СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(13.09–26.09)

2017 № 16

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(13.09–26.09)
№ 16

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

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

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2017

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

13.09.2017
Демченко Д.
Facebook тайно тестирует новое приложения для видеозвонков Bonfire

Facebook тайно тестирует свое новое приложения для видеозвонков Bonfire. Издание The Next Web обнаружило его в датском App Store (AIN.UA).

Bonfire предоставляет возможность проводить групповые видеозвонки, где могут участвовать до восьми человек. Во время разговора пользователи могут использовать «маски», как в Snapchat, а также делиться фотографиями, сделанными в приложении, в Instagram, Facebook и Messenger.

Когда пользователь приглашает друга в Bonfire, ему приходит уведомление в Facebook и Messenger.

Согласно данным аналитической фирмы Apptopia, приложение скачали около 2000 раз. В фирме подчеркивают, что в Дании обычно наблюдается хороший уровень удержания пользователей, что делает страну отличным местом для тестирования новых продуктов.

Как отмечает TechCrunch, у Facebook уже был опыт в развитии отдельных социальных приложений, и в целом он выдался неудачным. В прошлом году компания закрыла приложение Notify, а в этом остановила поддержку сервиса Groups и конкурента Snapchat Lifestage.

***

13.09.2017
Facebook тестирует автоматическую загрузку видео по Wi-Fi

Facebook тестирует новую функцию, благодаря которой у вас всегда будет что посмотреть через приложение социальной сети. При этом вам не придётся тратить ни мегабайта сотовых данных (IGate).

Нововведение называется Instant Videos («Мгновенные видео»). Оно предназначено для загрузки различных роликов, пока вы подключены к беспроводной сети. Так в приложении всегда будут доступны несколько видео, которые вы сможете просмотреть без ожидания.

Судя по всему, новая возможность предназначена для выполнения сразу нескольких функций. Поскольку Facebook уделяет видео особое внимание, она всеми силами старается заставить пользователей смотреть как можно больше роликов. Загрузка контента по Wi-Fi, в свою очередь, экономит мобильный трафик пользователей и вдохновляет на более продолжительный просмотр при подключении к сотовой сети.

Возможно также, что, как и в случае с Instant Articles, компания пытается получить больший контроль над экосистемой видео. В частности, издателям могут дать больше преимуществ за публикацию роликов, соответствующих определённым правилам. Впрочем, пока Facebook этим не занимается.

Компания подтвердила, что тестирует новую функцию среди небольшого числа пользователей приложения для Android. Пока не ясно, доберётся ли нововведение до широкой публики. Технические его подробности тоже не раскрываются.

***

13.09.2017

«Реальний конкурент Facebook». В Україні анонсували нову соцмережу ЄСвоє

Розробники соціальної мережі Ukrainians вирішили взятися за новий проект. Про це у Facebook повідомила один з розробників Олександра Струмчинська (Espreso.tv).

«Вчора я оголосила про презентацію нового і-продукту, який за рахунок свого масштабного підходу, інноваційності та грунтовності розуміння потреб від звичайних користувачів до бізнесу, об'єднає не лише українців, а й громадян інших держав», – пише вона.

За її словами, над розробкою соціальної мережі працює зовсім інша команда розробників, а масштабність проекту не поступатиметься світовим конкурентам.

«Коли ви побачите масштабність проекту, то зрозумієте, що це не сайт "'одноденка'", а реальний конкурент не тільки російським соцмережа, а й Facebook», – запевняє Струмчинська.

Так, за її словами, у мережі будуть доступні музика та відео, які будуть цілком легальні.

***

14.09.2017

Twitter начал автоматически делить текст на связанные сообщения по 140 символов

В мобильной версии сервиса микроблогов Twitter на Android появилась тестовая функция Tweetstorm. Как сообщает издание Cossa, это заметил пользователь под ником Devesh Logendran и поделился открытием с сотрудником The Next Web Мэттом Наваррой (Телекритика).

Максимально приложение автоматически может разделить текст на 352 части по 140 символов, публикуя их в виде связанной цепочки. То есть максимальный объем твитшторма 49 280 символов.

***

14.09.2017

В Twitter может появиться возможность публиковать множество сообщений одновременно

Twitter, предположительно, работает над новой функцией, которая позволит отправлять серии твитов, известных англоязычным пользователям как tweetstorms. Так у людей появится ещё один способ обхода ограничения в 140 символов на сообщение (InternetUA).

Пользователи отправляют серии твитов, оставляя одну публикацию и привязывая к ней все последующие. Так образуется древо сообщений, через которое человек может развёрнуто изложить свои мысли касательно той или иной проблемы или события.

Этот метод популяризировал технологический инвестор Марк Андриссен (Marc Andreessen), а термин tweetstorm придумал ещё один венчурный капиталист Крис Диксон (Chris Dixon). Теперь разработчики, судя по всему, хотят сделать метод официальной частью Twitter.

***

14.09.2017

Facebook таємно створює голосового помічника, – ЗМІ

Компанія Facebook у секретному режимі створює голосового помічника, який конкуруватиме з Siri та Alexa. Про це повідомляє Business Insider (Espreso.tv).

Виток даних про новий продукт виявив програміст Блейк Цузакі – він знайшов натяки на голосового помічника в останній версії мобільної програми Facebook. Згідно з отриманими даними, голосовий помічник виконуватиме традиційні завдання: шукати інформацію, робити різні пропозиції користувачеві, наприклад, оцінювати ймовірність виграшу тієї чи іншої спортивної команди.

Цузакі каже, що вперше побачив в коді сліди голосового помічника у вересні. Зараз він законсервований і нефункціональний, але програміст каже, що йому вдалося змусити його виконувати деякі команди. У прес-службі Facebook подробиць не повідомили, але зазначили, що наразі в додатку немає активного голосового помічника і тести на обмеженій аудиторії також не проводяться.

Офіційно компанія завжди спростовувала повідомлення про роботу над голосовим асистентом. Але поінформовані джерела повідомляють, що створенням помічника займається новий підрозділ, який відповідає за споживчі технології. Припускається, що помічник розробляють для нового домашнього девайсу від Facebook – проекту Aloha, який поєднає опції відеозв'язку та розумної колонки.

Очікують, що Aloha з’явиться в травні 2018 року. Пристрій має конкурувати з Amazon Echo і без потужного помічника це буде важко зробити.

***

15.09.2017

Facebook дозволить приховувати пости друзів на добу або місяць, – ЗМІ

Соцмережа Facebook почала тестувати функцію Snooze – тимчасового приховування постів друзів і спільнот. Про це повідомляє Techcrunch (Espreso.tv).

Як виявили журналісти, приховати оновлення можна на 24 години, тиждень або ж місяць.

Офіційно про вихід нової функції не оголошували. Поки Snooze працює тільки в США і лише в десктопній версії.

Кнопка знаходиться нижче функції «приховати публікацію».

Ще одна функція дозволятиме бачити в своїй стрічці більше або ж, навпаки, менше постів одного друга.

Зараз у Facebook можна скасувати підписку на оновлення конкретних користувачів, не видаляючи з друзів, але на постійній основі.

***

15.09.2017

Малышко Д.

Facebook запретил монетизацию постов об ураганах

Facebook более не позволит зарабатывать деньги на материалах оскорбительного, провокативного или шокирующего содержания, – сообщает CNet. Гигант сферы соцмедиа обновляет свои стандарты и руководящие принципы и фактически делает невозможным получение прибыли от контента, который является потенциально противоречивым и отвратительным.

Докладніше

***

16.09.2017

Месячная аудитория Facebook Messenger превысила 1,3 млрд человек

Facebook объявил, что ежемесячная аудитория сервиса для обмена сообщениями Messenger перешла отметку в 1,3 млрд человек (IGate).

В настоящее время компания продолжает активную работу над расширением функций Messenger. В числе последних нововведений значатся новые фильтры и реакции для видеочатов, больше подсказок в виртуальном помощнике M и расширение сервиса на отдельные страны за пределами США, новые игры и запуск Messenger Lite по всему миру.

Разработчики также изменили формат папки «входящие», чтобы доступ к важным функциям был проще.

***

17.09.2017

В Skype теперь можно создавать семейные чаты

Представители Skype в официальном блоге сообщили, что в сервисе появилась новая функция (iLenta.com).

В мессенджере появилась возможность создавать семейные чаты. Если вы станете членом семейства Майкрософт, члены вашей семьи, у которых есть учетная запись Skype, будут автоматически добавлены в список контактов Skype.

Что касается групповой беседы, то она создается автоматически со всеми членами вашей семьи, которые уже пользуются Skype, и имеет название «Моя семья».

По словам разработчиков, данное нововведение позволит гораздо проще общаться родным и близким. Осуществить видеозвонок или отправить сообщение можно невероятно быстро и для этого не нужно создавать отдельных диалогов. Удалить членов семьи из списка можно, как и обыкновенный контакт.

Новая функция также предусматривает осуществление родительского контроля и создание семейного календаря. Из семейной группы можно выходить точно так же, как и из любой другой беседы.

***

18.09.2017

Ольга Карпенко

Киевский программист собрал скрипты для работы с Facebook в Chrome-плагин

Киевский разработчик Макс Фрай ранее периодически выкладывал в общий доступ скрипты собственной разработки, которые облегчают использование социальных сетей. С их помощью можно фильтровать ботов, отписываться от групп, автоматизировать добавление в друзья и т. д.

Докладніше

***

18.09.2017

Новые функции Instagram оказались не по силам Windows-смартфонам

Разработчики Instagram выпустили обновление сервиса для устройств под управлением Windows 10, которое включает огромное количество новых

функций, в том числе поддержка эффектов в «Историях», возможность просматривать все доступные истории друзей и отвечать на них фотографиями. Кроме того, были внесены изменения в пользовательский интерфейс приложения. Но главным нововведением стала поддержка фильтров для лица, позволяющих добавить на него украшения и эффекты. Однако как выяснилось, Windows-смартфонам эти нововведения оказались не по силам (InternetUA).

Владельцы смартфонов под управлением Windows 10 Mobile жалуются на плохую оптимизацию сервиса. Например, на Lumia 640 при запуске новых фильтров для лиц приложение закрывается с ошибкой. Некоторые связывают это с недостаточным объёмом оперативной памяти.

Проблемы периодически наблюдаются даже на флагманском Lumia 950 XL. При просмотре историй приложение начинает зависать, а при запуске фронтальной камеры – закрывается.

Возможно, с будущими обновлениями разработчики решат проблему оптимизации.

***

19.09.2017

В Instagram реализовали небольшое, но важное нововведение

В приложении социальной сети Instagram для мобильных устройств на днях было реализовано небольшое, но важное нововведение, которое касается воспроизведения видеороликов (InternetUA).

Приложение автоматически воспроизводит видеоролики, которые появляются в вашей персональной ленте, однако ранее звук в каждом ролике был отключен. Чтобы услышать музыкальное сопровождение видеоролика, приходилось каждый раз нажимать на окошко плеера (или на кнопку регулировки громкости). С одной стороны, это очень удобно, когда вы находитесь в местах, где нельзя шуметь.

Для тех же, кому не нравилось включать звук для каждого ролика, и было выпущено последнее обновление. Теперь достаточно включить звук в одном ролике, после чего он автоматически будет включаться во всех последующих видеороликах в ленте. И наоборот, выключив звук в одном ролике, вы отключите его во всех остальных.

***

22.09.2017

Instagram добавил «маски» в прямые трансляции

Запись эфира можно будет оставить в разделе Stories или удалить (Зеркало недели. Украина).

Фотосервис Instagram добавил возможность накладывать «маски» на видео во время прямых трансляций в Stories, сообщается в блоге компании.

Пользователям доступны все традиционные «маски», а также несколько специальных, использовать которые можно ограниченное время. «Маску» можно наложить еще до начала трансляции или уже во время, нажав на соответствующую иконку.

В компании рассказали, что фильтры для прямых эфиров станут доступны для всех пользователей к середине октября.

***

25.09.2017

Twitter тестирует Lite-версию приложения под Android

Команда платформы микроблогов Twitter запустила тестирование облегченной версии приложения для устройств, работающих под управлением операционной системы Android (InternetUA).

Приложение Twitter Lite ориентировано на регионы с плохим подключением к интернету и слабых устройств. По словам разработчиков, его можно быстро установить на небольшой объем свободной памяти, а затем расходовать меньше трафика, чем в обычном приложении. Для установки потребуется 3 МБ свободного места. Пользователь может активировать режим экономии трафика для загрузки только тех изображений и видео, которые требуются пользователю.

***

26.09.2017

Ежемесячная аудитория Instagram превысила 800 млн

За пол года Instagram вырос на 100 миллионов пользователей (IGate).

Ежемесячная аудитория фотосервиса Instagram в сентябре превысила 800 млн пользователей в сравнении с 700 млн в апреле 2017 года. Об этом со ссылкой на заявление компании пишет CNBC.

По данным компании, ежедневное число активных пользователей приложения составило 500 млн человек. Представители Instagram также сообщили vc.ru, что ежемесячное число рекламодателей сервиса на 25 сентября 2017 года превысило 2 млн человек.

В марте 2017 года компания зафиксировала всего 1 млн рекламодателей в месяц, уточнили в Instagram. Представители фотосервиса также рассказали, что бизнес-профилями Instagram пользуются около 15 млн компаний.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

13.09.2017

В Азербайджані соцмережі не вбивають, а рятують журналістику – блогер

Азербайджанський блогер Гамід Гамідов переконаний, що в його країні Facebook перебрав на себе роль незалежних ЗМІ (Media Sapiens).

Про це він сказав на на Другій медіа-конференції Східного партнерства, яка відбувалася 13 вересня в Києві.

«Дуже часто ми чуємо слова про те, що соцмережі вбивають журналістику. У нас геть інша ситуація. В Азербайджані соцмережі рятують журналістику і журналістів. Адже в нас активно закриваються газети та сайти. Без роботи лишаються багато відомих, досвідчених журналістів. Вони йдуть з професії в піар чи інші сфери. Але журналістика – це в першу чергу покликання. Тож багатьох із нас Facebook врятував – тут ми можемо продовжувати оперативно ділитися важливою інформацією, висловлювати свою думку, аналізувати події, хоча й не отримувати за це зарплату. Коли в мене питають, яке в нас найпопулярніше медіа, я кажу Facebook, і це не іронія», – розповів він.

Гамід Гамідов зазначив, що саме Facebook має найбільшу популярність в його країні. За його словами, з майже 10 мільйонів населення близько Азербайджану близько 2 зареєстровані в цій соціальній мережі.

«Тож нашим медіа не треба виборювати популярність у соціальних мереж, ми їм вдячні за можливість вільно висловлюватися», – зазначив блогер.

Проте пан Гамідов уточнив, що нерідко азербайджанські блогери й у Facebook утримуються від коментування гострих тем, побоюючись за свою безпеку.

***

14.09.2017

No Kid Hungry предлагает с помощью эмодзи накормить голодных детей

Кампания EmojiMeals от BBH New York призвана вовлечь пользователей соцсетей в борьбу с детским голодом (Marketing Media Review).

Некоммерческая организация No Kid Hungry в сотрудничестве с агентством BBH New York создала кампанию, чтобы повысить осведомленность о проблеме детского голода в США. Согласно их статистике,

один из шести детей в Америке голодает. В рамках кампании EmojiMeals креативщики из BBH New York создали короткие видеоролики, которые также отображаются и в Instagram Stories. Сюжет видео – это такая себе инструкция, которая подсказывает, как можно поучаствовать в благотворительной акции. Сначала мы видим пустую тарелку, затем нужно наполнить ее едой в виде эмодзи: курица, фрукты, овощи, сладости и другое. Всякий раз, как на тарелку пользователь добавляет еду, сверху на экране выводится сумма денег, которую в итоге пользователь готов пожертвовать на борьбу с детским голодом.

***

19.09.2017

Украинские пивовары запустили флешмоб ради ответственного потребления пива

19 сентября пивовары Украины и отраслевая ассоциация пивоваров «Укрпиво» провели Всемирный день ответственного потребления пива, который ежегодно проходит в более чем 70 странах. В этом году, с целью вынести обсуждение проблемы продажу алкоголя несовершеннолетним на более широкий уровень, организаторы акции инициировали проведение социального флешмоба #не_останусь_в_стороне.

Докладніше

***

25.09.2017

Алексей Симончук

Что религиозные лидеры делают в соцсетях

Как и для чего мировые религиозные лидеры используют соцсети, кто из них открыто критикует государства, а кто постит проповеди, почему глава УГКЦ не хочет заводить Facebook и что думает о социальных сетях папа римский.

Докладніше

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

13.09.2017

Укрпошта запустила чат-бот в Telegram

Компанія Укрпошта запустила віртуального співрозмовника в одному з найпопулярніших месенджерів Telegram (Espreso.tv).

Про це повідомляє прес-служба компанії.

За допомогою чат-бота клієнти зможуть шукати та відстежувати поштові відправлення за номером. Бот також повідомлятиме про зміну статусу посилки, шукатиме відділення та його геолокації за індексом та ознайомлюватиме з базовими тарифами компанії.

Як додають в Укрпошті, згодом функціонал чат-бота буде розширюватися. Зокрема, планують поповнити мовні модулі та додати тарифний калькулятор, щоб бот міг розрахувати вартість відправлення.

Найближчим часом чат-боти запустять й на інших платформах – в Messenger від Facebook та у Viber.

***

19.09.2017

Facebook открыла лабораторию по исследованию ИИ в Монреале

Facebook сообщила о расширении команды исследователей искусственного интеллекта. Компания открыла новую лабораторию по изучению ИИ в Монреале, что в Канаде. Таким образом, сеть лабораторий в Менло-Парке, Нью-Йорке и Париже пополнилась ещё одной.

Докладніше

***

24.09.2017

Facebook будет показывать рекламу на основе посещения реальных магазинов

Таргетинг рекламы в Facebook выходит на новый уровень (IGate).

Если пользователь разрешит Facebook отслеживать свое местоположение, соцсеть сможет подбирать рекламу, основываясь на посещении реальных магазинов.

Согласно сообщению в блоге Facebook Business, в социальной сети появилась новая функция, позволяющая подбирать рекламу в зависимости от того, где пользователь бывает в реальной жизни.

К примеру, если пользователь посетил один из магазинов-партнеров Facebook, при этом приложение отслеживало его местоположение, то в дальнейшем на странице в соцсети появится реклама этой торговой точки.

