Соціальні мережі як чинник інформаційної безпеки

Огляд інтернет-ресурсів
(25.04–9.05)

2018 № 9

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(25.04–9.05)
№ 9

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

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

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2018

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ 4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 10
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 13
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 16
Інформаційно-психологічний вплив мережевого спілкування на особистість 16
Маніпулятивні технології 17
Спецслужби і технології «соціального контролю» 20
Проблема захисту даних. DDOS та вірусні атаки 23
ДОДАТКИ 34

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

25.04.2018
Twitter изменил политику конфиденциальности

Компания Twitter изменила политику конфиденциальности в рамках нового закона Евросоюза о защите данных. Об этом сообщается на сайте соцсети (InternetUA).

«Мы считаем, что вы должны знать, какими данными вы делитесь с нами и как мы их используем, а также, что важнее всего, вы должны иметь преимущественный контроль по управлению над сбором и использованием ваших данных», – говорится в сообщении.

Как отмечается, основные изменения коснутся средств управления личными данными пользователей.

***

26.04.2018
Майя Яровая
Теперь вы можете скачать всю свою информацию из Instagram

В веб-версии популярного сервиса Instagram появилась функция, с помощью которой пользователь может скачать всю свою информацию. Для этого нужно перейти в настройки конфиденциальности своего аккаунта и кликнуть по ссылке «Запрос на загрузку» (AIN.UA).

После этого Instagram предложит выслать архив ваших данных на почту, которую пользователь указал при регистрации (можно указать другой адрес).

Как говорится в описании инструмента, Instagram предоставит пользователю ссылку на архив, в котором будут содержаться все его «фотографии, комментарии, информация из профиля и другое». Также отмечается, что на формирование этого архива может понадобится до 48 часов.

Пока возможность скачать свои данные из Instagram доступна только в веб-версии сервиса, но вскоре она должна появится также на iOS и Android, сообщает The Verge. Выполнена она по аналогии с таким же инструментом Facebook, который стал доступен гораздо раньше.

Как ранее отмечал TechCrunch, наличие возможности загрузить из соцсети все свои данные и посмотреть, что сервису известно про его конкретного пользователя, важно для соблюдения новых европейских норм в отношении персональных данных. Также это необходимый шаг на фонескандала вокруг материнской компании сервиса.

***

26.04.2018
За пользователями WhatsApp теперь можно незаметно следить

Наиболее популярным мессенджером в мире является WhatsApp, в котором полно различных функциональных возможностей. С его помощью можно отправлять текстовые и голосовые сообщения, осуществлять аудио- и видеозвонки, обмениваться файлами (фотографиями, документами и видео), а также делать многие другие вещи. Хоть команда разработчиков и постоянно работает над улучшением своего сервиса, в том числе над его защитой, однако теперь за пользователями этого мессенджера можно незаметно следить, причем вполне законно (InternetUA).

Состоялся релиз приложения под названием Chatwatch, которое позволяет всем желающим незаметно следить за определенными пользователями WhatsApp, просто добавив их номер в специальную базу. Программа пока что доступна только на iPhone, однако в скором времени планирует выпустить ее Android-версию. При помощи данного программного обеспечения можно посмотреть, когда собеседник последний раз заходил в приложение, даже если у него отключена функция отображения сетевого статуса.

Специальный алгоритм, встроенный в Chatwatch, отображает информацию о том, когда пользователь WhatsApp просыпается и ложится спать. Более того, через данное программное обеспечение можно узнать о том, общаются ли между собой выбранные люди из списка контактов или же нет. Чтобы получить эти данные приложение следит сразу за несколькими пользователями, в течение нескольких часов или дней, сверяя их данных друг с другом, чтобы с большой точностью дать ответ на этот вопрос.

Приложение стоит $1,99 за одну неделю использования, причем за такую сумму денег речь идет о слежке лишь за двумя пользователями, тогда как за все излишки придется доплачивать.

***

26.04.2018
В WhatsApp появились неприятные изменения

Подросткам, живущим в странах Европы, запрещено пользоваться WhatsApp, если они не достигли 16-летнего возраста. Об этом говорится в обновленных «Условиях предоставления услуг», опубликованных официальном на сайте мессенджера (InternetUA).

«Если вы живете в стране европейского региона, ваш возраст должен быть не менее 16 лет, чтобы вы могли использовать наши сервисы», – уточняется в правилах. В ряде стран этот возраст может быть больше, уточняют в WhatsApp.

В остальных странах минимальный возраст для использования WhatsApp составляет 13 лет. Ранее жители стран Европы также могли подключаться к мессенджеру, начиная с этого возраста.

Как именно администрация WhatsApp намерена проверять возраст пользователей, неизвестно. Новый возрастной ценз связан с принятием в странах ЕС новых правил защиты персональных данных, в соответствии с которыми использование личной информации людей, не достигших 16-летнего возраста, допускается только с разрешения родителя или опекуна.

***

2.05.2018

В Instagram появились видеозвонки, но не у всех

Со второго мая в Instagram появилась функция групповых видеозвонков. Об этом рассказал Марк Цукерберг на ежегодной конференции для разработчиков Facebook f8 (InternetUA).

Функция уже доступна некоторой части пользователей. Остальные же обзаведутся поддержкой в ближайшие несколько недель.

Идея видеозвонков появилась благодаря Instagram Direct. Разработчики заметили, что пользователи часто общаются друг с другом с помощью этой функции.

***

2.05.2018

Facebook тестирует новую кнопку

Социальная сеть Facebook в некоторых странах тестирует новую кнопку «downvote», что делает возможным выражать несогласие с публикациями (InternetUA).

Об этом сообщает Би-би-си.

В данный момент кнопку «downvote» тестируют в Новой Зеландии после такого же исследования, которое состоялось в США в феврале.

Также о новой опции сообщают пользователи из Австралии. Кнопка появилась на некоторых публичных страницах.

В компании Facebook уточнили, что эта кнопка не является дизлайком, а дает возможность пользователю соцсети пожаловаться на комментарии под постами публичных страниц.

Представители соцсети ранее объясняли, что этот тест нового инструмента корректно было бы называть «изучением функции, которая позволит пользователям дать обратную связь на комментарии к публичной страницы».

***

2.05.2018
Михаил Сапитон
Почему Instagram – главная надежда Facebook

Издание Bloomberg Businessweek изучило историю развития Instagram – сервис, купленный Facebook, превратился в одну из крупнейших мировых соцсетей. Однако несмотря на тесные связи с проектом Марка Цукерберга, компании удается сохранять собственную идентичность и даже избегать репутационных скандалов. Если ситуация не изменится, в будущем Instagram может превзойти по значимости сам Facebook.

Докладніше

***

2.05.2018
Facebook решил запустить сервис для знакомств

В социальной сети Facebook появится возможность знакомиться для серьезных отношений. Об этом заявил основатель Facebook Марк Цукерберг на конференции F8, пишет The Verge (InternetUA).

«Это направлено на создание настоящих, длительных отношений, а не мимолетных связей», – подчеркнул Цукерберг.

По его словам, сервис станет частью мобильного приложения соцсети и будет сугубо опциональным. Основатель Facebook также успокоил, что друзья пользователя не узнают, что тот ищет себе партнера: сервис будет предлагать только тех людей, которых нет у него в друзьях.

Помимо этого, сервис будет доступен только для тех, кто укажет в профиле, что у него нет пары.

The Verge отмечает, что на фоне новостей от Цукерберга на 17 % обрушились акции компании Match Group, которая владеет приложением для знакомств Tinder.

***

2.05.2018
WhatsApp появятся групповые видеочаты

Видеочаты будут доступны в течение нескольких недель. Функция в Instagram будет поддерживать групповые и индивидуальные чаты, а также предоставит возможность минимизировать видео и продолжить чат, занимаясь другими делами в Instagram. Пользователи также получат возможность размещать контент с приложений таких как Spotify и GoPro в свои Instagram Stories. Вскоре Instagram запустит

обновленную страницу Explore. В WhatsApp кроме групповых видеочатов добавятся и стикеры . Напомним, несколько дней назад сооснователь приложения Ян Кум покинул компанию. Среди причин – его озабоченность по поводу использования данных пользователей Facebook (Marketing Media Review).

***

2.05.2018

Facebook разрешил пользователям удалять свою историю

Функция под названием «Удали историю» позволит очистить историю браузера в Facebook, включая сайты, на которые пользователь заходил с сети и рекламу, на которую он кликал. В своем посту Цукерберг отметил: «когда мы запустим обновление, вы сможете увидеть информацию о приложениях и сайтах, с которыми вы взаимодействовали, и сможете удалить эту информацию из вашего аккаунта. Вы сможете даже отключить опцию хранения этой информации в аккаунте» (Marketing Media Review).

***

4.05.2018

В сервисе Instagram появилась суровая цензура и своя платежная система

С каждым днем сервис Instagram для любителей фотографий становится все более популярным, а чтобы его аудитория росла и дальше, разработчики постоянно внедряют новые функции.

Докладніше

***

8.05.2018

Шоу продолжается: как Facebook искупит вину перед пользователями

Бизнес-функции для WhatsApp, дополненная реальность для бизнес-партнеров в Messenger, знакомства в Facebook и другие функции, которые изменят продукты компании Марка Цукерберга.

Докладніше

***

8.05.2018

YouTube ежемесячно посещают 1,8 млрд зарегистрированных пользователей

Видеохостинг YouTube ежемесячно посещают 1,8 млрд зарегистрированных пользователей. Об этом сообщила глава компании Сьюзан Войчицки на презентации для рекламодателей Brandcast.

В июне 2017 года эта цифра составляла 1,5 млрд. Таким образом, за 10 месяцев ежемесячная аудитория зарегистрированных пользователей YouTube увеличилась на 300 млн человек.

Войчицки также поделилась новыми рекордами, установленными на платформе. Так, клип на песню Despacito собрал 5 млрд просмотров, а прямую трансляцию выступления певицы Бейонсе на фестивале Coachella смотрели 41 млн человек.

На презентации Войчицки не только рассказала об успехах сервиса, но и коснулась его проблем. В частности, присутствия на площадке неподобающих видео с детьми, в которых показывалась реклама компаний.

«Это влияние открытой платформы: она объединяет мир теми способами, которые не были возможны ранее. Но мы также видели, что эта открытость сопровождается проблемами, поскольку некоторые пытались извлечь личную выгоду из наших сервисов. Для меня и для каждого в YouTube очень важно, чтобы мы росли ответственно», – заявила Войчицки.

Она также пообещала, что наймёт ещё 10 тысяч модераторов для борьбы с неприемлемым контентом.

***

9.05.2018

В приложении Instagram нашли секретную функцию

В программном коде бета-версии приложения Instagram найдена возможность прикрепления аудиозаписей к историям – коротким видеороликам, ссылки на которые появляются в верхней части окна программы (InternetUA).

При создании новой истории пользователи смогут использовать музыкальные треки для звукового оформления, выбирая их из каталога, пишет TechCrunch. Благодаря договоренности Facebook с музыкальными издателями это будет возможно без нарушения авторских прав.

Секретная функция найдена в приложении Instagram для Android.

Длительность музыкальных вставок, вероятнее всего, будет ограничена длительностью самих пользовательских историй. Поиск песен будет доступен в «ручном» режиме или по музыкальному каталогу.

Представители Instagram не прокомментировали новую возможность. Не исключено, что она появится в одной из ближайших

версий приложения.

***

9.05.2018

Видео из Facebook и Instagram можно смотреть в WhatsApp

Новая версия мессенджера WhatsApp получила новую возможность – теперь видео, опубликованные в соцсети Facebook и на сервисе Instagram, можно смотреть, не покидая приложение (InternetUA).

Ранее в WhatsApp поддерживалось только воспроизведение роликов, размещенных на YouTube. В случае с другими сервисами нажатие на ссылку приводило к переходу в другое приложение или на сайт в браузере.

Как пишет WABetaInfo, сейчас команда разработчиков мессенджера занимается усовершенствованием данной возможности, чтобы добавить поддержку других сервисов.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

26.04.2018

Чиновникам Дніпра заборонили лаятися в соцмережах, пиячити на людях та ходити в міні-спідницях

Чиновникам мерії Дніпра заборонили лаятися в соцмережах, пиячити на людях та носити занадто короткі спідниці – міськрада затвердила кодекс поведінки посадовців.

Їх зобов'язали бути ввічливими, неупередженими та приязними. А ще – носити спідниці по коліно та не «світити» тілом крізь прозорий одяг. Заборонили також з'являтися нетверезими в публічних місцях навіть у позаробочий час (ТСН.Ранок).

«Час закінчувати цю вакханалію, коли, наприклад, у соцмережах пишуть у збудженому стані. За хамство, пияцтво і не зовсім товарний зовнішній вигляд чиновники повинні звільнятися», – сказав міський голова Дніпра Борис Філатов.

За дотриманням правил стежитиме спеціальна комісія. За порушення – покарання аж до звільнення. Першим показати приклад пообіцяв і сам мер міста. Його не раз ловили на лайвивих виразах у соціальних мережах.

***

27.04.2018

Захисника «майданівців» через пост в соцмережі хочуть позбавити адвокатського свідоцтва

Дарія Козій, відома також як засновниця фейкової ГО «Реанімаційний пакет реформ», подала скаргу на Маселка через пост у Фейсбуці, звинувативши його у вчиненні дисциплінарного проступку. У цьому пості Роман Маселко висловив своє бачення судового процесу у справі щодо нібито незаконності обрання його до Ради громадського контролю НАБУ.

Хоча автор поста в соцмережі опублікував його не як адвокат, а як безпосередній учасник справи, на думку Козій, повідомлення, яке поширив Роман Маселко, «містить викривлену інформацію, яка паплюжить та підриває престиж професійної діяльності адвокатури». Крім цього, на її думку, Роман Маселко періодично зловживає своїм службовим становищем та здійснює тиск на правосуддя, а також вдається до неприпустимих методів захисту своїх прав та інтересів (очевидно, йдеться про пости у Facebook). Тому позивачка радить Дисциплінарній палаті Комісії розглянути її звернення та позбавити Романа Маселка права зайняття адвокатською діяльністю та виключенням із Єдиного реєстру адвокатів.

У разі втрати адвокатського свідоцтва буде поставлено під сумнів членство Романа Маселка у Громадській раді доброчесності. Також він не зможе захищати в судах потерпілих на Майдані.

Громадська рада доброчесності переконана, що дисциплінарна справа проти Маселка була ініційована через його антикорупційну діяльність та зусилля, спрямовані на реальне очищення судової влади від негідних суддів (Експрес).

***

2.05.2018

Львівська чиновниця захоплюється україножобськими дописами у соцмережах

Начальник відділу внутрішньої та інформаційної політики Червоноградської міської ради Надія Земницька ставить вподобання у соцмережах на дописах антиукраїнського змісту (Вголос).

Як уже писав «Вголос», червоноградський журналіст Рулан Іванець зневажливо ставиться до України і називає державу «генетичною випадковістю».

