017

Обнаружен вирус, безвозвратно удаляющий данные

«Лаборатория Касперского» сообщила о появлении вируса StoneDrill, который безвозвратно удаляет данные с устройства, а также шпионит за жертвами и старательно маскируется от защитного программного обеспечения (InternetUA).

Хакерские атаки на компании при помощи StoneDrill замечены в странах Европы и Ближнего Востока. Программа остается незаметной на зараженном устройства благодаря двум сложным антиэмуляционным методам. Как только зловред попадает в компьютер, он встраивается в процесс памяти чаще всего используемого браузера. Сразу после установки вирус начинает уничтожать файлы на жестком диске.

Кроме модуля, стирающего информацию, StoneDrill содержит бэкдор для шпионажа за жертвами. В «Лаборатории Касперского» обнаружили четыре сервера управления, с помощью которых злоумышленники вели слежку на зараженных устройствах.

Эксперты отмечают, что StoneDrill сильно напоминает нашумевшую пять лет назад аналогичную программу Shamoon. В 2012 г. этот зловред парализовал работу 35 тыс. компьютеров в нефтегазовой компании на Ближнем Востоке и таким образом поставил под удар всю мировую нефтепромышленность.

***

9.03.2017

На черном рынке за бесценок продают личные данные пользователей Gmail и Yahoo!

Некто под псевдонимом SunTzu583 продает на черном рынке в даркнете 1 млн скомпрометированных учетных записей пользователей Gmail и Yahoo!, полученных в результате целого ряда утечек (Экономические известия).

Одна из выставленных на продажу баз данных содержит 100 тыс. аккаунтов Yahoo!, похищенных в результате атаки на подписчиков сайта Last.FM в 2012 г. В частности, SunTzu583 предлагает имена пользователей, электронные адреса и пароли пользователей в открытом виде. Стоимость товара составляет всего 0,0079 биткойна (порядка 10,75 долл.). Такая низкая цена объясняется тем, что с прошлого года эти данные уже доступны в Сети, информирует news.eizvestia.com.

Еще одна база данных, содержащая 145 тыс. учетных записей пользователей Yahoo!, продается за 0,0102 биткойна (13,75 долл.). В БД хранятся имена пользователей, электронные адреса и расшифрованные пароли, похищенные в результате взлома Adobe в октябре 2013 г. и MySpace в 2008 г.

Всего за 0,0219 биткойна (28,24 долл.) SunTzu583 предлагает 500 тыс. взломанных учетных записей пользователей Gmail, полученных после атак на Bitcoin Security Forum в сентябре 2014 г., MySpace в 2008 г. и Tumblr в 2013 г. Еще 450 тыс. аккаунтов Gmail можно приобрести за 0,0199 биткойна (25,74 долл.). Электронные адреса и пароли в открытом виде были похищены в результате утечек данных Bitcoin Security Forum, Tumblr, Last.fm, 000webhost, Adobe, Dropbox, Flash Flash Revolution, LookBook и Xbox360 ISO, имевших место в 2010–2016 гг.

***

10.03.2017

Скачати безкоштовно. Чим загрожує Україні статус одного з головних піратів світу

Як Україна опинилась серед восьми головних порушників інтелектуальних прав світу і чому цей статус загрожує країні санкціями (Espreso.tv).

9 лютого Міжнародний альянс інтелектуальної власності (IIPA) вчергове включив Україну в Priority Watch List 2017 – коло країн, де найбільше порушуються права інтелектуальної власності в світі. Крім України в список головних порушників потрапили ще сім країн: Китай, Чилі, Індія, Мексика, Росія, Тайвань і В'єтнам.

З 2013 р. Україна має статус країни, де не цінується і не захищається інтелектуальна власність. Через подібний статус Україна часто потрапляє в «301» – список, який формується Торговим представництвом США.

З країною, яка потрапила в цей список, складаються позбавлені довіри економічні відносини, застосовуються санкції. Усе це позначається на

інвестиційній привабливості країни, а українських підприємців відмовляються сприймати всерйоз.

Згідно зі звітом Міжнародного альянсу інтелектуальної власності, Україну рекомендують залишити в списку пріоритетного спостереження, оскільки будь-яких глобальних змін щодо дотримання авторських прав у країні не спостерігається.

Уряд США не задоволений законодавством щодо прав інтелектуальної власності в Україні. Заповнення таких прогалин, на думку американського уряду, сприятиме економічному розвитку країни.