Также система теперь будет различать постоянных и потенциальных клиентов одного и того же магазина. Если пользователь бывает в одном и том же месте постоянно, то он не получит рекламное сообщение, рассчитанное на человека, который никогда там не был и мог бы заглянуть. В то же время, постоянный клиент увидит сообщение с обновлениями, скидками или бонусами, действующими в настоящее время.

***

23.09.2017

Цукерберг намерен продать до 75 млн акций Facebook

Основатель Facebook Марк Цукерберг заявил о намерении продать до 75 млн акций компании в ближайшие полтора года. Об этом он написал на своей странице в Facebook (InternetUA).

«Я ожидаю, что мы продадим от 35 до 75 млн акций Facebook в ближайшие 18 месяцев, чтобы финансировать нашу работу в сферах образования, науки и юриспруденции», – написал Цукерберг.

***

25.09. 2017
Майя Яровая
«Нет явной стратегии»: как украинские бренды работают с YouTube

На конференции для рекламодетелей в YouTube представители мультиканальной медиасети AIR поделились интересными наблюдениями. Они проанализировали YouTube-каналы украинских брендов в различных отраслях, чтобы понять, насколько эффективно бизнес в нашей стране работает с данной площадкой.

Докладніше

***

25.09.2017
Microsoft и Facebook создали новый подводный кабель: 160 терабит в секунду

Microsoft, Facebook и телекоммуникационная корпорация Telxius завершили создание Marea – самого технологически продвинутого подводного кабеля на сегодняшний день. Marea может передавать до 160 терабит данных в секунду, что, согласно заявлению Microsoft, более чем в 16 миллионов раз быстрее, чем среднестатистическое домашнее интернет-соединение, что позволяет одновременно транслировать 71 миллион видеороликов в HD-качестве.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

13.09.2017

На грани лайка: как украинцы ведут себя с коллегами в соцсетях

Специалисты кадрового портала hh.ua проанализировали активность украинцев в социальных сетях в контексте профессиональных отношений.

Докладніше

***

19.09.2017

Видео показало уродливую правду отношений, прикрытую постами в сетях

Движение, посвященное борьбе с жестоким обращением в отношениях, One Love и креативная студия Framestore объединились ради новой кампании под тэгланом «За постом». Цель кампании – помочь людям заменить предупреждающие признаки нездоровых отношений и увеличить осведомленность о том, как легко дурное отношение проходит незамеченным. Креативщики выпустили 7-минутный фильм от режиссера Рейчел Макдональд, пятиминутную версию, два 30-секундных ролика и 10 коротких видео для каждого предупреждающего знака, такого как «ревность», «изоляция», «комплекс вины». Ролики предназначены для кампании в социальных сетях, объединенных под хэштегом #behindthepost (Marketing Media Review).

***

20.09.2017

Ученые назвали самую опасную соцсеть для человека

Ученые в Великобритании выяснили, какая из социальных сетей оказывает наибольший вред для человека. Исследование было проведено в рамках проекта #StatusOfMind (InternetUA).

С февраля по май более 1,5 тыс. молодых людей от 14 до 24 лет отвечали на вопросы социологов и анализировали различные ситуации, в которых соцсети могли бы как-то повлиять на самочувствие.

Были проанализированы 5 самых популярных соцсетей, среди которых YouTube получил оценку как платформа, которая не вредит ментальному здоровью человека.

На втором месте оказался Twitter, за ним идет Facebook, дальше Snapchat. А последнее место – за Instagram.

По результатам опроса Instagram назвали таким, что вызывает раздражение и депрессию, а также становится площадкой для издевательств.

Кроме того, британские ученые не рекомендуют более двух часов в сутки проводить в социальных сетях, поскольку это побуждает человека сравнивать себя с другими и дает ощущение неприятия себя.

***

25.09.2017

Израильтянин попросил суд запретить его жене пользоваться Facebook и Instagram

Житель центра страны обратился в суд по семейным делам с просьбой запретить его жене пользоваться Facebook и мобильными приложениями. По словам истца, которого в этом деле представляет Сарин Солан, его жена испытывает болезненную зависимость от интернета и мобильных аппликаций, типа WhatsApp (InternetUA).

По информации сайта «Маарив», менее года назад женщина начала пользоваться Facebook. Она создала несколько учетных записей в социальной сети. В общей сложности, она «подружилась» с 33.000 пользователей интернета, из которых 28.000 – это мужчины.

Мужчина говорит, что зависимость от интернета, от которой страдает его жена, похожа на зависимость от наркотиков. Женщина больше не может заботиться о семье, она не может работать. Истец в своем обращении в суд указывает, что жизнь его семьи превратилась в кошмар. Мужчина просит суд временно запретить его жене общаться в интернете с тем, чтобы он после 16 лет супружеской жизни мог решить, что делать дальше. Сайт «Маарив» отмечает, что трагедия произошла в семье бизнесмена, известного в деловых кругах Израиля.

Маніпулятивні технології

13.09.2017

Росія використала Facebook для організації антиімміграційних мітингів у США

Працівники російських спецслужб стояли за організацією антиімміграційного та антимусульманського мітингу в Айдахо. Для цього вони використали одну з функцій Facebook для організації подій та створили фейкові акаунти в соцмережі.

Докладніше

***

18.09.2017

Дипломатия социальных сетей: случай Facebook

О феномене цифровой дипломатии в мире заговорили не так уж давно – около десяти лет назад и, разумеется, вначале на Западе. С появлением социальных сетей «конвенциональные» веб-страницы и пресс-релизы утратили свою актуальность в качестве оперативных источников информации.

Созданные изначально как развлекательные платформы и средства межличностного общения, Facebook и Twitter быстро превратились в важный инструмент внешней политики.

Докладніше

***

19.09.2017

Дмитро Золотухін: «Україні та Європі потрібно ділитися досвідом протистояння дезінформації»

13 вересня 2017 року заступник Міністра інформаційної політики України Дмитро Золотухін взяв участь у подіумній дискусії «Українські уроки: боротьба з дезінформацією та захист демократії», організованій НУО «Democracy Reporting International» у Берліні.

Докладніше

***

21.09.2017

Twitter заблокировал 300 тысяч аккаунтов, связанных с терроризмом

Под давлением властей и регуляторов Twitter усиливает борьбу с распространением экстремизма онлайн, передает Bloomberg. Согласно опубликованным компанией данным, за последние полгода сервис микроблогов по всему миру заблокировал около 300 тысяч аккаунтов Twitter, связанных с терроризмом. Из этого числа около 95 % было выявлено с помощью автоматизированных инструментов, уточнили в Twitter. Также компания сообщила об увеличении запросов на выдачу данных пользователей со стороны властей: в период с января по июнь 2017 года их поступило около 3900 (InternetUA).

Автоматизация поиска экстремистских материалов – необходимая функция для социальных сетей, ведь вручную было бы невозможно проверить миллионы сообщений, которые ежедневно отправляют пользователи. В настоящее время у Twitter насчитывается около 328 млн подписчиков, а в США ежемесячная активная аудитория составляет около 68 миллионов.

В Twitter подчеркнули, что около 75 % заблокированных аккаунтов были закрыты до отправки с них каких-либо сообщений. В общей сложности с августа 2015 года Twitter приостановила 935 897 учетных записей, из которых две трети пришлось на этот год.

«Наши инструменты по борьбе со спамом позволяют нам быстрее и эффективнее блокировать аккаунты, нарушающие наши правила», – говорится в заявлении Twitter.

***

22.09.2017

Олег Дмитренко

Цукерберг зробив відео-звернення з приводу використання Росією Facebook для втручання у вибори

Росія через фейкові акаунти у Facebook поширювала політичну рекламу під час минулих виборів президента США, і соцмережа вже передала інформацію про ці факти ФБР – повідомив у своєму відео-зверненні керівник та засновник Facebook Марк Цукерберг.

Докладніше

***

23.09.2017

США обвинили российских хакеров в атаках на 21 штат

Министерство внутренней безопасности (МВБ) США заявило, что в ходе президентской кампании в 2016 году хакерским атакам со стороны России подвергся 21 штат, передает Reuters (InternetUA).

По данным агентства, хакерам, якобы работавшим из России, удалось просканировать связанную с выборами избирательную инфраструктуру штатов и внедриться в доступ к регистрационным базам данных избирателей.

Также сообщается, что попытки хакеров не привели к каким либо последствиям.

***

24.09.2017

Вибори в Німеччині: росіяни у Twitter «рекламують» ультраправих

У неділю, 24 вересня, в день німецьких парламентських виборів російські інтернет-боти у Twitter активізували підтримку ультраправої партії «Альтернатива для Німеччини» (AfD) (Espreso.tv).

Про це повідомляє Bild.

Так, видання проаналізувало визначило низку пов'язаних із Росією акаунтів, які раніше поширювали рекламу нерухомості та автомобілів у Росії, а потім раптово розгорнули підтримку AfD.

Лабораторія цифрової судової експертизи Atlantic Council (DFRLab) у свлжєму звіті припускає, що партія винайняла російські бот-мережі для поширення повідомлень.

Водночас Bild зазначає, що німецькі боти також активно підтримують правих, піднявши хештег «фальсифікація виборів» у топ актуальних.

Спецслужби і технології «соціального контролю»

13.09.2017

Проти Луценка відкрили провадження через записи у Facebook

Кваліфікаційно-дисциплінарна комісія прокурорів почала дисциплінарне провадження проти генпрокурора Юрія Луценка (Espreso.tv).

Про це повідомляє «Українська правда» з посиланням на документи, які виданню надали ініціатори дисциплінарного провадження Володимир Петраковський та Злата Симоненко.

Водночас кваліфікаційно-дисциплінарна комісія прокурорів веде аналогічне провадження й проти головного військового прокурора Анатолія Матіоса.

Згідно з дисциплінарною скаргою, Луценку та Матіосу ставлять в провину публікації у соцмережах, які порушують презумпцію невинуватості.

Відповідно до Закону України «Про прокуратуру» публічне висловлювання, яке є порушенням презумпції невинуватості, є підставою для притягнення прокурора до дисциплінарної відповідальності.

***

14.09.2017

Іспанія заблокувала сайт референдуму про незалежність Каталонії

У середу, 13 вересня, влада Іспанії закрила офіційний сайт сепаратистського референдуму про незалежність Каталонії, запланованого на 1 жовтня. Про це повідомляє іспанське видання La Razon (Espreso.tv).

Таким чином, правоохоронні органи країни виконали рішення суду Барселони щодо підготовки до референдуму, який центральна влада вважає незаконним.

Проте місцева влада Каталонії через деякий час відкрила сайт про референдум вже на іншому домені, а глава регіону Карлес Пучдемон у Twitter повідомив адресу нової сторінки.

«Веб-сайт референдуму доступний з іншої адреси. Ввійти через посилання ref1oct.cat», – написав Пучдемон.

***

15.09.2017

Малышко Д.

Соцсети будут массово «зачищать» пользовательский контент

ЕС ищет новые пути заставить социальные сети Google, Facebook и Twitter контролировать контент и удалять посты, которые носят экстремистский характер, разжигают ненависть или являются незаконными по ряду других причин. Однако контролировать процесс нелегко, ведь, согласно законодательству, соцсети не несут ответственности за информацию, размещенную пользователями. ЕС готов обязать их платить штрафы, если ситуация не улучшится.

Докладніше

***

19.09.2017
Сенат США запретил использование антивируса Касперского

Сенат Конгресса США проголосовал за запрет использования продукции «Лаборатории Касперского» американскими государственными учреждениями (InternetUA).

Данная поправка была включена в оборонный бюджет на 2018 финансовый год. За него проголосовали 89 сенаторов, восемь выступили против. Сенатор-демократ Жанна Шахин, одна из авторов поправки, заявила, что отказ от продукции Касперского «убирает реальную уязвимость нашей национальной безопасности».

Принятый законопроект запрещает использование программ «Лаборатории Касперского» в гражданских и военных ведомствах. 13 сентября МВБ США призвало все гражданские государственные учреждения страны в течение 90 дней удалить любые продукты Касперского, однако силовые структуры неподконтрольны данной директиве.

В конце июня агенты Федерального бюро расследований (ФБР) посетили не менее 10 сотрудников «Лаборатории Касперского», проживающих в США. Тогда в спецслужбе отмечали, что не имеют претензий к сотрудникам антивирусной компании и пытались выяснить, какую информацию антивирус может передавать в Россию.

***

20.09.2017
Саудовская Аравия снимет запрет на звонки в мессенджерах

Власти Саудовской Аравии снимут запрет на голосовые звонки в мессенджерах WhatsApp и Skype, сообщает «Би-би-си» (InternetUA).

Министерство связи сообщило, что Voice over Internet Protocol (VoIP) будет «доступен для пользователей» с 20 сентября. Ранее власти блокировали VoIP из-за отказа от соблюдения «правил».

Незадолго до этого Snapchat заблокировал доступ к катарскому телеканалу Al Jazeera в королевстве.

Саудовские официальные лица обвинили катарскую сеть в том, что она являются «вредным и пропагандистским каналом, поддерживающим экстремизм».

Цензура в интернете в Саудовской Аравии усилилась после событий «арабской весны» в 2011 году, когда власти приняли решение заблокировать доступ к 400 тыс. веб-сайтов.

***

23.09.2017

Мешканця Сєвєродонецька судитимуть за публічні антиукраїнські заклики

Прокуратурою Луганської області здійснюється процесуальне керівництво у кримінальному провадженні за ознаками кримінального правопорушення, передбаченого ч. 1 ст. 110 КК України (посягання на територіальну цілісність і недоторканність України) (InternetUA).

Розслідуванням встановлено, що у лютому 2017 року мешканець Сєвєродонецька систематично розміщував у соціальній мережі «ВКонтакте» тексти, що містять ознаки публічних закликів до проведення акцій громадської непокори та підтримки терористичних організацій «ЛНР» та «ДНР», а також заклики до зміни меж території України, шляхом визнання терористичних організвацій «ЛНР» та «ДНР» незалежними республіками та входження їх до складу Російської Федерації, тощо.

Наразі обвинувальний акт у вказаному кримінальному провадженні направлено до суду.

***

25.09.2017

Террористы «ДНР» заставляют Интернет-провайдеров шпионить за пользователями

«Министерство связи ДНР» рекомендует операторам телекоммуникаций собирать информацию об активности пользователей в сети Интернет и принять меры по их идентификации (InternetUA).

Как сообщает Цензор.НЕТ, об этом говорится в письме «министра» Виктора Яценко.

«Рекомендуем провести мероприятия по организации сбора и хранения учетных данных абонентов телекоммуникационной сети, данных об их сеансах выхода в сеть Интернет, а также иную информацию, позволяющую однозначно ассоциировать запрашиваемый IP-адрес с конкретным физическим (юридическим) лицом на определенный момент времени», – сказано в «документе».

***

25.09.2017

Правительство Китая собирает личные данные пользователей популярного мессенджера

Самый популярный мессенджер Китая WeChat добавил новый пункт в свою политику приватности, согласно которому приложение теперь может собирать личные данные пользователей и передавать их напрямую властям. Об этом сообщает The Next Web (InternetUA).

Таким образом, WeChat по специальному запросу от правительства может сообщить конфиденциальную информацию о пользователе, включая его имя, номер телефона, адрес электронной почты и даже геолокацию. Эта мера была принята на фоне ужесточения политики КНР касательно контроля интернета и онлайн-сервисов.

***

25.09.2017

Китай заблокировал самый популярный в мире мессенджер

Власти Китая заблокировали в стране доступ к мобильному мессенджеру WhatsApp. Об этом в понедельник, 25 сентября, сообщает газета The New York Times (InternetUA).

Специалист по интернет-коммуникациям Университета Гонконга Локман Тсуи (Lokman Tsui) заявил, что серьезные проблемы в работе WhatsApp начались 24 сентября. При этом он отметил, что существует вероятность, что некоторые пользователи по-прежнему могут пользоваться мессенджером.

Представитель компании Symbolic Software Надим Кобеисси (Nadim Kobeissi) в разговоре с изданием допустил, что власти КНР, возможно, разработали специальное программное обеспечение, чтобы помешать работе сервиса. В настоящее время пользователи из Китая не могут поделиться через WhatsApp ни фотографиями, ни видеозаписями, ни текстовыми сообщениями. «Подобный метод блокировки обычно не используется властями КНР», – отметил Кобеисси.

Проблема захисту даних. DDOS та вірусні атаки

13.09.2017

Злоумышленники используют «Интернет вещей» для рассылки спама

Количество вредоносных программ, способных заражать «умные» устройства под управлением ОС Linux, непрерывно растет. Значительная их часть предназначена для DDoS-атак и обеспечения анонимности в сети.

Докладніше

***

13.09.2017

Функція Google «безпечний перегляд» захищає вже більше 3 мільярдів пристроїв

Компанія Google повідомила, що її технологія «безпечний перегляд» (Safe Browsing) вже захищає понад 3 млрд пристроїв (Media Sapiens).

«Безпечний перегляд» був запущений в 2007 році. Ця функція надає список URL, які містять шкідливі програми та фішингових контент, браузерам Chrome, Firefox і Safari, а також провайдерам інтернет-послуг. За даними Google, у травні 2016 року технологія «безпечний перегляд» автоматично захищала понад 2 млрд. пристроїв. За оцінками компанії, таке стрімке поширення технології відбулося завдяки зростанню популярності мобільних пристроїв.

Повідомлення від Safe Browsing про перехід на потенційно небезпечну сторінку.

Google також розширила її використання й в інших свої продуктах: Android, Ads, Analytics, Gmail, Google Play. Також компанія почала використовувати в технології машинне навчання, яке виявляє більше загроз та типізує їх.

***

13.09.2017

Північнокорейські хакери атакують біткоін-гаманці та біржі обміну криптовалют

Хакери з Північної Кореї почали атакувати обмінники криптовалют та індивідуальні біткоін-гаманці.

Докладніше

***

14.09.2017

Число мобильных кибератак возросло на 40 %

Эксперты отметили всплеск числа кибератак на устройства на базе операционной системы Android (InternetUA).

Во втором квартале 2017 года число мобильных кибератак на пользователей Android выросло на 40 % по сравнению с аналогичным периодом в прошлом году – среднемесячный показатель увеличился с 1,2 млн до 1,7 млн инцидентов. Исследователи выяснили, что каждый месяц появляется около 788 новых вариантов вирусов, которые заражают мобильные телефоны и планшеты.