Тепер же журналісти пишуть, що україножобські дописи – це послідовний прояв ненависті та неповаги Іванця до Української держави та її загальновизнаних українських героїв, зокрема Степана

Бандери та Тараса Шевченка.

Разом з тим, начальник відділу внутрішньої та інформаційної політики Червоноградської міської ради Надія Земницька ставить вподобання під такими дописами.

До всього, журналісти опублікували відеозапис обговорення особистості Путіна редакторським колективом «Ехо-Червоноград», у якому працює Руслан Іванець. Так, під час бесіди Іванець запитує свою колегу Аллу Березюк: «Що тобі поганого зробив Путін, і чого ти до нього причепилася?».

Алла у відповідь спромоглася лише визнати Путіна світовим лідером.

***

3.05.2018

Через вислів лідерки одеського «Правого сектору» про євреїв у соцмережах розгоряється скандал

Другого травня, під час мітингу представників націоналістичних партій та організацій в Одесі, лідерка одеського «Правого сектору» Тетяна Сойкіна закликала «очистити Україну від жидів» (Depo.Одеса).

Слова Сойкіної не залишилися поза увагою. «Цікаво, вона має на увазі єврейські погроми або відразу Голокост? Вірити їй чи ні? Євреям збиратися на вихід чи в країні є правоохоронна система?» – написав на своїй сторінці у Facebook директор Українського єврейського комітету Едуард Долінський.

***

7.05.2018

Після розголосу в соцмережах і медіа у франківському пологовому значно покращало харчування жінок

Після публікацій скандальних фото з двома скибками хліба та чаєм, які жінки у франківському перинатальному центрі отримують на сніданок, меню в закладі різко змінилося на краще (Kurs).

Франківчанки отримали перемогу: жалюгідне харчування у міському перинатальному центрі раптово покращало після розголосу в мережах і ЗМІ.

***

8.05.2018

Закликаємо припинити спроби розколювати країну

У соціальних мережах активно обговорюють ролик, змонтований із запису концерту на одному з каналів до Дня Перемоги (Офіційний веб

-сайт Національної ради України з питань телебачення і радіомовлення).

Потрібно пам'ятати, що засоби масової інформації мають великий вплив на суспільство. Спроби фіксації радянських стереотипів не мають нічого спільного з реальністю, в якій живе сьогоднішня українська держава. Покоління, що сьогодні творять нові смисли, активне демократичне суспільство, яке живе в часі підкорення космосу, унікальних технологій, освіти без кордонів, відкритого світу потребує й адекватної інформаційної сфери. І це має бути простір, вільний від маніпуляцій.

У соціальних мережах зараз спалахнуло обурення поширеним роликом, змонтованим із кадрів грядущого «святкового» телепродукту на одному з каналів.

Чергова маніпуляція і танці на ранах суспільства, якими, як правило, є старозавітні концерти на кшталт «голубого огонька» – є ніякою не свободою слова, не точкою зору, а діями, що спрямовані на розкол суспільства, спробою чергової атаки в інформаційній війні, використанням людей як матеріалу для пропаганди, а тим більше – старших людей, чиї життя заслуговують на шану.

***

8.05.2018

«Мир, труд, Путін!». Як соцмережі відреагували на інавгурацію президента Росії

Сьомого травня відбулась інавгурація Володимир Путіна, який вчетверте вступив на посаду президента Росії. Користувачі соцмереж висміяли активно зреагували на цю подію. Висміяли Наталю Поклонську, яка очікувала на початок інавгурації, новий автомобіль «Кортеж», на якому приїхав новоспечений президент та навіть Стівена Сігала, який був серед гостей заходу. Які ще «перли» видають користувачі соцмереж? Дивіться у нашій підбірці (Експрес).

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

25.04.2018

Услуги ПУМБ теперь можно заказать через Viber

Первый Украинский Международный Банк (ПУМБ) с апреля запустил для своих розничных клиентов канал коммуникации в мессенджере Viber.

Докладніше

***

26.04.2018

Популярный финансовый эксперт судится с Facebook за незаконное использование его лица в криптовалютной рекламе

Мартин Льюис, известный журналист и эксперт в финансовой сфере, подает в суд на Facebook за диффамацию и незаконное использование его лица в рекламе свыше пяти десятков мошеннических проектов, связанных с криптовалютами.

Докладніше

***

2.05.2018

Проект Internet.org от Facebook уже охватывает около 100 млн

Проект Internet.org, запущенный Facebook с целью предоставления доступа к интернету жителям развивающихся стран, уже охватывает почти 100 млн человек. Об этом заявил глава компании Марк Цукерберг во время конференц-звонка по итогам I квартала 2018 года. В ноябре 2016 эта цифра составляла 40 млн (IGate).

В рамках проекта Facebook использует приложение Free Basics, открывающее бесплатный доступ ко многим популярным сайтам и сервисам, а также точки доступа Express Wi-Fi. В настоящее время компания также тестирует дрон Aquila, работающий на солнечной энергии, который планируется использовать для раздачи интернета в отдалённых уголках планеты. Кроме того, Facebook экспериментирует с лазерами и спутниками, чтобы обеспечить интернет-соединение в тех регионах, где отсутствуют мобильные сети.

Несмотря на благородные цели, у проекта есть противники, которые считают, что Free Basics нарушает принцип сетевого нейтралитета. Эта точка зрения, в частности, привела к запрету приложения в Индии.

При этом сторонники проекта убеждены, что наличие хоть какого-нибудь интернета – это лучше, чем полное его отсутствие.

***

3.05.2018

Telegram готов отказаться от публичного размещения токенов TON

Павел Дуров готов отказаться от планов публичного размещения

собственных токенов. Об этом сообщила Wall Street Journal со ссылкой на собственные источники (InternetUA).

Telegram в ходе закрытого ICO собрал столько денег (~$1,7 млрд) от 200 инвесторов, что уже готов отказаться от планов по размещению публичных токенов.

Все вырученные средства пойдут на развитие блокчейна TON и поддержание работы самого Telegram.

Токены – это цифровой актив, который инвестор получает от компании в обмен на деньги. В случае с Telegram, инвесторы покупают токены-жетоны для блокчейна, которые в будущем могут вырасти в цене.

***

3.05.2018

Facebook начал ранжировать СМИ по рейтингу достоверности

Основатель Facebook Марк Цукерберг заявил, что социальная сеть начала ранжировать СМИ по рейтингу достоверности, пишет BuzzFeed (InternetUA).

Цукерберг встретился с группой руководителей средств массовой информации после выступления на ежегодной конференции разработчиков F8. Во встрече приняли участие представители BuzzFeed News, New York Times, CNN, Wall Street Journal, NBC, Daily Beast, Economist, HuffPost, Insider, Atlantic, New York Post и другие.

По его словам, компания уже начала внедрять систему, которая оценивает СМИ на основе рейтинга достоверности и позволяет продвигать или скрывать контент на основе этой метрики.

Цукерберг рассказал, что компания собрала данные о том, как пользователи воспринимают различные СМИ и доверяют ли они им.

«Мы помещаем [эти данные] в систему, и она работает на усиление или подавление, мы собираемся нарастить интенсивность этой системы с течением времени», – сказал он.

***

4.05.2018

Ершов Антон

Instagram включил опцию собственных платежей

Instagram добавил функцию встроенных платежей в свое приложение. Пока она тестируется в США, пишет ресурс TechCrunch (IT новости).

Сообщается, что новая функция позволяет привязать к профилю в Instagram дебетовую или кредитную карту. Безопасность обеспечивает PIN-код. Опция позволяет совершать платежи, не покидая приложение

и не переходя на сторонние сайты для ввода информации.

Instagram пока официально не объявлял о запуске новой функции. В ответ на запрос TechCrunch, представитель сервиса подтвердил, что опция действительно находится в стадии тестирования. По его словам, пользователи смогут забронировать столик в ресторане или записаться в салон и расплатиться внутри приложения.

Сейчас функция доступна только для некоторых сервисов-партнеров. В будущем соцсеть планирует добавить в приложение функцию оплаты других услуг: например, покупки билетов в кино.

Как отмечает TechCrunch, новая функция вписывается в концепцию Instagram, согласно которой пользователи должны проводить в приложении как можно больше времени (именно поэтому там запрещены ссылки на внешние ресурсы). Внутренние платежи позволят им совершать покупки быстрее и привлечет на платформу больше компаний.

***

7.05.2018

Дмитрий Демченко

Bloomberg: Facebook раздумывает над созданием платной версии соцсети без рекламы

В течение последних нескольких недель Facebook проводила исследования рынка в попытках выяснить, сможет ли платная версия соцсети без рекламы привлечь больше пользователей. Об этом сообщает Bloomberg, ссылаясь на собственные источниками (AIN.UA).

Как отмечает Bloomberg, компания изучала такую возможность в прошлом и вернулась к ней из-за недавнего скандала с утечкой пользовательских данных. Раньше внутренние исследования Facebook показывали, что пользователи с недовольством воспринимали идею подписки, указывая на то, что компания хочет заработать с того, что, по ее словам, всегда будет бесплатным.

Сейчас же в Facebook думают, что настроения пользователей меняются. Это связано с кризисом доверия к соцсети после скандала с Cambridge Analytica. И сейчас компания более открыта к радикальным изменениям, чем раньше, внедряя, например, ранжирование СМИ и реакции в комментариях.

Ранее во время дачи показаний в Конгрессе в прошлом месяце Марк Цукерберг заявил, что «бесплатная версия Facebook будет всегда».

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

28.04.2018
П’ять фобій, викликаних гаджетами і соцмережами

Боязнь висоти, привидів та дзеркал – вчорашній день. Сьогодні люди божеволіють через інтернет-троллінг, соціальні мережі, відсутність чи надмірну присутність гаджетів у їхньому житті. Проникнемо у світ фобій сучасної людини.

Докладніше

***

5.05.2018
Як соцмережі впливають на жінок

Психолог Мартін Графф (Martin Graff) з колегами з Університету Південного Уельсу провів невелике дослідження, яке показало, що дівчата, які приділяють багато уваги соцмережам, визнають худобу привабливою і прагнуть до неї (Максимум). Про результати він розповів на науковій конференції в Ноттінгемі.

У його експерименті брали участь сотня студенток. Вони розділилися на чотири групи – відповідно до часу, проведеного в соціальних мережах (враховувалися Facebook, Instagram і Pinterest). В першу групу потрапили дівчата, які витрачали на них менш як 30 хвилин на день, далі цей показник збільшувався на півгодини. Так, респонденти четвертої групи проводили в соцмережах більше півтори години на день.

Учасниці відповідали на питання анкети, яка вимірювала три показники: ступінь згоди з образом «ідеального тіла», який популяризується в суспільстві, ступінь стурбованості тим, як інші люди сприймають їх власне тіло, і мотивація до схуднення. Рівень об'єктивації визначався завдяки оцінці, яку студентки давали заявами на кшталт «худі дівчата – більш привабливі».

Дослідники виявили, що ті учасниці, які проводили в соцмережах понад годину на день, отримали найвищі показники у всіх трьох категоріях.

Мартін Графф прокоментував: «Ми продемонстрували, що часте відвідування тих сервісів, де люди викладають власні фотографії для порівняння з іншими, пов'язане з нездоровим ставленням до тіла і тому,

які зусилля для цього необхідні».

***

8.05.2018
Як смартфони та соцмережі крадуть дитинство

Дослідники стверджують, що соціальні медіа можуть провокувати депресію у підлітків, а багато батьків переймаються тим, що смартфони поглинають усю увагу їхніх дітей.
Докладніше

Маніпулятивні технології

25.04.2018
ПАРЄ ухвалила резолюцію щодо протидії російській пропаганді

Депутати ПАРЄ одноголосно ухвалили резолюцію про підтримку протидії російській пропаганді на рівні ЄС (Espreso.tv).
Про це повідомив народний депутат та віце-президент ПАРЄ Володимир Ар'єв у Facebook.
Документ також рекомендує країнам-членам Ради Європи заснувати органи (observatories) для відстежування дезінформації та фейків.
У резолюції йдеться, що у деяких випадках державні засоби масової інформації були перетворені на пропагандистські інструменти та використані для передачі фальшивих новин або розпалювання ненависті ксенофобії проти меншин та певних груп.
«Це призводить до відсутності незалежності та низьких етичних стандартів у ряді засобів масової інформації та пояснює дедалі більшу недовіру населення. У зв'язку з цим Асамблея підтверджує свою підтримку рішенню Європейської Ради 2015 про боротьбу з потоком дезінформації та відвертої неправди, що походять з засобів масової інформації та онлайн-аккаунтів у Російській Федерації, шляхом створення Спеціальної групи East StratCom», – цитує Ар'єв резолюцію.

***

1.05.2018
Російська «фабрика тролів» спробувала підірвати енергетичні ринки США

Російська «фабрика тролів» у Санкт-Петербурзі після втручання в президенську кампанію 2016 року у США продовжує активно впливати на енергетичні ринки Штатів (Народна правда).

Про це йдеться в дослідженні профільного комітету Палати представників американського Конгресу, опублікованому виданням The Hill.

Комітет з питань науки, космосу і технологій Палати представників у своєму березневому звіті, в якому детально проаналізовано діяльність російського Інтернет-дослідницького агентства, що має назву «фабрики тролів», заявив, що російські інтернет-тролі активно намагаються підірвати енергетичні ринки Сполучених Штатів.

У документі, зокрема, зазначається, що росіяни вживали деструктивні заходи з метою підриву американських енергетичних ринків та впливу на внутрішню енергетичну політику, в тому числі, і через американські медіа-платформи Instagram, Facebook і Twitter.

Як зазначається, це не перша спроба Росії завдати шкоди енергетичній галузі на Заході. Американські законодавці пригадали скоординовану кампанію росіян з дезінформації, спрямовану проти видобутку сланцевого газу в Європі, про яку ще в 2014 році говорив тодішній генеральний секретар НАТО Андерс Фог Расмуссен.

Російські пропагандисти намагаються і надалі створювати ілюзії для Європи щодо необхідності продовжувати закупівлю природного газу з Росії.

***

5.05.2018

В Facebook для дискредитації ООС створено фейкову сторінку

В мережі Facebook для дискредитації Операції Об'єднаних сил створено фейкову сторінку ООС. Про це кореспонденту УНН повідомили в прес-центрі ООС (InternetUA).

«Друга сторінка ООС в Facebook – фейкова. ЇЇ використовують, можна сказати, російські спецпідрозділи. Вони створили "дзеркало" (справжньої сторінки ООС – ред.), щоб ця сторінка набирала своїх читачів, а потім запускати там фейки та дискредитувати Об'єднані сили. Наша справжня сторінка має більше 5 тисяч людей, які на неї підписалися, та має адресу "pressjfo.news"», – повідомили в прес-центрі ООС.

В ООС додали, що найкращим варіантом для закриття цієї фейкової сторінки, стане відповідна скарга до адміністраторів мережі Facebook.

