

**СОЦІАЛЬНІ МЕРЕЖІ
ЯК ЧИННИК
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

*Огляд інтернет-ресурсів
(21.06–4.07)*

2018 № 13

Соціальні мережі як чинник інформаційної безпеки

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

Огляд інтернет-ресурсів
(21.06–4.07)

№ 13

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

© Національна бібліотека України
імені В. І. Вернадського, 2018

Київ 2018

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ.....	4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА.....	10
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ	13
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ.....	17
Інформаційно-психологічний вплив мережевого спілкування на особистість.....	17
Маніпулятивні технології	18
Спецслужби і технології «соціального контролю»	19
Проблема захисту даних. DDOS та вірусні атаки	25
ДОДАТКИ	32

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

21.06.2018

Майя Яровая

Instagram перешагнув отметку в 1 млрд пользователей и представил вертикальные видео до 60 минут

20 июня на презентации в Сан-Франциско Instagram представил новый сервис IGTV – это раздел с 60-минутными видеороликами, которые могут создавать сами пользователи. Также компания объявила, что Instagram перешагнув отметку в 1 млрд пользователей (AIN.UA).

IGTV – это отдельное приложение, в котором пользователи могут записывать свои ролики, а также подписываться на любимых креаторов и смотреть их вертикальные видео. Просмотр IGTV доступен и в родном приложении Instagram, в специальном разделе. В отличие от стандартных видео в Instagram, ролики в IGTV не ограничены минутой и могут длиться до часа.

Проигрываются ролики в IGTV автоматически. В приложении, помимо подписок, также есть персонализированные рекомендации, раздел с популярными видео, возможность комментировать, лайкать и присылать видео в директ. А еще в IGTV у креаторов есть каналы, наподобие YouTube.

IGTV станет доступен во всем мире в ближайшие несколько недель на Android и iOS. Уже сегодня в сервисе появились первые каналы таких селебрити, как певица Селена Гомез и арт-директор Louis Vuitton Вирджил Абло.

22.06.2018

Facebook запустила тестирование платных подписок на группы

Facebook в тестовом режиме разрешила администраторам групп создавать платные подписки. За плату пользователи получают доступ к эксклюзивному контенту, консультациям и советам от администраторов, а также специальные отметки для профилей участников. Стоимость подписок варьируется от \$5 до \$30, комиссию Facebook пока не берёт (IGate).

Одна из групп, получивших доступ к новой функции – Declutter My Home. В ней публикуют чеклисты, учебные пособия, онлайн-трансляции по обустройству дома.

До появления функции администраторы платных проектов были вынуждены создавать две отдельные страницы: открытую для всех и закрытую для оплативших подписку, а деньги принимать через сторонние сервисы вроде PayPal.

Facebook и ранее пыталась стимулировать создание контента на платформе с помощью подписок. В марте 2018 года социальная сеть начала тестировать подписку на видеоблогеров. В обмен на \$5 пользователи получали эксклюзивный контент и значок о поддержке в профиле. В июне 2018 года Facebook объявила о расширении функции для большего числа создателей контента.

24.06.2018

40 % пользователей за год удалили аккаунт хотя бы в одной социальной сети

Согласно исследованию, которое провело маркетинговое агентство Edelman, около 40 % пользователей за последний год удалили свой аккаунт хотя бы в одной из социальных сетей.

[Докладніше](#)

26.06.2018

Instagram возглавил рейтинг «самых любимых брендов»

NetBase проводит уже четвертое по счету ежегодное исследование. В этот раз лидером стал Instagram. Соцсеть находится на первом месте. Соответственно, пользователи больше всего любят именно этот продукт ([IGate](#)).

На втором месте оказался YouTube. Третье, четвертое и пятое место заняли Facebook, Amazon и Google соответственно. Затем следует Apple, а замыкают первую десятку Disney, Snapchat, Spotify и Netflix.

Сотрудники NetBase использовали большой набор инструментов для анализа данных в 16 странах мира.

«Бренды в нашем ТОП-100 демонстрируют множество новых и старых брендов, которые успешно взаимодействуют с аудиторией и привлекают их внимание. Неудивительно, что на первом месте обосновалась соцсеть. Подобные продукты умеют зацепить аудиторию и длительное время удерживать», – прокомментировал рейтинг маркетолог NetBase Пэйдж Лейди.

Ранее Apple заняла второе место в рейтинге самых дорогих брендов по версии BrandZ.

26.06.2018

Google запустила соцсеть для соседей, чтобы решать локальные вопросы

В ней можно задавать вопросы и самому помогать с ответами ([Телекритика](#)).

Теперь не обязательно из-за каждой мелочи бежать в Facebook и раздражать друзей своими вечными вопросами. Для этого компания Google запустила собственную локальную социальную сеть для соседей по району Neighbourly.

Соцсеть позволяет задавать соседям вопросы и отвечать на чужие. Пользователи могут оценивать ответы своих соседей, при этом комментарии с высокой оценкой показываются в ленте выше. Нужные вопросы и ответы можно добавлять в закладки.

Также приложение позволяет не делиться личной информацией с другими: оно показывает пользователям только имена. Более того, Neighborly поддерживает голосовой ввод запросов.

26.06.2018

Instagram почти догнала Facebook по времени, которое пользователи проводят в приложении

Если стагнация Facebook продолжится, компании придётся полагаться на рост аудитории Instagram, считает Recode ([IGate](#)).

В июне 2018 года пользователи Android-приложения Instagram в США проводили в нём почти столько же времени в день, сколько в Facebook. Об этом говорится в исследовании аналитической компании Similar Web.

В среднем пользователи Instagram тратили по 53,2 минуты в день на Android-приложение – на пять минут меньше, чем пользователи Facebook. В среднем пользователи Snapchat тратили примерно по 49,5 минут на приложение.

Facebook купила Instagram в 2012 году, однако в скором времени компании придётся рассчитывать в основном на рост пользователей фотосервиса из-за стагнации основного приложения компании, считают журналисты Recode.

Ещё в 2017 году Snapchat немного опережал Instagram, однако активная аудитория фотосервиса с тех пор выросла, отмечает издание.

Проведённое в приложениях время в том числе отображает рост количества просмотренной пользователями рекламы, уточняет Recode, – поэтому показатель важен для соцсетей.

26.06.2018

В Telegram теперь можно узнать, что мессенджер знает о вас

Telegram для настольных компьютеров обновился до стабильной версии 1.3.8. И этот апдейт привнёс одно важное нововведение ([InternetUA](#)).

Помимо исправления багов разработчики добавили функцию для загрузки всех имеющихся о вас данных в Telegram. Это необходимо для

полного соответствия правилам GDPR – нового европейского регламента по защите данных.

Так что теперь юзеры смогут свободно скачать/экспортировать все данные, которые есть на вас у Telegram.

На момент написания статьи обновление доступно только владельцам Windows-ПК и Mac в виде отдельных файлов. Ждём, когда команда мессенджера выпустит апдейт и в App Store. Загрузить актуальную версию можно с GitHub.

27.06.2018

Всесильный Facebook: соцсеть готова предсказать, когда вы поженитесь и когда умрете

Несмотря на заявления владельца и руководителя Facebook Марка Цукерберга в Конгрессе США и Европарламенте о том, что все данные компания будет собирать только с разрешения пользователей, а процедура будет прозрачной, некоторые патенты этой социальной сети, обнаруженные The New York Times, порождают много вопросов.

[Докладніше](#)

2.07.2018

WhatsApp представил каналы по аналогии с Telegram

Принадлежащий Facebook мессенджер WhatsApp рассказал о внедрении функции Broadcast Only для групповых чатов в последней версии своего приложения. Она запрещает отправлять сообщения в группу всем её участникам, кроме администраторов. В компании отметили, что функция стала доступна для пользователей по всему миру начиная с 29 июня ([IGate](#)).

«Пользователи уже используют группы для получения важной информации – например, педагоги отправляют родителям учеников новости об учебном процессе, некоммерческие организации и региональные центры рассказывают о своей работе. С новой функциональностью делать это будет проще», – объяснили в WhatsApp.

В Telegram каналы используются в качестве микроблогов. Их может создать любой пользователь мессенджера и публиковать там все, что вздумается. Будь то изображения, файлы, музыка или какие-то новости. Функцию активно используют различные бренды, разработчики приложений, СММ крупных компаний и так далее. Каналы считаются одной из ключевых функций мессенджера.

2.07.2018

Instagram добавил музыку в Stories

Новая функция позволит юзерам добавить музыку с помощью музыкального стикера, который появится рядом с другими опциями, такими как GIF, местоположение и другие. В библиотеке приложения есть тысячи песен и пользователи могут предварительно прослушать песню, прежде чем добавлять ее в свой пост. На iOS пользователи могут выбрать песню прежде чем сделать фото или видео. Вскоре функция появится и в Android. После выбора песни инструмент позволит выбрать, какую ее часть вы хотите проиграть во время истории ([Marketing Media Review](#)).

3.07.2018

В LinkedIn теперь можно переводить публикации более чем на 60 языков

В LinkedIn появилась возможность переводить публикации других пользователей на родной язык. Сервис учитывает целый ряд вещей, включая установленный по умолчанию язык и текущую страну. Если социальная сеть обнаружит в ленте публикацию на иностранном языке, то предложит её перевести ([InternetUA](#)).

За перевод отвечает API анализа текста Microsoft и Azure Cognitive Service. На базе них работают переводы и в других сервисах и приложениях компании, включая Office, Skype и Bing.

«Поскольку Microsoft постоянно улучшает качество перевода, вы можете надеяться на то, что переводы со временем будут становиться всё лучше и лучше», – написал старший менеджер по продукту LinkedIn Зак Хендлин (Zack Hendlin).

В других социальных сетях, включая Facebook и Twitter, аналогичная возможность присутствует уже достаточно давно. По словам Хендлина, эта функция была одной из самых востребованных среди пользователей LinkedIn.

Перевод публикаций в ленте работает более чем на 60 языках, включая русский, украинский, испанский, японский и немецкий. Нововведение доступно большинству пользователей сервиса в настольной и мобильной версиях сайта. В ближайшие несколько недель оно должно добраться и до приложений LinkedIn для iOS и Android.

3.07.2018

Facebook отключит все уведомления с помощью одной кнопки

В Facebook появится возможность выключить все уведомления с помощью кнопки «Не беспокоить». Об этом сообщает Mashable ([InternetUA](#)).

Новая функция на текущий момент находится в стадии тестирования. Она позволит временно отключить любые уведомления из Facebook, нажав на специальную кнопку. Сообщается, что у пользователя также будет возможность поставить таймер, по истечении времени которого уведомления снова будут доступны.