«Объем кибератак стремительно растет, так как хакеры используют более гибкие и опасные стратегии. Наибольшей угрозе подвергаются личные данные и конфиденциальность пользователей, – прокомментировал ситуацию Гаган Сингх, старший вице-президент и генеральный директор департамента мобильных и IoT-разработок Avast.

***

14.09.2017

Миллиарды устройств с поддержкой Bluetooth уязвимы к атакам BlueBorne

Исследователи безопасности из компании Armis обнаружили восемь уязвимостей в реализациях Bluetooth, используемых более чем в 8 млрд. устройств по всему миру. Набор уязвимостей получил название BlueBorne.

Докладніше

***

14.09.2017
Малышко Д.
Касперский уходит из Вашингтона

Подозреваемая в пособничестве российским шпионам «Лаборатория Касперского» уходит их Вашингтона и открывает офисы в других городах США и Канады. Проблема состоит в том, что правительственные агентства, фактически не могут пользоваться услугами «Лаборатории».

Докладніше

***

14.09.2017
Кіберполіція викрила велику схему з продажу фальсифікованих ліків

Працівники Департаменту кіберполіції Нацполіції припинили діяльність злочинної групи, учасники якої виготовляли та продавали через інтернет сильнодіючі ліки (Espreso.tv).

Про це повідомляє прес-служба кіберполіції.

«Сильнодіючі лікарські засоби потрапляли на територію України контрабандним шляхом. Деякі з препаратів виготовлялися безпосередньо на складі, орендованому членами угруповання», – розповів глава департаменту Сергій Демидюк.

Він додав, що фальсифікат також продавали і за кордон.

За його словами, до складу злочинної групи входили шість осіб, а ролі кожного з них були чітко розподілені. До групи входили IT-фахівці та співробітники спеціально створеного call-центру. В останньому надавали консультації щодо вживання сильнодіючих медпрепаратів.

Всі платежі здійснювалися через платіжні картки, оформлені на осіб, підконтрольних організаторам злочинної схеми.

Вдома у організаторів кустарного бізнесу правоохоронці провели 16 обшуків. За його результатами у організаторів нелегальної компанії та їхніх співучасників вилучили зброю, комп’ютерну техніку, мобільні телефони, сотні сім-карт, банківські платіжні картки та більше $70 тис. готівки.

***

14.09.2017

Футбольная ассоциация Англии опасается атак российских хакеров во время ЧМ-2018

Футбольная ассоциация Англии (The Football Association, FA) порекомендовала игрокам английской сборной и обслуживающему персоналу не использовать Wi-Fi-сети в общественных местах и гостинницах во время ЧМ-2018, который пройдет в России, из-за угрозы хакерских атак. FA опасается утечки конфиденциальной информации, такой как данные о травмах, процессе отбора команды и тактике игры (InternetUA).

Опасения относительно хищения данных возросли после взлома хакерской группировкой Fancy Bear электронной почты руководства FIFA в августе текущего года. Хакеры опубликовали в открытом доступе данные о футболистах, предположительно принимавших запрещенные препараты. Согласно опубликованным данным, в 2015 году 160 игроков не прошли допинг-контроль, а в 2017 году их число увеличилось до 200.

Футбольная ассоциация направила в FIFA письмо, в котором выразила обеспокоенность касательно вопросов кибербезопасности. В ответ на письмо представитель FIFA заявил, что организация делает все возможное для предотвращения повторной хакерской атаки. В настоящее время FIFA проводит расследование кибератаки Fancy Bear, с целью выяснить, были ли скомпрометированы системы организации.

***

15.09.2017

Сайт Минобразования опять взломали и выложили фото девушки «ню»

Сайт Министерства образования и науки утром, 15 сентября, снова взломали и опубликовали фото обнаженной девушки с оскорбительными подписями. Об этом сообщают «Украинские новости», которые успели сделать скриншот, пока все не поправили (InternetUA).

Во время перехода с поисковых систем на сайт mon.gov.ua сначала появлялось фото обнаженной девушки.

Снимок сопровождался подписью с оскорблениями в адрес некой Дарьи Севастьяновой. По контексту можно догадаться, что за кибератакой стоит бывший парень девушки, который, видимо, на нее за что-то сильно обиделся.

По состоянию на 12:40 сайт уже работал в привычном режиме.

***

18.09.2017

Новый вирус BlueBorne взламывает смартфон за 10 секунд

Команда компании Armis Labs сообщила об обнаружении нового опасного вируса, который может взломать смартфон всего за 10 секунд (iLenta.com).

Зловред получил название BlueBorne. По словам экспертов, он является на столько же опасным, как и бушевавший недавно в Сети вирус WannaCry.

BlueBorne действует через Bluetooth. Если на вашем смартфоне он включен, то время заражения может составить около 10 секунд. Причем, действует зловред незаметно и может распространяться самостоятельно на находящиеся рядом устройства.

Уже известно, что устройства компании Apple, работающие под управлением iOS 10 и выше, не подвержены заражению. Компания Microsoft выпустила обновление Windows в июле, а Google — в августе. Эксперты заявляют, что сейчас в опасности, в основном, оказались лишь Linux устройства.

***

18.09.2017

Хакери зламали додаток CCleaner

Хакерська атака дозволила зловмисникам викрасти дані користувачів (ZN.UA).

Додаток CCleaner піддався хакерській атаці, яка дозволила зловмисникам отримати доступ до даних користувачів, повідомляє компанія-розробник програми Piriform.

Як зазначається на сайті компанії, злому піддалися 32-бітні версії CCleaner 5.33.6162 (випущена 15 серпня) і версії CCleaner Cloud 1.07.3191 (випущена 24 серпня). Повідомлення про те, що ці версії можуть вести себе некоректно, з'явилися 12 вересня. Тоді ж компанія випустила оновлення, які вирішують цю проблему.

За даними компанії, після злому додатки починали відправляти ім'я комп'ютера, IP-адресу, список встановлених програм і мережевих адаптерів на спеціальний сервер на території США. Цей сервер був відключений правоохоронними органами 15 вересня.

Зламані версії додатків могли бути встановлені на 3 % пристроїв, тобто від хакерської атаки могли постраждати 2,3 мільйона чоловік.

27 червня державні і комерційні структури України постраждали від вірусу Petya A (Петя А). За даними DT.UA, хакерської атаки зазнали близько 30 банків. Вірус Petya A, який вдарив по комп'ютерних системах в Україні, також нашкодив банкам, електромережам, телефонним компаніям та метро у країнах Європи.

***

18.09.2017

Антивирус Google не смог выявить вирус, поразивший 20 млн устройств

Пару месяцев поисковый гигант Google запустил собственный антивирус на основе машинного обучения Play Protect, задачей которого является выявление зловредов в магазине Google Play и на мобильных девайсах. (iLenta.com).

Интересно то, что одному из вирусов достаточно успешно удалось обходить защиту Google. В результате, он смог заразить более 20 млн Android-устройств.

Речь идет о вирусе ExpensiveWall, который удалось выявить специалистам Check Point. Он попадал на гаджеты при помощи популярных приложений, типа Lovely Wallpaper.

ExpensiveWall подписывает пользователей на платные SMS-услуги, средства от которых идут его разработчикам. Причем, пользователи об этом не знают. Эксперты предполагают, что зловред способен на кражу данных или удалённую съёмку владельца устройства через камеру. Заражённые вирусом ExpensiveWall приложения запрашивают разрешения на доступ к Интернету и SMS-сообщениям.

Эксперты выяснили, что разработчики вирусу ExpensiveWall специально модифицировали его, чтобы Play Protect не обнаружил его.

***

19.09.2017
Вирус из Google Play заразил миллионы смартфонов

Исследователи из Check Point выяснили, что через Google Play распространялось более 50 приложений, заражённых вирусом ExpensiveWall. В общей сложности они были установлены от 1 до 4,2 миллиона раз (в Google Play нет точной статистики) (InternetUA).

В ExpensiveWall используется техника обфускации кода: вирус сжимается и шифруется, из-за чего антивирусы не могут его опознать. Заражённые этим вредоносом приложения были удалены ещё в начале августа, однако через несколько дней ExpensiveWall появился в новых приложениях и долгое время оставался незамеченным.

В Expensive Wall предусмотрен интерфейс между действиями в приложении и кодом JavaScript, выполняемым через веб-интерфейс WebView. Другими словами, код JavaScript, работающий через WebView, может вызывать операции в приложении. После установки и получения нужных разрешений Expensive Wall отправляет сведения о зараженном устройстве на свой командный сервер, в том числе информацию о его местоположении и уникальные идентификаторы, такие как MAC- и IP-адреса, IMSI и IMEI.

Приложения с Expensive Wall запрашивают доступ к интернету и SMS, благодаря чему могут подписывать пользователей на платные сервисы и отправлять SMS-сообщения на премиум-номера.

***

19.09.2017

Рекламный троян крадет данные из учетных записей в Facebook и Twitter

Эксперты заметили новую кампанию по распространению трояна AdService, похищающего пароли от учетных записей. Вредонос, распространяющийся в составе комплектов рекламного ПО, использует метод подмены оригинальных DLL-библиотек (динамически подключаемая библиотека) Chrome для загрузки и хищения информации из учетных записей пользователей в Facebook и Twitter (InternetUA).

AdService помещает вредоносную версию winhttp.dll в папку C:\Program Files (x86)\Google\Chrome\Application. Таким образом при запуске Chrome процесс chrome.exe загрузит вредоносную winhttp.dll вместо оригинальной.

После запуска браузера троян связывается с удаленным сервером для отправки/получения информации и пытается подключиться к Facebook и Twitter с целью хищения различной информации, в том числе сведений о настройках профиля, закладках, используемых методах оплаты и сохраненных данных кредитных карт (типе карты, последних 4 цифрах карты, дате окончания срока ее действия и привязанном к карте почтовом индексе), списке друзей, адресе электронной почты и пр.

***

19.09.2017

Wow-эффект: как одна компания создает самые вирусные видео в Facebook

Видео, которое собрало 382 млн просмотров и почти 12 млн шеров, было создано страницей Blossom, которая принадлежит родительской компании First Media. Обращаясь к продвинутым мамам, которые чувствуют себя как дома в онлайн-сообществах, этот аккаунт фокусируется на гениальных бытовых DIY-трюках для молодых родителей. Страница Blossom обошла по популярности даже аккаунт BuzzFeed Tasty, войдя в топ-10 Facebook страниц с самым большим количеством просмотров. (У Blossom 1,3 млрд ежемесячных просмотров, у Tasty - 917 млн) (Marketing Media Review).

Как отмечает Adweek, компания работает со специалистами по обработке данных, которые тестируют сотни оригинальных видео, создавая систему, которая определяет отличительные черты топ-видео и выбирает вирусные идеи. Чтобы гарантировать успех видео, компания концентрируется на двух вопросах: почему пользователи перестают скролить и смотрят видео, и

почему они делятся им. «Нам нужен wow-эффект, это и есть момент шера – когда информация либо вдохновляет, либо полезна, либо очень классная». Оказывается, заставка к видео очень важна и буквально останавливает пользователя. К примеру, «самое вирусное видео в Facebook» начинается с изображения нижнего белья. Еще одно видео о том, как починить старые джинсы, начиналось с изображения женщины, застегивающей свои джинсы. это видео собрало 172 млн просмотров.

Чтобы пользователи не только просмотрели видео, но и поделились им, брендированный контент не должен напоминать рекламу, но при этом увеличивать осведомленность о бренде и вовлечение. Поэтому видео должно быть очень интересным, вдохновляющим и полезным. Другими словами, зрители должны чувствовать, что в нем достаточно ценности, чтобы поделиться со своими друзьями. «Контент должен быть полезным и не открыто рекламным, если вы хотите достичь аудиторию миллениалов».

***

19.09.2017

В Харькове задержан хакер-шпион, следивший за гражданами Украины

В Харькове правоохранители задержали хакера, который вмешивался в личную жизнь как граждан Украины и других государств, путем подключения к их персональным компьютерам на правах администратора. Об этом сообщает пресс-служба Национальной полиции Украины.

Докладніше

***

20.09.2017

Популярный антивирус для Android тайно шпионил за пользователями

Google удалила, а затем снова вернула в магазин Google Play один из самых популярных мобильных антивирусов. Компании пришлось удалить приложение DU Antivirus Security от DU Group (является частью китайского конгломерата Baidu), поскольку, по словам исследователей из Check Point, оно втайне от пользователей собирало данные с их смартфонов.

Докладніше

***

20.09.2017

Уязвимость в Fitbit позволяет получить доступ к данным о пользователе

Исследователи из Университета Эдинбурга (Шотландия) проанализировали фитнес-трекеры Fitbit One и Fitbit Flex и обнаружили способ перехвата сообщений, передаваемых устройствами на облачные серверы. Это позволило им получить доступ к личной информации и создать ложные записи о физической активности пользователя (InternetUA).

Предприимчивые мошенники могут отправлять фальшивые данные о физической активности пользователя компаниям, предлагающим корпоративные оздоровительные программы. Таким образом злоумышленник может добиться скидки на страхование или получить вознаграждение в виде подарочных карт.

По словам экспертов, пока роль носимых устройств в повседневной жизни невелика, но в будущем это может измениться. Носимые устройства продолжают совершенствоваться и собирать больше данных о пользователях, но это также увеличивает потенциальные риски.

Исследователи уведомили Fitbit об уязвимости и компания оперативно выпустила патч, устраняющий ее.

***

20.09.2017

Незадокументированная функция MS Office позволяет собирать данные о пользователях

Эксперты «Лаборатории Касперского» обнаружили в пакете MS Office незадокументированную функцию, использование которой позволяет злоумышленникам собирать данные о целевой системе путем простой отправки жертве специально сформированного документа Microsoft Word, причем без активного контента: VBA-макросов, встроенных объектов Flash или PE-файлов. Функция присутствует в версии Microsoft Word для Windows, а также мобильных версиях Microsoft Office для iOS и Android. LibreOffice и OpenOffice ее не поддерживают.

Докладніше

***

18.09.2017

Сергей Решодько

Антон Коков, E-COM: «Опасность кибервойны у нас недооценивают»

Директор департамента по развитию сервисов е-документооборота E-COM, об отношении в Украине к кибербезопасности, потерях компаний, связанных с атакой вируса Petya.A, а также, почему во время атаки выстояли сервисы E-COM.

Докладніше

***

19.09.2017

Рекламный троян крадет данные из учетных записей в Facebook и Twitter

Эксперты заметили новую кампанию по распространению трояна AdService, похищающего пароли от учетных записей. Вредонос, распространяющийся в составе комплектов рекламного ПО, использует метод подмены оригинальных DLL-библиотек (динамически подключаемая библиотека) Chrome для загрузки и хищения информации из учетных записей пользователей в Facebook и Twitter (InternetUA).

AdService помещает вредоносную версию winhttp.dll в папку C:\Program Files (x86)\Google\Chrome\Application. Таким образом при запуске Chrome процесс chrome.exe загрузит вредоносную winhttp.dll вместо оригинальной.

После запуска браузера троян связывается с удаленным сервером для отправки/получения информации и пытается подключиться к Facebook и Twitter с целью хищения различной информации, в том числе сведений о настройках профиля, закладках, используемых методах оплаты и сохраненных данных кредитных карт (типе карты, последних 4 цифрах карты, дате окончания срока ее действия и привязанном к карте почтовом индексе), списке друзей, адресе электронной почты и пр.

***

20.09.2017

«Датагруп» будет защищать сайт Кабмина от DDoS-атак почти за 815 тыс. грн

«Датагруп» будет защищать правительственный портал от DDoS-атак до конца этого года за 812 640 гривен (InternetUA).

Хозяйственно-финансовый департамент секретариата Кабинета министров заключил договор с компанией 6 сентября, сообщают «Украинские новости» со ссылкой на ProZorro.

Телекоммуникационная компания «Датагруп» создана в 2003 году путем объединения «Датасат» и «Датаком», входивших в холдинг «Информационные компьютерные системы». Она является крупным игроком на рынке фиксированной спутниковой связи и интернет-доступа.

По информации IKS Consulting, по итогам 2015 оператор контролировал 48,5% украинского оптового рынка передачи данных.

Основателем и владельцем «Датагруп» является Александр Кардаков.

2015 год компания «Датагруп» завершила с прибылью 86,64 млн гривен, а в 2016 сократила прибыль на 18,5 % до 70,6 млн гривен.

***

23.09.2017

Хакеры требуют выкуп у тысяч компаний, угрожая DDoS-атаками

Хакерская группировка Phantom Squad организовала массовую спам-кампанию, направленную на тысячи организаций по всему миру. В письмах злоумышленники угрожают 30 сентября нынешнего года осуществить DDoS-атаку на сайты компаний, если те не выплатят выкуп в размере 0,2 биткойна (приблизительно $720).

Докладніше

***

24.09.2017

Хакер взломал сотни компаний через уязвимости на сайтах служб техподдержки

Независимый исследователь безопасности Инти Де Кекелайре (Inti De Ceukelaire) обнаружил уязвимость, позволяющую получить доступ к внутренним коммуникациям компаний. Эксплуатируя данную уязвимость, злоумышленники могут получить доступ к внутренним сетям организации, учетным записям в соцсетях и службам поддержки в корпоративных сетях Yammer и Slack.

Докладніше

***

21.09.2017

Правообладатели пролоббировали запрет на копирование авторского контента в интернете

Сторонники авторского права в Сети одержали крупную победу: всемирный консорциум по стандартизации объявил использование автоматических средств защиты от копирования в интернете официальной рекомендацией.

Докладніше

***

21.09.2017

Новая вымогательская кампания заставляет пользователей платить дважды

Киберпреступники запустили новую спам-кампанию по одновременному распространению двух вымогательских программ – Locky и FakeGlobe. Жертвы вынуждены дважды выплачивать выкуп, опасаясь потери своих данных. Об этом сообщили исследователи из Trend Micro в своем блоге (InternetUA).

В ходе новой вредоносной кампании хакеры одновременно используют вымогательское ПО Locky, впервые появившееся в начале 2016 года, и

похожую программу-вымогатель под названием FakeGlobe. Компьютеры жертв, переходящих по вредоносной ссылке в спам-письме, могут быть заражены сначала Locky, а по прошествии часа FakeGlobe. Подобный формат кампании увеличивает шансы повторного заражения, отмечают исследователи. География спам-рассылки охватывает более 70 стран, в основном затрагивая пользователей из Японии (25 %), Китая (10 %) и США (9 %).