***

7.05.2018

США хочуть опублікувати тисячі політичних оголошень російської «фабрики тролів» // Їх розміщували у соцмережі під час президентських

перегонів 2016 року

Демократи у Спецкомітеті з розвідки Палати представників Конгресу США мають намір опублікувати 3 тисячі рекламних оголошень політичного характеру, розміщених у Facebook на замовлення організації «Агентство інтернет-досліджень» (російська «фабрика тролів», базується в Санкт-Петербурзі) (uatv).

Про це повідомляє УНН із посиланням на The Wall Street Journal.

«За відомостями джерел видання, зазначені матеріали можуть бути опубліковані вже протягом цього або наступного тижня. За версією американської сторони, їх розміщували у соцмережі під час президентських перегонів 2016 року в США, а також після неї. Законодавці мають намір вказати, на які групи населення були націлені оголошення, скільки вони коштували, яка кількість людей їх бачила», – йдеться у повідомлені.

***

8.05.2018

В китайской соцсети WeChat за год заблокировали около 500 млн публикаций со слухами

Крупнейшая в Китае социальная сеть WeChat, которая насчитывает почти один миллиард пользователей, в 2017 году заблокировала около 500 миллионов публикаций, которые являлись слухами, говорится в опубликованном докладе Китайской академии телекоммуникационных исследований при Министерстве промышленности и информационных технологий (InternetUA).

«По состоянию на данный момент более 800 сторонних компетентных ведомств присоединились к борьбе со слухами. Они перехватили слухи более 500 миллионов раз, опубликовали 40 списков слухов, перенаправили более 1,2 миллиона запросов и наказали более 180 тысяч официальных аккаунтов», – говорится в опубликованном докладе.

К декабрю 2017 года мини-программой «Помощник опровержения слухов» в WeChat воспользовались более 19,7 миллиона подписчиков, которые активировали ее в среднем 300 тысяч раз в день. В общей сложности программа выдала 37 миллионов напоминаний.

За последние годы в Китае был принят целый ряд нормативных и идеологических документов, предписывающих национальным интернет-компаниям и СМИ тщательно следить за качеством

распространяемой в интернете информации. Председатель КНР Си Цзиньпин заявил, что гарантировать национальную безопасность и экономическую стабильность в стране без полного обеспечения кибербезопасности невозможно.

Спецслужби і технології «соціального контролю»

1.05.2018

Удар по Google и Facebook. Как ЕС защитит своих граждан от киберслежки

С мая в Евросоюзе вступают в силу новые правила обработки персональных данных. Они касаются всех стран Европейского союза. Также их должны придерживаться все предприятия, которые оказывают услуги в ЕС.

Докладніше

***

2.05.2018

Эксперт: Через несколько дней Telegram полностью заблокируют в России

Эксперты прогнозируют, что до полной блокировки Telegram на территории России осталось всего несколько дней. Дело в том, что Amazon отказалась предоставлять хостинги запрещенному месседжеру, как раньше поступила и Google (InternetUA).

Эксперты озвучили подтверждение тому, что до блокировки Telegram осталось несколько дней. Согласно решению суда Роскомнадзор уже две недели подряд пытается заблокировать данный ресурс за отказ сотрудничать с ФСБ, но месседжеру удавалось оставаться в работе благодаря хостингам иностранных компаний, таких как Amazon и Google. Руководство Google ранее уже сообщило, что больше не будет предоставлять свой облачный хостинг Telegram, а теперь его примеру решила последовать и компания Amazon.

Как оказалось, иностранные компании вынуждены пойти на данные меры, чтобы оставить в работе другие ресурсы в своих хостингах, которые ранее массово блокировал РКН. Кроме того, блокировка ресурсов Google и Amazon могла оказаться не случайной, а осознанной за то, что компании помогали запрещенному месседжеру обходить блокировку.

В настоящее время в использовании Telegram остаются хостинги Apple и Microsoft, но эксперты прогнозируют, что эти компании

вынуждены будут «уступить» месседжер государственному регулятору РФ.

***

7.05.2018

Роскомнадзор наделил себя правом самостоятельно блокировать любые ресурсы в Сети

Члены рабочей группы «Связь и IT», экспертного совета при правительстве РФ, раскритиковали проект приказа Роскомнадзора о правилах блокировки запрещенных ресурсов. По их словам, новая версия проекта приказа, опубликованная 23 апреля, фактически дает Роскомнадзору возможность самостоятельно заблокировать любой ресурс (InternetUA).

Ожидалось, что в ведомстве подготовят приказ об идентификации сайтов и сервисов, которые используются для обхода блокировок. Он должен был позволить блокировать сервисы VPN и анонимайзеры, а также легализовать блокировку миллионов IP-адресов в рамках борьбы с Telegram. Но в Роскомнадзоре написали совсем другое, наделив себя правом самостоятельно определять сетевой адрес и доменное имя страницы с запрещенной информацией «в случае выявления ошибок». То есть полностью заменив функции органов, которые должны устанавливать факт отнесения информации к запрещенной.

Сам порядок идентификации сайта проект приказа не описывает, отмечает «Коммерсант». Также неясно, какие критерии Роскомнадзор будет использовать при проверке, соответствует ли информация на ресурсе той, которая послужила основанием для блокировки. Непонятно, должен ли текст быть идентичным или просто совпадать по смыслу.

Эксперты подчеркивают, что это вообще не задача Роскомнадзора определять, запрещенная ли информация размещена на том или ином ресурсе. Это должен определять суд по решению прокуратуры, обращений правообладателей и т. д.

В самом ведомстве заявили, что приказ позволяет править лишь технические ошибки и опечатки – например, в случаях, когда в решении суда содержится неточность в написании доменного имени.

***

8.05.2018

СБУ запобігла провокаціям російських спецслужб до 9-го травня, організованим через соціальні мережі

Оперативники спецслужби виявили двох мешканців Київської та

Сумської областей, які адміністрували антиукраїнські спільноти у соцмережі «ВКонтакте». Співробітники СБ України задокументували, що зловмисники отримали вказівку від російських спецслужб організувати підбір бажаючих за гроші взяти участь у так званому «Марші Безсмертного полку» у різних містах країни (InternetUA).

За інформацією СБ України, напередодні 9-го травня значно активізувалася пропагандистська діяльність представників так званого «Міністерства інформації ДНР». Його працівники розсилають «методички» власникам антиукраїнських спільнот у соцмережах для проведення масової агітації в інтересах Кремля та терористичних організацій «Д/ЛНР».

У рамках реалізації комплексу заходів із протидії російській інформаційній агресії напередодні травневих свят співробітники СБУ заблокували у соцмережах вісім антиукраїнських спільнот, які розповсюджували заклики до участі у провокаційних фейкових акціях в інтересах країни-агресора.

***

9.05.2018

В России учителям поручили «лайкать» чиновников в соцсетях и создавать об этом отчеты

В Воскресенском районе Подмосковья в России учителя и работники культуры получили распоряжение ставить лайки к постам местных чиновников во всех социальных сетях (InternetUA).

Об этом сообщает Meduza со ссылкой на документ, предположительно подготовленный в администрации Воскресенского района, пишет realist.online.

Согласно документу, от сотрудников образовательных и культурных учреждений района потребовали ставить лайки к постам руководителей района во «ВКонтакте», Facebook, Instagram и «Одноклассниках».

К документу приложена инструкция с указаниями, как правильно это делать и как отчитываться о проделанной работе.

Бумага называется «Регламент работы специалиста в социальных сетях».

***

8.05.2018

У Львові СБУ припинила ретрансляцію телеканалів країни-агресора та терористів «ДНР»

Співробітники СБУ припинили у Львові ретрансляцію заборонених на території нашої країни пропагандистських телеканалів РФ та терористичної організації «ДНР» (InternetUA).

Правоохоронці встановили, що група місцевих жителів організувала нелегальний продаж телевізійних приставок із завчасно налаштованим доступом до забороненого контенту. Своїх клієнтів зловмисники підшукували через створений у мережі Інтернет власний веб-ресурс.

Під час санкціонованих обшуків в офісному приміщенні ділків оперативники спецслужби виявили обладнання, що підтверджує їх протиправну діяльність.

У рамках відкритого кримінального провадження за ч. 2 ст. 361 Кримінального кодексу України тривають слідчі дії.

Операція із викриття зловмисників проводилась спільно з поліцією.

Проблема захисту даних. DDOS та вірусні атаки

25.04.2018

Уровень защищенности банковских приложений для Apple iOS выше, чем у аналогов под Google Android

Согласно исследованию Positive Technologies доля мобильных банковских приложений, в которых обнаруживаются критически опасные уязвимости, снижается с каждым годом.

Докладніше

***

1.05.2018

Все пользователи WhatsApp оказались в огромной опасности

Специалисты антивирусной компании Dr. Web выяснили, что за последний год более чем в 5 раз возросло количество новых модификаций вредоносных приложений, маскирующихся под

мессенджер WhatsApp. Самым популярным из них является его Plus-версия.

Докладніше

***

1.05.2018

Хакеры могут проникнуть в корпоративную сеть 73 % промышленных компаний

Аналитики Positive Technologies подготовили исследование векторов атак на корпоративные информационные системы промышленных компаний (InternetUA).

Так согласно собранной статистике, злоумышленники могут преодолеть периметр и попасть в корпоративную сеть 73 % компаний промышленного сегмента. В 82 % компаний возможно проникновение из корпоративной сети в технологическую, в которой функционируют компоненты АСУ ТП.

Одной из главных возможностей для получения взломщиком доступа к корпоративной сети оказались административные каналы управления. Часто администраторы промышленных систем создают для себя возможности удаленного подключения к ним – это позволяет им, например, не находиться все время на объекте, а работать из офиса.

В каждой промышленной организации, в которой исследователям Positive Technologies удалось получить доступ к технологической сети из корпоративной, были выявлены те или иные недостатки сегментации сетей или фильтрации трафика – в 64 % случаев они были внесены администраторами при создании каналов удаленного управления.

Наиболее распространенными уязвимостями корпоративных сетей стали словарные пароли и устаревшее ПО – эти ошибки были обнаружены во всех исследуемых компаниях. Именно эти недостатки позволяют развить вектор атаки до получения максимальных привилегий в домене и контролировать всю корпоративную инфраструктуру. Важно отметить, что часто файлы с паролями к системам хранятся прямо на рабочих станциях сотрудников.

***

1.05.2018

Передавший данные пользователей Facebook сотрудник также купил информацию у Twitter

В корпорации Twitter Inc. рассказали, что продали доступ к публичным данным в соцсети компании Александра Когана Global Science Research, предоставившей данные пользователей Facebook

сторонней компании Cambridge Analytica. Об этом сообщает Bloomberg (InternetUA).

Как отмечается, компания Когана получила доступ к публичным твитам, размещенным в соцсети в течения пяти месяцев с декабря 2014 до апреля 2015 года. В Twitter подчеркнули, что при этом речь идет исключительно о размещенной в открытом доступе информации, а не о личных данных пользователей.

***

1.05.2018

Хакеры сканируют интернет в поисках уязвимых серверов Oracle WebLogic

В течение почти двух недель киберпреступники сканируют интернет в поисках серверов Oracle WebLogic. Сканирование началось после 17 апреля, когда компания Oracle выпустила свои квартальные плановые обновления безопасности (InternetUA).

Апрельские обновления в частности содержат патч для уязвимости (CVE-2018-2628) в ключевом компоненте WebLogic – WLS. Уязвимость получила оценку в 9,8 балла из 10, поскольку позволяет неавторизованному злоумышленнику выполнить код на удаленном сервере WebLogic.

Проблема была обнаружена экспертом NSFOCUS Security Team Ляо Синьси (Liao Xinxi) и независимым исследователем безопасности loopx9. Спустя день после выхода исправления Синьси рассказал в китайской соцсети, как работает уязвимость, и на основании его публикации пользователь GitHub под псевдонимом Brianwrf опубликовал для нее PoC-эксплоит.

Публикация рабочего PoC-эксплоита незамедлительно привела к всплеску числа сканирований порта 7001, используемого уязвимым сервисом WebLogic «T3». Тем не менее, по словам экспертов компании GreyNoise, первыми обнаруживших рост интереса к порту 7001, пока что дальше сканирований дело не идет, и случаи эксплуатации уязвимости в реальных атаках пока не подтверждены.

***

1.05.2018

Страницу штаба АТО в Facebook взломали

Хакеры взломали страницу штаба АТО, сейчас там опубликована реклама вступления в ряды незаконных вооруженных формирований (InternetUA).

Речь идет о странице с адресом www.facebook.com/ato.news.

Напомним, штаб АТО официально прекратил свою работу в связи

со сменой формата Антитеррористической операции на Операцию объединенных сил (ООС).

***

2.05.2018

Кібербезпека: чому сайти українських держструктур легко зламати

Попри низку ініціатив із захисту власного кіберпростору, Україна досі пасе задніх у сфері інформаційної безпеки, попереджають експерти.

Докладніше

***

2.05.2018

Мошенники выманивают криптовалюты через Twitter

Учетная запись проекта Vertcoin в соцсети Twitter накануне оказалась под контролем неизвестных злоумышленников. Вскоре после этого был опубликован твит о якобы раздаче 10 биткоинов, для участия в которой пользователям предлагалось отправить 0,005 BTC на указанный сторонний адрес (InternetUA).

Твит сразу же вызвал подозрения со стороны сообщества. Помимо того что сами разработчики Vertcoin нигде не упоминали указанную раздачу, само сообщение оказалось очень похожим на один из многочисленных скамов, которые можно встретить в Twitter.

Впоследствии один из ведущих разработчиков Vertcoin Джеймс Лавджой подтвердил опасения сообщества.

На момент публикации Twitter-аккаунт Vertcoin, судя по всему, все еще находится под контролем злоумышленников: твит с раздачей до сих пор не удален, однако скамеры пока что не публиковали новых сообщений.

Стоит отметить, что за это время на указанный в твите адрес было переведено чуть менее 0,007 BTC, причем лишь одна транзакция составила запрашиваемые 0,005 BTC. Таким образом, пользователи оказались не такими уж и доверчивыми – максимум один человек действительно попался на скам.

***

2.05.2018

Владимир Кондрашов

CERT-UA просит собственников сайтов на Drupal немедленно принять меры против взлома

Команда реагирования на компьютерные чрезвычайные происшествия Украины CERT-UA напоминает о необходимости принятия мер для устранения критической уязвимости CMS Drupal (InternetUA).

Соответствующее сообщение было опубликовано сегодня на официальной странице в Facebook Государственной службы специальной связи и защиты информации, передает InternetUA.

– Команда CERT-UA Госспецсвязи напоминает владельцам сайтов, построенных на CMS Drupal, о необходимости принятия мер для устранения уязвимости «Drupalgeddon2», которую сейчас активно используют для взлома web-ресурсов, – говорится в сообщении.