Кнопка «Не беспокоить» может быть запущена в рамках нового курса компании, направленного на «цифровое здоровье» своих пользователей – теперь Facebook будет следить за тем, сколько времени люди проводят внутри социальной сети, и предупреждать их о негативных последствиях интернет-зависимости.

3.07.2018

Лайфхак: как быстро собирать информацию для новостей из Twitter

В поисках информации журналисты мониторят десятки изданий по всему миру, а также различные социальные сети. Одной из самых оперативных и активных платформ сегодня остается Twitter, в котором медиаперсоны наравне с простыми пользователями размещают короткие и емкие посты. Сайт journalism.co.uk предлагает новичкам и опытным работникам СМИ обратить внимание на приложение TweetDeck, удобный интерфейс которого значительно облегчит поиск новостей ([Телекритика](#)).

TweetDeck является десктопным приложение и пользоваться им можно сразу без установки и без дополнительной регистрации. Приложение позволяет просматривать несколько категорий в одном интерфейсе, что очень удобно при работе с несколькими профилями в соцсети.

4.07.2018

Instagram будет указывать пользователям, что они слишком часто сидят в соцсетях

Сервис Instagram со 2 июля ввел новую функцию – социальная сеть будет уведомлять пользователей, что они посмотрели все посты в ленте за последние 48 часов. В такой ситуации пользователь увидит большую галочку и надпись «На этом пока все» ([InternetUA](#)).

После этого в ленте будут появляться посты, опубликованные ранее, вперемешку с новыми. В дальнейшем компания намерена ввести функцию «Не беспокоить», которая отключит все оповещения из Instagram и Facebook на заданное количество времени.

Пользователи проводят в Instagram около 32 минут в день, в среднем по 3,2 минуты за сессию. Основатель Instagram Кевин Систром у себя в твиттере добавил, что новые функции позволят людям контролировать время, которые они тратят на социальные сети.

Согласно новому исследованию ученых МІТ, половина американских пользователей готовы перестать пользоваться соцсетями всего за \$300 в год. При этом отказ от поисковых систем они оценили в \$17 тыс. ежегодно.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

21.06.2018

Днепровский горсовет заведет свое посольство в Telegram

Нынешние городские власти стараются быть поближе к народу и активно используют для этого социальные сети. К примеру, мэр Днепра Борис Филатов активно общается с избирателями на своей странице в Facebook и стал чуть ли не одним из самых популярных блогеров в городе. Свои странички в соцсетях заводят отдельные чиновники и целые департаменты. Частично на это тратят бюджетные деньги (49000.com.ua).

Они идут на дизайн и обеспечение своевременной реакции на обращения граждан и информирование о деятельности горсовета. Для того чтобы налогоплательщики знали, чем занимаются депутаты и чиновники в Днепре, существуют целые коммунальные предприятия, которые активно отслеживают все возможности донести информацию до жителей города.

Недавно чиновники решили выйти еще на одну популярную площадку – мессенджер Telegram. КП «Информационные системы» планирует закупить специального бота (программу). Бот будет принимать обращения днепрян о коммунальных авариях, транспортных проблемах и других вопросах в онлайн-режиме. Фактически любой сможет рассказать о сломанном лифте или прорванной трубе прямо со своего телефона. Бот будет в автоматическом режиме рассылать жалобы в соответствующие ведомства горсовета, а те, в свою очередь, должны оперативно устранить проблему. Обойдется это налогоплательщикам в четыре миллиона гривен. Согласно планам коммунального предприятия система обращений должна появиться к 10 августа этого года.

23.06.2018

Звільнена за фото у соцмережах вихователька з Рівненщини розпочала флешмоб

Вихователька з Радивилова Віта Черешньова стала відома на всю Україну завдяки фото в купальнику. І не через особливі параметри, а через звільнення через ці фото (Кулемет.com)

Однак не всі розуміють, чому вчителі не можуть публікувати фото з пляжу, як представники інших професій. Тому вихователі та вчителі з інших міст вирішили підтримати Віту, і публікують свої фото з відпочинку з хештегом #явчительмійвідпочинок. Віта Черешньова закликає захищати свої права та підтримати флешмоб.

25.06.2018

Фото Олега Ляшка зі школярами у партійних футболках зчинило скандал у соцмережах

Агітація чи подарунок. Фото Олега Ляшка з двома десятками школярів у партійних футболках зчинило скандал у соцмережах. І зацікавило навіть Міністерство освіти. Бо знімок радикал зробив в освітньому закладі. А це – пряме порушення закону про агітацію. В оточенні нардепа це заперечують, і кажуть, що то діти самі попросили в них футболки ([ТСН](#)).

30.06.2018

«Нехай на Аляску подивиться». У соцмережах обурилися новою заявою Трампа про Крим

Заяви президента США Дональда Трампа про те, що він «подивиться», чи визнавати російську окупацію Криму, викликали хвилю гніву в соціальних мережах ([Інформатор](#)).

Нагадаємо, коли журналісти в спілкуванні з главою Білого дому торкнулися теми анексії півострова і запитали про можливість її визнання американцями, Трамп відповів: «Подивимося» («We're going to have to see»), – пише Сьогодні.

Нагадаємо, це не перша заява Трампа про окупований Росією Крим. На саміті «Великої сімки» американський президент сказав світовим лідерам, що «Крим – російський, бо всі там говорять російською».

Білий дім відмовився коментувати такі слова Трампа щодо «російського Криму».

29.06.2018

Як політичні сили почали виборчий сезон у соцмережах?

Анастасія Багаліка

Співробітник Центру контент-аналізу Артем Захарченко підкреслює, що не всі політики однаково працюють в соцмережах, не всі вони порушують певні теми та далеко не всі політики зрозуміли, чого чекати від соціальних мереж і як їх опанувати.

[Докладніше](#)

4.07.2018

Апеляційний суд Закарпатської області «вийшов» у соцмережі

Офіційну сторінку Апеляційного суду Закарпатської області у соціальній мережі Facebook створено з метою реалізації політики відкритості та прозорості у роботі суду, а також задля забезпечення права громадян на отримання всебічної, об'єктивної та оперативної інформації про діяльність Апеляційного суду Закарпатської області (uzhgorod.net.ua).

Ознайомитися зі сторінкою Апеляційного суду Закарпатської області у Facebook можна за посиланням: <https://www.facebook.com/Апеляційний-суд-Закарпатської-області-267137773864030>.

1.07.2018

Українські військові моряки приєдналися до всесвітньої акції на підтримку Сенцова

Першого липня українські військові моряки приєдналися до всесвітньої акції на підтримку режисера Олега Сенцова, якого незаконно утримують у колонії в Росії.

Відео флешмобу опубліковано на сторінці Військово-морських сил Збройних сил України у Facebook.

«Український флот своїх не кидає. Крим це Україна!», – йдеться у повідомленні.

4.07.2018

В українському Інтернеті пройшов флешмоб з закликом проти схвалення законопроекту №6688

Законопроект №6688 був внесений в порядок дня Парламенту України 21 червня 2018 року. Це чергова спроба ухвалити законопроект, що може викликати суттєві обмеження свободи Інтернету ([Конфликты и законы](#)).

Стейкхолдери, включно з ГО «Інформаційна безпека», ГО «Інтерньюз-Україна» та Інтернет Асоціацією України ініціювали флешмоб з закликом до парламентарів відхилити законопроект №6688. Користувачі та сторінки організацій поміняли обкладинки у соцмережах з відповідним гаслом. До флешмобу також приєдналися такі сайти, як Українські Новини, опублікувавши банер на своєму сайті, повідомляється на своїй сторінці Фейсбук MEDIANEXT UKRAINE.

Реакція Олександра Федієнка, Голови правління Інтернет Асоціації України: «Близько рік тому, без перебільшення, ВСЯ громадськість виступала проти цього злочинного законопроекту! Тоді відбили, зараз, бачу, цей нафталін знову витягнули. Це там, під дахом, вимкнули кондиціонери?»

Реакція Тетяни Поповій, ГО «Інформаційна безпека»: «Пропонуємо для користувачів, кому важлива свобода Інтернету, зробити заклик до депутатів #рада8 відкликати законопроект #6688, який дозволяє досудове блокування сайтів».

Реакція Віталія Мороза – ГО «Інтерньюз-Україна»: «Пропонуємо для активістів, зацікавлених в свободі Інтернету, зробити заклик до депутатів #рада8 через зміну обкладинки у ФБ – адже у вас в друзях точно є депутати:)».

Змінили також обкладинку партнери – Інститут розвитку регіональної преси, ГО «Інтерньюз-Україна».

Сайт Українські новини опублікував банер на своїх сторінках.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

22.06.2018

YouTube вводить платну підписку на популярні канали

Видеохостинг YouTube намерен ввести функцію Channel Memberships, которая позволит оформить платную подписку на каналы с количеством подписчиков более 100 тыс. Функция уже стала доступной для ограниченного числа пользователей, сообщается в пресс-релизе, опубликованном в четверг на сайте компании ([IGate](#)).

«Новая бизнес-модель имеет успех у ряда пользователей. Поэтому мы расширим действие функции Channel Memberships на каналы с более чем 100 тыс. подписчиков», – говорится в сообщении.

Отмечается, что подписка будет стоить \$4,99 в месяц. Оформившие ее получают доступ к дополнительному контенту популярный каналов YouTube, эксклюзивным прямым трансляциям и новому набору смайликов Emojis.

26.06.2018

Facebook начал выпускать печатный журнал для бизнес-лидеров

Grow, «ежеквартальный журнал для бизнес-лидеров», появился в залах бизнес-класса аэропорта Хитроу и в еще нескольких местах Лондона в июне.

[Докладніше](#)

27.06.2018

Цукерберг может потерять пост главы Facebook

Инвесторы Facebook планируют уволить Марка Цукерберга с поста председателя правления компании. Об этом сообщает Business Insider ([InternetUA](#)).

По данным издания, инвесторы недовольны работой Цукерберга, в частности, из-за крупного скандала с утечкой данных из социальной сети.

Однако, по мнению инвесторов, Цукерберг неприкосновенен, так как занимает пост исполнительного директора и председателя правления Facebook.

26.06.2018

Подсчитано: сервис Instagram за шесть лет подорожал в 100 раз

Оценка соцсети, которую Facebook купил в 2012 году, выросла с \$1 млрд до \$100 млрд ([Телекритика](#)).

По прогнозам аналитика Bloomberg Intelligence Джитендра Варала, к середине 2019 года годовая выручка Instagram может преодолеть десять миллиардов долларов, а к 2023 году число активных пользователей платформы в месяц может удвоиться и достигнуть двух миллиардов.

Кроме того, аудитория Instagram моложе, и это делает платформу привлекательной для рекламодателей.