Письма содержат ссылку и вредоносное вложение, замаскированное под счет или квитанцию. Скрипт во вложении аналогичен тому, что находится в архиве, загружаемом по ссылке, однако они подключаются к различным URL-адресам для загрузки вымогательского ПО. Один из них загружает Locky, второй – FakeGlobe. С поочередным заражением Locky и FakeGlobe файлы жертв шифруются несколько раз, то есть пользователям придется дважды заплатить выкуп или потерять свои данные.

Конечная цель атакующих – финансовая выгода. Данная кампания является ярким примером того, что хакеры разрабатывают более агрессивные методы для достижения своих целей, отметил исследователь безопасности из Trend Micro Эд Кабрера (Ed Cabrera).

***

21.09.2017
Раскрыта хакерская схема кражи денег по номеру телефона

Хакеры способны украсть деньги с электронных кошельков, используя уязвимость мобильных сетей. Об этом говорится в исследовании компании Positive Technologies.

Докладніше

***

24.09.2017
Популярная Android-клавиатура шпионит за пользователями

Как сообщают исследователи из Adguard, популярная клавиатура GO Keyboard шпионит за пользователями. Созданное китайскими разработчиками GOMO Dev Team приложение передает персональные данные пользователей на удаленный сервер, а также «использует запрещенную технику для загрузки опасного исполняемого кода», заявили эксперты.

Докладніше

***

24.09.2017
Вирус-вымогатель вместо денег требует обнаженные фото

Группа исследователей сайта MalwareHunterTeam, посвященного кибербезопасности, наткнулась на новый вирус-вымогатель nRansomware.

Поведение у вируса довольно странное: вместо денег за разблокированный компьютер он требует от жертвы выслать минимум 10 фотографий голышом (InternetUA).

При этом киберпреступники отмечают, что они сперва проверят, принадлежат ли фотографии именно жертве. И только потом разблокируют компьютер.

Сетевые антивирусные инструменты классифицируют nRansom.exe как вредоносный файл. А потому на шутку «айтишников» факт существования такого вымогателя списать довольно сложно. Сколько компьютеров уже подверглось заражению и сколько лет вымогателям, установить пока не удалось.

По сведениям MalwareHunterTeam, при заражении вирус воспроизводит музыкальный файл под названием your-mom-gay.mp3. А лицом вируса является паровозик Томас.b

***

24.09.2017

Эксперты вынудили АНБ отказаться от двух методов шифрования

Международная группа экспертов по криптографии вынудила Агентство национальной безопасности США отказаться от двух методов шифрования, известных как Simon и Speck, которые спецслужба предлагала установить в качестве международных стандартов. Как полагают эксперты из разных стран, включая Германию, Японию и Израиль, АНБ продвигает новые методы не по причине их эффективности, а потому, что знает, как их взломать.

Докладніше

***

25.09.2017

Anonymous взломали греческий аукцион по продаже недвижимости должников

Активисты движения Anonymous Greece атаковали греческий правительственный сайт по продаже недвижимости должников банков. По заявлениям участников движения в Facebook, работа сайта deltio.tnomik.gr будет остановлена на 27 часов (InternetUA).

Активисты также опубликовали послание греческому правительству, в котором раскритиковали позицию властей касательно вопросов здравоохранения и заявили о неприемлемости конфискации жилья у малоимущих. По словам участников движения, они «не будут больше смотреть, как иностранцы отбирают имущество бедных греков».

Также участники Anonymous Greece заявили, что аукцион по продаже жилья только первая цель в их списке. В дальнейшем они планируют атаковать и другие правительственные сайты.

***

25.09.2017

Фальшивые отпечатки пальцев сделают смартфоны более безопасными

Исследователи из Университета штата Мичиган в США разработали технологию, позволяющую тестировать защиту, которую предоставляют сканеры отпечатков пальцев. С помощью специального материала они воссоздают реалистичный отпечаток пальца и проверяют, сработает ли он для разблокировки устройства (InternetUA).

Слепки, имитирующие папиллярные узоры пальца, использовались хакерами со времени появления первых дактилоскопических сканеров. Как только находится способ обойти защиту, инженеры начинают разрабатывать новые, более сложные технологии. Самые надёжные сканеры – те, в которых сочетается несколько методов идентификации пользователя, например, с помощью ИК-сенсора и ультразвука.

В новом смартфон Apple нет сканера отпечатков пальцев, вместо него используется сканер лица и глаз. Не исключено, что будут найдены способы обхода и этой защиты, и тогда компании придётся совершенствовать её.

***

25.09.2017

Дмитрий Малышко

Ян Леви: Грядет кибератака невиданной силы

Западный мир готовится к самой мощной за свою историю кибератаке. Вот только антивирусы и фаерволы не способны удержать злоумышленников. Всю надежду эксперты возлагают на простых работников.

Докладніше

***

25.09.2017

Приложение с 200 млн установок шпионит за пользователями

Специалисты компании AdGuard сообщили о том, что Android-приложение GO Keyboard регулярно следит за пользователями (iLenta.com).

Примечательно, что GO Keyboard имеет более 200 млн установок, поэтому об уровне популярности рассказывать не придется. В AdGuard выяснили, что приложение отправляет на сервер информацию об электронной почте Google, размере экрана, версии Android, сборке и модели устройства.

Так как с помощью клавиатуры пользователи вводят логины и пароли, то имеется высокий шанс того, что и эти данные могут попасть в руки разработчикам GO Keyboard.

Разработчики приложения в свою очередь заявили, что ни в коем случае не планируют собирать указанные данные, так как они заботятся о конфиденциальности того, что и кому пишут пользователи.

Во время конференции Bloomberg Global Business Forum основателю Microsoft задали вопрос по поводу использования клавиш Ctrl+Alt+Delete.

В AdGuard советуют владельцам Android-устройств удалить приложения GO Keyboard-Emoji keyboard, Swipe input, GIFs и GO Keyboard-Emoticon keyboard, Free Theme, GIF. Что касается поискового гиганта Google, то он пока принимает решение по поводу судьбы данного ПО в официальном магазине.

***

25.09.2017

Платные антивирусы признаны бесполезными в современном мире

Эксперт популярного ресурса Mashable рассказал, почему среднестатистические пользователи интернета могут отказаться от антивирусных программ. Джек Морес считает, что время платных сервисов Avast, «Лаборатории Касперского», «Доктор Веб» и их аналогов безвозвратно уходит.

Докладніше

***

26.09.2017

Дмитрий Малышко

Лидер в сфере кибербезопасности «Deloitte» стал жертвой хакеров

В марте и мае этого года хакеры осуществили атаку на консалтинговую компанию «Deloitte», являющуюся лидером в сфере кибербезопасности, и похитили конфиденциальную информацию миллионов американцев. Однако сама компания долго держала взлом в секрете.

Докладніше

***

26.09.2017

Названа дата возможной атаки хакеров на крупнейшие компании мира

Группа вымогателей Phantom Squad угрожает массовой DDoS-атакой тысячам компаний, которые не успеют откупиться в указанный срок. Об этом сообщает Bleeping Computer (InternetUA).

Электронные письма с требованиями выкупа обнаружил специалист по кибербезопасности Деррик Фармер. Рассылка содержит простой текст с у требованием заплатить авторам 0,2 биткоина (около 720 долларов) или подготовиться к тому, что их сайт уйдет в офлайн 30 сентября.

Отмечается, что хакеры буквально завалили ящики компаний спамом с требованием небольшой суммы. Специалисты допускают, что группа Phantom Squad не обладает достаточной мощью для одновременного запуска DDoS-атак, рассчитанных на такое количество целей. По мнению экспертов, мошенники запугивают крупнейшие корпорации.

Исследователь компании Radware Даниэль Смит отметил, что текст заявления был почти идентичен тому, что использовалось в июне 2017 года группой вымогателей, назвавшихся именем известной хакерской группировкой Armada Collective. Тогда лже-хакеры ограничились пустыми угрозами, но все же получили выкуп от некоторых компаний. Стиль Phantom Squad же более всего напоминает мошенников-подражателей.

***

26.09.2017

Обнаружена новая масштабная спам-кампания по распространению Locky

Спустя неделю после появления спам-кампании, в ходе которой злоумышленники одновременно распространяли две вымогательские программы – Locky и FakeGlobe, исследователи безопасности из Trend Micro зафиксировали новую массовую спам-рассылку с использованием вымогательского ПО Locky. Количество вредоносных писем уже преодолело отметку в несколько миллионов (InternetUA).

В рамках кампании операторы Locky используют несколько типов спам-писем. Первый преставляет собой поддельное письмо якобы от компании Herbalife International с приложением в виде архива, замаскированного под квитанцию. Во втором типе писем также используется архив для доставки вредоносного ПО, однако в графе отправителя значится просто «copier» без какой-либо дополнительной информации в тексте письма. Третий тип писем маскируется под уведомление службы голосовой почты.

Все письма содержат архив с расширением .7z. В архиве находится вредоносный VBS-скрипт, который при исполнении загружает вымогательское ПО Locky на компьютер пользователя.

По данным исследователей, основными объектами атак злоумышленников стали Чили, Япония, Индия и США. На долю России в среднем пришлось 6 % от общего количества атак.

В то время как функционал Locky остается неизменным, масштабы атак и скорость распространения вымогательского ПО говорят об особой эффективности спама как метода доставки программ-вымогателей, отмечают исследователи.

***

26.09.2017

Владимир Кондрашов

Четыре крупных украинских портала майнили криптовалюту

Четыре крупных портала Украины – Корреспондент.NET, Football.ua, iSport и tochka.net – майнили криптовалюту через браузеры своих пользователей (InternetUA).

Сами пользователи ресурсов обнаружили проблему 25 сентября.

О майнинге на сайте Football.ua первым сообщил один из сотрудников IT-компании «Ciklum» по ником Evg Bell. Он написал, что на портале майнится довольно популярная криптовалюта Monero.

– Используется плагин coin-hive, который был специально разработан для майнинга именно этой монеты, – сообщил пользователь Evg Bell на своей странице в Facebook. – Все дело в том, что для майнинга Monero необходимо считать хеш-суммы по алгоритму Cryptonight, «выхлоп» от которого как раз максимален на процессорах, а не на видеокартаах, как для Биткоина и Эфира. А запустив скрипт в браузере, как раз можно использовать вычислительные мощности пользовательских процессоров (особенно Intel Core I7).

По данным Evg Bell, кроме «Football.ua» в «заработке» были уличены также новостной портал «Корреспондент», спортивный сайт iSport и развлекательный ресурс tochka.net.

Все эти ресурсы входят в медиахолдинг UMH.

Три портала (кроме tochka.net) извинились перед своими читателями и сообщили, что вредоносный скрипт использовал «один из партнеров».

– Наша техническая служба убрала вредоносный скрипт, а работа с партнером была остановлена. Ресурс вновь работает в привычном безопасном режиме. – дословно скопировали «Корреспондент» и «iSport» извинения портала «Football.ua».

На порталах также уточнили, что под удар попали только зарубежные пользователи сайта или те, кто пользовался зарубежными VPN.

Кто именно был тем «партнером», что так подставил UMH, ни один из порталов не сообщил.

***

26.09.2017

ИБ-эксперты оценили убытки от кибератак в первой половине 2017 года

По итогам первой половины 2017 года глобальный ущерб из-за кибератак, включая расходы на устранение последствий и потери производительности, достиг 4 млрд долларов США, подсчитали эксперты ИБ-компании Trend Micro. Специалисты отметили растущее число случаев кибервымогательства, фишинговых атак типа Business Email Compromise (BEC), ориентированных на бизнес-пользователей, а также IoT-взломов, передает Economic Times (InternetUA).

За январь-июнь 2017 года в Trend Micro зарегистрировали более 82 млн угроз с использованием вредоносного ПО для вымогательства (ransomware), а также более 3 тысяч попыток BEC-атак. В связи с этим эксперты рекомендовали предприятиям в первую очередь выделять финансирования на создание эффективной системы защиты, поскольку последствия взлома дорого обходятся компаниям и часто превышают их бюджет.

В апреле и июне вирусы-шифровальщики WannaCrypt и Petya атаковали тысячи компаний по всему миру. По данным ФБР, фишинговые атаки с компрометацией корпоративной электронной почты увеличили общий объем глобальных потерь до 5,3 млрд долларов США.

В Trend Micro также предупредили, что злоумышленники все чаще атакуют IoT-устройства, и что взлом промышленных роботов может привести к огромному финансовому ущербу и потере производительности.

Кроме того, специалисты отметили рост злоупотреблений социальными сетями, распространение пропаганды и фальшивой информации, что также может привести к серьезным финансовым последствиям для бизнеса.

ДОДАТКИ

Додаток 1

15.09.2017
Малышко Д.
Facebook запретил монетизацию постов об ураганах

Facebook более не позволит зарабатывать деньги на материалах оскорбительного, провокативного или шокирующего содержания, – сообщает CNet (InternetUA).

Новая политика также направлена против кликбейта (искусственного накручивания кликов через мнимую сенсационность заголовков в ущерб качеству или точности информации) и распространения фейков.

Новые правила были опубликованы в блоге Ника Грудина, вице-президента Facebook по вопросам медиа партнерства. Компания приняла это решение после длительных споров о том, что соцсеть стала «виртуальным мегафоном» для всех подряд – от неонацистов до российских групп, которые, как утверждается, влияют на политику и выборы в США.

С этой поры на Facebook нельзя монетизировать контент со следующим содержанием:

«Неправомерное использование детских образов»
«Трагедия и конфликт»
«Дискуссионные социальные проблемы»
«Контент, изображающий или провоцирующий насилие»
«Контент для взрослых»
«Контент, касающийся запрещенной деятельности»

«Нецензурированный контент»

«Наркотики или употребление алкоголя»

«Ненормативная лексика»

Разъяснения о том, что подпадает под ту или иную категорию, находятся на странице «Руководства по монетизации контента».

Например, «Неправомерное использование детских образов» – это сцены с насилием, насмешками над детьми, даже если они носят комический или сатирический характер. Сюда же относятся материалы с детьми, имеющие хотя бы небольшой эротический характер.

К категории «Трагедия и конфликт» стоит отнести сцены катастроф и бедствий. К ним нельзя прикрепить рекламу, даже если это информативные или просветительские материалы.

К нецензурированному контенту относятся изображения открытых ран, крови, медицинских процедур и другие пугающие и шокирующие материалы.

Однако, если пользователь считает, что монетизация его контента соответствует правилам сайта, он может подать апелляцию единоразово по каждому посту и компания пересмотрит свое решение.

Также, согласно Нику Грудину, для монетизации контента необходимо быть пользователем соцсети как минимум один месяц и иметь то количество друзей, которое потребует Ad Breaks.

«Пользователи, неоднократно нарушающие Руководство, “шарящие” кликбейт или публикующие неправдивую информацию, могут лишиться права на публикацию и монетизацию постов», – написал вице-президент Facebook.

(вгору)

Додаток 2

18.09.2017

Ольга Карпенко

Киевский программист собрал скрипты для работы с Facebook в Chrome-плагин

Киевский разработчик Макс Фрай ранее периодически выкладывал в общий доступ скрипты собственной разработки, которые облегчают использование социальных сетей. С их помощью можно фильтровать ботов, отписываться от групп, автоматизировать добавление в друзья и т. д. Они были рассчитаны как на администраторов страниц в Facebook, так и на обычных пользователей. На днях он добавил все эти функции в единый плагин для Chrome (AIN.UA).

Этот плагин может:

– отклонить все входящие заявки в друзья и отменить все исходящие;

– добавить 100 любых возможных друзей, а также добавить 100 возможных друзей с 50 и более общими друзьями;

– фильтровать ботов и неактивных друзей;

– добавить в друзья всех, кто написал комментарий;

– пригласить вступить в группу лайкнувших пост;
– покинуть публичные группы;
– скрыть рекламные публикации;
– скрыть посты с меньше 15 лайков;
– скрыть посты со ссылками на СМИ;
– скрыть публикации со стоп-словами и т. д.

По словам Макса, сначала он писал этот плагин под себя. Затем добавил к нему скрипты, которые ранее публиковал по отдельности: вывод списка неактивных аккаунтов (те, с которыми меньше всего взаимодействий), отмена входящих/исходящих заявок в друзья, лайкание ленты, выход из всех публичных групп и т. д. Так что в результате получился плагин, комбинирующий возможности фильтровать свою ленту и функции для SMM-специалистов.

Макс подготовил и плагин для Opera, но он пока проходит модерацию. Разработчик планирует постоянно обновлять плагин, добавлять новые функции, будет также рассматривать предложения по новым функциям от пользователей.

(вгору)

Додаток 3

19.09.2017

Украинские пивовары запустили флешмоб ради ответственного потребления пива

19 сентября пивовары Украины и отраслевая ассоциация пивоваров «Укрпиво» провели Всемирный день ответственного потребления пива, который ежегодно проходит в более чем 70 странах. Таким образом, пивоваренная отрасль снова привлекает внимание общественности к проблеме продаж алкоголя несовершеннолетним. Статистика потребления алкоголя украинскими подростками, как и подростками во всем мире, остается довольно высокой. Так, согласно данным международного проекта-опроса Фонда UNICEF «Здоровье и поведенческие ориентации молодежи», проведенного в 2015 году, почти 84 % украинцев, не достигших 18 лет, пробовали алкоголь, а пиво употребляли более 20 % подростков. Тем не менее, в течение последних нескольких лет наблюдается положительная динамика: с 2011 года данный показатель снизился на 6%. 19-30 сентября этого года около 100 волонтеров «САН ИнБев Украина» и Carlsberg Ukraine посетят более 500 точек продаж пива в 3 городах Украины. Сотрудники компаний снова проверят, как соблюдаются основные принципы Меморандума об ответственном потреблении. Волонтеры также еще раз напомнят покупателям и продавцам о том, что алкоголь можно продавать только лицам, достигшим 18 лет. В этом году с целью вынести обсуждение проблемы на более широкий уровень организаторы акции инициировали проведение социального флешмоба #не_останусь_в_стороне. Для того чтобы стать участником флешмоба,

необходимо добавить к своей аватарке в Facebook уникальную рамку с логотипом акции, расширить один из акционных плакатов. Затем предлагается поделиться в Facebook или Instagram постом с хештегом #не_останусь_в_стороне (#не_залишуся_осторонь) и рассказать об отношении к потреблению алкогольных напитков несовершеннолетними, предложить свои методы решения проблемы, а также рассказать о конкретных ситуациях, связанных с нарушением запрета на продажу алкоголя несовершеннолетним и вашей реакцией на них (Marketing Media Review).