Ну а поки що, Альянс інтелектуальної власності пропонує зупинити застосування економічних пільг для України. Це означає, що тепер збуття української продукції буде ускладнено і законодавчо.

Такі основні галузі авторського права як фільми, музика, книги, комп'ютерні ігри та програмне забезпечення є основним сегментом економіки США, генеруючи більш 1,2 трлн дол. на рік і забезпечуючи 5,5 млн людей роботою.

Як до такого дійшли

Не дивно, що до України, де на кожному третьому комп'ютері стоїть неліцензійне програмне забезпечення, хочуть застосовувати санкції. Це є зовсім невтішним фактором для країни, в якій IT сфера збільшується на 25 % щорічно, а розробки українських програмістів (як і самі програмісти) цінуються у всьому світі.

Завдяки слабкому цифровому праву, ніщо не перешкоджало розвитку піратства. А деякі міжнародні «пірати» спеціально переносили свої сервери в Україну, користуючись беззаконною ситуацією.

Україна з 2015 р. посідає 3 місце в світі за кількістю тимчасових мереж, що беруть участь у несанкціонованому спільному використанні файлів. Простіше кажучи, Україна входить у трійку лідерів з нелегального «файлообміну» в Інтернеті, копіюючи і поширюючи інтелектуальну власність, не маючи на це прав.

Однією з причин безкарності є неможливість застосування кримінального покарання за крадіжку інтелектуальної власності. Порогом кримінального переслідування є 16 000 грн за крадіжку. Але підрахунок завданого збитку в рамках інтелектуальної власності – процедура не з легких.

Відсутній єдиний підхід до підрахунку та оцінки авторського матеріалу. Історія з порогом не дає застосовувати кримінальне покарання до порушників прав інтелектуальної власності (ПІВ), замінюючи його на адміністративну.

Тортуга вже не та

Однак у звіті відзначені і невеликі позитивні події. Одним з таких поліпшень є створення кіберполіції, яка почала боротьбу з інтернет-піратством. Серед заслуг кіберполіції – закриття таких сайтів як EX.UA і FS.TO, що теж є позитивною зміною.

Ще однією перемогою стало закриття одного з найбільших торрент-трекерів. Українським та американським правоохоронним органам (не без

допомоги Apple і Facebook), вдалося зупинити роботу трекера Kickasstorrents (kat.cr). Торрент-трекер – це файлообмінник, який дає змогу копіювати та поширювати продукти інтелектуальної праці (фільми, музику, ігри, програми).

На Kickasstorrents заходило від одного мільйона людей на день і 50 млн щомісяця. Прибуток з ресурсу становив від 16 млн дол. щорічно. А за приблизними підрахунками, за вісім років існування, сайт приніс збитки правовласникам на 1 млрд дол.

Власником торрента був харків'янин А. Ваулин, який тимчасово проживав у Польщі. За іронією долі, король інтернет-піратів був затриманий при покупці легального контенту в iTunes.

Піратські ринки

Серед загальних рекомендацій – посилення контролю за «піратськими» сайтами, контроль вуличної торгівлі (на ринках і біля метро). Про контроль «ринків на повітрі» говориться дуже багато, мабуть коробочки з написом «1500 ігор на одному диску» або різноманітна добірка програм з надрукованими на звичайному принтері обкладинками дуже вразили Альянс інтелектуальної власності.

Однак і тут є позитивні зміни. Наприклад, на Петрівському ринку в Києві були введені системи контролю продукції та вдосконалені механізми примусового виконання. А в першій половині 2016 р. поліція конфіскувала близько 5 000 контрафактних дисків у Львівській області.

Однак ринок «7-й кілометр» в Одесі з більш ніж 5 000 кіосків і ринок Барабашово в Харкові залишаються значними джерелами нелегальних матеріалів, особливо для кіноіндустрії.

Як повернути честь

Серед вимог Міжнародного альянсу інтелектуальної власності: ввести в дію закон «Про колективне управління» для того, щоб дії організації були максимально прозорими та організованими.

Також необхідно повністю реалізувати договори Всесвітньої організації інтелектуальної власності (ВОІВ) з авторських прав (ДАП) в Інтернеті. Ці договори допоможуть відрегулювати норми і поняття інтелектуальної власності в Інтернеті.

Змінити закон про авторське право в Кримінальному кодексі, а саме прибрати з цього закону виняток про зйомку на відеокамеру в кінотеатрі для особистого використання. Тому що при такому винятку будь-якого спійманого в кінотеатрі «оператора» можна виправдати особистими обставинами.