Указанная уязвимость в ядре CMS Drupal позволяет злоумышленникам выполнить произвольный код и полностью скомпрометировать файлы сайта. Все файлы могут быть удалены или изменены независимо от прав доступа. На официальном сайте Drupal указано, что рабочий эксплойт (программа для эксплуатации уязвимости) разработан и широко используется, поэтому нужно считать все сайты, которые не были обновлены до 11.04.2018 – потенциально скомпрометированными.

28 марта на официальном сайте Drupal были опубликованы обновления, устраняющие критическую уязвимость CVE-2018-7600 в CMS Drupal версий 7.x, 8.5.x, 8.4.x, 8.3.x.

Также 23 апреля на официальном сайте Drupal появились новости о выпуске дополнительных обновлений, которые устраняют уязвимости в ядре CMS версий 7.x, 8.4.x, 8.5.x. Новые уязвимости будут иметь номер CVE-2018-7602.

***

4.05.2018

Twitter посоветовал всем пользователям оперативно поменять пароль

Сервис микроблогов Twitter обнаружил критическую ошибку, позволяющую получить доступ к чужим учетным записям. Техническая служба соцсети выпустила сообщение, в котором пользователям рекомендовано сменить пароль (InternetUA).

«Недавно мы обнаружили и исправили ошибку, в которой сохраненные пароли были раскрыты во внутреннем логе. Мы не фиксировали случаи неправомочного использования чужих паролей

кем-либо. Тем не менее в качестве меры предосторожности подумайте об изменении пароля для всех служб», – указано в заявлении.

В августе 2017 года стало известно, что хакеры научились воровать телефонные номера абонентов для последующего взлома социальных сетей и онлайн-кошельков. Издание The New York Times выяснило, что злоумышленники звонят в службу поддержки оператора связи и с помощью информации, найденной на просторах соцсетей, убеждают сотрудников настроить переадресацию всех звонков и сообщений на другое устройство. После этого киберпреступники сбрасывают пароли учетных записей.

***

6.05.2018

Уязвимость в «ВКонтакте» позволяла просматривать список пользователей приложений

Пользователи «ВКонтакте» обнаружили в социальной сети уязвимость, позволяющую с помощью поиска по людям просматривать всех, кто использовал то или иное приложение (InternetUA).

Для успешной эксплуатации проблемы достаточно подставить числовой идентификатор приложения со знаком минус в в ссылку вида «https[://]vk.com/search?c[photo]=0&c[group]=[идентификатор приложения]».

Таким образом можно увидеть список всех пользователей, использующих какое-либо приложение. Если сайт поддерживает авторизацию с помощью соцсети, злоумышленник может с помощью идентификатора определить, является ли человек посетителем данного ресурса.

По словам представителей «ВКонтакте», уязвимость была оперативно устранена вскоре после обнаружения, однако неизвестно, как долго просуществовала данная проблема.

***

6.05.2018

Большинство наиболее популярных туристических сайтов признаны небезопасными

Почти 90 процентов сайтов по бронированию жилья и авиабилетов не удовлетворяют требованиям цифровой безопасности (InternetUA).

Согласно данным компании Dashlane, которая проанализировала 55 наиболее популярных туристических сайтов, каждому из которых компания присудила оценку от 1 до 5 баллов согласно пяти критериям

безопасности.

В частности, эксперты проверяли, насколько строгие требования сайты предъявляют к паролю пользователя.

В результате только шесть порталов (11 % от общего числа) получили удовлетворительные баллы от четырех и выше. Среди худших в рейтинге с оценкой 1/5 оказались сайты по бронированию отелей Trivago, Agoda, Accor Hotels, а также Tripadvisor.

Современный путешественник должен считаться со многими цифровыми опасностями, связанными с кражей личных данных о бронировании рейсов и гостиничных номеров, аренды автомобиля или поиска онлайн-рекомендаций, что создает возможности для мошенничества, – заявил генеральный директор компании Dashlane Эммануэль Шалит.

Большинство сайтов не имеют двухфакторной аутентификации, а некоторые позволяют ввести в качестве пароля комбинацию «12345» или «password».

Порталы Hotels.com и Couchsurfing получили оценку 2/5. Сайт по бронированию отелей Booking.com, сервис по аренде автомобилей Hertz, а также поисковики авиабилетов Skyscanner и Momondo – 3/5. Наивысших баллов удостоились сайты отелей Hilton и Marriott, а также портал круизной компании Royal Caribbean. Самым безопасным сайтом эксперты признали Airbnb – он единственный получил оценку 5/5.

***

7.05.2018
Пользователи Facebook оказались самыми самоуверенными

Американские пользователи Facebook чаще, чем владельцы аккаунтов в других соцсетях, уверены, что знают, как защитить личные данные. Об этом свидетельствуют данные опроса Reuters, проведенного в конце апреля на всей территории США (InternetUA).

Так, 74 процента пользователей соцсети уверены, что достаточно осведомлены о настройках конфиденциальности своих аккаунтов. Еще 78 процентов заявили, что умеют их менять. Для сравнения, среди владельцев Instagram-аккаунтов (принадлежит компании Facebook) о своих настройках безопасности знают 60 процентов, среди пользователей Twitter осведомлены об этом 55 процентов.

При этом только 23 процента использующих Facebook полагают, что имеют полный контроль за безопасностью личной информации. Еще 20 процентов уверены, что вообще не контролируют конфиденциальность, 49 процентов считают, что обладают «некоторым контролем».

Опрос Reuters проводился после скандала с утечкой данных: в апреле Facebook признала, что информация о 87 миллионах человек

ненадлежащим образом была передана компании Cambridge Analytica. Консалтинговая фирма собирала сведения через стороннее приложение для опросов.

Агентство пишет, что утечка не повлияла на лояльность пользователей соцсети: почти половина американских пользователей Facebook не стали реже заходить на сайт, еще 25 процентов начали делать это чаще. По итогам первого квартала 2018 года в США и Канаде число ежемесячных пользователей Facebook выросло до 241 миллиона.

***

7.05.2018

Android P запретит приложениям отслеживать сетевую активность

Разработчики с форума XDA обнаружили новые изменения в правилах режима SELinux для приложений, ориентированных на уровень API 28 в версии операционной системы Android P. Данные изменения касаются проблемы безопасности, позволяющей любому приложению на Android контролировать доступ к сети другого приложения (InternetUA).

Во всех версиях операционной системы вплоть до Android Oreo любое приложение может отслеживать сетевую активность устройства без ведома пользователя. Приложения не могут получить доступ к содержимому сетевых вызовов, однако способны проверить любое исходящее или входящее соединение через протокол TCP/UDP и выявить, подключился ли пользователь к определенному серверу. Например, приложение может обнаружить, когда другая программа на устройстве подключается к серверу финансового учреждения.

Согласно сообщению участников проекта Android Open Source Project, разработчики намерены «начать процесс блокировки доступа к proc/net». Данная директория содержит большое количество связанных с сетевой активностью данных из ядра ОС. В настоящее время у приложений нет ограничений на доступ proc/net, что позволяет им анализировать сетевую активность устройства.

Новые изменения SELinux позволяют получать доступ к некоторой сетевой информации только определенным VPN-приложениям. Как отметили разработчики, уязвимость еще будет существовать какое-то время, поскольку Android-приложениям не обязательно настраивать API до уровня 28 до 2019 года.

***

7.05.2018

Мошенники посредством поддельного сайта Netflix охотятся на

данные банковских карт

Специалисты ESET предупреждают о новой фишинговой атаке. Злоумышленники подделали сайт Netflix и собирают с его помощью данные банковских карт пользователей (Компьютерное Обозрение).

Потенциальная жертва получает по электронной почте фишинговое сообщение о завершении срока действия подписки на Netflix. В письме утверждается, что продлить подписку не удалось из-за проблемы с оплатой, поэтому она будет отменена – конечно, если пользователь не активирует ее вручную. Для «активации подписки» предусмотрена красная кнопка в письме.

Кнопка «активации» ведет на поддельный сайт Netflix, дизайн которого копирует настоящий. Более того, фишинговый сайт имеет сертификат безопасности, а его веб-адрес начинается с префикса https.

На поддельном сайте пользователю предлагается ввести email и пароль от личного кабинета Netflix, а затем заполнить анкету, включающую информацию о банковской карте. После этого пользователь будет перенаправлен на настоящий сайт Netflix, а его данные поступят в распоряжение мошенников.

ESET рекомендует игнорировать подозрительные сообщения, не переходить по ссылкам из них.

***

7.05.2018

Пользователи уанета обнаружили бота, который выдает ФИО человека по номеру телефона

Пользователи украинского сегмента интернета обнаружили Telegram-бота, который позволяет определить личность человека по номеру его телефона. При этом в описании бота говорится о том, что в его базе находится более 30 миллионов украинских номеров, источниками которых указаны сайты по поиску работы и данные Android-приложений. Как сообщает AIN, проверка работы бота показывает, что он может безошибочно определить абонентов (Зеркало недели. Украина).

Для того, чтобы получить имя и фамилию владельца номера телефона, необходимо ввести номер в формате 380xxxxxxxxx и нажать ввод. Результат выдается мгновенно. Вместе с тем, бот дает информацию только по трем номерам в сутки. Чтобы расширить свои возможности, в качестве платы боту необходимо ввести номер из своей телефонной книги.

Кто разработал бота – выяснить не удалось. Его владельцем указан аккаунт @bot_creaters, но на запрос журналистов создатели аккаунта не ответили.

***

7.05.2018
Михаил Сапитон
Android-троян ZooPark способен воровать почти любые данные

«Лаборатория Касперского» сообщила об идентификации вредоносного приложения ZooPark. Оно распространялось на Ближнем Востоке с 2015 года. Зараженные смартфоны находятся в Марокко, Ливии, Иордане, Египте и Иране. За время существования ZooPark сменило четыре версии. Первая имела доступ лишь к контактам и аккаунтам пользователя, но со временем функциональность увеличивалась.

Докладніше

***

7.05.2018
Одно сообщение позволяет сломать любой смартфон на Android

Пользователи смартфонов под управлением Android заметили, что в сети стало распространяться сообщение с эмодзи в виде черного круга и надписью «Ты не можешь нажать его». На самом деле, нажать на этот кружок можно, но сразу после касания экрана приложение начинает вести себя нестабильно и требует перезагрузки (InternetUA).

Простое на первый взгляд сообщение состоит примерно из двух тысяч невидимых символов, последовательность которых выводит из строя движок рендеринга текста на Android. Невидимая часть сообщения состоит из специальных символов, которые Юникод использует, для указания направления текста: должен ли идти справа налево или наоборот. То есть, используется функция, отвечающая за правильное написание иврита и арабского языка.

На самом деле смартфоны уже давно легко справляются с изменениями направления текста, но именно Юникод-кодировка этого сообщения приводит к ошибке в движке рендеринга. Кодирующая текст и эмодзи последовательность символов заставляет движок несколько раз менять направление текста и на какой-то из строк символов происходит аварийное завершение работы. Что интересно, в отличие от «поломок» iOS при помощи сообщений, Android может корректно отображать текст, а проблемы появляются только при нажатии на сообщение.

Самыми устойчивыми к проблемному сообщений оказались Chrome и Google Pixel 2. Браузер не восприимчив к ошибке, а смартфоны начинают тормозить, но быстро возвращают работоспособность. Устройства других производителей, особенно

старые, так не могут и требуют действий от пользователя – закрытия приложения или перезагрузки.

***

8.05.2018
Владимир Кондрашов
Интернет-мошенники охотятся на абонентов крупных украинских провайдеров

Несколько крупных украинских интернет провайдеров предупредили своих клиентов о возможном мошенничестве, цель которого – хищение личных данных и средств клиентов, передает InternetUA (InternetUA).

В частности, на протяжении месяца о возможном мошенничестве предупредили Vega, Ланет и Паутина.NET.

7 мая появилось предостережение на официальной странице Vega Telecom Group в Facebook. У телеком-оператора обратили внимание на участившиеся случаи мошенничества: абоненты телеком-оператора стали получать сообщения якобы от Vega в личном кабинете пользователя, на страницах в социальных сетях и всплывающие окна в интернет-браузерах с предложением принять участие в конкурсе и/или оплатить получение приза от компании.

В Vega заявляют, что компания не проводит розыгрыш призов с оплатой доставки подарка (приза) получателем, не требует от абонентов предоставления персональных данных по кредитным карточкам и не отправляет письма с адресов других компаний:

– Убедительно просим: при получении любых сообщений обращать внимание на адрес рассылки, а также адрес (URL), по которому вас просят перейти. Не отвечайте на сообщения и не переходите по ссылкам/адресам от компании Vega, если они подозрительные. При необходимости уточнения запроса просим обращаться на официальную линию поддержки.

3 мая предупреждение о мошенничестве опубликовала «Мережа Ланет».

– Несколько наших пользователей прислали нам снимки экранов своих устройств, на которых они зафиксировали окна, всплывающие на некоторых сайтах, якобы с розыгрышем призов от имени «Мережі Ланет», – но будьте осторожны, это мошенничество. В первую очередь обратите внимание на странные URL-адреса, которые фигурируют в тексте сообщения или в адресной строке браузера. Далее, если есть сомнения, узнайте информацию о действительных акциях у наших консультантов по телефону или написав в чате, на странице в личном кабинете или на электронную почту, – предупреждают в «Ланет».

По мнению провайдера, вероятней всего, сработал скрипт

(программа), которая самостоятельно определяет, какого интернет-провайдера использует жертва и автоматически подставляет его название в текст для повышения уровня доверия.

***

9.05.2018

Мошенники за год украли у пользователей Сети $172 млрд

В 2017 году жертвами интернет-мошенников в 20 странах мира стали стали 978 млн пользователей, а общая сумма хищений составила 172 млрд долларов (InternetUA).

Согласно докладу о кибер-безопасности Norton Cyber Security Insights, подготовленному компанией Symantec, все эти деньги были похищены у пользователей в результате различных интернет-афер, включая мошенничество при совершении покупок в интернет-магазинах, аферы с кредитными картами, а также похищение платежных данных.

Чаще всего жертвами хакеров становятся люди, которые пользуются большим количеством устройств дома и на работе и при этом имеют слабое представление об основах кибербезопасности.

Данные по киберпреступлениям приведены только по 20 странам мира. В алфавитном порядке это – Австралия, Бразилия, Великобритания, Германия, Гонконг, Индия, Индонезия, Испания, Италия, Канада, Китай, Мексика, Нидерланды, Новая Зеландия, ОАЭ, Сингапур, США, Швеция, Франция и Япония.

В докладе отмечается, что в среднем каждая жертва преступлений в Сети потеряла около 142 долларов.

Больше всего от киберпреступлений пострадали пользователи в Китае – там почти 353 млн человек в совокупности потеряли рекордные 66 с лишним млрд долларов.