27.06.2018

Facebook разрешил рекламу криптовалют

Ранее в этом году сеть запретила рекламу бинарного опциона, первичного размещения монет и криптовалюты – финансовых продуктов, которые ассоциируются с «вводящими в заблуждение или обманчивыми промо-практиками». Сегодня сеть пересмотрела свое решение относительно криптовалют – но только для рекламодателей, которые были одобрены компанией. Реклама бинарного опциона и первичного размещения монет все еще под запретом. «Рекламодатели, которые хотят размещать рекламу криптовалют должны подать заявление, чтобы помочь нам оценить их правомерность, включая любые лицензии, которыми они обладают», – отметили в компании. Представитель компании отметил, что политика относительно размещения этих финансовых услуг была намерена широкой, чтобы компания смогла определить, как рекламодатели использовали вводящие в заблуждение практики для продвижения этих услуг и продуктов. Ранее Уоррен Баффет предрек «плохой конец» криптовалюте ([Marketing Media Review](#)).

27.06.2018

Украинские торговцы смогут принимать платежи в мессенджерах

Украинский стартап PayLastic презентовал решение для бесконтактной оплаты товаров и услуг банковскими карточками через чат-боты в мессенджерах.

[Докладніше](#)

2.07.2018

Facebook собирается повысить уровень ответственности рекламодателей

Крупнейшая соцсеть в мире представила несколько нововведений, обеспечивающих новый уровень прозрачности рекламы и страниц в соцсети. Тем самым предоставив пользователям больше информации ([Телекритика](#)).

Теперь люди смогут просмотреть те рекламные объявления, которые организация запускает на страницах Facebook, в Instagram, Messenger или в партнерской сети Facebook, даже если они не являются целевой аудиторией этой рекламы. Достаточно зайти на любую страницу и выбрать раздел «Информация и реклама» – тут можно найти рекламное объявление и его текст, а в случае чего и пожаловаться, заявив о подозрительном контенте.

В скором времени Facebook запустит маркировку политической рекламы в Бразилии в преддверии всеобщих выборов в стране в октябре. Любой, кто собирается запускать политическую рекламу в Бразилии, сможет зарегистрироваться в следующем месяце. Все маркированные рекламные сообщения будут добавлены в архив Facebook.

В соцсети отметили, что в настоящее время большинство рекламных объявлений на ее площадках запускаются легитимными организациями. Однако злоупотребления по-прежнему возможны, поэтому компания продолжит и дальше предпринимать шаги по борьбе с ними.

2.07.2018

Facebook патентует «прослушку» через смартфон

Компания Facebook запатентовала систему, которая может удаленно активировать микрофон на телефоне пользователя, чтобы записывать окружающие звуки. Эта технология может быть использована для оценки эффективности рекламы или популярности телепрограмм.

[Докладніше](#)

3.07.2018

Ирина Фоменко

Facebook и Twitter раскрыли информацию о покупателях рекламы

Два социальных медиа-гиганта раскрыли информацию, кто покупает рекламу на их платформах. Об этом сообщает The Star Online.

[Докладніше](#)

2.07.2018

Facebook проектирует панорамную камеру виртуальной реальности

Управление США по патентам и торговым маркам (USPTO) рассекретило новую разработку Facebook в области виртуальной реальности ([InternetUA](#)).

Нужно сразу оговориться, что обнародованный патент относится к классу дизайнерских. В нём описывается лишь внешний вид разработки, тогда как технические детали не раскрываются.

Документ носит название «Панорамная камера виртуальной реальности» (Panoramic virtual reality camera). Устройство представляет собой специальный модуль, установленный на штанге с тремя опорами.

По окружности модуля располагаются многочисленные объективы. Кроме того, оптические блоки есть в верхней и нижней частях. Таким образом, камера позволяет записывать панорамные видеоматериалы с круговым охватом.

Теоретически разработка Facebook может применяться для создания контента, рассчитанного на просмотр в шлемах виртуальной реальности. Впрочем, о возможных сроках выхода устройства с описанным дизайном на коммерческий рынок ничего не сообщается.

По оценкам IDC, в первом квартале текущего года поставки шлемов виртуальной и дополненной реальности составили 1,2 млн единиц. По итогам 2018 года в целом, как ожидается, отгрузки таких устройств достигнут 8,9 млн штук.

4.07.2018

Чат-боты для бізнесу: безліч переваг і трохи ризиків // Все, що потрібно знати про цей інструмент маркетингу й нематеріальний актив

Використання чат-ботів дає безліч переваг, що робить їх повноцінними нематеріальними активами. Причому покупка подібного активу може обійтися порівняно дешево, зате згодом принесе бізнесу більш ніж значиму вигоду.

[Докладніше](#)

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

25.06.2018

Facebook покажет пользователям, сколько времени они тратят на социальную сеть

Тренд на заботу о «цифровом здоровье» и борьбе с зависимостями дошел и до Facebook. Социальная сеть предоставит пользователям статистику о времени, проведенном на ресурсе ([IGate](#)).

Руководство Facebook сообщило о том, что в новой версии мобильного приложения появится раздел «Ваше время на Facebook». В нем будет содержаться информация о том, сколько времени пользователь провел в социальной сети за прошедшие семь дней, и усредненное значение за неделю. При желании подписчики смогут устанавливать ограничения на посещение ресурса. В таком случае приложение пришлет уведомление, когда лимит будет исчерпан.

Аналогичная функция вскоре появится у другой социальной сети, принадлежащей Марку Цукербергу, – Instagram.

«Мы всегда работаем над новыми способами, чтобы помочь людям, находящимся на Facebook, хорошо провести время», – сообщила пресс-служба компании.

Предложение Facebook перекликается с новой функцией Screen Time, которая станет доступна с выходом iOS 12. Корпорация Apple позволит пользователям iOS-устройств понять, к каким приложениям они обращаются чаще всего. По мнению разработчиков, эти данные помогут человеку оптимизировать время, потраченное на гаджет, и будут способствовать избавлению от цифровой зависимости.

25.06.2018

Мифы о технологиях и зависимости от них

В наши дни как никогда активно обсуждают возможную зависимость людей от технологий. Технологические компании даже были вынуждены встроить в свои программные продукты специальные счетчики и ограничители, которые заставляли бы нас задумываться о времени использования смартфонов. Доктора признают зависимость от компьютерных игр, и сложно даже представить, что будет дальше. Но так ли все серьезно на самом деле?

[Докладніше](#)

26.06.2018

Все больше детей ради эффектных фото и видео рискуют здоровьем

Все больше детей ради эффектных фото и видео рискуют здоровьем. Так, подростки в погоне за лайками в социальных сетях залезают на поезда, крыши высоток или прыгают на железнодорожные пути. Многие из них на всю жизнь остаются калеками ([InternetUA](#)).

Лечение травм от поражения током длительное и дорогое, говорят медики. За последние 5 лет количество подростков, пораженных напряжением, выросло. Так, за сезон без рук или с обожженным лицом в среднем остаются 7-8 детей.

Психологи подчеркивают: таким образом молодежь завоевывает себе авторитет среди сверстников.

Тем, кому удалось выжить в погоне за красивым фото, грозит штраф, правда, не более 300 гривен. А вот в Германии такие отчаянные должны уплатить 50 000 евро.

Чтобы убедить подростков не рисковать, в столичном метрополитене установили плакаты с популярным персонажем Гусаком. Он призывает беречь голову, а не предпочтения.

4.07.2018

Фахівці заявляють, що соцмережі посилюють почуття самотності у дітей

Як свідчать нові статистичні дані, усе більше дітей скаржаться на відчуття ізоляції та самотності. Фахівці вважають, що ситуацію погіршують соціальні мережі ([Вголос](#)).

Як пише Independent, у Великобританії дані про почуття самотності збирають лише другий рік поспіль: раніше служби фіксували їх як «низька самооцінка» або «відчуття себе нещасним». Цього року цифри демонструють 14 % зростання кількості звернень через самотність, порівняно з попереднім.

Зібрані дані свідчать, що майже 80 % консультаційних звернень припадають на дівчаток, багато з яких стверджували, що вплив соціальних мереж і порівнювання себе з іншими користувачами інтернету змушують їх відчувати себе все більш ізольованими.

У той час як більшість тих, хто звернувся за допомогою, були підлітками. Наймолодшому, хто дзвонив на лінію допомоги, було всього 10 років.

Маніпулятивні технології

26.06.2018

Ірина Фоменко

Apple планує опередити Facebook в боротьбі з фейковими новинами

У Apple News з'явилася нова місія: команда досвідчених редакторів буде аналізувати політичні новини замість неконтрольованих алгоритмів, які всі перебільшують.

[Докладніше](#)

3.07.2018

Facebook купив AI стартап для боротьби з фейковими новинами

Продукт лондонського стартапа Bloomsbury AI – це НЛП програма, яка допомагає машині відповідати на запитання по інформації, витягненій з документів. Facebook планує використовувати команду компанії та технології в боротьбі з фейковими новинами, які поширюються з президентських виборів в США в 2016 році. Угода оцінюється від \$23 до \$30 млн ([Marketing Media Review](#)).

25.06.2018

Скільки заробляють «фабрики ботів»: назвали суми

Науковці з Нідерландів дослідили, скільки коштує створити мережу фейкових акаунтів та скільки на цьому можна заробити.

Про це пише журналіст Андрій Бродецький в Telegram-каналі «Технології, медіа та суспільство» ([24 канал](#)).

Науковці з'ясували, що зараження пристроїв вірусом обійдеться в даркнеті в суму від 2 до 10 центів за інсталювання.

«Окремі витрати – підтримка ботнету в формі (моніторинг пристроїв, повторне зараження та інше), – додає журналіст.

Науковці підрахували, що ботнет на 10 мільйонів пристроїв обходиться приблизно в 16 мільйонів доларів.

Дохід власнику мережі приносять різні послуги: наприклад, мережа для DDoS з 30 тисяч пристроїв генерує 26 тисячі доларів на місяць, спам-розсилка на 10 тисяч ботів приносить 300 тисяч доларів на місяць, банерні кліки – до 20 мільйонів доларів на місяць.

Спецслужби і технології «соціального контролю»

21.06.2018

Дмитрий Демченко

«Ужасающая» реформа авторского права в ЕС и война с мемами, в которой невозможно победить

Европейский союз 20 июня ввел в действие процесс, который может впоследствии обязать онлайн-платформы – Facebook, Reddit, 4chan и другие – цензурировать контент пользователей еще до того, как он будет опубликован. Союз хочет, чтобы компании использовали технологии распознавания контента, чтобы определять видеоролики, фото, текст и код, защищенные авторским правом.