І необхідно прийняти законопроект № 3081-д «Про державну підтримку кінематографа», в якому містяться всі необхідні зміни для ефективної боротьби з піратством в Інтернеті. 17 листопада 2016 р. Закон уже майже був ухвалений, але в останній момент на нього наклав вето Президент України П. Порошенко.

Можливо, виконуючи ці рекомендації, Україні вдасться повернути собі статус країни, в якій цінується інтелектуальна праця. Однак, ухвали одних лише законів мало.

В українців виробилася звичка не платити за те, що не можна відчути фізично. Тут людина виправдовує себе тим, що «матеріально» вона нічого не відбирає у інших, а значить, і факту крадіжки немає.

Але це не так, як кінокомпанії повернути свої витрачені гроші на фільм, коли його вже виклали в Інтернет і подивилися мільйони людей безкоштовно?

Тут усе просто, і для тих, хто запитує, чому кіноіндустрії в Україні розвивається повільно – відповідь повинна бути очевидною: українці не звикли платити за те, що не можна помацати. А на законодавчому рівні все ще не має таких норм, які могли б вплинути на ситуацію примусово.

***

12.03.2017

WSJ: Розслідування витоку інформації з ЦРУ стрімко просувається

У США розслідування витоку даних кіберрозвідки ЦРУ сфокусувалося на програмістах, пише Wall Street Journal (Корреспондент.net).

Як стало відомо газеті, 9 березня невелика група цивільних службовців, які працювали на ЦРУ у Вашингтоні, була допитана і пройшла перевірку на поліграфі.

Арештів поки що не було, проте, як підкреслив один зі співрозмовників видання, розслідування «стрімко просувається».

Зокрема, за його словами, основна увага слідчих зосереджена на команді розробників ЦРУ, які безпосередньо створювали інструменти для злому цифрових пристроїв.

Ще один співрозмовник WSJ розповів, що одна група службовців, які працювали за контрактом за кордоном, очікувала надання нових робочих місць, проте ці позиції були скорочені.

***

12.03.2017

Вредоносное Android-приложение заставляет пользователей ставить ему пятёрки

Специалисты из компании ESET предупреждают пользователей об обнаружении в магазине Google Play Store приложения, которое требует ставить ему высокую оценку, обещая после этого разблокировать доступ ко всем функциональным возможностям. Внутри приложения найден показывающий рекламу троян, при этом оно выдаёт себя за программу для скачивания видео с YouTube. Скачано приложение уже было более 5000 раз (InternetUA).

ESET называет приложение Android/Hiddad.BZ. Оно засыпает пользователей рекламой и обещает убрать её, если поставить приложению пять звёзд на его странице в магазине Play Store. Исследователи нашли в магазине семь версий Hiddad с названиями вроде Tube.mate или Snaptube. Если их

установить, в списке приложений на устройстве они отображаются под одним и тем же названием Music Mania.

После запуска появляется фальшивый системный экран, который предлагает установить плагин. Убрать этот экран невозможно и пользователь вынужден выполнять его требования; нажав на кнопку установки, пользователь на самом деле устанавливает рекламу. Затем плагин требует права администратора, отказаться тоже нельзя.

После получения прав администратора приложение начинает отображать рекламу и требует поставить ему высшую оценку. Права администратора для приложения можно убрать в настройках, после чего доступно удаление приложения вручную. Специалисты говорят, что эта программа может быть одной из многих, которые скоро начнут требовать высокой оценки в магазине. В качестве примера они приводят приложение под названием Subway Sonic Surf Jump; достаточно почитать отзывы на него, чтобы узнать о недостоверности его высокой оценки.

***

13.03.2017

Google освободит пользователей от теста «Я не робот» на сайтах

Интернет-гигант Google усовершенствовал систему защиты сайтов от роботов reCAPTCHA, «научив» ее автоматически отличать живых пользователей от искусственных алгоритмов без дополнительной проверки, сообщается в официальном блоге компании (Телекритика).

Обновленная система работает на основе комбинации технологий машинного обучения и анализа рисков, что позволяет ей определять пользователей без специальной проверки. Она анализирует несколько параметров, среди которых - IP-адрес, предыдущие взаимодействия посетителя сайта с reCAPTCHA, движения мыши и т. д.