(вгору)

Додаток 4

25.09.2017
Алексей Симончук
Что религиозные лидеры делают в соцсетях

Как и для чего мировые религиозные лидеры используют соцсети, кто из них открыто критикует государства, а кто постит проповеди, почему глава УГКЦ не хочет заводить Facebook и что думает о социальных сетях папа римский (Телекритика).

Папа Римский Франциск I считается одним из самых прогрессивных глав Католической церкви. Не удивительно, что он активен и в социальных сетях.

«Бежать за трендом, за лайком, собирать больше фолловеров в соцсетях – вот в чем мы, человеческие существа, оказались пойманы. Это то, что современное общество предлагает – одиночество со страхом ответственности и безумные усилия для самоутверждения», – считает он.

На его странице в Instagram (4,8 млн. подписчиков) регулярно публикуются новые фотографии.

В Twitter есть сразу девять официальных аккаунтов Франциска, все они на разных языках (есть даже на арабском). «Я призываю к миру и разоружению: в этом мире, раненном насилием, нам нужно братство между народами», – пишет Папа Римский.

Отметим, что официальной страницы в Facebook у Франциска нет.

Духовный лидер последователей тибетского буддизма также довольно активен в социальных сетях. На его Instagram подписаны 894 тыс. человек. Там он публикует фотографии с различных встреч, проповедей и событий. Примечательно, что практически на каждом фото Далай-лама улыбается.

В Twitter (14,9 млн. подписчиков) он также делится собственными мыслями касательно происходящих вокруг событий. Как и Папа Римский, он использует площадку для призывов к миру.

В Facebook у Далай-ламы 13,8 млн. подписчиков. Там он публикует, в основном, видео со своим участием (различные встречи и эфиры), а также пишет посты о том, что его волнует.

Али Хаменеи

Великий аятолла, духовный лидер Ирана активно ведет свои социальные сети, в отличие от многих других представителей ислама.

В Instagram у него 1,6 млн. подписчиков. Там он публикует фото и видео с различных встреч, а также просто фотографии, под которыми пишет посты. Чаще всего, он цитирует отрывки из Корана или пишет собственные мысли. Также там можно найти критику Соединенных Штатов Америки.

В Twitter (359 тыс. подписчиков) он часто критикует руководство США. В частности, много достается президенту Дональду Трампу.

В Facebook (185 тысяч подписчиков) он также много критикует руководство США, публикует видео и фото своих выступлений, а также пишет о том, что его волнует в данный момент.

Патриарх Кирилл

Глава Российской православной цекви неоднократно высказывался об интернете и социальных сетях. Однако то он критикует священников за то, что они недостаточно активно общаются в соцсетях с паствой, то призывает не пользоваться интернетом, ведь «не должно быть никакого приспособления монашеской жизни к современным условиям».

У патриарха есть аккаунты в Facebook (25,8 тыс. подписчиков) и во «Вконтакте» (392 тыс.подписчиков). Примечательно, что в российской соцсети Кириллу нельзя написать сообщение, зато можно отправить подарок.

Патриарх Филарет

У главы Украинской православной церкви Киевского патриархата есть аккаунт в Facebook, где на него подписаны 4,1 тысяча человек.

Очень заметно, что страничкой никто особенно не занимается. В основном, на ней публикуются новости с сайта УПЦ КП или посты о деятельности церкви и ее председателя.

Святослав (Шевчук)

У предстоятеля Украинской греко-католической церкви также есть лишь аккаунт в Facebook с 40 тысячами подписчиков. Большую часть контента занимают перепечатки с официального сайта УГКЦ, посвященные деятельности Святослава и церкви. Однако эта страничка является, скорее, представительством самой церкви, ведь сам Шевчук говорил, что у него нет времени для того, чтобы вести Facebook, а нанимать помощников для этого он не хочет.

Давид Лау

Главный раввин Израиля имеет свой аккаунт в Facebook. На него подписаны 13,2 тысячи человек. Он ориентирован на местную аудиторию, поэтому пишет посты лишь на иврите.

Очевидно, что активнее всего занимаются социальными сетями Папа Римский и Далай-лама. Это и показывает, почему именно они являются самыми популярными духовными лидерами в мире.

(вгору)

Додаток 5

19.09.2017
Facebook открыла лабораторию по исследованию ИИ в Монреале

Facebook сообщила о расширении команды исследователей искусственного интеллекта. Компания открыла новую лабораторию по изучению ИИ в Монреале, что в Канаде. Таким образом, сеть лабораторий в Менло-Парке, Нью-Йорке и Париже пополнилась ещё одной (InternetUA).

«В монреальской лаборатории исследователи и инженеры будут работать над широким спектром амбициозных научных проектов в сфере искусственного интеллекта, но также в ней будет уделено особое внимание обучению с подкреплением и системам диалогов», – заявил старший научный сотрудник Facebook Ян Лекун (Yann LeCun).

Руководителем лаборатории выступит Джоэль Пино (Joelle Pineau) – профессор информатики Университета Макгилла и содиректор расположенной в учебном заведении Лаборатории аргументации и обучения. В своих исследованиях она фокусируется на планировании, обучении и принятии решений, а также на взаимодействиях человека и робота. Она опубликовала ряд работ на тему систем диалогов и трудилась в команде, которая разработала интеллектуальное роботизированное инвалидное кресло.

Лекун заявил, что, как и другие исследовательские лаборатории Facebook, учреждение в Монреале будет взаимодействовать с сообществами учёных через публикации, конференции и совместные проекты. Компания также собирается сотрудничать с Университетом Макгила, Канадским институтом продвинутых исследований, Монреальским институтом алгоритмов обучения и Монреальским университетом.

«В Монреале уже существует фантастическое академическое сообщество в сфере ИИ, экосистема стартапов и многообещающие правительственные установки, вдохновляющие на исследования в области ИИ, – сказал Лекун. – Мы рады стать частью этого большого сообщества и с нетерпением ждём, когда сможем начать взаимодействовать со всей экосистемой и помогать ей процветать».

(вгору)

Додаток 6

25.09. 2017
Майя Яровая
«Нет явной стратегии»: как украинские бренды работают с YouTube

На конференции для рекламодетелей в YouTube представители мультиканальной медиасети AIR поделились интересными наблюдениями. Они проанализировали YouTube-каналы украинских брендов в различных отраслях, чтобы понять, насколько эффективно бизнес в нашей стране работает с данной площадкой. Несмотря на то, что в США, Европе и России бренды уже давно научились общаться со своей целевой аудиторией на YouTube, в Украине таких

примеров удручающе мало. Если не считать каналы интернет-магазинов: «Розетки», F.ua и «Цитруса» (AIN.UA).

Ниже – подробные результаты исследования и несколько примеров – удачных и не очень – от специалистов AIR Веры Сливинской и Дмитрия Ковальчука.

Почему брендам важно работать с платформой YouTube? Потому что если вы не будете говорить о себе на YouTube, это за вас сделают другие.

И вам может не понравится то, что о вашем бренде говорят на YouTube, а контролировать это не всегда получается. Приведу пример. Если вы на своих смартфонах сделаете поисковой запрос «Альфа-банк», первое, что вы увидите – ролик под названием «Быдло в Альфа-Банке». Сомнительная реклама для финучреждения. У бренда уже около полугода такой вопиющий PR-конфликт и они ничего не делают.

YouTube-стратегия бренда должна быть синхронизирована с общей стратегией маркетинговых коммуникаций бренда. Есть три основных стратегии работы с YouTube в зависимости от поставленных задач:

Если же вам необходимо более глубокое доверие аудитории – то это работа с видеоблогерами.

Мы решили посмотреть, как дела с YouTube у украинских брендов. Для этого мы проанализировали каналы крупнейших игроков рынка в пяти категориях e-commerce, телеком, потребительская электроника, FMCG food и FMCG not food. При этом мы учитывали несколько основных факторов, которые влияют на развитие YouTube-канала:

– стратегия, которую бренд выбрал на YouTube и выбрал ли он ее вообще,

– базовая оптимизация в настройках контента для получения органического трафика, частота публикаций, что очень важно для продвижения контента,

– активность работы с видеоблогерами.

E-commerce

E-commerce на YouTube – это наиболее активная ниша по сравнению с другими. Мы проанализировали свыше 30 брендов в сфере электронной коммерции в Украине по различным направлениям: автотовары, фешн, электроника и т.д. и выбрали топ-10 представителей. Явным лидером является канал «Розетки», который набрал почти миллион подписчиков и считается одним из самых успешных ecommerce-проектов на YouTube в мире.

Как правило ecommerce-компании используют свои каналы как один из основных медиа-источников привлечения трафика. Конкуренция очень большая во всех направлениях, но бренды пытаются как-то выделиться: создают уникальный контент, делают ставку на информационно-развлекательную тематику с упором на поисковую оптимизацию для привлечения трафика.

Для получения дополнительного внимания к своим каналам ecommerce-бренды все больше работают с видеоблогерами. Хотим поделиться кейсом

Comfy, с которым мы работаем уже пару лет. Сегодня на канале Comfy уже больше 130 000 подписчиков, а когда мы начинали – их было около 20 000.

Для Comfy мы проводим конкурсы с привлечением блогеров, причем механика может быть разная. Видео с условиями конкурса может «жить» как на канале бренда, так и блогеров. Причем, на канале блогеров они вызывают больше доверия.

Телеком

YouTube-каналы телеком-брендов в Украине ведутся скорее как хостинг рекламного контента – сюда сливаются рекламные и промо-ролики, а также корпоративные хроники. Живого общения с аудиторией нет. Контент создается, но без учета интересов пользователей, поэтому он не вызывает желания подписаться и не может приносить полноценный трафик. Активность на каналах невысокая.

FMCG, продукты питания

В данной категории мы проанализировали более 60 крупнейших продуктовых FMCG-брендов на рынке Украины. Большинство из них ведут свои каналы, но эти каналы выглядят скорее как визитные карточки, где также публикуется много рекламного контента, который за редким исключением рассчитан на взаимодействие с аудиторией.

Даже те бренды, которые создают свой контент, делают это не систематично, тем самым нивелируя все свои старания. Они не получают трафика, который могли бы получать. Например у «Торчина» есть интересный контент. Если немного поработать над его дистрибуцией и стратегией привлечения аудитории с помощью тех же блогеров, бренд бы получил совсем другой результат.

Также несколько лет назад ребята из McDonald’s создавали контент, в котором рассказывали о внутренней кухне ресторана и о том, чем живут его сотрудники. Со временем они перестали вкладываться в развитие канала, а если бы продолжали – он бы рос.

Некоторые FMCG-бренды в Украине вообще не ведут локальные YouTube-каналы – они ссылаются на глобальные каналы или ближайшие представительства в России.

Что можно делать пищевому FMCG, чтобы привлечь аудиторию на YouTube? Для украинского бренда Mirinda мы делали проект с популярными блогерами музыкального развлекательного канала ND Production. Кейс называется «Эксперименты цитрусовых». С двумя блогерами мы отсняли семь видео, которые разместили на канале бренда. Также в колаборации участвовал интернет-магазин «Цитрус» – видео были размещены и на его канале.

Чтобы получить максимально таргетированный охват именно украинской аудитории, было принято решение использовать коммерческий трафик, но помимо этого мы получили часть органического трафика за счет подписчиков «Цитруса». Суммарно проект сгенерировал более 1,6 млн просмотров, при этом средняя глубина просмотра видео составила 58 % – это намного выше

показателя в целом по YouTube, который даже на блогерских каналах составляет в среднем 35 %.

Такой эффект был достигнут за счет двух факторов. В роликах участвовали два персонажа – плоть и кровь YouTube, поэтому ролик не вызывает резкого отторжения, как часто бывает с рекламой. И правильное программирование кампании, выстраивание настроек и правильная ЦА.

Еще одним примером эффективной работы бренда с блогерами является кампания по продвижению йогурта «Растишка». Результат превзошел прогнозы уже в первые четыре недели. При этом результаты шести месяцев удвоили показатели первого. Видео продолжает набирать просмотры и это совершенно ничего не стоило бренду – он заплатил один раз, за интеграцию с блогерами.

Также бывают и вовсе счастливые случаи. С тем же брендом Danone мы сделали одно видео с откровеннейшим продакт-плейсментом – видно, что оно заказное. Видео было посвящено выводу на рынок нового формата йогурта – питьевой «Растишка» с трубочкой. Ролик завирусился и на данный момент набрал почти 23 млн просмотров.

FMCG non food

Представители этой категории менее активны, чем в FMCG food. Но здесь тоже есть явный лидер – канал Maybelline, который создает собственное YouTube-шоу, приглашая на канал бьюти-блогеров из Украины. Просмотров такие ролики набирают много – бренд работает в правильном направлении.

Все остальные представители сферы публикуют видео очень редко, и активность на их каналах в разы меньше, чем у Maybelline.

Потребительская электроника

В данной категории мы проанализировали более 30 компаний. Лидером является Samsung Ukraine, но контент преимущественно рекламный. Есть и собственный, но к сожалению, выпускается он не системно.

(вгору)

Додаток 7

25.09.2017

Microsoft и Facebook создали новый подводный кабель: 160 терабит в секунду

Microsoft, Facebook и телекоммуникационная корпорация Telxius завершили создание Marea – самого технологически продвинутого подводного кабеля на сегодняшний день. Об этом сообщает Популярная механика (InternetUA).

Marea пересекает Атлантический океан на глубине более чем на 5200 метров ниже уровня моря, соединяя Вирджиния-Бич с Бильбао, что в Испании. Длина этого чуда инженерной мысли составляет целых 6 600 км, а общий вес порядка 4,65 миллионов килограммов.

Marea может передавать до 160 терабит данных в секунду, что, согласно заявлению Microsoft, более чем в 16 миллионов раз быстрее, чем

среднестатистическое домашнее интернет-соединение, что позволяет одновременно транслировать 71 миллион видеороликов в HD-качестве.

К 2025 году ожидается восьмикратное увеличение трафика на текущих цифровых сервисах, а потому потенциал нового кабеля будет реализован на все 100 %.

Важным достоинством Marea является также и то, что в будущем его можно будет кастомизировать и настраивать для взаимодействия с различными сетевыми устройствами. В настоящее время в Microsoft представлен широкий спектр облачных сервисов, которые компания планирует улучшить с помощью Marea: от Bing и Office 365 до Skype и Xbox Live. Для Facebook Marea в первую очередь интересен как средство, которое позволит социальной сети поддерживать VR-интерфейс.

Рафаэль Арранз, главный операционный директор Telxius, в предыдущем заявлении упомянул, что все современные приложения, особенно связанные с видео, потребляют огромные сетевые ресурсы. Чтобы обеспечить их корректную работу, необходимо привязать каждый сервис к высокопроизводительной системе с высокой пропускной способностью.

Стимулом для создания кабеля стал ураган Сэнди, который в 2012 году вызвал массовое нарушение сетевых коммуникаций и оставил США без интернета и телефонной связи на несколько дней.

«Это было серьезное происшествие, – говорит Фрэнк Рей, директор глобальной сетевой стратегии подразделения Microsoft Cloud Infrastructure and Operations, в заявлении для прессы. – Вся сеть между Северной Америкой и Европой была изолирована в течение нескольких часов. Ураган выявил потенциальную проблему в консолидации трансатлантических кабелей, которые были локализованы в Нью-Йорке и Нью-Джерси».

После встречи с руководителями Facebook на собраниях, компании в конечном итоге согласились объединить усилия для создания мощного и надежного кабеля. Работа началась в прошлом году – в августе 2016 года.

(вгору)

Додаток 8

13.09.2017

На грани лайка: как украинцы ведут себя с коллегами в соцсетях

Специалисты кадрового портала hh.ua проанализировали активность украинцев в социальных сетях в контексте профессиональных отношений. Согласно результатам опроса, 55 % респондентов устанавливают дружбу с большинством коллег в социальных сетях, а вот каждый четвертый участник опроса добавляет «в друзья» только тех коллег, с которым он дружит в реальной жизни. 16 % опрошенных предпочитают разделять личную жизнь и работу, поэтому не добавляют сотрудников «в друзья» (Marketing Media Review).

Как показывают результаты опроса, 32 % респондентов указывают все места работы в своих аккаунтах, 30 % опрошенных шерят только те места, где работают длительное время. А вот 17 % обозначают место работы только в некоторых социальных сетях.

В Facebook и LinkedIn место работы указывают чаще других социальных сетей, что может быть связано со спецификой сетей и аудитории.

Относительно реакций на активность компании в социальных сетях, то наиболее распространенной практикой является подписка на страницу (57 %). Практически все публикации лайкают 17 % респондентов, а 25 % вообще никак не реагируют на активность компании в соцсетях.

Как показывает опрос, так или иначе, профессиональная жизнь имеет свою реализацию и в онлайн-формате. Украинцы расширяют свой круг «друзей» в соцсетях, включая в него коллег по работе, презентуют себя, идентифицируя с местом работы, реагируют на онлайн-активности компании, в которой работают. И хотя есть те, кто предпочитает разграничивать личную жизнь и работу, для многих, по крайней мере онлайн, эта грань становится все менее ощутимой.

(вгору)

Додаток 9

13.09.2017

Росія використала Facebook для організації антиіммміграційних мітингів у США

Працівники російських спецслужб стояли за організацією антиіммміграційного та антимусульманського мітингу в Айдахо, з'ясувало видання The Daily Beast (Media Sapiens).

Для цього вони використали одну з функцій Facebook для організації подій та створили фейкові акаунти в соцмережі. Прес-секретар Facebook підтвердив The Daily Beast, що компанія заблокувала декілька подій на своїй платформі й що це відбулося в рамках ширшої кампанії із блокування, про яку соцмережа повідомила минулого тижня. При цьому компанія не стала коментувати, чи просувалися ці події за допомогою платних оголошень в Facebook.