[Докладніше](#)

21.06.2018

Владимир Кондрашов

Украинские депутаты хотят ввести цензуру в Интернете

Верховная Рада Украины включила в повестку дня законопроект №6688 о внесудебной блокировке сайтов, который де-факто, устанавливает цензуру в сети Интернет.

[Докладніше](#)

23.06.2018

Владимир Кондрашов

СБУ прислала провайдерам список из 181 сайта на блокировку

Служба безопасности Украины прислала Интернет Ассоциации Украины письмо со списком из 182 доменов, к которым ограничен доступ на территории Украины ([InternetUA](#)).

– Решением СНБОУ расширено использование такого вида санкций как «блокировка интернет провайдерами доступа к ресурсам, в том числе к их субдоменам», – говорится в письме. – Учитывая вышеизложенное, с целью предупреждения угроз информационной безопасности Украины и ввиду статутных заданий Интернет Ассоциации Украины, просим довести к участникам рынка интернет-услуг перечень доменов, к которым ограничен доступ на территории Украины.

Перечень доменов занял 4 листа – в нем 182 пункта.

Отметим, что ранее издание «Страна» опубликовало похожее письмо от Департамента контрразведывательной защиты интересов государства в сфере информационной безопасности, однако в том списке был 181 домен. Как оказалось, в «свежем» списке от СБУ, полученном ИНАУ, дважды встречается один и тот же сайт – miaistok.su (под 86 и 113 номерами).

26.06.2018

В Венесуэле заблокировали доступ к сети Tor

Власти Венесуэлы заблокировали доступ местным пользователям к анонимной сети Tor, пишет The Verge со ссылкой на данные организации Access Now. По информации сетевых активистов, речь идет о блокировке как прямых подключений, так и подключений через так называемые мосты, которые до сих пор избегали блокировок ([InternetUA](#)).

Количество подключений к сети Tor в Венесуэле недавно резко выросло в связи с блокировкой сайтов ряда местных новостных изданий. Обойти эту блокировку при помощи серверов Google и CloudFlare невозможно и для многих местных пользователей сеть Tor оставалась единственным средством доступа к запрещенным ресурсам.

The Verge напоминает, что в апреле этого года в ООН официально осудили интернет-цензуру в Венесуэле наравне с ростом числа задержаний журналистов.

«Даже в условиях чрезвычайного положения регулирование, а также ограничение доступа к веб-сайтам и телевизионным сигналам, передаваемым через интернет, несоразмерны и несовместимы с международными стандартами», – говорилось в официальном заявлении.

Сеть Tor представляет собой систему прокси-серверов, позволяющую устанавливать анонимное соединение, защищенное от прослушивания. Технология Tor обеспечивает защиту от механизмов анализа трафика, которые ставят под угрозу не только интернет-анонимность пользователя, но также конфиденциальность коммерческих тайн, деловых контактов и т. д.

26.06.2018

СБУ викрила адміністраторів антиукраїнських груп у соцмережах

Співробітники Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБ України та його регіональних підрозділів викрили у червні групу адміністраторів антиукраїнських спільнот в соціальних мережах, які діяли за вказівкою спецслужб РФ.

[Докладніше](#)

27.06.2018

На Дніпропетровщині проросійські агітатори провокували заворушення до Дня Конституції

У Дніпропетровській області СБУ викрила двох місцевих жителів на проросійській агітації, сепаратизмі та провокуванні масових заворушень до Дня Конституції України. Про це повідомляє прес-служба СБУ (Espresso.tv).

Мешканці Дніпра та Жовтих Вод за завданням представників спецслужб РФ поширювали у соцмережах спеціально підготовлені матеріали, які адаптували саме для мешканців регіону. Упродовж останнього місяця основні зусилля зловмисників були спрямовані на провокацію масових заворушень та порушень громадського порядку під час урочистих заходів до Дня Конституції України.

Серед матеріалів російських агентів також виявлені наклепи на підрозділи Об'єднаних сил щодо провокацій обстрілів на території окремих районів Донецької та Луганської областей, а також брехливі «довідки» прибічників терористів зі значно завищеними втратами ЗСУ.

Зловмисники також агітували за входження центральних і східних областей України до складу Росії та закликали до насильницької зміни конституційного ладу в державі.

Під час обшуків правоохоронці вилучили комп'ютерне обладнання, використане для розповсюдження антиукраїнських матеріалів та сепаратистських закликів. У агітаторів також виявили інструкції від спецслужб Росії по обходу блокування заборонених в Україні соцмереж та інших сайтів.

Відкрито провадження за ст. 110 Кримінального кодексу України (посягання на територіальну цілісність і недоторканність України).

27.06.18 20:37

Twitter вводити идентификацию пользователей для борьбы со спамом

Руководство соцсети Twitter решило ввести процедуру обязательного подтверждения аккаунтов через e-mail и телефонные номера.

Об этом говорится в блоге Twitter ([Бизнес Цензор](#)).

В компании надеются, что эта мера позволит сократить число недобросовестных пользователей, создающих огромное количество фальшивых страниц со спамом и агрессивным контентом.

По данным Twitter, с прошлого года значительно выросла статистика отключения ботов от соцсети. Сейчас компании приходится еженедельно отключать около 9,9 млн спам- или бот-аккаунтов.

2.07.2018

Ирина Фоменко

Силовики злоупотребляют технологией распознавания лиц

За последние несколько лет технология распознавания лиц была спокойно принята властями Соединенных Штатов, в том числе полицейскими, и стала частью стандартного инструментария правоохранительных органов.

[Докладніше](#)

2.07.2018

Роскомнадзор возобновил массовые блокировки IP-адресов Telegram

Около 13:30 Роскомнадзор заблокировал почти 1000 IP-адресов мессенджера Telegram. Такого количества одновременно заблокированных адресов не было уже больше месяца ([InternetUA](#)).

Неожиданную блокировку заметил telegram-канал RKNSHOWTIME. Представители Роскомнадзора пока никак не комментировали ситуацию.

Еще в апреле Роскомнадзор начал процедуру блокировки Telegram на территории России, однако мессенджер по-прежнему продолжает работать у большинства пользователей. Причиной решения о блокировки стало то, что представители мессенджера отказались передавать ФСБ ключи шифрования сообщений пользователей.

По данным Mediascope, блокировка Telegram лишь незначительно повлияла на популярность мессенджера в России. В мае 2018 года приложениями и веб-версией Telegram в среднем ежедневно пользовались около 3.667 миллиона россиян, а в начале апреля в мессенджер ежедневно заходило 3,716 млн человек.

3.07.2018

К расследованию утечки данных миллионов пользователей Facebook подключилось ФБР

Федеральное бюро расследований (ФБР) США, а также ряд других федеральных агентств подключились к расследованию утечки данных десятков миллионов пользователей социальной сети Facebook, в результате которой информация об этих пользователях в 2015 году попала в распоряжение британской компании Cambridge Analytica ([InternetUA](#)).

Как пишет газета The Washington Post, запросы в Facebook о предоставлении информации, касающейся утечки, направили ФБР, Комиссия по ценным бумагам и биржам (SEC) и Федеральная торговая комиссия (FTC). Ранее сообщалось, что расследованием утечки занимается Минюст США.

По данным источников, ведомства намерены выяснить, какими данными об утечке специалисты Facebook располагали в 2015 году и почему компания не раскрывала информацию о них. Также в ФБР и других агентствах изучают показания главы Facebook Марка Цукерберга и его подчиненных, которые они ранее давали в конгрессе.

В соцсети подтвердили получение запросов, сообщив, что компания предоставляет ведомствам информацию и сотрудничает с официальными лицами в США, Великобритании и других странах.

3.07.2018

Владимир Кондрашов

СБУ регулярно фиксирует российские кибератаки

Служба безопасности Украины постоянно фиксирует кибератаки, которые поддерживаются государством-агрессором ([InternetUA](#)).

Об этом на круглом столе, посвящённом урокам от атаки вируса Petya A, сообщил сотрудник ситуационного центра обеспечения кибербезопасности СБУ Андрей Окаевич, передает InternetUA.

По словам сотрудника СБУ, часто такие атаки происходят с использованием так называемых «zero day»-уязвимостей, то есть ранее неизвестных уязвимостей.

То, что атаки «поддерживаются» РФ, как утверждает Окаевич, стимулирует СБУ больше внимания уделять вопросам кибербезопасности.

Андрей Окаевич также отметил, что СБУ фиксирует тенденцию атакующих к компрометации инфраструктуры производителей программного обеспечения:

– Это лёгкий путь для проникновения к клиентской базе разработчиков программного обеспечения, – пояснил эксперт.

В течение года Службе удалось остановить на «первичной стадии» три таких атаки, и на сегодняшний день в Ситуационном центре обеспечения кибербезопасности СБУ постоянно работают с компаниями из перечня крупнейших производителей программного обеспечения в стране.

4.07.2018

Комитет Рады рекомендовал принять скандальный законопроект о блокировке сайтов

Комитет Верховной Рады Украины по вопросам национальной безопасности и обороны рекомендовал принять в первом чтении законопроект № 6688, предусматривающий временную блокировку сайтов без решения суда ([InternetUA](#)).

Об этом проинформировали в пресс-службе «Народного фронта».

Речь идет о законопроекте «О внесении изменений в некоторые законодательные акты Украины относительно противодействия угрозам национальной безопасности в информационной сфере».

«Согласно этому законопроекту, информационный ресурс смогут заблокировать на 48 часов “в исключительных неотложных случаях, связанных

со спасением жизни людей и предотвращением совершения тяжкого или особо тяжкого преступления”; а по решению следственного судьи, суда, прокурора или СНБО – на более длительные периоды за размещение “запрещенной информации”», – говорится в сообщении.

В ходе заседания глава комитета, нардеп от «Народного фронта» Сергей Пашинский заявил о важности принятия указанного документа.

4.07.2018

В СБУ рассказали о борьбе с российской интернет-угрозой

Заместитель председателя Службы безопасности Украины Олег Фролов заявляет, что в течение 5 месяцев 2018 года СБУ выявила использование российскими спецслужбами 181 интернет-ресурса для дестабилизации ситуации в Украине (InternetUA).

Как передает корреспондент, об этом он сказал во время заседания Комитета Верховной Рады Украины по вопросам национальной безопасности и обороны.

«В течение 5 месяцев 2018 года Службой безопасности Украины выявлено и задокументировано использование российскими спецслужбами 181 интернет-ресурса с целью дестабилизации социально-политической ситуации в Украине», – сообщил Фролов.

На вопрос, располагает ли СБУ надлежащим образом зафиксированными доказательствами, что большинство информационных атак происходит именно с территории России, он отметил, что ранее большинство IP-адресов были из сети Российской Федерации.