***

13.03.2017

Proton – самый опасный троян для Mac

Давно прошли те времена, когда считалось, что Mac не страшны трояны, так как их попросту никто не пишет. Эксперты Sixgill обнаружили на русскоязычном форуме в даркнете и выставили на продажу самый опасный «вредонос» для macOS, получивший название Proton. Авторы рассчитывают продать его за 40 биткоинов, что по текущему курсу равняется примерно 50 000 долл. Для тех, у кого нет таких денег, есть предложение подешевле: 2 биткоина (2500 долл.) за одну установку (InternetUA).

Согласно данным специалистов, Proton написан на Objective C и не обнаруживается существующими антивирусными решениями. Вредонос рекламируется как «профессиональное FUD-решение для слежки и контроля»,

способное получить root-доступ к компьютеру и фактически перехватить над ним контроль. Распространять зловред предлагается под видом различных легитимных приложений. Покупатель сможет легко изменить иконку и название вируса.

Proton включает себя функции кейлоггера, может делать снимки рабочего стола, дистанционно активировать веб-камеру. Также он способен похищать пользовательские файлы, загружая их на удаленный сервер, или скачивать произвольные файлы на зараженную машину. Помимо этого, Proton может показывать жертве кастомное окно, запрашивая информацию о банковской карте, водительских правах или другие конфиденциальные данные. Кроме того, по данным Xaker, вредонос способен получить доступ к iCloud маковода, даже если активна двухфакторная аутентификация.

Но хуже всего тот факт, что создатели Proton смогли обойти механизмы контроля Apple, ведь компания предъявляет строгие требования к приложениям сторонних разработчиков. В итоге код трояна обладает подлинной подписью, которая обманывает защитные механизмы. Исследователи предполагают, что вирусописатели либо используют поддельный Apple ID для Apple Developer Program, либо используют похищенные у других разработчиков учетные данные. Как бы то ни было, в результате у злоумышленников есть все необходимые сертификаты.

Proton рекламируется не только в даркнете. Помимо этого у вредоноса есть официальный сайт и даже демонстрационные ролики на YouTube.

По мнению экспертов, для получения root-привилегий на компьютере Proton эксплуатирует уязвимость «нулевого дня», которая, очевидно, неизвестна широкой публике и является собственностью авторов малвари.

***

13.03.2017

У Британії призначили міністра для боротьби з підривною діяльністю Росії

Прем’єр-міністр Великобританії Т. Мей призначила міністра з боротьби з підривною діяльністю, в тому числі хакерськими атаками й інформаційним впливом Росії. Про це повідомляє видання The Times (LB.ua).

За даними видання, Б. Гаммер, міністр Кабінету, керує «широкими зусиллями в рамках дій уряду щодо захисту цілісності британської демократії після побоювань щодо того, що російські кібератаки, фейкові новини і гроші можуть дестабілізувати демократію».

Крім того, британські спецслужби нині пропонують протестувати комп’ютерні мережі політичних партій, щоб побачити, чи можуть вони протистояти «ворожій кіберактивності».

Фахівці Центру урядового зв’язку (GCHQ) проведуть ряд технічних семінарів для політичних партій. Національний центр кібербезпеки (NCSC) також готовий дати політичним партіям свої рекомендації.

***

13.03.2017

Эксперты рекомендуют заклеивать камеру iPhone после последних разоблачений WikiLeaks

Пока некоторая часть американской общественности ждала компромата на президента США Д. Трампа, желая получить повод для импичмента, настоящей сенсацией стали новые публикации на WikiLeaks (InternetUA).

7818 веб-страниц, 943 приложения – таков объём очередного разоблачения WikiLeaks. И это лишь первая часть – дальше будет больше. Утечку уже называют крупнейшей в истории ЦРУ, а журналисты стремятся любыми способами поднять тиражи на информации, которую скрывало разведывательное управление.

Одна из самых громких тем этой утечки – сведения о том, что ЦРУ годами находило бреши в операционных системах iOS и Android. Вместо того чтобы сообщить об этих уязвимостях Apple и Google, агентство тайно пользовалось обнаруженными «дырами» безопасности в собственных интересах.

«Сейчас ЦРУ потеряло контроль над своим киберарсеналом. Речь идет о троянах, вирусах, вредоносных шпионских программах, разработанных для проникновения в смартфоны, телевизоры, ноутбуки. Чтобы можно было контролировать их дистанционно, снимать информацию, включать или выключать их», – говорит главный редактор WikiLeaks Дж. Ассанж.