***

9.05.2018

Хакеры украли банковские идентификаторы половины населения США

Бюро кредитных историй Equifax завершило оценку объема и состава данных, украденных хакерами летом 2017 г. Злоумышленники получили в свое распоряжение 145,5 млн номеров социального страхования, которые в США позволяют взять кредит или оформить банковскую карту.

Докладніше

***

9.05.2018

В Украине вступил в силу закон о кибербезопасности

Девятого мая в Украине вступил в силу закон о кибербезопасности.

ЗУ «Об основных принципах обеспечения кибербезопасности Украины» опубликовали в официальной парламентской газете «Голос Украины» 9 ноября 2017 года. Он вступил в силу через шесть месяцев со дня опубликования (InternetUA).

Теперь согласно документу, в стране должна быть создана Национальная телекоммуникационная сеть и Государственный центр киберзащиты. Также должна быть сформирована правительственная команда реагирования на компьютерные чрезвычайные происшествия CERT-UA для анализа данных о киберинцидентах и для предоставления практической помощи по устранению их последствий.

Новый закон определяет основные объекты киберзащиты, которые составляют критическую инфраструктуру страны, принципы обеспечения кибербезопасности и национальную систему кибербезопасности.

Согласно закону, президент координирует деятельность в сфере кибербезопасности через возглавляемый им Совет национальной безопасности и обороны.

Документом уточняются понятия «кибербезопасность», «киберзащита», «киберпреступность», «кибероборона» и ряд связанных понятий и, соответственно, разграничены объекты кибербезопасности/киберзащиты.

Сообщается, что «киберзащитой» являются меры, направленные на безопасность систем и информационных ресурсов.

***

9.05.2018

В системах управления «умным» домом Logitech Harmony обнаружены опасные уязвимости

Специалисты команды FireEye Mandiant Red Team обнаружили ряд уязвимостей в системах управления «умным» домом Logitech Harmony, позволяющие атакующему с локальным доступом получить полный контроль над устройствами, подключенными к хабу, а также скомпрометировать другие устройства в сети (InternetUA).

По мнению исследователей, проблемы представляют серьезную угрозу, поскольку многие владельцы «умных» домов используют систему для управления смарт-замками и термостатами. В общей сложности эксперты выявили четыре уязвимости, позволяющие получить доступ с правами суперпользователя к устройству через SSH-

подключение.

Проблемы затрагивают линейку продуктов Logitech Harmony, в том числе Harmony Elite, Home Hub, Ultimate Hub, Home Control, Pro, Smart Control, Companion, Smart Keyboard, Ultimate, Ultimate Home и harmony Hub.

Одна из уязвимостей связана с наличием информации об отладке в образе прошивки, вторая проблема присутствует в связи с некорректной проверкой SSL-сертификатов при обновлении прошивки. Сам механизм обновления также оказался небезопасным, позволяя атакующему внедрить вредоносную прошивку на устройство.

Поскольку в устройстве не установлен корневой пароль, злоумышленник может получить доступ с правами суперпользователя по протоколу SSH, если ему удастся включить Dropbear SSH-сервер, к примеру, загрузив специально сформированную прошивку.

Исследовали проинформировали производителя о проблемах в конце января нынешнего года. В середине апреля компания выпустила обновление прошивки 4.15.96. Всем пользователям рекомендуется установить обновление как можно скорее.

ДОДАТКИ

Додаток 1

2.05.2018
Михаил Сапитон
Почему Instagram – главная надежда Facebook

Издание Bloomberg Businessweek изучило историю развития Instagram – сервис, купленный Facebook, превратился в одну из крупнейших мировых соцсетей. Однако несмотря на тесные связи с проектом Марка Цукерберга, компании удается сохранять собственную идентичность и даже избегать репутационных скандалов. Если ситуация не изменится, в будущем Instagram может превзойти по значимости сам Facebook. Редакция AIN.UA приводит адаптированный перевод материала (AIN.UA).

С 2012 года, когда Facebook Inc. приобрела компанию со штатом в 13 человек за $715 млн, ее принципы ведения бизнеса стали центральными для Instagram. В первые годы, проведенные в качестве собственности Facebook, фотосоцсеть работала в том же здании, где трудится и Марк Цукерберг. Сейчас 700 сотрудников Instagram находятся в отдельном офисе, примечательная сторона которого – почти полное отсутствие брендинга своей материнской компании, даже несмотря на то, что до штаб-квартиры Facebook всего пять минут езды. У Instagram также своя миссия – «Укреплять отношения через

совместный опыт», собственный фирменный стиль, и корпоративная культура, построенная вокруг креативности и дизайна, в противовес инженерным способностям и данным, которые почитают в Facebook. Но зато соцсеть Марка Цукерберга привнесла сюда главную идею: одержимость ростом.

В Азии и Латинской Америке количество регистраций в Instagram растет небывалыми темпами. В течение этого года аудитория соцсети должна превысить 1 млрд пользователей. Сооснователь компании Майк Кригер до сих пор с трудом верит в подобное: «Так мало соцсетей доходят до подобного масштаба. Это значит, что у тебя невероятное влияние на мир».

Когда Кригер вместе со вторым сооснователем Кевином Систромом подписали контракт на $715 млн, главным обещанием сделки был неформальный договор – куда бы Facebook не пошел, Instagram за ним последует. Таким образом, Instagram «одолжил» у старшей соцсети рекламную модель заработка. Сейчас доля Instagram в общей структуре доходов Facebook составляет 18%. Но копировать остальные элементы со временем стало не так разумно.

К примеру, у Facebook сейчас более 2 млрд пользователей, однако компания все еще не может по-настоящему осознать свое влияние. Алгоритмы ее новостной ленты, созданные чтобы вознаграждать эмоциональный контент, стали идеальным инструментов для российских пропагандистов во время президентских выборов 2016 года в США. Привычка Facebook быстро запускать продукты тоже не способствует детальному изучению возможных ошибок. Последний пример подобного: ситуация вокруг маркетинговой компании Cambridge Analytica, которая неправомерно получила доступ к данным 87 млн пользователей и могла применить их для политической агитации. Из-за продолжительного скандала акции Facebook в марте продемонстрировали падение на 15 %.

Instagram долго полагался на успех Facebook, но теперь пришло время, когда долговечность Facebook зависит от Instagram. Колумнист The New York Times описал эту ситуацию одним вопросом: «Что, если более здоровый Facebook – это Instagram?». У этого предположения есть доказательства. Аудитория Instagram моложе пользователей Facebook – с маркетинговой точки зрения это большое преимущество.

В отличие от Facebook, который недавно отчитался о первом в истории уменьшении количества пользователей из Северной Америке, Instagram все еще растет на домашнем рынке. Джейсон Кинт, CEO компании Digital Content Next объясняет: «Без Instagram ситуация, в которой находится Facebook, будет выглядеть совершенно иначе». Он подчеркивает, что соцсеть Цукерберга может прекратить и международный рост, что делает фото-сервис невероятно важным с точки зрения перспектив.

Очевидно, аналогичными мыслями занята и голова Марка Цукерберга – он регулярно отмечает успехи Instagram на традиционных еженедельных совещаниях. Когда топ-менеджеров Facebook спрашивают об оттоке молодой аудитории, они тоже обращаются к одному аргументу: молодежь любит Instagram, что неплохо для общего бизнеса. Особенно учитывая, что данные для таргетинга, собранные в Instagram, можно использовать и на Facebook.

Многие пользователи об этом просто не догадываются – Instagram выглядит как безопасная гавань для побега из Facebook. Поэтому компания очень осторожно выстраивает свою репутацию. Майк Кригер, занимающий должность CTO, подчеркивает, что они не хотят повторять ошибок материнской корпорации: «Мы не намерены заучивать на себе те же уроки».

Работа Кригера, которая заключается в устранении технологических барьеров для пользователей, с международным ростом соцсети стала особенно важна. У сооснователя подходящий для этого бекграунд: Майк родился в Сан-Паулу, но семья много переезжала вслед за отцом – они жили в Португалии, Аргентине и США. Вместе с Систромом они познакомились уже в Стенфорде, где в 2010 стали работать над прототипом соцсети для Burbn, для чекинов в барах и ресторанах. Тогда это был горячий тренд, но Кригер убедил добавить к нему еще и шеринг фотографий.

Первый прототип собрали за 8 недель – это меньше, чем потребовалось Кригеру для получения американской рабочей визы. Кригер говорит, что видел потенциал сервиса с первых дней, поэтому защищал простоту интерфейса. Дизайн Instagram построен с минимальным использованием текста во избежание лингвистических барьеров.

В интервью Bloomberg Businessweek Кригер настаивает – идея Instagram в том, чтобы по-настоящему узнать других людей, даже если вы никогда с ними не встречались. Он приводит собственный пример: Кригер давно следит за аккаунтом какого-то незнакомца из Японии, потому у того интересная собака. Профиль самого сооснователь Instagram тоже пестрит снимками его пса Джуно. Когда Instagram запустил функцию постинга видео в 2013 году, Майк увидел у собаковода из Японии видео его дочери – и почувствовал такую тесную связь с этим человеком, что буквально расплакался.

Еще одно ключевое решение в истории Instagram – отсутствие привычной кнопки шеринга, с помощью которой пользователи могли бы делиться чужими постами. Со временем создатели соцсети поняли, что ее введение бы лишь спровоцировало чувство отчужденности. Кроме того, это спасло Instagram от проклятия виральности: соцсеть не заполонили кричащие новости или мемы. Приложение стало местом, где люди скорее делились переживаниями и собственноручно

созданным контентом, а не писали «на злобу дня». Даже ссылки, основа основ других соцсетей, в Instagram почти нигде нельзя прикрепить.

Цукерберг говорил своим инженерам – делайте то, чего хотят пользователи. Слоганом компании было «Двигайтесь быстро и меняйте положение вещей». В Instagram другая установка – «Не разрушь». Она проявилась еще на одной из первых встреч, предшествующей покупке Instagram. Марк Цукерберг хотел детально изучить статистику использования сервиса, чтобы убедиться в его активном росте (на тот момент у Instagram было около 30 млн активных пользователей). Оказалось, что к моменту продажи соцсеть почти не использовала аналитику – Систром лишь вспоминает, что у них была одна панель с общим количеством регистраций, по которой они и отслеживали рост. После заключения сделки в 2012 к сотрудникам Instagram приставили членов команды Facebook по росту. Теперь в офисе соцсети висят интерактивные табло с множествами графиков, которые измеряют активность на платформе – Instagram усвоил уроки старшего брата.

Постороннему наблюдателю может показаться, что приложение Instagram осталось почти без изменений. Но это обманчивое впечатление – за кулисами развернулась настоящая драма. В 2015 году Snapchat, еще одна молодая соцсеть, начала уводить у Instagram ее ключевую аудиторию, американских подростков. Ключевой фичей Snapchat были Stories, исчезающие через 24 часа записи. Также пользователи могли использовать маски и яркие подписи, что было противоположностью утонченного образа Instagram.

Согласно информации осведомленного источника, Кригер и Систром отказывались развивать аналогичные возможности внутри своего приложения до того момента, когда их об этом не попросил сам Марк Цукерберг. Глава Facebook беспокоился, что если фотосервис вовремя не изменит свой продукт, то рискует потерять целое поколение пользователей. К весне 2016-го Stories в Instagram все таки запустились – и уже за год стали популярнее, чем в Snapchat.

Это было лишь одним из масштабных изменений. С тех пор фотографии больше не должны быть квадратными, посты стали появляться в алгоритмической последовательности и даже логотип Instagram, напоминающий камеру, претерпел серьезного пересмотра. Результат оказался положительным – соцсеть демонстрирует феноменальный рост.

При этом Instagram необходимо постоянно встречать новые, международные вызовы. К примеру, в Индии инженеры столкнулись с проблемой – рядовые пользователи смотрели за фотографиями знаменитостей, но не публиковали собственные снимки. Многие считали свою жизнь слишком скучной. Чтобы решить проблему,

сотрудники Instagram обратились к коллегам из Facebook и сделали ставку на формат Stories – менеджеры по связям попросили местных лидеров мнений больше пользоваться исчезающими роликами. Другая странность приключилась в Индонезии. Инженеры заметили странное обращение трафика: множество фотографий появлялись и затем исчезали. В США это верный признак спама, но в Индонезии разгадка оказалась сложнее – очень многие использовали площадку как маркетплейс и добавляли/удаляли фотографии товаров.

На американском рынке Instagram помогает его независимый образ – согласно прошлогоднему опросу, большинство американцев не знают о связи соцсети с Facebook. Проявилось это и во время скандала с Cambridge Analytica. Илон Маск, который стал одним из главных последователей флешмоба #DeleteFacebook, не тронул страницы своих компаний в Instagram. По его словам, с фотосервисом «все нормально» пока он остается достаточно независимым.

Bloomberg отмечает, что уникальная позиция Facebook (компания владеет первой и третьей самой популярной соцсетью в мире) – это большое преимущество, пусть и совмещенное с угрозой антимонопольных разбирательств в будущем. За время владения Instagram этот проект сменил экспериментальный статус на серьезное место в общей корпоративной структуре и, не исключено, может даже когда-то превзойти по размерам сам Facebook. Правда, у таких перспектив есть и критики. Один из самых активных – Роджер МакНамии, ранний инвестор Facebook, который активно оспаривает нынешние методы работы компании. По его мнению, история с эмоциональной неподготовленностью пользователей к фейковым новостям в случае с Instagram повторится, но уже в отношении нездорового представления реальности и боди-шейминга.

Темная сторона соцмедиа не проявляется по случайности. Это побочный эффект последовательных дизайнерских решений, созданных ради максимального увеличения прибыли от рекламной бизнес-модели.

Даже основатели сервиса успели столкнуться с моральной дилеммой. На момент покупки в 2012 году возникла проблема – оригинальные условия пользования Instagram были в буквальном смысле скопированы из сети. Юристы Facebook настояли на написании новой оферты. В одной из формулировок закралось предположение о том, что Instagram может продавать ваши снимки. На него быстро накинулись критики, желающие показать, как Facebook все портит. Систром и Кригер наблюдали за тем, как росло количество удаленных аккаунтов – им пришлось убрать из документов спорную формулировку, написать извинительный блог-пост и несколько твитов. Лишь затем все пришло в норму.

Условия пользования все еще не до конца ясны, но в ходе

последнего аудита Facebook окончательно уяснил хотя бы одно положение. Перед слушаниями в Конгрессе сотрудники Facebook проводили проверку всех дочерних компаний – нужно было убедиться, что использование пользовательских данных идет на пользу юзерам. В одном из подзаголовком содержалось и указание Instagram. С точки зрения данных, говорилось в заметке, Instagram и Facebook идентичны.

(вгору)

Додаток 2

4.05.2018

В сервисе Instagram появилась суровая цензура и своя платежная система

С каждым днем сервис Instagram для любителей фотографий становится все более популярным, а чтобы его аудитория росла и дальше, разработчики постоянно внедряют новые функции. Четвертого мая стало известно сразу о двух значимых новшествах. В частности, теперь в рамках данного сервиса можно использовать встроенную платную систему для оплаты различных покупок. Кроме того, в «Инстаграме» повилась суровая цензура, работающая автоматически за счет ИИ (InternetUA).