«Сейчас ситуация несколько изменилась. Мы видим IP-адреса из стран ЕС», – добавил представитель Службы.

Кроме того, Фролов добавил, что в этом году отражено уже более 50 кибератак различной степени мощности, последствия некоторых из них могли быть «гораздо хуже, чем Petya.A».

Также представитель СБУ отметил, что в 2017 году было зарегистрировано 43 уголовных производства и вынесено 36 обвинительных приговоров по делам о киберпреступности. В этом году уже зарегистрировано 24 уголовных производства и 15 лицам объявлено подозрение.

Проблема захисту даних. DDOS та вірусні атаки

22.06.2018

Нацполиция задержала хакера, который взламывал соцсети украинцев и требовал выкуп

Правоохранители разоблачили хакера из Львовской области, занимавшегося несанкционированным вмешательством в работу учетных записей социальных сетей и распространением вредоносного программного обеспечения. Об этом сообщает пресс-служба Департамента киберполиции Нацполиции Украины.

[Докладніше](#)

25.06.2018

Как защитить свои данные в Интернете

Адвокат рассказала, как обезопасить фотографии и другие данные в интернете авторским правом.

[Докладніше](#)

25.06.2018

Мошенники распространяют вирусы под видом информации о ЧМ-2018

Исследователи из компании Check Point выявили новую схему заражения компьютеров вирусами. Их распространяют под видом файлов с расписанием игр и турнирной таблицы Чемпионата мира по футболу 2018. В случае открытия сомнительного «футбольного» файла приложение запускает вариант вредоносного ПО под названием DownloaderGuide.

[Докладніше](#)

26.06.2018

В ЕС решили создать силы быстрого реагирования на киберугрозы

Министр обороны Литвы Раймундас Кароблис рассказал, что литовская сторона предложила создать силы быстрого реагирования на киберугрозы в рамках постоянного структурированного сотрудничества ([InternetUA](#)).

По словам Кароблиса, ряд стран-членов ЕС подпишет декларацию, в которой говорится о намерении создать европейские силы быстрого киберреагирования, а также механизм совместной поддержки.

«Подписывают шесть стран – Эстония, Хорватия, Румыния, Литва, Испания и Нидерланды», – рассказал Кароблис.

Он добавил, что некоторые другие страны ЕС также поучаствуют в проекте без подписания декларации.

26.06.2018

Представлен проект по повсеместному шифрованию трафика почтовых серверов

Правозащитная организация «Фонд Электронных Рубежей» (Electronic Frontier Foundation, EFF) представила новую инициативу STARTTLS Everywhere, в рамках которой предлагается повсеместно использовать шифрование трафика почтовых серверов ([InternetUA](#)).

Авторы инициативы также разработали специальный сервис, позволяющий проверять, поддерживают ли почтовые серверы команды STARTTLS, а также используют ли они надежные алгоритмы шифрования и заслуживающие доверия сертификаты. При обнаружении проблем, сервис предлагает ряд рекомендаций по их устранению.

Инициатива STARTTLS Everywhere является дополнением к проекту HTTPS Everywhere, направленному на повсеместное внедрение защищенного протокола HTTPS. В настоящее время, несмотря на большое количество почтовых серверов, поддерживающих STARTTLS, большинство из них не выполняет проверку сертификатов. Помимо этого, многие серверы используют сертификаты, не заверенные удостоверяющим центром. В данной ситуации злоумышленники могут с легкостью осуществить MitM-атаку (атака типа «человек посередине») после чего перехватывать и модифицировать трафик.

Авторы проекта также представили скрипт, позволяющий бесплатно получить сертификат Let's Encrypt для домена и сгенерировать готовый блок конфигурации.

26.06.2018

Киберпреступники массово похищают данные у финансовых фирм

В попытке похитить конфиденциальные данные киберпреступники нацелились на финансовые фирмы, используя скрытые туннели для проникновения в сети компаний. Согласно опубликованному экспертами безопасности из компании Vectra докладу, поведение атакующих подобно тому, как вели себя хакеры, похитившие данные у Equifax в 2017 году ([InternetUA](#)).

Атакующие используют скрытые туннели для проникновения в защищенные сети компаний. Данный метод используется и некоторыми легитимными приложениями для обхода решений безопасности, которые иногда могут ограничивать полный функционал.

«Каждая отрасль имеет профиль сети и определенные модели поведения пользователей, который применимы к конкретным бизнес-моделям, приложениям и пользователям. Атакующие могут имитировать данное поведение, что затрудняет их обнаружение», – отметили специалисты.

По словам исследователей, в различных отраслях на каждые 10 тыс. устройств приходится порядка 11 скрытых HTTPS-туннелей, однако в сфере финансов данное число увеличилось почти вдвое – до 23. Скрытые туннели

трудно обнаружить, поскольку коммуникации скрыты многочисленными соединениями, использующими распространенные протоколы. Например, коммуникации могут быть встроены в текст в HTTP-GET-запросах, заголовках, cookie-файлах и других полях.

«Все это указывает на один факт: крупнейшие корпоративные организации в мире остаются заманчивыми целями для киберпреступников», – говорится в докладе.

26.06.2018

Российские хакеры готовят масштабную атаку против Украины

Российские хакеры заражают украинские компании вредоносными программами, чтобы обеспечить себе несанкционированный доступ (так называемый бэкдор) для масштабной скоординированной атаки, заявил глава украинской киберполиции Сергей Демедюк ([InternetUA](#)).

В комментарии Reuters он подчеркнул, что образцы зловредов, которые были обнаружены и проанализированы киберполицейскими, говорят о том, что хакеры намерены активировать вредоносный код в определенный день.

По словам Демедюка, масштабы последних обнаруженных подготовок к хакерским атакам не уступают атаке с помощью вируса NotPetya в июне прошлого года.

«Это поддержка на правительственном уровне – очень дорогая и очень синхронизированная. Без помощи государственных органов это было бы невозможно. Сейчас мы говорим о Российской Федерации», – сказал он, добавив, что в 99-ти случаях из ста следы указывали на Россию.

Демедюк добавил, что Украина лучше подготовлена к тому, чтобы противостоять таким атакам благодаря сотрудничеству с иностранными союзниками.

26.06.2018

Хакеры-вымогатели атаковали американские города

Американский госсектор подвергся систематическим атакам хакеро-вымогателей. Об этом сообщает издание Wall Street Journal ([InternetUA](#)).

В последние месяцы муниципальные сети многих городов США (Атланта, Рокпорт, Сент-Луис и другие) стали жертвами вирусо-шифровальщиков. Местные власти потратили немало средств на восстановление данных, модернизацию системы и ее страхование, а в безвыходных случаях – на выкуп для преступников.

Наиболее показательным служит так называемый рокпортский инцидент, произошедший в пятницу, 13 апреля. Сотрудники местной организации уже планировали уйти домой, закончив работу, однако заметили, что часть файлов

на корпоративных компьютерах заблокирована. За получение доступа к ним неизвестные требовали определенную сумму в биткоинах.

Руководство было готово оплатить выкуп данных: цена оказалась невысокой. Однако в итоге было принято решение не идти на уступки. Восстановление файлов обошлось в 40 тысяч долларов (сам процесс восстановления обошелся в четверть этой суммы, остальное составили расходы на усиление безопасности и систему облачного резервного копирования).

По данным Института Понемона (Ponemon Institute), объемы атак в госсекторе растут быстрее, чем в частном. По оценкам специалистов, около 38 процентов государственных организаций в этом году пострадают от вымогателей. Для сравнения – в 2016 году таких было 13 процентов.

Федеральное бюро расследований советует чиновникам не платить вымогателям и предупреждает, что некоторые преступники не выполняют своих обещаний и не предоставляют ключи для дешифровки файлов после получения денежной суммы.

26.06.2018

Вирусные сообщения WhatsApp привели к жестокому избиению людей на улице

Пользователи из Индии распространяли в WhatsApp сообщения о преступниках, которые переодевались в нищих и убивали людей. В результате, около 50 человек вышли на улицы, чтобы найти и наказать «убийц» ([InternetUA](#)).

Как было сказано в послании, рассылаемом в WhatsApp, в Индии появилась банда из 500 человек в одежде бедняков, которые убивали людей и продавали их органы. Полицейские сразу же опровергли эту информацию, однако толпа из 50-60 человек жестоко избивала двух невинных нищих.

Представители власти вычислили трех мужчин, с которых началось распространение ложной информации, и арестовали их, сообщает Reuters. Это не первый случай, когда невинные люди становятся жертвами дезинформации в соцсетях. Индия – это страна, в которой более миллиарда абонентов имеют доступ к мессенджерам, и любая поддельная новость может стать вирусной в считанные минуты, создав массовую истерию и усилив общую напряженность.

«К сожалению, некоторые люди используют WhatsApp для дезинформации. Мы наращиваем наши образовательные мощности для того, чтобы люди знали о функциях безопасности и умели выявлять фальшивые новости и мистификации», – сказано в официальном заявлении мессенджера.

27.06.2018

Ирина Фоменко

Новая технология мешает хакерам взламывать Wi-Fi

Wi-Fi теперь пользуются повсюду – не только дома и в офисе, но и в общественных местах. Тем не менее, остаются нерешенные проблемы с безопасностью. Однако впервые за 14 лет стандарт Wi-Fi получит обновление. Об этом сообщает The Fortune ([InternetUA](#)).

Wi-Fi Alliance запустил WPA3, новый стандарт беспроводного Интернета, который лучше шифрует данные, что затрудняет перехват этой информации третьими лицами. Ввод пароля также обеспечит дополнительный уровень защиты.

Кроме того, программа, объявленная вместе с WPA3, упростит подключение домашних смарт-устройств к сети Wi-Fi. Easy Connect дает возможность использовать смартфон для настройки соединений.

Новый стандарт не будет автоматически отображаться на нынешних устройствах. Пользователю придется вручную устанавливать обновления, а некоторые старые девайсы могут не получить их вовсе.

В ближайшее время стандарт WPA2 останется без изменений. Два протокола, WPA2 и WPA3, совместимы, хотя WPA3 в будущем, предполагается, что к 2020 году, станет обязательным. Напомним, обновление WPA2 вышло в 2004 году, а обязательным стало в марте 2006 года.

27.06.2018

Атаковавшие Bithumb хакеры используют HWP-документы в новой вредоносной кампании

Северокорейские хакеры используют документы текстового редактора Hangul Word Processor (HWP) в новой вредоносной кампании на криптовалютные обменники. Ответственность за кампанию предположительно несет хакерская группировка Lazarus, сообщают исследователи безопасности из компании AlienVault ([InternetUA](#)).