Сейчас опасен даже выключенный телевизор – особенно, судя по опубликованным документам, «умные» модели от Samsung. Якобы они скрытно могут записывать звук и передавать информацию ЦРУ на серверы с ожидаемым названием – «Карманный Путин». Смысл просьбы «выключить свои мобильные телефоны» уже никогда не будет прежним.

Аналитик Л. Нейшн – не параноик. Но от его советов по сохранению конфиденциальности напряжение только растет. Чтобы заклеить камеру телефона он рекомендует использовать любую наклейку, но вот что делать с микрофоном, эксперт не уточняет.

«Ты не сможешь выключить iPhone простым нажатием кнопки. Возможно, ты будешь думать, что выключил его, но на самом деле это не так. Он все еще работает, потому что из него просто нельзя вытащить батарею. Удачи!» – заявил эксперт.

Основатель Facebook М. Цукерберг всегда это знал. Сначала его фото с заклеенными камерой и микрофоном на ноутбуке вызывало улыбку. Но в итоге шутки сменились размышлениями: лидер индустрии не мог сделать это просто так.

***

13.03.2017

Смартфоны Samsung и Xiaomi продаются с предустановленными вирусами

Операционная система Android давно удерживает репутацию наиболее наполненной вирусами мобильной платформы, опережая iOS и Windows. Google старается противостоять «вредоносам», но сделать это не так просто. Зачастую эксперты говорят о необходимости устанавливать ПО только из проверенных источников, но что делать, если вирусы стоят на мобильном устройстве уже при его покупке? Такие смартфоны обнаружила исследовательская компания Check Point (InternetUA).

Обычно вредоносное ПО активируют сами пользователи, когда теряют бдительность, но в этот раз специалисты выявили иной подход к распространению зловредов. Эксперты обнаружили в 38 различных Android-устройствах предустановленные троянские программы, которые могли получить полный доступ к смартфонам и следить за любыми действиями пользователей. В зоне риска модели компаний Samsung, LG, Xiaomi, Asus, Nexus, Oppo и Lenovo, причём троянское ПО устанавливалось на них ещё до покупки.

Злоумышленники могли красть пароли и платёжные данные, устанавливать на смартфоны любые программы. Предустановленное вредоносное ПО позволяет удаленно отслеживать местоположение аппарата, активировать камеру, отправлять SMS на платные номера.

По данным экспертов, вирусы загружаются на смартфоны на заключительном этапе дистрибуции. Особенному риску подвержены те пользователи, которые покупают гаджеты в небольших магазинах или выбирают устройства в Интернете.

Среди моделей, которые были проданы покупателям с вирусом специалисты назвали Samsung Galaxy Note 2, 3, 4 и 5, Galaxy S7, LG G4, Xiaomi Mi 4i, вся линейка Xiaomi Redmi, ZTE x500, Lenovo A850 и др.

***

13.03.2017

Микола Оліярник

Творець Інтернету розповів про основні загрози для розвитку всесвітньої павутини

World Wide Web 12 березня відзначив свою 28-му річницю і на сьогодні його подальшому існуванню загрожує три фактори (ООО «Видавничий дім «МЕДІА-ДК»).

Сер Тім Бернес-Лі, очільник World Wide Web Consortium, якого вважають творцем Інтернету, оприлюднив відкритий лист. У ньому він виклав три основні загрози, які можуть істотно завадити розвитку всесвітньої мережі, а також способи їх вирішення.

Бернес-Лі заявив, що 28 років тому від представив своє бачення відкритої платформи, яка дозволила б усім, незалежно від географічних і культурних кордонів, обмінюватися інформацією. Однак за останні 12 місяців він дедалі чіткіше спостерігав прояв трьох тенденцій, які можуть завадити Інтернету реалізувати свій потенціал як інструменту, що служить усьому людству.

1. Ми втратили контроль над нашими особистими даними

Дуже широкого розповсюдження набула бізнес-модель, яка пропонує безкоштовний контент в обмін на персональні дані. Більшість інтернет-користувачів погоджується на такі умови. Але, зазначив Бернес-Лі, ми втрачаємо переваги, якими могли би скористатися, якщо би самі володіли власними даними. Тоді люди самі могли би вирішувати, коли, з ким і якою інформацією ділитися.