Пока что пользоваться платежной системой в рамках Instagram могут лишь жители США, однако вскоре это ограничение будет снято. Функция работает по простому принципу. Сначала пользователь должен привязать к сервису свою банковскую карту, после чего появляется возможность в бизнес-аккаунтах пользователей просматривать доступные услуги и оплачивать их прямо в пределах сервиса. В настоящий момент новшество работает лишь с некоторыми партнерами, однако в 2018 году все желающие смогут использовать новые функциональные возможности.

В добавок к этому новшеству, администрация Instagram ввела еще одно. Начиная с 4 мая заработала суровая цензура, которая должна помочь пользователям бороться с недоброжелателями. Специальный искусственный интеллект, поддерживающий машинное обучение, автоматически удаляет все оскорбительные и запугивающие комментарии. За счет специальных алгоритмов он способен выявлять даже такие оскорбления, которые специально написаны неправильно или замаскированы.

По словам представителей Instagram, с каждым днем данная функция будет работать все лучше, потому как удаляя каждый комментарий она понемногу обучается, а еще ей в этом помогают сами разработчики. Новая функциональная возможность уже работает по всему миру, а представляет она из себя значительно улучшенный и доработанный «умный» алгоритм защиты, запущенный еще в 2017 году.

Новшество работает автоматически для всех и отключить его вручную нельзя. Единственное, что может сделать автор, так это включить показ оскорбительных комментариев и таковых с угрозами, но в таком случае они все равно будут видны только ему.

(вгору)

Додаток 3

8.05.2018

Шоу продолжается: как Facebook искупит вину перед пользователями

Бизнес-функции для WhatsApp, дополненная реальность для бизнес-партнеров в Messenger, знакомства в Facebook и другие функции, которые изменят продукты компании Марка Цукерберга (InternetUA).

Первым публичным мероприятием Facebook после скандала с Cambridge Analytica стала F8 – крупнейшая конференция компании для разработчиков. Как соцсеть планирует вернуть доверие и интерес пользователей, разработчиков и инвесторов?

Неудивительно, что заострять внимание на инциденте с утечкой пользовательских данных глава Facebook Марк Цукерберг не стал. И в целом изучал уверенность и позитив – выражение «Show must go on» («Шоу должно продолжаться») как нельзя лучше подходит к описанию того, что происходило на F8.

Совсем без внимания ситуация, конечно, не осталась. На открытии F8 Цукерберг пошутил по поводу своего выступления перед Конгрессом США в апреле, а также сообщил более чем 100 000 разработчикам, которые создают контент и приложения для платформы, что Facebook возобновила процесс рассмотрения новых приложений. Напомним, что компания приостановила рассмотрение приложений 26 марта, в самый разгар скандала, чтобы перепроверить уже работающие на ее платформе сервисы.

Последняя новость должна была как минимум порадовать тех разработчиков, чьи приложения выстроились в очередь к редакторам. Однако этот анонс далеко не единственный и даже не самый крупный, который компания озвучила на F8.

Приватность и конкуренция с Tinder

Не секрет, что Facebook давно позиционирует себя не только как «социальная сеть». Запустив Stories («Истории», пост о событиях дня, который исчезает через 24 часа) на основной платформе и в Instagram, Facebook бросила вызов Snapchat, Instant Articles (быстрый доступ к статьям) составляют конкуренцию собственным сайтам СМИ и проекту Google AMP, а Marketplace – ответ различным торговым площадкам для товаров, продаваемых пользователями напрямую.

В этом году на F8 компания анонсировала поход против Tinder и других дейтинговых сервисов. По словам Цукерберга, будущая функция позволит находить потенциальных партнеров в группах или в мероприятиях и отправлять им сообщения, используя только личные имена. Точный срок запуска функции пока не известен, однако на фоне сообщения акции компании Match Group (разрабатывает Tinder и OkCupid) упали 1 мая на 20 % и с тех пор так и не выросли до прежнего уровня.

Среди других обновлений в самой соцсети – Watch Party, функция для совместного просмотра и комментирования видео, покупки внутри Instant Games, новая вкладка «Группы». Чтобы показать, что компания готова дать пользователям больше контроля над своими данными, Facebook анонсировала Clear History – инструмент для очистки истории просмотров на платформе. Эта функция позволит видеть, какие данные сайты и приложения передают Facebook, удалить эту информацию из своего аккаунта и запретить Facebook хранить эти данные в будущем.

WhatsApp без Кума

В то же время вопрос с обработкой персональных данных остался открытым. Тем более что за день до открытия F8 основатель мессенджера WhatsApp Ян Кум, который в 2014 году продал сервис Facebook за $19 млрд, объявил о планах покинуть компанию. По данным Washington Post, причиной тому стали противоречия с руководством Facebook относительно попыток использовать информацию платформы WhatsApp для основного сервиса, что может ослабить их защиту.

На F8 Кум удостоился краткой ремарки с признанием его достижений и вклада в развитие платформы. В Facebook рассказали, что, к примеру, в целом пользователи WhatsApp отправляют по 65 млрд сообщений в день. Сервис получит несколько новых функций, включая групповые видеозвонки и стикеры. В компании также заявили, что готовят функции для бизнеса – то, от чего WhatsApp до сих пор оставался в стороне. Однако обновления оказались в тени другого сервиса – Facebook Messenger.

Messenger с AR

За последнее время приложение Messenger далеко ушло от своего прямого назначения и оказалось переполнено различными надстройками. Удивительно, но в Facebook тоже с этим согласились – мессенджер получит новый, упрощенный дизайн.

Одна из новых функций – M suggestions. С ее помощью пользователи сервиса Marketplace, получая сообщение в Messenger на языке, который отличается от их основного, увидят предложение перевести это сообщение. Таким образом Facebook хочет упростить процесс покупки-продажи между пользователями.

Главный сюрприз Facebook сделал брендам – они получат возможность интегрировать эффекты дополненной реальности (AR) в коммуникацию с пользователями: потенциальные покупатели смогут кастомизировать продукты, виртуально «примерить» их и так далее. Функция пока находится на стадии закрытого бета-тестирования с рядом брендов-партнеров, включая Kia, Nike и Sephora.

Фильтры для Instagram

Учитывая, что функцией Stories на Instagram пользуются 450 млн пользователей ежедневно или более половины активных пользователей, становится понятен фокус Facebook на развитие именно этой функции. На F8 компания объявила, что в скором времени пользователи смогут опробовать новые AR-фильтры от брендов и известных личностей. Одновременно Facebook запустил новую версию AR Studio – инструмента для создания контента с дополненной реальностью на своей платформе.

Среди других обновлений Instagram – интеграция с GoPro (экстрим-камеры) и Spotify (музыкальный сервис), функция индивидуального и группового видеочата в личных сообщениях и обновленный раздел Explore, в котором предложенный контент будет организован по темам.

Oculus Go

Там, где у Facebook появляется аббревиатура AR, редко обходится без упоминания другого популярного сочетания – VR (виртуальная реальность). Главным действующим лицом на этом направлении стал мобильный VR-шлем Oculus Go. Первое беспроводное устройство Oculus уже можно приобрести в 23 странах мира за $199 – и здесь не обошлось без конфуза, так как Amazon случайно открыл предзаказ на Oculus Go за несколько часов до официального анонса.

По словам представителей Facebook, Oculus Go на запуске поддерживает более тысячи приложений и игр, а также просмотр концертов и других шоу в режиме реального времени. Учитывая, что VR -технологии пока не получили широкого распространения практически нигде, кроме игр, у Facebook есть шанс сделать бизнес на этом направлении.

По итогам конференции F8 создалось впечатление, что Facebook достаточно зрелый, чтобы пережить непростой во всех отношениях апрель, вынести из него уроки и идти дальше. Теперь дело за реализацией обещаний. Тем более что кредит доверия инвесторы Facebook дали – с первого дня конференции акции компании подросли на 2,6 %.

(вгору)

Додаток 4

25.04.2018

Услуги ПУМБ теперь можно заказать через Viber

Первый Украинский Международный Банк (ПУМБ) с апреля запустил для своих розничных клиентов канал коммуникации в мессенджере Viber (ITnews).

Онлайн-банкинг ПУМБ в Viber предоставляет клиентам в формате 24/7 актуальную информацию о движении средств, сумме минимального платежа по карте и сумме до полного погашения, размере последнего зачисленного и следующего платежа по кредиту. Также через Viber можно оформить кредитную, дебетную карты и подать заявку на оформление кредита.

«Предоставление продуктов и услуг через Viber – это первый шаг ПУМБ по внедрению social commerce. Банк активно развивает новые функционалы в социальных сетях и мессенджерах, тем самым предоставляя клиентам традиционно качественный сервис в удобном формате. Ежемесячно в колл-центр ПУМБ поступает порядка 44 тысяч звонков – с целью уточнения суммы досрочного погашения кредита, обязательного платежа и последнего поступления. Теперь все эти клиенты смогут в любое удобное время оперативно получить необходимую информацию, приложив для этого минимум усилий. В планах банка масштабировать услуги и на другие мессенджеры», – прокомментировал Себастиан Рубай, заместитель председателя правления ПУМБ.

Перечень услуг ПУМБ в Viber представлен удобным и простым в навигации меню на трех языках – украинском, русском и английском. Меню содержит шесть основных разделов:

– карточные продукты
– кредитные продукты
– информация о движении средств
– курсы валют
– пополнить мобильный
– изменить язык.

Использование онлайн-банкинга ПУМБ в Viber позволит качественно снизить нагрузку на колл-центр. Ежемесячно центр обслуживания клиентов ПУМБ получает около 7 тысяч звонков по вопросу уточнения суммы последнего поступившего платежа по кредиту, около 20 тысяч звонков касательно уточнения суммы досрочного погашения кредита, около 2 тысячи звонков с целью узнать сумму обязательного платежа по кредиту. Теперь эту информацию клиенты смогут получить в течении нескольких минут, выбрав соответствующий раздел в меню.

Чтобы начать работу в онлайн-банкинге ПУМБ в Viber, необходимо сначала зайти в паблик-аккаунт ПУМБ (находится в открытом доступе во вкладке «Публичные аккаунты»), и перейти в чат. После этого

пользователю будет предложено меню, в котором в несколько кликов можно выбрать вышеописанные продукты и услуги. Подключение к Онлайн-банкингу ПУМБ в Viber абсолютно бесплатно и позволит клиентам банка получать услуги 24/7 в любой точке мира.

(вгору)

Додаток 5

26.04.2018

Популярный финансовый эксперт судится с Facebook за незаконное использование его лица в криптовалютной рекламе

Мартин Льюис, известный журналист и эксперт в финансовой сфере, подает в суд на Facebook за диффамацию и незаконное использование его лица в рекламе свыше пяти десятков мошеннических проектов, связанных с криптовалютами. Льюис также известен как «Эксперт по экономии денег в Великобритании» (InternetUA).

«В течение прошлого года сайт социальной сети опубликовал более 50 поддельных рекламных роликов, в которых использовалось мое изображение и которые регулярно просматриваются, вероятно, миллионами людей в Великобритании», – сказал Льюис. «Наиболее распространенными являются схемы быстрого обогащения, в настоящее время известные как «биткойн-код» или «облачный трейдер», которые на самом деле являются фронтами бинарных торговых фирм, расположенных за пределами ЕС».

Торговля бинарными опционами – очень рискованный процесс (особенно для начинающих инвесторов). Британская служба отзывов клиентов «What?» объясняет: «Когда вы торгуете бинарными опционами , вы делаете ставку на то, будет ли цена акции, фондового рынка или других активов выше или ниже установленной цены в будущем. Если ваша ставка верна, вы можете получить крупную прибыль; если вы проиграете, вы потеряете все».

Судебное разбирательство с Мартином Льюисом может стать большим ударом для Facebook.

В иске Льюис утверждает, что никогда не принимал участие в рекламных кампаниях на Facebook. Именно поэтому любой проект с использованием его имени, фотографии или видео с ним для продвижения криптовалютных проектов в социальных сетях и на сторонних ресурсах следует считать мошенническими.

«Я борюсь больше года, чтобы заставить Facebook запретить мошенникам использовать мое имя и фото для обмана людей. Я просил Facebook проверять законность любого объявления с моим участием, достаточно было просто обратиться ко мне за подтверждением подлинности. Мне очень больно каждый раз, когда

вижу, что в сети мошенников попала очередная жертва из-за доверия, которое люди испытывают ко мне», – отмечает истец.

«Я не понимаю почему это оказалось так сложно! В конце концов, Facebook – лидер в распознавании лиц и текста. Тем не менее, сеть просто продолжает многократно публиковать эти рекламные объявления, а затем полагается на то, что я лично сообщу о скаме, как только урон будет нанесен».

Facebook не признавал свою вину на протяжении всего разбирательства, заявив, что «На Facebook мы не разрешаем ложные объявления, которые вводят в заблуждение и мы объяснили Мартину Льюису, что он должен сообщать о любых рекламных объявлениях, которые нарушают его права, и они будут удалены».

Гигант социальных сетей сумел убедить законодателей и сотрудников правоохранительных органов, что он не несет ответственности за то, что другие люди предпочитают публиковать. Если Льюис в итоге выиграет это дело, это это может повлечь за собой череду разбирательств против Facebook.

В прошлом социальная сеть взяла на себя ответственность за защиту своих пользователей от вредоносных рекламных объявлений. По состоянию на 30 января 2018 года Facebook решил удалить все рекламные объявления, связанные с криптовалютой.

При этом, несмотря на все усилия Льюиса, Facebook, по его утверждению, продолжает допускать появление новых рекламных объявлений с использованием его имени и лица. И это даже после того, как Льюис удалил все фотографии со своей страницы.

Вопросы вызывает тот факт, почему после введенных запретов на Facebook по-прежнему появляется реклама криптовалютных проектов. Судя по всему, мошенники легко обходят фильтры социальной сети и продолжают обманывать людей.

(вгору)

Додаток 6

28.04.2018

П’ять фобій, викликаних гаджетами і соцмережами

Боязнь висоти, привидів та дзеркал – вчорашній день. Сьогодні люди божеволіють через інтернет-троллінг, соціальні мережі, відсутність чи надмірну присутність гаджетів у їхньому житті. Проникнемо у світ фобій сучасної людини.

Синдром фантомних вібрацій

У 2015 році термін «синдром фантомних вібрацій» було названо «словом року» за версією словника Маккуорі. Цей факт відзначає поширеність цього явища у всьому світі. Відчувати вібрацію телефону, коли ніхто не дзвонить, і тягнутися до нього – це нормально:

нейробіологи пов'язують явище з соматосенсорною корою мозку, яка сприймає за вібрацію навіть тертя одягу по шкірі. Але якщо ви чуєте дзвінок або сигнал вхідного повідомлення, коли насправді їх немає, слід задуматися. Швидше за все ви перевтомилися або нервуєте в очікуванні важливого дзвінка. Щоб вийти з цього стану, спробуйте відволіктися за допомогою прогулянки чи перегляду фільму і не думати про телефон принаймні кілька годин.