Атаки включают недавнее нападение на Bithumb, крупнейшую криптовалютную биржу в Южной Корее, клиентами которой являются более 1 млн пользователей. В рамках атаки хакерам удалось украсть криптовалюту на сумму более \$30 млн.

Как сообщают исследователи, хакеры используют серию вредоносных документов для атак на участников предстоящего саммита G20 в Аргентине. Исследователи проанализировали три похожих вредоносных документа, которые ранее использовали Lazarus. В одном из них упоминается совещание рабочей группы «большой двадцатки», направленное на координацию экономической политики. Файлы HWP включают вредоносный код, который загружает вредоносное ПО (32-битную или 64-битную версию Manuscript).

Помимо этого, исследователи отметили, что фишинговые сайты злоумышленников зарегистрированы на тот же номер телефона, что и домен itaddnet [.]com и содержат некоторые из вредоносных программ. По словам

специалистов, это свидетельствует о заинтересованности злоумышленников в хищении учетных данных.

«Необычно видеть, что Lazarus регистрирует домены – обычно они предпочитают компрометировать легитимные сайты», – отметили специалисты.

2.07.2018

Неудаляемый вирус внезапно появился на компьютерах с Windows

Пользователи со всего мира обнаружили на своих компьютерах неудаляемую программу All-Radio 4.27 Portable, которая оказалась вредоносной. Впервые сообщения о вирусе появилась на форуме [Malwarebytes \(InternetUA\)](#).

Неизвестный алгоритм появлялся внезапно на компьютерах под управлением Windows. Удивленные пользователи пытались избавиться от него, однако никаких механизмов удаления не нашли.

Официально программа российского производства All-Radio 4.27 Portable является бесплатным универсальным плеером, позволяющим слушать музыку и смотреть телепередачи онлайн. Неизвестные хакеры подделали ее и выдали зараженное ПО за оригинал.

Эксперты из BleepingComputer обнаружили, что большинство юзеров сообщили о внезапном появлении плеера после загрузки некоторых активаторов продуктов Microsoft (к примеру, достаточно популярного KMSpico). Их анализ показал, что под видом «ключей» жертвы получали рекламный пакет aimr, который и стал причиной заражения. Среди возможных инфекций – майнеры, спамеры, различные трояны, а также руткиты, скрывающие заражение.

Судя по характеру ПО, хакерская группировка намерена построить бизнес на данной схеме заражения (добыча криптовалюты, кража данных). Эксперты уверены, что пользователям лучше избегать программ-активаторов, поскольку они могут быть инфицированы злоумышленниками.

2.07.2018

Ирина Фоменко

Интернет вещей способствует домашнему насилию

Такие сетевые устройства, как дверной звонок Nest Hello и Nest Learning Thermostat, значительно упрощают жизнь. Однако существуют две вещи, на которые стоит обратить внимание.

[Докладніше](#)

2.07.2018

Уязвимости в 4G LTE позволяют отслеживать трафик абонентов и подменять данные

Объединенная группа исследователей из Рурского и Нью-Йоркского университетов опубликовала доклад, в котором описала три типа атак, эксплуатирующих уязвимости в стандарте 4G LTE. Две из них являются пассивными и позволяют отследить LTE трафик и узнать различные подробности о целевом объекте. С помощью третьей, получившей название aLTEr, атакующие могут подменять отправляемые на устройство данные и определить, какие сайты посещает жертва с гаджета ([InternetUA](#)).

Исследователи протестировали атаку aLTEr в серии экспериментов, в ходе которых им удалось перенаправить пользователей на вредоносные сайты, подменив DNS пакеты. Видео с демонстрацией процесса представлено ниже:

Все три уязвимости затрагивают канальный уровень (Data Link layer, уровень 2) 4G LTE. Проблемы связаны с отсутствием должной проверки целостности при передаче пакетов, что предоставляет атакующим возможность перехватывать и модифицировать зашифрованные пакеты данных 4G и затем ретранслировать их на сотовые вышки. Атаки нельзя провести удаленно – злоумышленник должен находиться вблизи и заставить пользователя подключиться к своему устройству.

По словам экспертов, уязвимости также затрагивают стандарт 5G в его текущем виде. Хотя в стандарте предусмотрены дополнительные функции безопасности, защищающие от атаки aLTEr, в настоящее время они опциональны.

Команда уже передала информацию об уязвимостях Международной ассоциации мобильных операторов (GSM Association), консорциуму 3GPP (разрабатывает спецификации для мобильной телефонии) и ряду телекомкомпаний.

ДОДАТКИ

Додаток 1

24.06.2018

40 % пользователей за год удалили аккаунт хотя бы в одной социальной сети

Согласно исследованию, которое провело маркетинговое агентство Edelman, около 40 % пользователей за последний год удалили свой аккаунт хотя бы в одной из социальных сетей. Специалисты прокомментировали, что это связано с «кризисом доверия к социальным сетям». Потребители ожидают, что бренды срочно найдут решения этих проблем ([InternetUA](#)).

В комментарии к исследованию социологи отмечают, что проблемы конфиденциальности и распространение поддельных новостей способствуют недоверию людей к площадкам. Причем 70 % респондентов ожидают, что отток посетителей и рекламодателей окажет давление на сайты, которые будут работать с такого рода контентом и устранят его. Как выяснилось, для них также важен контекст – 48 % заявили, что если его реклама появляется рядом с жестоким контентом или ненавистными комментариями, то это вина бренда.

«Мы узнали, что существует серьезная нехватка доверия к медиа во всех регионах мира. Это крик сердца, люди боятся. Они возмущены нарушением их конфиденциальности и не уверены в правде из-за распространения ложных новостей», – отметил президент и генеральный директор консалтинговой компании Ричард Эдельман.

Компания, главой которого он является, опросила 9 тысяч человек в Бразилии, Канаде, Китае, Франции, Германии, Индии, Объединенных Арабских Эмиратах, США. Ричард Эдельман призвал компании быть честными в том, как они используют социальные сети, в том числе для рекламы, заявив, что люди хотят четко идентифицировать, когда контент оплачен, а когда их данные собирает площадка.

Исследование социальных сетей основывается на ежегодном «барометре доверия Эдельмана». В первом отчете говорилось о том, что 41 % людей в глобальном масштабе доверяют социальным сетям, и с 2017 году их число падает в большинстве западных стран.

[\(вгору\)](#)

Додаток 2

27.06.2018

Всесильный Facebook: соцсеть готова предсказать, когда вы поженитесь и когда умрете

Несмотря на заявления владельца и руководителя Facebook Марка Цукерберга в Конгрессе США и Европарламенте о том, что все данные компания будет собирать только с разрешения пользователей, а процедура будет прозрачной, некоторые патенты этой социальной сети, обнаруженные The New York Times, порождают много вопросов ([InternetUA](#)).

По словам вице-президента компании Аллена Ло, большинство запатентованных технологий не используются и не будут использоваться компанией в будущем, а являются лишь преимуществом перед конкурентами.

Однако довольно страшно, когда социальная сеть умеет определять эмоциональное состояние человека, чтобы подбирать для него «правильную» рекламу. Еще более пугает, когда программа пытается угадать дату смерти пользователя и даты смерти его друзей.

Отношения

Соцсеть будет пытаться определить чувства человека к другим пользователям на основании того, как часто он заходит на их профили. Также

Facebook будет определять социальные отношения путем подсчета количества людей на фото и процентного соотношения представителей разных полов в друзьях.

Характер

Анализируя посты, программа будет идентифицировать пользователя как «интроверта», «открытого» или «эмоционально нестабильного» для таргетирования новостей и рекламы.

Пророчества

Анализ постов, информация по операциям с банковской карточкой и определение местоположения помогут Facebook предусматривать важные жизненные события пользователей: свадьба, рождение ребенка и даже смерть.

Идентификация камеры

Социальная сеть будет анализировать уникальный «отпечаток» камеры с помощью поврежденных пикселей и царапин на линзе. Это поможет определить, кто загружает снимки, сделанные на этом устройстве, и насколько пользователи близки.

Подслушивание

Facebook проверит информацию об использовании микрофона гаджета для подслушивания разговоров пользователей, чтобы предлагать им соответствующую рекламу.

Новый патент предусматривает использование микрофона для «подслушивания» телепрограмм, которые просматривает пользователь. Эта технология также позволяет определять, какую рекламу человек выключает. С таким патентом прослушивания становится реальностью.

Образ жизни

Facebook планирует записывать режим дня пользователя и отправлять отчеты об отклонении от него другим пользователям. Он также будет отслеживать местоположение телефона ночью, чтобы определить, где человек живет.

Привычки

Facebook будет сравнивать геолокации друзей, чтобы определить, с кем человек проводит время. Программа также будет определять продолжительность сна пользователя на основании того, как долго устройство находится без движения.

Несмотря на заверения топ-менеджмента компании о том, что эти технологии не будут использоваться, большинство из них – новые способы сбора, анализа и использования личных данных пользователей, а также «упаковки» этой информации для рекламы, которая приносит компании более 99 % дохода.

Причем эта информация может использоваться и с менее «благородной» целью, чем целенаправленная реклама. Например – для манипуляций на выборах. Как уже делала компания Cambridge Analytica, когда к ней попали такие данные.

[\(вгору\)](#)

29.06.2018

Як політичні сили почали виборчий сезон у соцмережах?

Анастасія Багаліка

Гість ефіру – співробітник Центру контент-аналізу Артем Захарченко ([Громадське радіо](#)). «Далеко не всі політики зрозуміли, чого чекати від соціальних мереж і як їх опанувати. Якщо говорити про останні тренди, то можна сказати, що весь той масив людей, які раніше були зареєстровані в «Однокласниках», тепер перейшли в Фейсбук. Ця аудиторія недостатньо звична до середовища Фейсбуку і, напевно, найлегше піддається маніпуляціям. Люди, які пройшли у Фейсбуці 2013 – 2014 роки виробили у себе певний імунітет до різних маніпуляцій, не 100 %, але певну медіаосвіту вони мають. Оскільки це люди старшого віку і часто зі східних регіонів, то це певна електоральна база Опозиційного блоку та інших подібних сил. Дійсно, цією категорією людей досить успішно маніпулюють. Ми це бачимо за компанією проти Лінчевського, яка мала досить велику увагу в соціальних мережах з боку цієї категорії користувачів», – розповідає Артем Захарченко.

Він зазначає, що Петро Порошенко досить активно просуває саме патріотичні меседжі: «На деякий час це спрацювало, він зміг очолити ці позиції, а тепер таке враження, що випробовують, наскільки вдасться порушити теми прав людини, протиставити темам патріотизму, але ми бачимо, що політики топового рівня не готові очолити ці ідеї. Вони дивляться, які верстви суспільства реагують».