Клінт Уоттс (Clint Watts), колишній агент ФБР та експерт з кампаній російського впливу, вважає, що це «наступний крок після поширення фейків». «Метою впливу є змінити поведінку. Найпростіша зміна у поведінці – змусити когось поширювати пропаганду, яку створила і посіяла Росія. Друга частина таких змін – змусити людей зробити щось фізично», – пояснив експерт.

Так, в мережі з'явилася подія під назвою «Citizens before refugees» (Громадяни важливіші, ніж біженці), в якій мешканців міста Твін-Фоллс в штаті Айдахо закликали вийти на антиіммміграційний протест під міською радою. Подія була створена сторінкою «SecuredBorders» (Безпечні кордони), яка позиціонується як американська антиіммміграційна спільнота й була згодом

викрита як пропагандистська сторінка, керована з Росії. На момент, коли Facebook її заблокувала, у сторінки було 133 тисячі підписників. До того, як подію заблокувала адміністрація соцмережі, 4 особи клікнули, що підуть на мітинг та ще 48 клікнули, що зацікавилися подією. Деякі профілі зацікавлених учасників містили інформацію про те, що вони є мешканцями Твін-Фоллз.

«Значна частина російської пропагандистської рекламної кампанії у Facebook з тих пір була видалена. Але її фрагменти залишаються видимими в кеші пошукових систем, включаючи повідомлення про організовані події в Facebook у 2016 році», – пише The Daily Beast.

Минулого тижня соцмережа Facebook визнала, що Росія використала фейкові акаунти та опублікувала близько 3000 оголошень, спрямованих на поширення політично суперечливих постів у США до та після виборів. За оцінками компанії, їх побачили від 23 до 70 мільйонів користувачів, а вартість цієї кампанії склала $100 тисяч.

(вгору)

Додаток 10

18.09.2017
Дипломатия социальных сетей: случай Facebook

О феномене цифровой дипломатии в мире заговорили не так уж давно – около десяти лет назад и, разумеется, вначале на Западе. С появлением социальных сетей «конвенциональные» веб-страницы и пресс-релизы утратили свою актуальность в качестве оперативных источников информации. Созданные изначально как развлекательные платформы и средства межличностного общения, Facebook и Twitter быстро превратились в важный инструмент внешней политики. Госдеп и британский Форин офис в числе первых поняли все преимущества новейших технологий коммуникаций. Именно они и сегодня остаются среди лидеров по использованию IT-платформ во внешнеполитической деятельности. Кстати, проведенные университетом Оксфорда исследования показали, что и МИД Украины входит в десятку лучших внешнеполитических ведомств мира по использованию Twitter. (Новости ИТ).

Первая Facebook-страница МИД Украины появилась в декабре 2010 года. Примерно в это же время Государственный департамент разработал «Стратегию государственного развития в 21-м столетии», в которой электронная, или, как точнее ее следует называть, цифровая дипломатия была определена одним из ключевых механизмов реализации внешней политики США. Сегодня Twitter стал едва ли не основной платформой для политических баталий (и взаимных провокаций, и операций спецслужб тоже), а для многих политиков их аккаунты выступают еще и в качестве своеобразных визитных карточек. Об исключительной важности социальных сетей особенно ярко свидетельствует опыт последних американских выборов. Дотошные журналисты подсчитали, что во время избирательной кампании Дональд Трамп

стал автором вдвое большего числа твиттов, чем Хилари Клинтон, а их часто неоднозначный характер стал одной из причин его популярности среди избирателей – «синих воротничков». На сегодняшний день широчайшее использование Twitter-дипломатии уже является повсеместным, и даже породило новый термин – twiplomacy. То есть, классическая дипломатия переговоров и вербальных нот никуда не исчезла, однако оказалось, что гораздо более оперативным, доступным и свободным от строгих протокольных рамок способом ведения внешнеполитических дискуссий являются 140 знаков короткого сообщения, которое вмиг достигает сотен, если не тысяч подписчиков – “followers”.

С Twitter-дипломатией все понятно, поговорим теперь о Facebook. По оценкам экспертных организаций, среднее ежемесячное число пользователей Twitter в мире оценивается, по данным CNBC, в 284 млн., WhatsApp – 500 млн., а Facebook – в 2 млрд. человек. Каждый день в Facebook заходят более 1,3 млрд. пользователей (и их число растет – по сравнению с прошлым годом на 17%). Facebook “живет” на 1,74 млрд. мобильных устройств. Каждую минуту в Facebook появляются 510 тыс. новых комментариев, 293 000 обновленных статусов, 136 000 новых фото. Крайне интересна географическая статистика Facebook. Десять наиболее продвинутых Facebook-стран это: Индия (241 млн. пользователей), США (240 млн.), Бразилия (139 млн.), Индонезия (126 млн.), Мексика (85 млн.), Филиппины (69 млн.), Вьетнам (64 млн.), Таиланд (67 млн.), Турция (56 млн.), Великобритания (44 млн.). А вот в каких городах проживают наиболее активные пользователи: Бангкок (35 млн.), Джакарта (26 млн.), Дакка (25 млн.), Мехико (16 млн.), Стамбул (15 млн.), Нью Дели (15 млн.), Лима (15 млн.), Каир (14 млн.), Сан Пауло (14 млн.), Хо Ши Мин (14 млн.). При этом число активных участников сети в Индии растет вдвое быстрее, чем в США, что в общем характерно и для других стран Юго-восточной Азии. Среди пользователей этой социальной сети большинство составляют мужчины и молодежь от 25 до 35 лет.

Любопытно теперь взглянуть на другую статистику. В августе 2017 года авторитетное международное агентство по изучению общественного мнения Pew Global опубликовало данные опросов в 37 странах мира на всех континентах по крайне важному для Украины вопросу – отношение к России в целом и к Путину в частности. Агрессивная политика Москвы и необходимость “обуздания” Кремля через механизмы санкций породили множество дискуссий в многосторонних форматах, вовлекая в них страны, находящиеся за тысячи километров от Москвы. Оценка действий России на международной арене превратилась в фактор не только внешней, но и внутренней политики, ведь для государств, где власть меняется с помощью выборов, общественное мнение учитывается при принятии внешнеполитических решений. Поэтому крайне важно понимать, насколько глубоко в различных странах осознают роль питерских товарищей, которым существующий мировой порядок однажды показался несправедливым, в разрушении современной системы международной безопасности. Так вот, по данным Pew Global, в среднем

только 26% опрошенных доверяют России и Путину, однако лишь 31% считает, что Россия угрожает их стране (справедливости ради, столько же респондентов полагает, что угрозой является Китай и чуть больше – США). Если в государствах Европы (кроме Греции) и Северной Америки отмечается в целом адекватное восприятие политики РФ и ее лидера, то среди тех стран, население которых в большинстве своем считает, что Путин проводит правильную политику, а Россия – скорее друг, чем враг, лидируют государства Юго-восточной Азии, Африки, и Ближнего Востока. Лидерами "любви" к России являются Вьетнам (83%), Филиппины (55%) и Греция (64%), среди "колеблющихся", чьи граждане в значительной степени вообще отказались оценивать политику Путина, оказались Индия, Индонезия, Южная Африка и Аргентина. Граждане Вьетнама и Филиппин уверены, что в России соблюдаются права человека, а более позитивное, чем негативное отношение к нашему северному соседу присутствует также среди населения таких важных стран, как Мексика и Индия (в целом подобная картина наблюдается в 18 странах из 37, где проводились опросы). Удивительно, учитывая недавнее потепление двусторонних отношений, что в негативном свете видят Россию 62% опрошенных турок. И не удивительно, что среди всех респондентов Россию оценивают адекватно представители более старшего поколения, в то время как молодежь все еще питает иллюзии относительно Москвы.

Приведенная выше статистика вроде бы свидетельствует о том, что Facebook может стать важным инструментом внешней политики особенно в тех странах, где наше дипломатическое присутствие недостаточно. Учитывая, что среднее время посещаемости Facebook 20 минут, а наиболее заинтересованной аудиторией являются молодые люди от 25 до 35 лет, кажется логичным формирование и распространение специального контента, ориентированного на молодежь, возможно, даже на языке целевой страны, с тем, чтобы давать правдивую информацию о том, что представляет собой современная Россия, и что происходит на самом деле в Украине. Это могли бы быть музыкальные и киноролики, динамичные презентации культурного и информационного характера, даже политическая реклама. Среди стран "основной" целевой группы могли бы быть Вьетнам, Филиппины, Греция, Индия, Индонезия, Бразилия, Мексика. Facebook объявил о планах проактивного развития в Африке, включая инвестиции в инфраструктуру интернета, поэтому следующим этапом могли бы стать пророссийски настроенные пользователи в Южной Африке, Нигерии и других важных странах. При голосовании на Генассамблее ООН за критические для Украины резолюции голоса этих государств могут оказаться не лишними.

Однако не следует забывать, что с Facebook не все так просто. В сети, по авторитетным экспертным оценкам, насчитывается около 83 млн. "липовых" аккаунтов, существуют широчайшие возможности для распространения лживых новостей, просто используя ее встроенные сервисы. Хакерство – еще один риск, который присутствует со времен появления Интернета. Бывший кандидат в президенты США от Демократической партии Хиллари Клинтон

убеждена, что одной из причин ее поражения на выборах стало именно распространение ложной информации через Facebook. По мнению Хиллари Клинтон, фальшивые новости повлияли на восприятие данных избирателями. “Мои противники использовали контент, который был попросту лживым, применяя при этом персонализированные способы передачи информации”,— утверждает госпожа Клинтон.

И все же, как отмечают международные эксперты, “Facebook слишком велик, чтобы его игнорировать”, в первую очередь с точки зрения организации информационной работы. Еще в 2012 году на совещании российских послов и постпредов в Москве Путин поставил цифровую дипломатию в один ряд с наиболее действенными инструментами внешней политики. По его мнению, дипломаты должны использовать новейшие технологии на разных платформах, в том числе в социальных медиа, для разъяснения позиций государства. Как мы теперь знаем, эти ценные указания воплотились в создание огромной инфраструктуры лжи, включающей как армию “интернет-троллей”, так и вполне конвенциональные СМИ, целью которых является создание параллельной реальности, выгодной Кремлю. Буквально на днях очередной скандал, связанный с “российским следом” в американских выборах, разгорелся как раз вокруг Facebook. Общественная организация Campaign Legal Center, в центре внимания которой находятся вопросы законности ведения избирательных кампаний, обратилась к Марку Цукенбергу с письмом, в котором потребовала обнародовать данные о профинансированной “русскими” политической рекламе в Facebook во время избирательной кампании в США в 2016 году. По признанию руководителя подразделения безопасности Facebook Алекса Стамоса, было идентифицировано более 470 подставных аккаунтов, связанных с известной фабрикой “троллей” из Санкт-Петербурга, и 3000 образцов политической рекламы, размещенной за российские деньги с июня 2015 по май 2017 года. Образцы такой рекламы были переданы специальному прокурору Роберту Мюллеру в связи с расследованием Министерства юстиции о вмешательстве Москвы в президентские выборы. В то же время, Facebook отказался передавать информацию о клиентах в Конгресс. По имеющимся данным, российские заказчики заплатили Facebook не такую уж большую сумму – около 100 тысяч долларов, однако смогли охватить аудиторию в несколько десятков (до 70!) миллионов человек.

Три года войны против Украины убедили практически всех в Европе и в Северной Америке (но, как выясняется, далеко не всех за их пределами), что российские “новости” таковыми не являются, не смотря на все усилия дипломатов и пропагандистов Путина. Однако для Украины просто развенчивания мифов “Russia Today” и “Sputnik” уже, очевидно, недостаточно. Инфраструктуре лжи следует противопоставить инфраструктуру правды. Для выстраивания собственной новостной “истории” Facebook является одним из вполне подходящих инструментов, если умело им пользоваться.

(вгору)

Додаток 11

19.09.2017

Дмитро Золотухін: «Україні та Європі потрібно ділитися досвідом протистояння дезінформації»

13 вересня 2017 року заступник Міністра інформаційної політики України Дмитро Золотухін взяв участь у подіумній дискусії «Українські уроки: боротьба з дезінформацією та захист демократії», організованій НУО «Democracy Reporting International» у Берліні (Міністерство інформаційної політики).

Розповідаючи про гібридну агресію РФ в Україні, Дмитро Золотухін зазначив: «Все, що зараз відбувається в українському інформаційному просторі, правильніше було б віднести до сфери роботи спецслужб. Це активні заходи. Це не дії, які вчиняються медіа, вони реалізуються організаціями, що лише вважають себе ЗМІ та представляються журналістами».

Заступник Міністра резюмував: «Україна отримала величезний досвід боротьби з дезінформацією, дуже багато якої, на жаль, надходить з Європи. Коли неправдиві відомості про Україну з'являються в європейських ЗМІ – це дуже болісно. У тому числі й для самої Європи. Тому Європі й Україні потрібно ділитися інформацією та досвідом в області протистояння дезінформації».

Виконавчий директор «Democracy Reporting International» Майкл Мейер-Резенде зазначив, що «українці мають досвід протидії тому, що лякає Європу», і саме тому необхідна співпраця України з європейською спільнотою в сфері захисту демократії та протидії дезінформації.

Ростислав Огризко, радник-посланник Посольства України в Німеччині, у своєму виступі спростував найпоширеніші наративи російської пропаганди, зокрема такі, що під час Другої світової війни українці співпрацювали з нацистами, в 2014 році до влади в України прийшли неонацисти, а Крим – споконвіку російська земля.

Участь у заході також взяли представники українських громадських організацій, які розповіли про суспільні ініціативи щодо розвінчування фейків і протидії неправдивій інформації.

(вгору)

Додаток 12

22.09.2017

Олег Дмитренко

Цукерберг зробив відео-звернення з приводу використання Росією Facebook для втручання у вибори

Росія через фейкові акаунти у Facebook поширювала політичну рекламу під час минулих виборів президента США, і соцмережа вже передала

інформацію про ці факти ФБР – повідомив у своєму відео-зверненні керівник та засновник Facebook Марк Цукерберг (Watcher).

Він повідомив, що Facebook активно співпрацює з американськими спецслужбами і допомагає їм розслідувати втручання російської влади у вибори президента США за через рекламу в соцмережі.

«Ми також повідомили про це Конгрес, і я розпорядився, щоб наші фахівці відправили всю інформацію про цю рекламу також і до комітетів Конгресу», – додав засновник Facebook.

Він також заявив, що в майбутньому, для уникнення таких інцидентів, Facebook вимагатиме, щоб розповсюджувачі політичної реклами розкривали, хто платить за рекламу. Наразі така вимога відповідно до законодавства США застосовується до політичної реклами на телебаченні, але не стосується соціальних медіа.

«У світі завжди будуть погані, брехливі люди і ми не можемо запобігти втручанням в уряди усіх країн, але ми можемо зробити це складнішим, набагато складнішим. І це те, на чому ми збираємося сконцентруватися», – завив він.

«Ми можемо знайти ще більше доказів, і якщо це трапиться, ми продовжимо працювати з урядом. Ми розслідуємо втручання угруповань з Росії, щоб зрозуміти, як вони використали наші інструменти», – додав він.

Раніше Facebook повідомив про виявлення фактів розміщення реклами в соцмережі, що могла вплинути на результати виборів США. Було заявлено, що принаймні $100 тис було заплачено з Росії за розміщення такої реклами.

(вгору)

Додаток 13

15.09.2017
Малышко Д.
Соцсети будут массово «зачищать» пользовательский контент

ЕС ищет новые пути заставить социальные сети Google, Facebook и Twitter контролировать контент и удалять посты, которые носят экстремистский характер, разжигают ненависть или являются незаконными по ряду других причин. Однако контролировать процесс нелегко, ведь, согласно законодательству, соцсети не несут ответственности за информацию, размещенную пользователями. ЕС готов обязать их платить штрафы, если ситуация не улучшится (InternetUA).

Европейская комиссия разработала новые инструкции, в которых подробно описывается, как компании должны бороться с так называемыми «хейтерами», разжигающими ненависть, и другими нарушителями. «Необходимо внедрять эффективные процедуры уведомления и реагирования на нарушение, устанавливать эффективные интерфейсы и уделять особое внимание информированию правоохранительных органов», – говорится в инструкции. Также предлагается объединить усилия программного

обеспечения и «доверенных сигнальщиков», жалобы от которых будут рассматриваться модераторами в первую очередь.

Уже в этом году руководства социальных сетей подписали «кодекс поведения», согласно которому незаконный контент должен быть удален с платформы в течение 24 часов с момента публикации.

ЕС отметил усилия, которые прилагает Facebook для борьбы с нарушителями. Однако Европейская комиссия считает, что их недостаточно. С другой стороны, само законодательство препятствует контролю за постами, ведь соцсети не несут ответственности за информацию, размещенную пользователями.

Члены Еврокомиссии предупредили, что если к весне 2018 года они останутся недовольными результатами проводимого контроля, будут приняты законы, предусматривающие штрафы для соцсетей и удаление контента с платформ.

Google, Facebook и Twitter отказались комментировать данное решение ЕС.

(вгору)

Додаток 14

13.09.2017

Злоумышленники используют «Интернет вещей» для рассылки спама

Количество вредоносных программ, способных заражать «умные» устройства под управлением ОС Linux, непрерывно растет (ITnews).

Значительная их часть предназначена для DDoS-атак и обеспечения анонимности в сети. Как показало проведенное специалистами «Доктор Веб» исследование, киберпреступники используют таких Linux-троянцев для массовых почтовых рассылок.

Речь идет о вредоносной программе Linux.ProxyM, о которой мы уже рассказывали в июне. Напомним, что этот троянец запускает на инфицированном устройстве SOCKS-прокси-сервер и способен детектировать ханипоты (от англ. honeypot – «горшочек с медом») – специальные ресурсы, созданные исследователями вредоносных программ в качестве приманки для злоумышленников. Соединившись со своим управляющим сервером и получив от него подтверждение, Linux.ProxyM загружает с этого сервера адреса двух интернет-узлов: с первого он получает список логинов и паролей, а второй необходим для работы SOCKS-прокси-сервера. Существуют сборки этого троянца для устройств с архитектурой x86, MIPS, MIPSEL, PowerPC, ARM, Superh, Motorola 68000 и SPARC. Иными словами, Linux.ProxyM может работать практически на любом устройстве под управлением Linux, включая роутеры, телевизионные приставки и другое оборудование.