Соціонетофобія

Боязнь соціальних мереж вважається сучасною версією страху переслідування і проявляється в боязні завести аккаунт в соцмережі, оскільки його можуть використовувати для стеження або маніпулювання. Страх не обов'язково пов'язаний зі спецслужбами, часто люди бояться того, що з особисті дані стануть відомим їх оточенню – сім'ї, начальству, клієнтам. Схожою симптоматикою відзначається «синдром шоу Трумана», при якому людині здається, що її телефон прослуховують, а камера і мікрофон працюють на спецслужби. Яскравими проявами синдрому стали випадки, коли пацієнти просили політичного притулку в керівництва сусідніх країн, вважаючи що все їх життя – частина реаліті-шоу.

Тролефобія

Будь-який інтернет-користувач знає, хто такі тролі. Годувати їх не можна, банити марно, краще просто ігнорувати. Але активне зростання популяції тролів в інтернеті призвело виникнення до відповідної реакції – тролефобіі або тролепараної. Пацієнт переконаний – усі коментатори, учасники його блогу або порталу – тролі, які переслідують тільки одну мету – розвалити його проект. Звідси прагнення до анонімності, бажання зайвий раз не привертати до себе увагу. На жаль, від тролефобіі немає медичних препаратів і лікарських технік. Вчені-психологи радять те ж саме, що і народні інтернет-премудрості – не ведіться на провокації, не годуйте тролів.

Кіберофобія

Молодих людей комп’ютером не злякати. Незрозумілим чином за лічені хвилини ноутбук чи планшет освоює навіть і дворічний малюк. А от у літніх людей, яким доводиться освоювати нову техніку, все дещо складніше. Лікарі виокремлюють такі симптоми кіберофобії – надмірна обережність при роботі з ПК, тривога і паніка під час контакту з гаджетом, уникання пристроїв і високоемоційні негативні відгуки про них. Іноді фобія може супроводжуватися фізичними реакціями – нудотою і запамороченням. Вихід є: використовувати ПК у присутності більш досвідченого користувача і поступово збільшувати час користування від 15 хвилин до 1-2 годин.

Імоджіфобія

Ще один дин приклад нових людських страхів, що з'явилися в результаті поширення чатів і соціальних мереж – імоджіфобія.

Відправляючи в повідомленні звичний усім смайлик або стікер, людина боїться, що її неправильно зрозуміють і прикріплений символ виявиться «не в тему». Імоджіфобію складно назвати серйозним психічним захворюванням, це всього лише чергова форма тимчасового неврозу. У певній мірі, кожен користувач соцмереж трохи імоджіфоб. В онлайн спілкуванні, де часто доводиться вести одночасно особисте і офіційне листування, переключитися з дружнього на представницький стиль встигають не всі.

Тредофобія

Назва походить від англійського слова «thread» – коментар в соціальній мережі. Тредофобія проявляється боязню коментувати записи в соцмережах, висловлювати свою думку. Зазвичай тредофоб сором'язливий і в реальному житті, але в інтернеті ця риса додатково загострюється. А що як раптом коментар виявиться неграмотним чи необдуманим? Посиплеться критика і образи! Якщо ця проблема дійсно турбує, подолати бар'єр допоможе анонімний аккаунт.

Селфіфобія

Хто би міг подумати, що страх перед поганим селфі стане психологічною проблемою, що вимагає медичного втручання. Цікаво, що культ Instagram привів до того, що багато дівчат роблять пластичні операції тільки заради того, щоб робити «якісні селфі» (Живи активно).

(вгору)

Додаток 7

8.05.2018

Як смартфони та соцмережі крадуть дитинство

Відтоді, як Сократ поскаржився на те, що написане слово руйнує спогади, люди замислювалися над потенційною шкодою технології (ZIK).

Зараз дослідники стверджують, що соціальні медіа можуть провокувати депресію у підлітків, а багато батьків переймаються тим, що смартфони поглинають усю увагу їхніх дітей.

1. Чи технологія руйнує дитинство?

Без сумніву. Врахуйте те, що сьогоднішні підлітки, які володіють смартфоном, діляться у соцмережах усіма своїми переживаннями та роздумами. Вони відкриваються перед аудиторією сотень, якщо не тисячі «друзів», коментують у режимі реального часу те, що вони роблять, а – через Snapchat та Instagram тим, як виглядають. Snapstreak, функція Snapchat, яка вітає користувачів за послідовне надсилання повідомлень своїм друзям, була піддана критиці дитячим комісаром Англії за те, що викликає залежність. Опитування, проведене Центром безпечного Інтернету Великобританії, 1500 дітей, віком від 8 до 17 років, показало, що кожна восьма дитина поділилася своїм селфі впродовж

останньої години.

2. Про що свідчать дослідження?

Дані різних досліджень свідчать про наступне: середній вік отримання першого смартфона – 10 років, а половина усіх дітей у США та Великобританії уже у віці 12 років мають облікові записи у соціальних мережах. Близько чверті підлітків стверджують, що «майже постійно» перебувають онлайн. Дослідження, проведене у 2015 року, виявило, що приблизно одна з десяти дівчат у Великобританії використовує соцмережі більше трьох годин під час навчання. Опитування дітей, віком від 8 до 17 років, проведене Центром безпечного Інтернету, виявило, що 22 % з них зіткнулися з тим, що хтось розмістив зображення чи відео, що ображає їх. У дослідженні, проведеному психологом Державного університету штату Сан-Дієго, США, було виявлено, що американські підлітки, які проводять більше часу в Інтернеті, є менш щасливими за тих, хто займається чимось іншим.

3. Чи існує протилежний погляд?

Дослідники з Оксфордського інституту Інтернету та Університету Кардіффа проаналізували дані 120 000 підлітків у віці 15 років та дійшли висновку, що у певній мірі благополуччя підлітків фактично зросло зі збільшенням їхнього доступу до Інтернету. У той час як тривале використання телефонів може мати негативний ефект, дослідження показало, що слід враховувати й інші важливі чинники, такі як споживання сніданку чи висипання.

4. Чи це не є частиною сучасного дитинства?

Поняття дитинства змінилося задовго до того, як з'явилися соціальні медіа. Американське дослідження, проведене у 2013 році, встановило, що, чим більше батьків відчували те, що вони живуть у небезпечному районі, тим більше дітей дивилися телевізор та мали надмірну вагу. Адже саме вони частіше залишали дитину вдома та спонукали до того, що вона проводила більше часу за смартфоном або планшетом.

5. Чи соцмережі мають вікові обмеження?

Мають, проте дуже важко простежити за їх дотриманням. На Facebook, Instagram, Snapchat та Twitter вам, як правило, має бути щонайменше 13 років, щоб ви могли створити обліковий запис. (Деякі країни мають більш суворі правила: наприклад, мінімальний вік для створення облікового запису у Google становить 14 років у Південній Кореї та 16 років у Нідерландах). Більшість сайтів пропонує новим користувачам зазначити дату свого народження, що робить їхні вікові обмеження досить простими для обходження.

6. Хто за цим стежить?

Звичайно, багато батьків просто хочуть викинути телефон у смітник та відпустити дітей бавитися надвір. Проте існують групи, що

виступають за більш конкретні дії. Група педіатрів та експертів з питань психічного здоров'я лобіює те, щоб Facebook припинив використання програми Messenger Kids – версію свого додатку Messenger для дітей у віці від 6 до 12 років, аргументуючи це тим, що маленькі діти «недостатньо дорослі для того, щоб підтримувати онлайн-відносини». Інша група колишніх співробітників Google, Facebook та подібних компаній, створила Центр гуманітарних технологій для інформування про загрози, що виникають внаслідок звикання до соцмереж. Співзасновник iPod закликав Apple Inc. створити відстеження онлайн-активності дітей.

7. Чи дослуховуються соцмережеві гіганти?

Принаймні, роблять вигляд, що так. У січні 2018 року, два великих акціонери компанії Apple закликали компанію надати батькам можливість налаштувати iPhone дитини для того, щоб обмежити час її перебування в Інтернеті та доступ до соціальних мереж. Компанія Apple заявила, що займається розробкою більш широких функцій для батьків.

8. Чи втрутяться уряди?

Цілком можливо. Під час квітневого виступу генерального директора Facebook Марка Цукерберга у Конгресі США, у сенатора штату Массачусетс, Еда Маркі, виникли певні зауваження щодо використання мережі дітьми. Законодавець закликав Цукерберга підтримати законопроект, який він подав у 2015 році, щоб розширити конфіденційність в Інтернеті для дітей у віці до 16 років. Маркі також порівняв технологічні гіганти з тютюновою промисловістю. У Великобританії міністр охорони здоров'я Джеремі Хант погрожує ввести контроль над Google, Twitter, Snapchat та іншими подібними компаніями.

(вгору)

Додаток 8

1.05.2018

Удар по Google и Facebook. Как ЕС защитит своих граждан от киберслежки

С мая в Евросоюзе вступают в силу новые правила обработки персональных данных. Они касаются всех стран Европейского союза. Также их должны придерживаться все предприятия, которые оказывают услуги в ЕС (InternetUA).

Конечно, речь идет прежде всего о крупных интернет-компаниях, имеющих американское происхождение. Например, Facebook, который недавно допустил утечку данных миллионов пользователей, чем вызвал гнев Евросоюза.

Доставалось от Еврокомиссии и другому гиганту родом из США – Google.

Правила нацелены на то, чтобы лучше защищать личные данные граждан и их права. Они обозначаются аббревиатурой GDPR (The General Data Protection Regulation, Общие правила защиты данных).

Кто должен соблюдать GDPR

Нововведения касаются любых данных, которые собираются, обрабатываются и/или хранятся в Европе. То есть, под их действие попадает любая компания, которая предоставляет услуги или продает товары жителям стран Европы, обрабатывая при этом их данные.

Правилами запрещена передача данных за пределы ЕС в любую страну, которую ЕС не считает соответствующей законам о защите персональных данных.

Если какая-либо компания передает личные данные пользователей за пределы ЕС для обработки или хранения, то предварительно должна получить явное согласие от пользователя.

О каких данных идет речь

Данные пользователей, которые охраняются правилами, можно разделить на две группы. Первая – это личные данные, к которым относится имя, дата рождения, электронная почта, местонахождение, логины и другие идентификаторы. Теперь к таким данным отнесли еще и IP-адрес.

Вторая группа – деликатные данные. К ним относят такие вещи, как религиозная и этническая принадлежность, политические убеждения, сексуальная ориентация, и так далее. В нововведенных правилах уделяется больше, чем ранее, внимания защите деликатной информации.

Новые правила обработки данных

В правилах прописаны шесть основных принципов, которые должны соблюдаться при обработке данных пользователей.

1) Персональные данные должны обрабатываться законно, справедливо и прозрачно. Любую информацию о целях, методах и объёмах обработки персональных данных следует излагать максимально доступно и просто.

2) Ограничение цели. Данные должны собираться и использоваться исключительно в тех целях, которые заявлены компанией (онлайн-сервисом).

3) Минимизация данных. Нельзя собирать личные данные в большем объёме, чем это необходимо для целей обработки.

4) Точность. Личные данные, которые являются неточными, должны быть удалены или исправлены (по требованию пользователя).

5) Ограничение хранения. Личные данные должны храниться в форме, которая позволяет идентифицировать субъекты данных на срок не более, чем это необходимо для целей обработки.

Это очень важный пункт. По сути, он предписывает автоматически удалять данные человека, если тот прекратил

использовать сервис (например, удалил свой аккаунт из социальной сети).

6) Целостность и конфиденциальность. При обработке данных пользователей компании обязаны обеспечить защиту персональных данных от несанкционированной или незаконной обработки, уничтожения и повреждения.

Права граждан ЕС

Также обозначены официальные права, которыми обладают владельцы данных. Это: право быть проинформированным, право доступа, право на исправления, право на объект, право на переносимость данных, право на удаление данных, право не подвергаться автоматическому принятию решений, право ограничить обработку данных.

GDPR значительно расширяет права граждан и резидентов ЕС по контролю за их данными. Они могут запрашивать подтверждение факта обработки их данных, место и цель обработки, категории этих данных данных, каким третьим лицам персональные данные раскрываются, период, в течение которого данные будут обрабатываться, а также уточнять источник получения персональных данных и требовать их исправления или прекращения. Кроме того, владельцы данных вправе требовать полного их удаления.

GDPR повышает требования в отношении формы получения согласия на обработку данных. Это согласие должно быть выражено в форме утверждения или в форме четких активных действий пользователя, то есть никаких по умолчанию проставленных галочек быть не может.

Что касается детей, то согласие на обработку их персональных данных должно быть дано их родителями или официальными представителями. С какого возраста ребенок сам может принимать решение о своих персональных данных, каждая страна регулирует самостоятельно.

Также компании обязаны предоставлять бесплатно электронную копию персональных данных другой компании по требованию самого субъекта этих данных. То есть, если пользователь переходит с одного сервиса на другой, он может потребовать у первого передать все его данные второму, чтобы не вносить их самому.

В любой организации, которая занимается обработкой данных, должен быть сотрудник, ответственный за их защиту.

Компании обязаны уведомлять регулирующие органы (а в некоторых случаях и субъектов данных) о любых нарушениях, связанных с персональными данными, в течение 72 часов после обнаружения.

Правила вступают в силу с 25 мая.

(вгору)

Додаток 9

25.04.2018

Уровень защищенности банковских приложений для Apple iOS выше, чем у аналогов под Google Android

Согласно исследованию Positive Technologies доля мобильных банковских приложений, в которых обнаруживаются критически опасные уязвимости, снижается с каждым годом. Если в 2015 г. уязвимости высокого уровня риска содержались в 90 % проанализированных систем, а годом позже было уже 71 %, то в 2017-м – только 56 %. Но несмотря на заметный рост уровня защищенности, текущие недостатки все еще несут серьезные угрозы для банков и их клиентов, отмечается в ежегодном исследовании Positive Technologies (Компьютерное Обозрение).

В среднем в 2017 г. на каждую систему дистанционного банковского обслуживания приходилось по 7 уязвимостей, что больше показателя 2016 года, когда на каждое финансовое приложение приходилось только 6 недостатков. Однако доли уязвимостей высокого и среднего уровня риска заметно снизились. Например, в трети онлайн-банков отсутствовали критически опасные недостатки, а годом ранее уязвимости высокого уровня риска были во всех финансовых веб-приложениях, кроме одного.