Гість ефіру підкреслює, що не всі політики однаково працюють в соцмережах, не всі вони порушують певні теми. За його словами, Олег Ляшко та Сергій Тарута намагаються іти не від тем, а від оповіді того, як буде в майбутньому. «Вони описують ситуацію, ніби вони вже є президентами. Олег Ляшко безперервно робить акцент на емоціях, використовує класичну концепцію постправди, він, напевно, зробив акцент на тому, щоб нічого не пояснювати, а змусити вірити. Тарута намагається бути логічним, але так само описує картинку, а не робить акцент на якійсь темі», – додає Артем Захарченко.

([вгору](#))

26.06.2018

Facebook начал выпускать печатный журнал для бизнес-лидеров

Grow, «ежеквартальный журнал для бизнес-лидеров», тихо появился в залах бизнес-класса аэропорта Хитроу и в еще нескольких местах Лондона в июне. Название и «выпуск первый» набран белым шрифтом на черной обложке с портретом шведского «гуру» дизайнера Оскара Олссона, креативного директора N&M. Издатель – Facebook ([Marketing Media Review](#)).

Никола Мендельсон, вице-президент Facebook по ЕМЕА пишет, что Grow «родился на небольшом ивенте в английской деревне около полугода назад». Его коллега Лия Вудингтон добавляет, что это скорее – маркетинговая программа: «Он предназначен для маркетинговых коммуникаций».

И вот внушительной толщины журнал стоит на полках книжного магазина в Хитроу. Президент консалтинговой компании Innovation Media Consulting Хуан Сенор прокомментировал: «Когда крупнейшая мировая социальная сеть хочет ассоциировать свой бренд с доверием, она запускает печатный продукт». В сенате США Марк Цукерберг говорил, что Facebook – не издатель и не несет ответственности за контент. И вот они начали издавать принт.

Первый номер Grow, объясняет Мендельсон, исследует нишевые бренды – «одну из самых интересных бизнес-историй за последние пару лет». Главным редактором стала Кейт Максвелл, бывший журналист Condé Nast (Vogue, GQ и другие медиабренды).

Это не первый печатный журнал от больших диджитальных платформ. Сервис бронирования жилья Airbnb начал выпускать журнал совместно с известным издательским домом Hearst (Marie Claire, Harper's Bazaar, Cosmopolitan) в ноябре 2016 года. Airbnbmag пишет о путешествиях и на него даже можно подписаться. Издатель Кристофер Люкзич считает, что «печать по-прежнему является лучшим средством для рассказывания историй словами и фотографиями». Причиной, которую Airbnb заявил для своего печатного продукта, было «побудить нынешних клиентов больше путешествовать и исследовать, а также объединить бренд Airbnb».

Финансирование журнала, печать, дистрибуция, целевая аудитория и будущие редакционные темы хранятся в тайне, – пишет Пит ван Никерк на Farr. Медиабренд Grow есть и в цифровом виде: «платформа для лидерства в мышлении, которая пишет о людях, компаниях и тенденциях, бросающих вызов статус-кво». Социальная сеть нигде не промотирует его.

[\(вгору\)](#)

Додаток 5

27.06.2018

Украинские торговцы смогут принимать платежи в мессенджерах

Украинский стартап PayLastic презентовал решение для бесконтактной оплаты товаров и услуг банковскими карточками через чат-боты в мессенджерах. Для этого не требуются терминалы или отдельные мобильные приложения. Торговец может подключить и настроить сервис за несколько минут и без бумажной волокиты ([PaySpace](#)).

После этого продавец может принимать безналичные платежи через чат-боты в Telegram, Viber и Facebook. Для этого ему понадобится открыть чат-бот в одном из мессенджеров и выбрать опцию «Создать чек». Чат-бот попросит

указать сумму к оплате и выбрать платежный сервис, после чего самостоятельно сформирует чек с платежным QR-кодом.

Покупатель перейдет к оплате, отсканировав этот код с помощью обычной программы для распознавания QR-кодов. Однако если его телефон не поддерживает такой возможности, продавец может отправить вместо кода ссылку по SMS или e-mail. Оплатить свою покупку клиент сможет как банковской картой, так и с электронного кошелька. После успешной оплаты продавец получит уведомление в мессенджер.

Подключение, настройка сервиса и первый месяц использования стартап предлагает бесплатно, второй месяц и далее – \$3. При отсутствии активности плата не удерживается.

PayLastic уже доступен клиентам LiqPay (ПриватБанк), Ощадбанка, Portmone.com, WayForPay и Fondy. При помощи сервиса уже принимают платежи сети Мафия, СушиЯ, СушиМастер Украина и MeiWei (ОККО). В ближайших планах компании – продвижение в странах СНГ, Польше и Вьетнаме.

([вГору](#))

Додаток 6

2.07.2018

Facebook патентует «прослушку» через смартфон

Компания Facebook запатентовала систему, которая может удаленно активировать микрофон на телефоне пользователя, чтобы записывать окружающие звуки ([Украинский телекоммуникационный портал](#)).

Включение микрофона производится после обнаружения устройством неслышимых сигналов в телевизионной трансляции. Эта технология может быть использована для оценки эффективности рекламы или популярности телепрограмм.

В поданной Facebook патентной заявке описывается система, в которой используется неразличимый человеческим ухом звуковой «маяк» (в документе он назван «аудио-отпечатком пальца»), встроенный в звуковую дорожку телевизионных шоу или рекламы.

Когда телефон, планшет или умная колонка «слышит» этот сигнал, то включает микрофон и начинает записывать окружающие звуки. Запись затем может быть сопоставлена с базой контента, позволяющей Facebook определять, что именно смотрел человек.

Предполагается, что в технологию будет заложена опция персонификации пользователя – с ее помощью можно определить, взрослый или ребенок наблюдал за трансляцией.

Таким образом, у рекламодателя или вещателя появится информация о конкретных данных (возраст, пол) целевой аудитории. Также технология позволит узнать, переключался ли пользователь с рекламы и сколько времени

он потратил на просмотр передачи. Рисунок из патентной заявки
Рисунок из патентной заявки

Кроме того, система может использоваться для создания профилей отдельных членов домохозяйства для улучшения эффективности и создания таргентной рекламы. Такая технология также может дать Facebook лучшее понимание социальных связей людей, поскольку покажет реальную сеть контактов, с которыми люди встречаются в реальной жизни.

Эксперты, узнав о технологии, обеспокоились конфиденциальностью пользователей. Ведь система, естественно, будет записывать не только звук трансляции, но и личные разговоры людей без их ведома. На это в Facebook, который сейчас испытывает большие проблемы с конфиденциальностью пользователей, отреагировали быстро:

«Подача патентов для защиты от других компаний – это обычная практика. В связи с этим патенты, как правило, подаются на перспективные технологии, чтобы их не смогли коммерциализировать конкуренты... Технология в этом патенте не была и никогда не будет включена ни в один из наших продуктов».

Идея о том, что Facebook слушает разговоры людей и использует эту информацию для целевой рекламы, довольно давно появилась у любителей теорий заговора. Поводом стало появление в мае 2014 года функции «Идентифицировать телевидение и музыку», которая с разрешения пользователя слушала окружающий шум. Конечно, в Facebook неоднократно опровергли факты несанкционированной «прослушки», но пользователей не убедили.

[\(вгору\)](#)

Додаток 7

3.07.2018

Ирина Фоменко

Facebook и Twitter раскрыли информацию о покупателях рекламы

Два социальных медиа-гиганта раскрыли информацию, кто покупает рекламу на их платформах. Об этом сообщает The Star Online ([InternetUA](#)).

Сотрудники Facebook, директор по управлению продуктами Роб Койн и директор товарного маркетинга Эмма Роджерс заявили, что компания предпринимает шаги для повышения прозрачности рекламы на Facebook.

«Предоставление людям большей информации о какой-либо организации и объявлениях говорит о повышенной ответственности рекламодателей, которые помогают предотвратить мошенничество на Facebook», – объяснили представители компании.

Ключевой особенностью является новый раздел «Информация и реклама», где пользователи смогут просмотреть рекламу, которую организации запускают на страницах Facebook, Instagram, Messenger.

Например, проверка раздела «Информация и реклама» на странице президента Соединенных Штатов Дональда Дж. Трампа показала, что Трамп проплачивает рекламные объявления для Donald J. Trump for President Inc.

Пользователи также могут отмечать посты как подозрительные, нажав «Сообщить об объявлении». Кроме того, они могут узнать больше о деятельности страниц, например, о любых недавних изменениях в названии и дате создания.

Компания утверждает, что большинство объявлений на Facebook контролируются законными организациями, будь то малый бизнес, ищущий новых клиентов, группы адвокатов или политики.

«Злоумышленники могут использовать наши услуги для мошенничества. Эти шаги – только начало – мы всегда ищем новые способы улучшения. Повышая уровень прозрачности рекламы, мы упростим процесс устранения злоупотреблений. Так преступники будут нести ответственность за рекламу», – заявили сотрудники Facebook.

Twitter также стремится к большей прозрачности – пользователи могут искать рекламодателей и просматривать детали рекламы, например, почему остановили показ объявлений.

«Twitter – это платформа, которая позволяет вести глобальный диалог, и мы считаем, что прозрачность является основной частью», – сообщается в Ads Transparency Center.

Те, кто ищут рекламодателей для федеральных выборов, будут видеть дополнительные сведения, в том числе информацию об организациях, финансирующих кампании.

[\(вгору\)](#)

Додаток 8

4.07.2018

Чат-боти для бізнесу: безліч переваг і трохи ризиків // Все, що потрібно знати про цей інструмент маркетингу й нематеріальний актив

Використання чат-ботів дає безліч переваг, що робить їх повноцінними нематеріальними активами. Причому покупка подібного активу може обійтися порівняно дешево, зате згодом принесе бізнесу більш ніж значиму вигоду. Безпрограшний варіант, що в інвестиційному середовищі саме по собі рідкість. Отже, про яку ж вигоду для бізнесу йдеться – Mind поцікавився у Сергія Беясова, старшого оцінювача Департаменту оцінки та бізнес-моделювання аудиторської компанії Kreston GCG ([mind](#)).

Збільшення прибутку. Дослідження консалтингової компанії Gartner показує, що бренди ризикують втратити до 15 % своїх клієнтів (а, отже, й дохід), якщо не будуть оперативно реагувати на їхні звернення та запитання у соціальних мережах, месенджерах, і тим більше – телефоном. Чат-боти якраз і дозволяють оптимізувати обслуговування до максимального рівня.