Вирусные аналитики «Доктор Веб» выяснили, что с использованием Linux.ProxyM злоумышленники рассылают спам. С управляющего сервера на

зараженное устройство поступает команда, содержащая адрес SMTP-сервера, логин и пароль для доступа к нему, список почтовых адресов и сам шаблон сообщения. В письмах рекламируются различные сайты категории «для взрослых». Типичное сообщение электронной почты, отправляемое с использованием зараженных Linux.ProxyM устройств, имеет следующее содержание:

Subject: Kendra asked if you like hipster girls
A new girl is waiting to meet you.
And she is a hottie!
Go here to see if you want to date this hottie
(Copy and paste the link to your browser)
http://whi*******today.com/
check out sexy dating profiles
There are a LOT of hotties waiting to meet you if we are being honest!

Согласно статистике, имеющейся в распоряжении компании «Доктор Веб», в среднем в течение суток каждое зараженное Linux.ProxyM устройство рассылает порядка 400 писем.

Можно предположить, что ассортимент реализуемых Linux-троянцами функций будет расширяться и в дальнейшем. «Интернет вещей» уже давно находится в фокусе интересов вирусописателей, о чем свидетельствует широкое распространение вредоносных программ для Linux, способных заражать устройства с различной аппаратной архитектурой.

(вгору)

Додаток 15

13.09.2017

Північнокорейські хакери атакують біткоін-гаманці та біржі обміну криптовалют

Хакери з Північної Кореї почали атакувати обмінники криптовалют та індивідуальні біткоін-гаманці.

Про це йдеться у доповіді фірми FireEye, що займається інформаційною безпекою (Espreso.tv).

У 2017 році хакери організували щонайменше п’ять атак на ресурси, зокрема на південнокорейську біржу Yapizon.

В квітні зафіксували атаки на чотири гаманця південнокорейської біржі криптовалюти Yapizon. Однак невідомо, хто стояв за цими атаками через різні методи взломів.

Іншою жертвою хакерів міг стати найбільший обмінник ефіріума Bithumb, припускають журналісти TechCrunch. В червні через атаку він втратив понад $1 млн.

В FireEye вважають, що КНДР почала частіше красти криптовалюту через посилення санкцій щодо країни.

Крім того, через відсутність регулювання у більшості країн багато бірж і обмінники ніяк не борються з відмиванням грошей. Це дозволяє північнокорейським хакерам обмінювати криптовалюту на реальні гроші.

У FireEye також відзначили, що в більшості випадків хакери використовували звичайний фішинг. Вони надсилали електронні листи з вірусами співробітникам бірж. Завдяки цим вірусам хакери крали дані для доступу до гаманців.

За даними південнокорейської влади, елітна група хакерів може щорічно приносити Північній Кореї близько $860 млн від кібератак на організації інших країн.

13 вересня курс криптовалюти біткоін різко обвалився.

(вгору)

Додаток 16

14.09.2017

Миллиарды устройств с поддержкой Bluetooth уязвимы к атакам BlueBorne

Исследователи безопасности из компании Armis обнаружили восемь уязвимостей в реализациях Bluetooth, используемых более чем в 8 млрд. устройств по всему миру. Набор уязвимостей получил название BlueBorne (InternetUA).

По словам исследователей, для эксплуатации проблем злоумышленнику не требуется ни взаимодействие с пользователем, ни сопряжение с целевым устройством. Единственное, что необходимо – это включенный Bluetooth. Уязвимости содержатся в реализациях Bluetooth в Android, iOS, Windows и Linux, затрагивая практически все типы устройств, от смартфонов до IoT-гаджетов и «умных» автомобилей.

Три из восьми уязвимостей BlueBorne оцениваются как критические и позволяют злоумышленникам получить полный контроль над устройством, выполнить вредоносный код или осуществить атаку «человек посередине» (Man-in-the-Middle, MitM). По словам исследователей, ранее выявленные уязвимости в Bluetooth содержались в основном на различных уровнях протокола связи, однако BlueBorne затрагивает реализации протокола, минуя различные механизмы аутентификации, что позволяет получит полный контроль над целевым устройством.

Эксперты Armis проинформировали Apple, Google, Microsoft и сообщество Linux о данных уязвимостях. Разработчики уже готовят патчи, которые будут выпущены в скором времени. Корректирующие патчи будут недоступны для устаревших устройств, которые уже не поддерживаются производителем. По оценкам Armis, число таких устройств составляет 40% или более двух миллиардов по всему миру.

Уязвимости BlueBorne получили следующие идентификаторы: CVE-2017-0781, CVE-2017-0782, CVE-2017-0783 и CVE-2017-0785 (Android); CVE-2017-

1000251 и CVE-2017-1000250 (Linux); CVE-2017-8628 (Windows). Уязвимости, затрагивающие iOS, на данный момент не имеют идентификаторов. Уязвимости BlueBorne не затрагивают Android-устройства, использующие технологию Bluetooth Low Energy.

(вгору)

Додаток 17

14.09.2017
Малышко Д.
Касперский уходит из Вашингтона

Подозреваемая в пособничестве российским шпионам «Лаборатория Касперского» уходит их Вашингтона и открывает офисы в других городах США и Канады, пытаясь сделать хорошую мину при плохой игре – сообщает Fortune (InternetUA).

Проблема состоит в том, что правительственные агентства, фактически не могут пользоваться услугами «Лаборатории». Все это из-за опаски того, что в их системы в очередной раз проникнуть хакеры или вредоносные программы.

К примеру, недавно появились сообщения, утверждающие, что между Касперским и российской разведкой существуют тесные связи. Несколько недель назад Комитет Палаты представителей США по вопросам науки, космоса и технологии попросил 22 правительственных учреждения предоставить документы об их отношениях с «Лабораторией».

Подозрения, павшие на Касперского, даже привели к тому, что сеть электроники США Best Buy прекратила пополнять запасы антивирусного программного обеспечения этой компании.

Таким образом, компания теряет часть своих самых крупных клиентов. Однако, Касперский заявил, что планирует открыть три новых офиса в Северной Америке в следующем году – в Чикаго, Торонто и Лос-Анджелесе – «в рамках своей постоянной приверженности рынку». А вот продажи программного обеспечения для американского правительства не было такой уж большой прерогативой, – сообщили в компании.

Интересно, что в России не так давно арестовали главу отдела расследования компьютерных инцидентов «Лаборатории Касперского» Руслана Стоянова. Его подозревали в госизмене. В ответ на это Руслан, будучи под стражей, сумел опубликовать открытое письмо, в котором сообщил, что российские властные органы пытаются договориться с хакерами и другими кибер-преступниками. «Самый ужасный сценарий – дать киберпреступникам иммунитет от возмездия за кражу денег в других странах в обмен на разведданные», – написал он.

(вгору)

Додаток 18

19.09.2017

В Харькове задержан хакер-шпион, следивший за гражданами Украины

В Харькове правоохранители задержали хакера, который вмешивался в личную жизнь как граждан Украины и других государств, путем подключения к их персональным компьютерам на правах администратора. Об этом сообщает пресс-служба Национальной полиции Украины (InternetUA).

Так, оперативники Слободского управления киберполиции и спецагенты Департамента киберполиции Национальной полиции Украины, совместно с работниками Слободского отдела полиции Харьковской области под процессуальным руководством Харьковской местной прокуратуры № 5, разоблачили 23-летнего хакера, который использовал вредоносное программное обеспечение, незаконно вмешивался в компьютерные сети, как украинских пользователей интернет-сети, так и иностранных государств.

При документировании преступной деятельности хакера полицейские установили, что мужчина получал доступ к персональным компьютерам на правах администратора.

Отмечено, что во время санкционированного обыска квартиры злоумышленника в городе Харьков, полицейские изъяли его персональный компьютер, на жестком диске которого находилось вредоносное программное обеспечение.

В настоящее время рассматриваются различные версии и мотивы действий подозреваемого.

«Анализируя ту информацию, и те данные, которые мы обнаружили на его компьютере, мы рассматриваем несколько версий и мотивов совершения хакером преступления, в том числе заказного характера, поскольку среди "жертв" хакера также и члены украинских политических партий», – отметил руководитель отдела противодействия киберпреступности в Харьковской области Денис Коленик.

Злоумышленнику объявлено о подозрении в совершении двух уголовных преступлений предусмотренных ч.ч.1,2 ст.361 (несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей) УК Украины.

Подозреваемому грозит до шести лет лишения свободы с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

(вгору)

Додаток 19

20.09.2017

Популярный антивирус для Android тайно шпионил за пользователями

Google удалила, а затем снова вернула в магазин Google Play один из самых популярных мобильных антивирусов. Компании пришлось удалить приложение DU Antivirus Security от DU Group (является частью китайского конгломерата Baidu), поскольку, по словам исследователей из Check Point, оно втайне от пользователей собирало данные с их смартфонов. Антивирус был скачан и установлен от 10 млн до 50 млн раз (InternetUA).

Как сообщили эксперты Check Point, когда пользователь впервые запускал DU Antivirus Security, приложение записывало уникальные идентификаторы устройства, список контактов, журнал звонков и геолокационные данные (если возможно). Затем в зашифрованном виде данные передавались на удаленный сервер с IP-адресом 47.88.174.218. Поначалу исследователи решили, что сервер контролируется операторами вредоносного ПО. Тем не менее, как показало изучение записей DNS и примыкающих поддоменов, размещенные на сервере домены зарегистрированы на сотрудника Baidu.

Собранная антивирусом информация затем использовалась другим приложением от DU Group под названием Caller ID & Call Block – DU Caller, предоставляющим пользователям данные о входящих звонках. 21 августа текущего года представители Check Point уведомили Google о неприемлемой активности антивируса, и 24 августа DU Antivirus Security был удален из Google Play. Производитель удалил из приложения часть кода, ответственную за сбор данных, и спустя несколько дней антивирус снова появился в магазине.

По словам исследователей, механизм сбора информации присутствует в DU Antivirus Security v3.1.5 и, возможно, в более ранних версиях (в Check Point не тестировали более ранние версии).

Эксперты решили проанализировать на наличие данного кода и другие приложения. В общей сложности они обнаружили его в 30 программах, 12 из которых опубликованы в Google Play. Как пояснили исследователи, разработчики могли реализовать вредоносный код в качестве внешней библиотеки, отправляющей собранные данные на тот же используемый DU Caller удаленный сервер. Вредоносные приложения, втайне собирающие данные пользователей, могли установить от 24 млн до 89 млн человек.

(вгору)

Додаток 20

20.09.2017

Незадокументированная функция MS Office позволяет собирать данные о пользователях

Эксперты «Лаборатории Касперского» обнаружили в пакете MS Office незадокументированную функцию, использование которой позволяет злоумышленникам собирать данные о целевой системе путем простой отправки жертве специально сформированного документа Microsoft Word, причем без

активного контента: VBA-макросов, встроенных объектов Flash или PE-файлов. Функция присутствует в версии Microsoft Word для Windows, а также мобильных версиях Microsoft Office для iOS и Android. LibreOffice и OpenOffice ее не поддерживают (InternetUA).

По словам исследователей, функционал уже эксплуатируется злоумышленниками в рамках многоэтапной атаки Freakyshelly, первая стадия которой предусматривает сбор данных о целевой системе. В ходе исследования данной атаки эксперты обнаружили фишинговую рассылку, содержавшую довольно интересные вложения в виде файлов в формате OLE2, которые не содержали ни макросов, ни эксплоитов, ни какого-либо другого активного контента. При ближайшем рассмотрении выяснилось, что файлы включали ряд ссылок на PHP-скрипты, расположенные на сторонних ресурсах. При попытке открыть файлы в MS Word, приложение отправляло GET-запрос по одной из ссылок, в результате злоумышленники получали данные об установленном на системе программном обеспечении.

В ходе анализа документа специалисты выявили поле INCLUDEPICTURE, сообщающее о том, что к определенным символам в тексте привязана картинка, однако атакующие использовали его для размещения подозрительной ссылки. Проблема заключается в том, что в документации Microsoft описание поля INCLUDEPICTURE практически отсутствует. В стандарте ECMA-376 описана только часть поля INCLUDEPICTURE до байта-разделителя и нет информации о том, что значатданные после него, и как их можно интерпретировать, отметили эксперты.

(вгору)

Додаток 21

18.09.2017

Сергей Решодько

Антон Коков, E-COM: «Опасность кибервойны у нас недооценивают»

Директор департамента по развитию сервисов е-документооборота E-COM, о халатном отношении в Украине к кибербезопасности, потерях компаний, связанных с атакой вируса Petya.A, а также, почему во время атаки выстояли сервисы E-COM (ITnews).

Что произошло в Украине 27 июня, и как это сказалось на системе электронного документооборота в целом?

Нарушение киберпространства Украины, которое произошло 27 июня, – не что иное, как часть информационной войны, которая идет сейчас во всем мире. На мой взгляд, учитывая геополитическую ситуацию нашей страны, рано или поздно подобное стоило ожидать. Удивляет другое – явную опасность кибервойны и ее последствий у нас почему-то недооценивают. Отсюда и

уровень кибернетической безграмотности и даже некое халатное отношение к вопросам безопасности, как на государственном, так и частном уровнях.

Безусловно, вирусная атака 27 июня не могла не повлиять на доверие к работе с программным обеспечением по электронному документообороту. Только сейчас пришло сознание того, что вопрос безопасности — так же важен, как и вопросы функционала сервисов е-документооборота. И это несмотря на то, что априори он должен стоять на первом месте.

Подверглась ли атаке ваша компания и/или сервисы/часть сервисов, которые она представляет?

Во время вирусных атак компания «Э-КОМ» и пользователи онлайн сервиса электронного документооборота E-DOC были только зрителями событий: работая в штатном режиме, мы обеспечивали клиентам беспрепятственный доступ ко всем нашим сервисам на EDI-платформе EXITE-EVOLUTION. Пользователи E-DOC без проблем регистрировали налоговые накладные, без перебоев сдавали отчетность в госорганы, обменивались документами с партнерами.

За счет чего удалось, скажем, так, выстоять (каких решений защиты)?

Как бы банально это не звучало, но надлежащий уровень защиты данных наших клиентов всегда стояли в приоритете работы нашей компании. К этому вопросу специалисты E-COM подошли с максимальной скрупулезностью. Из года в год мы работали над усовершенствованием уровня безопасности платформы электронного документооборота EXITE-EVOLUTION, в результате чего и выработали некий иммунитет к вирусным угрозам. Так, по версии ImmuniWeb безопасность нашей технологической платформы находится на наивысшим уровне защиты A+, который соответствует международному стандарту PCI DSS, используемый платежными системами MasterCard и Visa. Все данные зашифрованы самым надежным сертификатом SSL (Secure Sockets Layer) уровня EV (Extended Validation), издателем которого является компания по защите от киберугроз – Symantec. Кроме того, их дополнительную защиту обеспечивает облачное хранение и резервное копирование в трех дата-центрах.

Во-вторых, следует понимать механизм распространения данного вируса. Как выяснили специалисты киберполиции, заражение компьютера происходило при загрузке «исполняемого файла» с расширением *.exe. Далее осуществлялось обновление и активация вируса. Так вот, в отличие от ПО, для которых периодично нужно загружать обновления на свой ПК, архитектура программного обеспечения, к примеру, нашего сервиса E-DOC, не требует обновлений через загрузку исполняемых файлов.

Киберполиция и, соответственно, ряд СМИ указывают на то, что вирус Petya.A был разработан в России и распространен через компанию M.E.Doc. В то же время в самой M.E.Doc все это называют «неправдивой информацией» и «заказной компанией» против них. Как бы вы прокомментировали все это?

Все вопросы, связанные с происхождением вируса Petya.A и его распространением, – это полномочия киберполиции, органов следствия и СБУ.

Как и все, мы следим за новостями, доверяем только официальным источникам, анализируем информацию и делаем свои выводы.

Что отличает вашу компанию/сервисы от других игроков на этом рынке Украины?

Компания «Э-КОМ» является международным провайдером с 11-летним опытом работы в сфере электронного юридически значимого документооборота. Онлайн сервис E-DOC – наше универсальное и комплексное решение, которое подходит всем: как предпринимателям, так и крупному бизнесу, независимо от системы налогообложения. При этом учитывает все индивидуальные особенности каждого, в том числе возможность интегрироваться в любую учетную систему. На сегодняшний день общее количество пользователей сервиса составляет более 4000, и эта цифра растет с каждым днем. С E-DOC просто, удобно и самое главное — безопасно. В этом уже убедились такие крупные лидеры, как Киевский ЦУМ, МетИнвест, IT-компания Playtech, почтово-логистический оператор Meest Express, Райффайзен Банк Аваль, RedBull Украина, сетевой оператор ТРЦ Arricano и многие другие.

На ваш взгляд, возможна ли следующая такая атака и есть ли эффективные средства защиты, если говорить, исходя из опыта защиты от Petya.A?

По моему мнению, нужно адекватно оценить ситуацию и не ждать следующей атаки для того, чтобы обезопасить себя и защитить свой бизнес сегодня. К счастью, у каждого есть выбор: бояться дальше, надеясь на то, что кибератаки больше никогда не повторятся или что-то менять уже сейчас, выбрав альтернативный безопасный сервис, который выстоял во время «бомбежки Петей» и имеет надежный щит от возможных наступлений его аналогов.

(вгору)

Додаток 22

23.09.2017

Хакеры требуют выкуп у тысяч компаний, угрожая DDoS-атаками

Хакерская группировка Phantom Squad организовала массовую спам-кампанию, направленную на тысячи организаций по всему миру. В письмах злоумышленники угрожают 30 сентября нынешнего года осуществить DDoS-атаку на сайты компаний, если те не выплатят выкуп в размере 0,2 биткойна (приблизительно $720) (InternetUA).

Первым фишинговые письма заметил исследователь безопасности Деррик Фармер (Derrick Farmer). Спам-рассылка началась 19 сентября текущего года и продолжается до сих пор.

Эксперты отмечают необычайный размах кампании. Как правило, подобные письма с угрозами рассылаются небольшому числу компаний с тем, чтобы осуществить DDoS-атаку в случае, если организация откажется выплатить требуемую сумму. Поскольку в данном случае имеет место массовая

рассылка, ряд экспертов считает, что Phantom Squad не обладает достаточными мощностями для проведения такого количества DDoS-атак в один день и, скорее всего, использует тактику запугивания.