Наиболее распространенными уязвимостями онлайн-банков в 2017 году стали «Межсайтовое выполнение сценариев» (75 % систем) и «Недостаточная защита от атак, направленных на перехват данных» (69 %), которые позволяют совершать атаки на клиентов банков (например, перехватывать значения cookie или похищать учетные данные). Больше половины онлайн-банков (63 %) содержали уязвимость высокого уровня риска «Недостаточная авторизация», которая позволяет злоумышленнику получить несанкционированный доступ к функциям веб-приложения, не предназначенным для данного уровня пользователя. Кроме того, уязвимости в 94% онлайн-банков могли быть использованы злоумышленниками для доступа к сведениям, составляющим банковскую тайну клиентов, и личной информации.

С мобильными банковскими приложениями ситуация похожа: снизились доли уязвимостей высокого (29 % вместо 32 % в 2016 году) и среднего уровня риска (56 % вместо 60 %). Соответственно, увеличилась доля уязвимостей низкого уровня риска; компании стремятся в первую очередь принимать меры для устранения критически опасных уязвимостей. Тем не менее в половине систем (48 %) была выявлена хотя бы одна критически опасная уязвимость. В 52 % мобильных банков уязвимости позволяли расшифровать,

перехватить, подобрать учетные данные для доступа в мобильное приложение или вовсе обойти процесс аутентификации. В результате злоумышленник может получить возможность совершать операции в мобильном банке от лица легитимного пользователя.

При этом iOS-приложения вновь оказались защищены лучше, чем их аналоги для Android. Доля уязвимостей высокого уровня риска в iOS-приложениях составила всего 25 %, в то время как в Android-приложениях она занимает 56 %. Практически для всех рассмотренных мобильных банков (кроме одного) эксперты анализировали по два идентичных приложения, разработанных для разных операционных систем, и в некоторых случаях мобильное приложение для iOS не содержало уязвимостей, которые были обнаружены в Android-приложении.

Большинство исследованных систем (68 %) были разработаны финансовыми организациями самостоятельно. Но если в 2016 году приложения, созданные банками, содержали в два раза меньше уязвимостей, чем системы, развернутые на готовых платформах, то год спустя ситуация изменилась: у приложений, построенных на «коробочных» решениях, стало меньше критически опасных уязвимостей. Вендоры стали больше внимания уделять вопросам безопасности, в то время как банкам по-прежнему не хватает опытных разработчиков в штате и грамотно выстроенного процесса безопасной разработки.

(вгору)

Додаток 10

1.05.2018

Все пользователи WhatsApp оказались в огромной опасности

В мире полно популярных мессенджеров, но самым распространенным из них является WhatsApp. На втором месте идет Viber, а тройку замыкает Telegram. Последним пользуются, как правило, наиболее образованные и продвинутые пользователи, а на первые два делают ставку обычные люди, многие из которых крайне сильно далеки от современных технологий. На это и мешают ставку злоумышленники, из-за действий которых миллионы простых пользователей находятся в большой опасности (InternetUA).

Специалисты антивирусной компании Dr. Web выяснили, что за последний год более чем в 5 раз возросло количество новых модификаций вредоносных приложений, маскирующихся под мессенджер WhatsApp. Самым популярным из них является его Plus-версия. Подобное программное обеспечение, как уверяют эксперты по безопасности, распространяется через сомнительны сайты, а также через систему ротации рекламы, в том числе принадлежащую Google.

Злоумышленники действуют очень хитро, чтобы их программу доверчивые пользователи загружали и устанавливали. Для этого они обещают дополнительные возможности в WhatsApp, которые позволят, например, всегда оставаться в офлайн-режиме во время общения, либо, например, читать переписку из секретных чатов. Функций, с помощью которых пользователя заманивают, очень много, поэтому большинство ведется на подобный обман. Хуже всего то, что с каждым днем такого рода ПО становится все больше, а вместе с ним растет и число жертв.

После того как модифицированная версия WhatsApp попадает на смартфон, она сразу же просит выдать его набор различных разрешений. Их количество зависит о того, как сильно заражено это ПО. В некоторых случаях, самых безобидных, оно лишь показывает рекламу, тогда как в самых плохих – оформляет подписки на платные сервисы, ворует деньги с банковских счетов, снимать денежные средства с банковских карт, а также превращает смартфон в ферму для майнинга, из-за чего он может крайне быстро выйти из строя вследствие перегрева.

Эксперты советуют не вестись на подобные уловки мошенников и скачивать WhatsApp исключительно из магазинов приложений App Store и Google Play. В противном случае, по их словам, велик риск нарваться на вредоносное программное обеспечение, которое нанесет какой-то вред. Со специалистами в этом плане нельзя не согласиться, однако следует учитывать, что существуют проверенные временем сайты и ресурсы, откуда скачивать различные APK-файлы для Android можно без каких-либо опасений, потому как каждый из них проходит проверку.

(вгору)

Додаток 11

2.05.2018

Кібербезпека: чому сайти українських держструктур легко зламати

Попри низку ініціатив із захисту власного кіберпростору, Україна досі пасе задніх у сфері інформаційної безпеки, попереджають експерти (InternetUA).

Злам нового сайту міністерства енергетики та вугільної промисловості України «був випадковим». Так пояснив DW хакерську атаку, що сталась 24 квітня, спікер Українського кіберальянсу – спільноти кіберактивістів з різних міст України, – відомий під псевдонімом Sean Brian Townsend. За його словами, сайт знаходився на одному сервері з іншими комерційними сайтами і особа, ймовірно, з Марокко зламала один із них, «зламавши міненерговугілля за компанію», розповідає хакер, коментуючи цю подію для DW.

Атака й справді виглядала дещо дивно: на головній веб-сторінці міненерговугілля містилося залишене хакерами повідомлення і не було жодного доступу до інших його сторінок. А для розблокування сайту кіберзлочинці вимагали 0,1 біткоіна, що відповідає сумі у приблизно 24 тисяч гривень. Пізніше користувачі ніби почали помічати, що в цей час недоступними була ще ціла низка доменів, через що з'явилися повідомлення про злам інших державних сайтів. Однак пізніше у CERT-UA, команді швидкого реагування при Державній службі спеціального зв'язку та захисту інформації України, спростували ці чутки.

Зважаючи навіть на таку ніби примітивну атаку, Sean Brian Townsend досить скептично відгукується про державні зусилля у сфері захисту кіберпростору. «Якщо арабський школяр, що декілька слів англійською зв'язати не може, ламає сайт міністерства навіть не цілеспрямовано, а просто тому, що він трапився під руку, це свідчить про те, що, схоже, не змінилося нічого», – каже хакер. Тож тема вразливості української інфраструктури для потенційних кіберзагроз знову опинилась на порядку денному.

Масштабний захист?

Як повідомлялось, після низки хакерських атак, яких зазнали компанії та установи в Україні та світі у 2017 році, зокрема вірусів WannaCry у травні та Petya.A у червні, українська влада заявила про посилення зусилля у кіберпросторі. Так, у серпні минулого року ухвалено відповідне рішення Ради національної безпеки і оборони (РНБО), а двома місяцями пізніше Верховна Рада проголосувала за закон про кібербезпеку.

У лютому цього року, під час відкриття Центру реагування на кіберінциденти, голова РНБО Олександр Турчинов пішов ще далі та заявив про можливість створення кібервійськ у складі збройних сил. Тоді Турчинов запевнив – в Україні створено «захисний контур», який гарантуватиме цифрову безпеку всіх держустанов і об'єктів інфраструктури, а новий центр тісно співпрацюватиме із партнерами з країн НАТО.

Пізнє прозріння

«Те, що трапилося, не може не траплятися – від успішних атак ніхто не застрахований», – намагається пояснити слабкість кіберзахисту держустанов Віктор Жора, співзасновник компанії InfoSafe, яка здійснювала захист серверів ЦВК під час кібератак у 2014 році. Втім, і він визнає – наявність слабкого місця свідчить про те, що далеко не всі українські відомства зробили належні висновки після минулорічних

вірусних «епідемій».

Попри це, Жора закликає не применшувати важливість ухвалених українською владою рішень щодо захисту кіберпростору. На його думку, створення двох центрів реагування на базі СБУ та Держспецзв'язку вже було важливим кроком з боку держави. «Ми зараз знаходимося у стадії, коли масштаб загрози вже усвідомлюється та починаються перші кроки для захисту, але це прозріння настало занадто пізно, аби встигнути докорінно змінити ситуацію», – каже Жора. Він нагадує, що новий закон про кібербезпеку, наприклад, набере чинності лише на початку травня, і цей документ лише окреслить головні засади у цій сфері, після чого напрацювання нормативної бази триватиме щонаймнше до осені поточного року.

Втім, навіть наявність найдосконаліших центрів реагування та відповідного законодавства не гарантує стовідсоткової безпеки. За словами Sean Brian Townsend, необхідно перевіряти вже існуючі системи і завчасно розуміти, яка шкода може бути завдана, якими мають бути дії адміністраторів та прес-служби, якщо це все ж відбудеться. «Тобто треба починати з найпростіших речей і рухатися знизу догори, від простого до складного», – каже хакер.

(вгору)

Додаток 12

7.05.2018
Михаил Сапитон
Android-троян ZooPark способен воровать почти любые данные

«Лаборатория Касперского» сообщила об идентификации вредоносного приложения ZooPark. Оно распространялось на Ближнем Востоке с 2015 года. Зараженные смартфоны находятся в Марокко, Ливии, Иордане, Египте и Иране. За время существования ZooPark сменило четыре версии. Первая имела доступ лишь к контактам и аккаунтам пользователя, но со временем функциональность увеличивалась (AIN.UA).

Приводим все функции ZooPark по мере выпуска новых версий.

Версия №2 (2016 год)
логи звонков;
данные GPS;
SMS-сообщения;
информация об устройстве.
Версия №3 (2016 год)

запись аудиозвонков;
датели об установленных приложениях;
данные браузера (закладки и история);
фотографии и картинки, сохраненные на карте памяти.
Версия №4 (2017 год)
связки паролей;
данные буфера обмена;
произвольные системные файлы и папки;
данные браузера – история поиска;
запись фото, видео, аудио, съемка скриншотов и запись экрана;
данные сторонних приложений. По умолчанию заданы: Telegram, WhatsApp, IMO, Chrome. Список можно настраивать произвольно.
Дополнительные возможности для передачи данных:
«тихая» отправка SMS-сообщений;
совершение звонков;
исполнение произвольных команд.

По информации «Лаборатории Касперского», им удалось зафиксировать не более 100 зараженных устройств. Возможно, это говорит о скрупулезном подборе жертв. Компания также предполагает, что за разработкой и распространением ZooPark может стоять правительство, однако не уточняет, на какую страну падают подозрения. Главными источниками дистрибуции оказались Telegram-каналы и новостные сайты. Последние взламывались, чтобы активировать редирект на страницы, предлагающие загрузку зараженных APK-файлов.

Последняя версия вредоносного софта могла быть разработана и «на стороне». В «Лаборатории Касперского» полагают, что ее купили у сторонней компании, распространяющей приложения для слежки. Главными целями называют тех, кто поддерживает независимость Курдистана (ZooPark мимикрировал под каналы и приложения о выборах в регионе), а также сотрудников Ближневосточного агентства ООН для помощи палестинским беженцам.

(вгору)

Додаток 13

9.05.2018

Хакеры украли банковские идентификаторы половины населения США

Бюро кредитных историй Equifax завершило оценку объема и состава данных, украденных хакерами летом 2017 г. Злоумышленники получили в свое распоряжение 145,5 млн номеров социального страхования, которые в США позволяют взять кредит или оформить банковскую карту (InternetUA).

Масштабы кражи

Американское бюро кредитных историй Equifax раскрыло точные масштабы кражи данных, имевшей место летом 2017 г. Бюро подтвердило, что злоумышленники смогли получить имена, фамилии и даты рождения 146,6 млн резидентов США.

Помимо этого, были украдены 145,5 млн номеров социального страхования (SSN), 99 млн адресов, 20,3 млн телефонных номеров, 17,6 млн номеров водительских удостоверений и 1,8 млн адресов электронной почты. Кроме того, были похищены данные по 209 тыс. платежных карт, включая номер и дату окончания действия, а также 97,5 тыс. номеров налогоплательщика TaxID.

Также злоумышленники получили сканы или фотокопии 38 тыс. водительских удостоверений, 12 тыс. карт социального страхования или налогоплательщика и 3,2 тыс. паспортов. Эти изображения были загружены пользователями на портал Equifax.

Процесс оценки ущерба

Оценка масштабов кражи данных заняла у Equifax несколько месяцев потому, что в базах данных компании информация была представлена не единообразно. Например, колонка с фамилиями могла называться «firstname» или «user_first_name» или «first_nm». Привести данные в единообразный вид помогла компания Mandiant, специализирующаяся на информационной безопасности.

Кроме того, в некоторые ячейки стандартных таблиц не были внесены данные, особенно часто – номера паспортов, даты выдачи водительских удостоверений и коды подтверждения кредитных карт.

Кража SSN

Кража 145,5 млн номеров социального страхования представляет собой серьезную проблему. Девятизначный SSN изначально был предназначен для идентификации налогоплательщиков в программе социального страхования. На деле он широко используется в американских банках для идентификации личности при открытии счета, получении кредита или оформлении кредитной карты. Фактически SSN является национальным идентификационным кодом. Предполагается, что SSN не знает никто, кроме резидента, которому присвоен этот номер. Поэтому мошенники охотятся за номерами социального страхования для осуществления кражи личности.

Проблема усугубляется тем, что на карточке социального страхования, где указан номер, отсутствуют какие-либо биометрические идентификаторы. Поэтому карточку легко подделать с целью совершения мошеннических операций. Ее подлинность можно подтвердить другими документами, для изготовления которых в свою очередь достаточно SSN. Широкие возможности для мошенничества, которые предоставляет SSN, заставляют американских парламентариев периодически выступать с проектами по ограничению

его применения.

История вопроса

О масштабной краже данных Equifax сообщила в сентябре 2017 г. – через 1,5 месяца после того, как узнала сама. Издание Bloomberg назвало инцидент одной из самых масштабных краж данных в истории. Пострадала почти половина населения США – всего в стране проживает 323 млн человек.

В ходе атаки хакеры использовали уязвимость веб-сайта компании. Злоумышленники действовали в период с середины мая до конца июля 2017 г. Три топ-менеджера Equifax успели продать принадлежащие им акции на сумму $1,8 млн уже после того, как о краже данных стало известно компании, но еще до того, как об инциденте было объявлено публично.

Equifax – это американское бюро кредитных историй, основанное в 1899 г. Наряду с Experian и TransUnion входит в тройку крупнейших организаций такого рода в США. Главный офис компании расположен в Атланте, штат Джорджия. В распоряжении бюро имеется информация более чем о 800 млн потребителей и 88 млн предприятий по всему миру. Штат компании насчитывает около 10,3 тыс. сотрудников в 14 странах.

Акции Equifax торгуются на Нью-Йоркской бирже. Выручка компании по итогам 2017 г. составила $3,362 млрд, чистая прибыль – $587,3 млн.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

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