Крім того, уряди співпрацюють або ж примушують компанії ділитися персональними даними. Це нерідко призводить до зловживань, втручання в особисте життя. А у випадку з репресивними режимами – до арештів і вбивств. Постійне стеження за всіма в Інтернеті, це вже занадто, переконаний голова World Wide Web Consortium.

2. Дезінформація занадто легко поширюється в Інтернеті

Більшість людей для пошуку інформації використовує лише декілька соціальних мереж і новинних сайтів. Ці ресурси на основі алгоритмів, які вивчають наші особисті дані, відбирають, що саме нам показувати, підкреслив Бернес-Лі.

Як наслідок – сайти показують нам те, на що ми найімовірніше «клікнемо». Отже, різні фейкові новини чи відверта дезінформація може розповсюджуватися як лісова пожежа. І такі можливості зловмисники можуть використовувати у своїх фінансових чи політичних цілях.

3. Політичній рекламі потрібні прозорість і зрозумілість

Той факт, що більшість користувачів отримують новини лише від декількох платформ, а зростаюча складність алгоритмів спирається на масиви особистих даних, означає наступне – політична реклама стає дедалі більше індивідуальною. За деякими даними, під час виборів 2016 р. у США у Facebook щодня демонструвалося 50 тис. варіацій політичної реклами. Є підозра, що подібні інструменти використовувалися недобросовісно, для того, щоби маніпулювати виборцями.

Бернес-Лі зазначив, що боротьба не буде легкою, але деякі шляхи вирішення описаних вище проблем уже проглядаються. Наприклад, потрібно співпрацювати з веб-компаніями для того, щоби повернути контроль над даними в руки людей. Для цього можна використовувати такі інструменти, як особисті «пакети даних», передплата чи мікроплатежі.

Інтернет-спільнота повинна посилити тиск на таких інтернет-гігантів, як Google та Facebook, щоб вони посилили боротьбу з дезінформацією, вважає Бернес-Лі.

***

14.03.2017

Приложения из Google Play воровали логины и пароли от Instagram

Специалисты ESET обнаружили в Google Play Маркете тринадцать приложений с вирусом Android/Spy.Inazigram. Суммарно они были установлены более полутора миллионов раз (InternetUA).

Заражённые приложения обещали пользователям Instagram быстро увеличить число подписчиков, лайков и комментариев. Отчасти это оказывалось правдой, поскольку приложения воровали данные от учётных записей Instagram и использовались для накрутки подписчиков других пользователей. Схема увода учёток предельно проста: приложение запускалось, просило ввести логин и пароль от Instagram и отправляло эти данные злоумышленникам, а пользователь видел сообщение о неправильном пароле. На странице с поддельной ошибкой пользователю предлагалось пройти верификацию, после чего ему приходило сообщение о том, что кто-то пытался получить доступ к его аккаунту. Наивный пользователь подтверждал, что это был он сам.

Украденные учётные записи помимо накрутки подписчиков использовались для рассылки спама в комментариях других пользователей. Злоумышленники продавали подписчиков, комментарии и лайки пакетами стоимостью от 6 до 20 долл.

***

14.03.2017

Тепловой след поможет хакерам определить PIN-код смартфона

Киберпреступники могут узнать PIN-код смартфона при помощи теплового следа пальцев его владельца, предупредили ученые из Штутгартского университета и Мюнхенского университета им. Людвига-Максимилиана (InternetUA).

Как выяснили специалисты в ходе проведенных исследований, после ввода пользователем PIN-кода на дисплее смартфона тепловой след от пальцев на экране остается до 45 секунд. Таким образом, любой технически подкованный хакер или вор с тепловизором может обойти защиту устройства и извлечь нужные данные. Для этого потребуется всего лишь сделать снимок теплового следа и при помощи специального ПО преобразовать данные.

Как показали эксперименты, если злоумышленник просканирует устройство через 15 секунд после ввода PIN-кода, шанс распознавания составляет 90 %. После 30 секунд точность распознавания снижается до 80 %, а после 45 секунд и более падает до 35 % и ниже.

Для защиты от подобных «термических» атак эксперты рекомендуют прижимать руку к экрану сразу же после ввода пароля – так на дисплее появится ряд тепловых следов, перекрывающих следы нажатий. Эксперты

также советуют повысить яркость экрана, что увеличит его температуру и снизит время, которое тепловой след сохраняется на дисплее.

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник Терещенко Ірина

Редактор Федоренко Оксана

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, просп. 40-річчя Жовтня, 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
www.nbuv.gov.ua/siaz.html

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.