Тем не менее, инцидент получил широкую огласку в социальных сетях и на форумах web-мастеров. По словам исследователей безопасности из подразделения Trust&Safety компании Cloudflare, как минимум 5 клиентов сообщили о вымогательских письмах. Злоумышленники даже умудрились послать письмо с угрозами компании, занимающейся защитой клиентов от DDoS-атак.

Как отметил исследователь безопасности из компании Radware Дэниэл Смит (Daniel Smith), вымогатели могут быть лишь подражателями Phantom Squad - хакерской группировки, осуществившей серию DDoS-атак на игровые сервисы зимой 2015 года. Смит также отметил, что письмо практически идентично использовавшемуся кибергруппировкой Armada Collective в июне 2017 года.

Эксперты также отметили сравнительно низкую сумму выкупа. Ранее группа злоумышленников, известная как Anonymous, шантажировала подобным образом несколько банков, требуя в качестве выкупа 100 биткойнов.

(вгору)

Додаток 23

24.09.2017

Хакер взломал сотни компаний через уязвимости на сайтах служб техподдержки

Независимый исследователь безопасности Инти Де Кекелайре (Inti De Ceukelaire) обнаружил уязвимость, позволяющую получить доступ к внутренним коммуникациям компаний. Эксплуатируя данную уязвимость, злоумышленники могут получить доступ к внутренним сетям организации, учетным записям в соцсетях и службам поддержки в корпоративных сетях Yammer и Slack. Об этом исследователь сообщил в своем блоге (InternetUA).

Популярные инструменты бизнес-коммуникации, такие как Slack, Yammer и Facebook Workplace осуществляют авторизацию сотрудников компании через адрес корпоративной электронной почты (например, "@имя_компании"). Как только сотрудник нажимает ссылку подтверждения, отправленную на внутренний адрес электронной почты, он получает доступ к внутренним коммуникациям компании.

Сотрудник может получить приглашение для авторизации в корпоротивной учетной записи двумя способами. Администратор может вручную отправить приглашение по электронной почте или разрешить пользователю, у которого есть адрес электронной почты с одобренным доменным именем, создавать собственные учетные записи. В первом случае, злоумышленник может получить доступ к рабочему пространству Slack, получив доступ к учетной записи администратора, либо в результате ошибки

администратора. Во втором случае преступнику потребуется создать учетную запись электронной почты с доменным именем компании.

Как выяснилось, получить корпоративную почту не так сложно, как кажется. Де Кекелайре создал проект на Gitlab и получил уникальный электронный адрес @gitlab.com. Заметив, что Slack автоматически проверяет только доменное имя, он использовал электронный адрес, чтобы успешно зарегистрироваться в учетной записи Slack, принадлежащей одной из компаний-разработчиков. В службах поддержки наподобие Slack и Yammer отсутствуют механизмы проверки пользователя, то есть, если компания использует свое доменное имя для авторизации, но не проверяет пользователя, служба поддержки будет считать, что это подтвержденный электронный адрес сотрудника компании.

Подобным образом хакеру также удалось получить доступ к порталу Vimeo и создать учетную запись на странице поддержки команды Slack Vimeo. Исследователь сообщил Vimeo о проблеме, и компания выплатила ему вознаграждение в размере $2 тыс.

Ранее Де Кекелайре выявил новый метод, позволяющий получить доступ к скрытым мобильным номерам пользователей Facebook.

Slack – корпоративный мессенджер, который по состоянию на июнь 2015 года ежедневно использовали 1,1 миллиона пользователей.

Yammer – компания, занимающаяся поддержкой и развитием одноименной службы корпоративных социальных сетей на основе условно-бесплатной модели, выкуплена Microsoft в 2012 году.

(вгору)

Додаток 24

21.09.2017

Правообладатели пролоббировали запрет на копирование авторского контента в интернете

Сторонники авторского права в Сети одержали крупную победу: всемирный консорциум по стандартизации объявил использование автоматических средств защиты от копирования в интернете официальной рекомендацией (InternetUA).

Официально и настоятельно рекомендуем

Консорциум Всемирной паутины (World Wide Web Consortium – W3C), авторитетный, но неформальный орган, занимающийся выработкой добровольно используемых стандартов в Сети, объявил «официально рекомендованным» применение средств цифрового управления правами на интеллектуальную собственность (Digital Rights Management — DRM). Под DRM подразумеваются технические решения, которые ограничивают либо затрудняют просмотр и копирование контента, если у пользователя нет на это прав.

Конкретнее в документе W3C речь идет о разновидности DRM под названием «Расширения для шифрованных медиаресурсов» Encrypted Media Extensions (EME) – спецификации для технической копирайтной защиты веб-сайтов. Технологию EME активно лоббировали Netflix, Microsoft, Google и другие крупные правообладатли. Она призвана предотвратить нелицензионное копирование, сохранение и распространение пользователями копий фильмов и другого развлекательного контента без разрешения правообладателей.

В ходе голосования 58,4 % членов W3C подали голоса «за», 30,8 % высказались против EME, остальные воздержались.

Битва лидеров

Голосованию предшествовали месяцы яростных споров, которые не заканчиваются и теперь. Крупные правообладатели активно поддерживали введение EME как официальной рекомендации, и на их стороне неожиданно выступил Тим Бернерс-Ли, создатель HTTP, HTML и Всемирной паутины как таковой.

При этом он заявил, что W3C не является «ни Конгрессом США, ни Всемирной организацией по интеллектуальной собственности, ни судом», и представляет собой лишь «место, где люди собираются на обсуждения и вырабатывают консенсус по поводу лучших новый технологий для Сети». Бернерс-Ли отметил также, что хотя и существует расхожее убеждение, будто W3C обязан выступать против DRM в любом случае, сам по себе Консорциум обладает весьма ограниченными полномочиями.

Со своей стороны, однако, Бернерс-Ли заметил, что EME обеспечит улучшение взаимодействия и ограничит количество данных, производимых использованием контента, что позитивно скажется на приватности.

Комментарии экспертов

Против EME ожидаемым образом выступали сторонники открытого интернета, в первую очередь, Фонд электронного фронтира и сочувствующие. Ключевые претензии сводились к тому, что технология EME не обеспечивает достаточной защиты самим пользователям, плохо совместима с открытым (свободным) ПО и не обеспечивает юридической защиты исследователям безопасности, то есть, фактически, выводит их работу за рамки правового поля, когда им приходится обходить DRM-защиту.

В своем открытом письме лидерам W3C представитель Фонда электронного фронтира Кори Доктороу заявил, что интересы бизнеса стали важнее, чем технологии. «Где-то по дороге бизнес-ценности тех, кто находится вне Сети стали достаточно важными, а ценностями технологов, кто построил Сеть, стало возможным пренебрегать, настолько, что даже мудрые старейшины, определяющие наши стандарты, проголосовали за нечто, что, как они сами понимают, является пустой затеей», – написал Доктороу.

(вгору)

Додаток 25

21.09.2017

Раскрыта хакерская схема кражи денег по номеру телефона

Хакеры способны украсть деньги с электронных кошельков, используя уязвимость мобильных сетей. Об этом говорится в исследовании компании Positive Technologies (InternetUA).

Согласно эксперименту инженеров Positive Technologies, преступники могут установить адрес электронной почты держателя любого кошелька на самой крупной криптобирже, перехватив смс с одноразовым кодом. Затем злоумышленники меняют пароли от почты, связанной с кошельком, и получают доступ к средствам.

Такой тип кибератак возможен из-за недостатка в протоколе системы сигнализации SS7. Он разработан в 1975 году, и до сих пор используется большинством телефонных сетей мира. Весной 2017 года в Германии были совершены первые похищения денег через брешь SS7. Хакеры получили пароли пользователей мобильного банкинга, отправленные сотовым оператором Telefonica Germany.

Из-за уязвимости SS7 жертва может не подозревать о совершаемой атаке и не иметь возможности отменить транзакции. Но мобильные операторы утверждают, что отказ от смс-рассылки одноразовых паролей пока невозможен. Это самая понятная клиентам система двухфакторной идентификации: остается лишь чаще менять пароли для почты и приложений, придумывая все более сложные комбинации.

Держатели криптовалют могут обезопасить себя, используя биржи для обмена, но не для хранения средств, как в классическом банке. Вернуть украденные виртуальные деньги по-прежнему нельзя, а из-за полулегального статуса любая криптобиржа может неожиданно уйти в офлайн и не вернуться.

(вгору)

Додаток 26

24.09.2017

Популярная Android-клавиатура шпионит за пользователями

Как сообщают исследователи из Adguard, популярная клавиатура GO Keyboard шпионит за пользователями. Созданное китайскими разработчиками GOMO Dev Team приложение передает персональные данные пользователей на удаленный сервер, а также «использует запрещенную технику для загрузки опасного исполняемого кода», заявили эксперты (InternetUA).

Исследователи сделали свое открытие в ходе анализа потребления трафика и нежелательного поведения различных клавиатур для Android. С помощью инструмента AdGuard for Android app, позволяющего видеть, какой именно трафик генерируется приложением, эксперты обнаружили, что GO Keyboard осуществляет подозрительные подключения, использует трекеры и передает персональную информацию.

Согласно описанию GO Keyboard в Google Play, приложение не собирает персональные данные. Тем не менее, по словам исследователей, клавиатура начинает отправлять данные пользователя сразу же после инсталляции, подключается к десяткам отслеживающих сервисов и имеет доступ к хранящейся на устройстве конфиденциальной информации. Подобное поведение весьма распространено среди современных мобильных приложений, однако оно нарушает политику конфиденциальности Google Play.

«Без явного согласия пользователя GO Keyboard передает на свои серверы электронный адрес, привязанный к вашей учетной записи Google, а также выбранный язык, IMSI, местоположение, тип сети, размер экрана, версию Android, модель устройства и т.д.», – сообщили исследователи.

Помимо всего вышеперечисленного, GO Keyboard загружает со своих серверов код, идентифицируемый многими антивирусными решениями как рекламное или потенциально нежелательное ПО.

(вгору)

Додаток 27

24.09.2017

Эксперты вынудили АНБ отказаться от двух методов шифрования

Международная группа экспертов по криптографии вынудила Агентство национальной безопасности США отказаться от двух методов шифрования, известных как Simon и Speck, которые спецслужба предлагала установить в качестве международных стандартов. Как полагают эксперты из разных стран, включая Германию, Японию и Израиль, АНБ продвигает новые методы не по причине их эффективности, а потому, что знает как их взломать. Об этом сообщает Reuters со ссылкой на оказавшиеся в распоряжении агентства электронные письма и сообщения экспертов (InternetUA).

АНБ согласилась отказаться от данных алгоритмов, за исключением наиболее защищенных от взлома версий. Делегация США по вопросам шифрования в Международной организации по стандартизации (International Organization for Standardization, ISO) включает в себя несколько должностных лиц АНБ, хотя контролируется Американским национальным институтом стандартов (American national standards institute, ANSI).

Откровения бывшего подрядчика АНБ Эдварда Сноудена о попытках агентства манипулировать принятием стандартов шифрования вызвали подозрения касательно мотивов делегации США. По словам некоторых делегатов из других стран, большая часть скептицизма связана с 2000-ми годами, когда эксперты АНБ разработали метод шифрования Dual Elliptic Curve, который был принят в качестве мирового стандарта. Согласно документам, обнародованным Сноуденом, внутри агентства это считалось успехом.

Как пояснили представители АНБ, новые инструменты шифрования были разработаны для защиты правительственного компьютерного и коммуникационного оборудования без потери вычислительной мощности.

На сегодняшний день ISO дважды проголосовала за то, чтобы отложить процесс утверждения алгоритмов Simon и Speck.

(вгору)

Додаток 28

25.09.2017
Дмитрий Малышко
Ян Леви: Грядет кибератака невиданной силы

Западный мир готовится к самой мощной за свою историю кибератаке. Вот только антивирусы и фаерволы не способны удержать злоумышленников. Всю надежду эксперты возлагают на простых работников, – сообщает The Guardian (InternetUA).

«Самая мощная из всех возможных кибератак, кибератака «первой категории» произойдет в ближайшие несколько лет» – сообщает Национальный центр кибербезопасности (NCSC) Великобритании.

В своем докладе, направленному Центру правительственной связи, эксперты по кибербезопасности призвали правительство принять меры, чтобы защититься от злоумышленников.

NCSC был основан в 2016 году и год своего существования он насчитал 500 хакерских атак, из них 470-ти была присвоена третья категория и 30-ти – вторая категория. К последней принадлежит вирус-«червь» WannaCry, уничтоживший данные в нескольких фондах и департаментах Национальной службы здравоохранения (NHS).

Технический директор Национального центра кибербезопасности Ян Леви считает, что в ближайшее десятилетие произойдет самая мощная кибератака – атака первой категории – и единственный способ предотвратить ее – это изменить представление бизнеса и правительства о кибербезопасности.

Вместо того чтобы скупать антивирусный софт и выстраивать вокруг себя фаерволы, организации должны переосмыслить, какой информацией они владеют, какую ценность она несет и насколько большой бедой будет потерять ее, – считает Леви.

Выступая на встрече, организованной Symantec – американской компанией, производящей программы в сфере кибербезопасности, – Леви вспомнил о том, как хакеры взломали базу данных бюро кредитных историй Equifax в мае этого года. Киберпреспутники выкрали более 130 млн. различных личных данных американцев, включая имена, адреса, номера социального страхования и даты рождения – всю информацию, необходимую для кражи личности в Интернете.

Ян Леви считает, что путь к спасению от хакеров – в переосмыслении отношения к персоналу.

«Эксперты в сфере кибербезопасности 25 лет говорили нам, что люди – это слабейшее звено. Это глупость!» – заявил он.

Проблема состоит в том, что компьютерные системы создаются техниками для техников. И потому простые работники практически ничем не могут помочь в плане кибербезопасности, в то время как хакеры хорошо осведомлены о том, как работают программы. Леви же считает, что надо не искать готовых решений, покупая софт, а общаться с работниками и выявлять, что они могут сделать для безопасности компании.

(вгору)

Додаток 29

25.09.2017

Платные антивирусы признаны бесполезными в современном мире

Эксперт популярного ресурса Mashable рассказал, почему среднестатистические пользователи интернета могут отказаться от антивирусных программ. Джек Морес считает, что время платных сервисов Avast, «Лаборатории Касперского», «Доктор Веб» и их аналогов безвозвратно уходит (InternetUA).

Как отмечает Морес, в то время как многие антивирусные сервисы предлагают платные программы для защиты компьютера, пользователи легко могут воспользоваться бесплатными приложениями, встроенными в операционную систему. Например, владельцы устройств с Windows могут выбрать программу Windows Defender.

«Windows Defender – это защита от вредоносных программ, которая уже встроена в Windows. Это программное обеспечение помогает идентифицировать и удалять вирусы, программы-шпионы и другое вредоносное ПО», – отмечают представители Microsoft.

Различные антивирусные программы, установленные на один компьютер, могут конфликтовать друг с другом. Таким образом, если пользователь хочет установиться платное приложение, ему стоит удалить Windows Defender.

Компания Apple также предлагает владельцам Mac встроенную защиту от вирусов и троянов.

«Gatekeeper блокирует приложения, созданные разработчиками вредоносных программ. Если разработчик приложения не идентифицирован, то программа защитит компьютер, запретив установку файла», – сказано на сайте «яблочной» компании.

Эксперты подчеркивают, что встроенные средства безопасности в Windows или macOS не могут защитить компьютеры от всех киберугроз. Однако вместо покупки дорогостоящих решений, можно воспользоваться бесплатными предложениями. Например, Kaspersky Free «автоматически блокирует опасные загрузки и предупреждает о вредоносных веб-сайтах».

При этом специалисты советуют корпоративным пользователям не отказываться от покупки единых платформ для защиты компьютеров.

(вгору)

Додаток 30

26.09.2017
Дмитрий Малышко
Лидер в сфере кибербезопасности «Deloitte» стал жертвой хакеров

В марте и мае этого года хакеры осуществили атаку на консалтинговую компанию «Deloitte», являющуюся лидером в сфере кибербезопасности, и похитили конфиденциальную информацию миллионов американцев. Однако сама компания долго держала взлом в секрете из-за того, что тема – слишком «щекотливая», – сообщает Guardian (InternetUA).

«Deloitte» зарегистрированная в Лондоне, а ее главная штаб-квартира находится в Нью-Йорке. Компания предоставляет аудиторские, налоговые консультации и консультации по кибербезопасности некоторым из крупнейших мировых компаний. Среди ее клиентов банки, международные корпорации, мировые СМИ, фармацевтические гиганты и государственные учреждения.

Предприятия и правительственные учреждения обменивались с Deloitte важной информацией посредством электронной почты, которая и стала целью хакеров в марте и мае этого года. Злоумышленники смогли скомпрометировать электронный адрес Deloitte через «учетную запись администратора». Взломать ее было проще простого, ведь учетная запись затребовала только один пароль и не имела «двухэтапной» проверки.

Ворвавшись в «электронку», хакеры получили потенциальный доступ к именам пользователей, паролям, IP-адресам, архитектурным диаграммам для бизнеса и медицинской информации. В некоторых письмах были вложения с конфиденциальной информацией о безопасности и дизайне.

Есть подозрения, что в следствии кибератаки в марте и мае были украдены данные 143 млн. американцев и 400 тыс. британцев.

По данным Guardian, Deloitte обнаружила взлом в марте этого года, но есть причины полагать, что злоумышленники имели доступ к ее системам с октября или ноября 2016 года. Однако огласка взлома была бы настолько щекотливой, а последствия настолько значительными, что только ключевые партнеры были осведомлены о ней.

5 миллионов электронных писем из переписки, которую вели 244 000 сотрудников Deloitte, хранятся в облачном сервисе Azure от Microsoft. Это эквивалент веб-службы Amazon и облачной платформы Google.

По всей видимости, атака была нацелена на американские компании. На данный момент, по крайней мере, шесть компаний-клиентов сообщили о том, что их информация была украдена.

На данный момент, не ясно, кто «хакнул» почту и по чьему заказу. Сейчас эксперты пытаются определить путь, по которому пришли хакеры. Компания наняла юридическую контору Хогана Ловелла, чтобы та оценила так называемый «случай нарушения кибербезопасности». Также над

круглосуточным обеспечением безопасности клиентов работают эксперты из отдела кибер-расследований самой компании Deloitte .

«Мы по-прежнему глубоко убеждены в том, что наша защита кибербезопасности лучшая в своей роде», – говорят в корпорации.

(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.