Вони, з одного боку, позбавляють компанії від необхідності утримувати власні колл-центри, а з іншого – суттєво збільшують охоплення її аудиторії за рахунок цілодобової роботи. Алгоритм допоможе клієнту розібратися з важливими питаннями у будь-який час дня і ночі, не змушуючи його чекати і тим самим знижуючи його бажання піти до конкурентів. Це, звісно ж, обернеться зростанням доходів.

Зниження операційних витрат. За даними ПриватБанку, якими фінкомпанія поділилася на торішній ChatBot Conference, утримання чат-ботів обходиться на 90 % дешевше, ніж повноцінного колл-центру. При цьому різниця між рівнями задоволеності клієнтів від спілкування з живим оператором і чат-ботом зовсім невелика й складає лише 10 %.

Оптимізація внутрішньокорпоративних процесів. Сфера застосування віртуальних співрозмовників не обмежується одними лише колл-центрами. Чат-боти успішно виконують і цілий спектр інших завдань, включаючи:

- Збір та обробку даних про клієнтів.
- Включення їх до корпоративної бази даних.
- Організацію опитувань і збір відгуків про продукт компанії.
- Планування й нагадування про зустрічі, поїздки.
- Відправку розсилок в месенджери, що, до речі, куди ефективніше, ніж традиційні e-mail-розсилки. Практика показує, що кількість відкриття перших становить не менше 85 %, а от у другому випадку – лише 10-30 %.

Для малого бізнесу чат-боти також можуть бути дуже корисними. Використовуючи чат-боти у месенджерах, невеликі компанії можуть відмовитися від витрат на створення власного сайту та мобільного додатка. Досить завести публік-акаунт в Facebook і прив'язати до нього чат-бота – і ось вже клієнти можуть робити покупки або замовляти послуги через соціальну мережу так само, як якщо б користувалися офіційним сайтом компанії. Основним джерелом залучення клієнтів у такому випадку стає контекстна реклама безпосередньо в Facebook. Необхідність витратитися на Google Ads та інші рекламні майданчики помітно знижується. Це в свою чергу знижує витрати власників.

Чат-боти і Україна. В Україні одним з перших знакових прикладів застосування чат-ботів став застосунок «Приват24», запущений ПриватБанком. Чат-бот приймає заявки і обробляє їх без втрати у якості обслуговування, що спрощує роботу оператора. Останній підключається до клієнта тільки тоді, коли ситуація потребує участі людини. Функціонують також чат-боти, інтегровані ПриватБанком у платформи Telegram і Viber, через які можна здійснювати онлайн-платежі та перекази.

На медіаринку України показовий досвід використання чат-бота, створеного на платформі месенджера Viber і представленого телекомпанією «1+1». За допомогою цього чат-бота можна, не перемикаючи вкладку, подивитися проєкт «Танці з зірками». За весь час існування бота він зміг створити понад півмільйона підписників. Це ще раз доводить, наскільки ефективними можуть бути алгоритми у цифровому маркетингу.

Держустанови також освоюють чат-ботів. У сфері надання державних послуг вже функціонує чат-бот з назвою «Держслужбовець Тарас», який доступний на платформах Telegram і Facebook. Його основне завдання – допомагати в оформленні електронних декларацій, надаючи поетапні інструкції щодо заповнення. Відправною точкою для створення стала велика кількість помилок громадян при заповненні електронних декларацій.

Вартість. Зазвичай впровадження нових технологій – процес сам по собі недешевий. За ідеєю, так повинно бути і з чат-ботами, але вони в якомусь сенсі є винятком. Найпростіші алгоритми створюються швидко і не вимагають великих вкладень. Розробники чат-ботів навіть пропонують пакетні рішення у залежності від сфери застосування. Якщо немає бажання звертатися за допомогою до сторонніх організацій – в інтернеті можна знайти безкоштовні платформи для створення чат-ботів.

Одними з кращих у цьому плані вважаються Chatterpeople (створює ботів тільки для Facebook, зате безкоштовна у використанні), FlowXO (тут можна створювати ботів для різних месенджерів, але велика частина функціоналу платна), Facebook Messenger Platform (складніше у використанні і теж вимагає оплати, зате офіційна та краще інтегрована у месенджер Facebook).

Найдорожчі боти створюються на основі рішень штучного інтелекту (AI) і технологій машинного навчання (ML). До них можна віднести віртуальних помічників для мобільних телефонів, корпоративних асистентів. Вартість таких віртуальних співрозмовників може перевищувати \$100 000.

До речі, найбільш просунуті боти наразі розробляються для криптовалютного ринку. У 2018 році компанія Ephemium вийшла на ICO з метою створення криптовалютної біржі на платформі чат-бота, безпосередньо прив'язаного до месенджера. Компанія збрала софткеп у розмірі \$1,2 млн.

Hold.me, сервіс самообслуговування клієнтів за допомогою чат-бота, який веде діалог від імені реального співробітника компанії, зібрав понад \$1 млн. Одна з найяскравіших історій виходу на ICO пов'язана з проектом Drop1, який зміг залучити близько \$60 млн на розробку торгового чат-бота Dex. Останній призначений для аналізу волатильності ринку і пошуку найбільш перспективних активів. Після успіху бота Dex компанія вирішила створити нового бота – Arthur, який займається арбітражем криптовалют: він допомагає дізнатися, де вигідніше обміняти криптовалюту і отримати з цього максимальну вигоду.

Ризики. Незважаючи на свої очевидні переваги, чат-боти, як і будь-який інший актив, вимагають правильного використання. В іншому випадку їхнє впровадження в роботу бізнесу не дасть бажаного ефекту.

Перш за все слід пам'ятати, що всі створені чат-боти можуть замінити реальне спілкування тільки в досить простих бесідах. Для вирішення складних питань все одно буде потрібна допомога живого консультанта. Виняток становлять хіба що сервіси, що надають послуги доставки продуктів харчування, покупки квитків, віддаленого запису до лікаря тощо. Вони дуже

прості, і ймовірність того, буде потрібна допомога реального співробітника, вкрай низька.

У той же час важливо забезпечити оптимальну працездатність чат-бота. Тобто, програма має працювати швидко, без помилок і «гальм». В іншому випадку є ризик втратити клієнта. Адже нікому не сподобається, коли при спробі прийняти замовлення програма переплутає вимоги покупця або відповідатиме з великими інтервалами.

Також не варто намагатися замаскувати бота під живу людину. Краще відразу попереджати клієнтів, що з ними спілкується алгоритм. Так, по-перше, чесніше, а саме чесність при обслуговуванні, як показує опитування SEB, покупці цінують найбільше. По-друге, попередивши людей заздалегідь, можна уникнути неприємних непорозумінь у разі некоректної роботи бота. Уявімо, наприклад, що щось пішло не так, і ваш бот, відповідаючи клієнту в месенджері, раптом почав дублювати всі свої повідомлення. Людина, як мінімум, вирішить, що у компанії працює дивний персонал і навряд чи захоче звертатися туди у подальшому. А якщо він буде знати, що перед ним бот, то відразу зрозуміє, що це технічна несправність і, можливо, сам же попередить про це живих співробітників.

[\(вгору\)](#)

Додаток 9

25.06.2018

Мифы о технологиях и зависимости от них

В наши дни как никогда активно обсуждают возможную зависимость людей от технологий. Технологические компании даже были вынуждены встроить в свои программные продукты специальные счетчики и ограничители, которые заставляли бы нас задумываться о времени использования смартфонов. Доктора признают зависимость от компьютерных игр, и сложно даже представить, что будет дальше. Но так ли все серьезно на самом деле [\(InternetUA\)?](#)

Психолог Кристофер Фергюсон считает, что многие из заявлений о влиянии технологий на человеческий мозг и организм совершенно не заслуживают внимания. Более того, он готов разрушить несколько мифов для нас, основываясь на своем опыте работы с семьями, подростками, и их отношением к технологиям, играм и зависимостям.

Технологии – это не наркотик

Многие говорят, что использование технологий активирует те же центры удовольствия в мозге, что и наркотические вещества. Может быть это и так, но эти самые центры удовольствия вовсе не обязательно активируются чем-то вредным. Любое развлечение приводит к увеличению уровня дофамина. В этот список может попадать вкусная еда, занятия спортом или приятная беседа.

Приятные занятия увеличивают уровень дофамина на 50-100 процентов. Наркотические вещества увеличивают его на 200-350 процентов. С учетом

этого, сравнивать компьютерные игры с наркотиками – это все равно, что сравнивать каплю дождя с водопадом.

Технологическая зависимость – это не психическое заболевание

Всемирная организация здравоохранения добавила зависимость от компьютерных игр в список заболеваний. Кристофер Фергюсон считает, что люди, ответственные за это решение, не берут в расчет возможность того, что зависимость от игр может являться симптомом других психологических расстройств.

Существует огромное количество противоречий, которые не позволяют считать зависимость от технологий самостоятельным расстройством. Многие врачи это признают. Кроме того, люди, которых называют зависимыми от технологий, как правило, могут избавляться от своих расстройств легче, чем при психических заболеваниях. Обходится и без лечения.

Технологическая зависимость не вызвана технологиями

Обычно в обсуждениях утверждают, что людей привлекает сама технология. Кристофер Фергюсон считает, что люди начинают переключать свое внимание на технологии из-за депрессии, беспокойства и других проблем. Ведь никто не думает, что у людей, которые находятся в депрессии и проводят весь день в постели, постельная зависимость.

С учетом этого, стоит обратить внимание на способы лечения технологической зависимости. Если она является симптомом, значит лечить надо не ее, а реальную болезнь.

Внимание захватывают не только технологии

В этом пункте Фергюсон обращает внимание на то, что люди уделяют не меньше времени и другим занятиям. К примеру, можно увлечься йогой или танцами. Увлечься можно настолько, что это тоже станет похожим на зависимость. К слову, можно найти несколько научных статей о танцевальной зависимости. Сложно предоставить доказательства того, что технологии вызывают зависимость больше, чем танцы.

Использование технологий не приводит к самоубийствам

В качестве доказательства того, что мир современных технологий несет нам проблемы, некоторые эксперты предоставили данные о росте количества самоубийств среди подростков женского пола. Не учитывается то, что уровень самоубийств увеличился для всех возрастных групп. Рост начался в 2008 году во время финансового кризиса. Возможно, в обществе существует и более серьезная проблема, которую не замечают в пылу борьбы с технологиями.

Ученые иногда делают страшные заявления, основанные на малом объеме данных. С тем же успехом можно сказать, что употребление картофеля в пищу и самоубийства как-то связаны. К этому утверждению можно прикрепить и определенную статистику.

Разумеется, проблемы с использованием технологий могут быть. Но многие просто не могут представить сегодня свою работу без компьютеров и смартфонов, с удовольствием отдыхая от них потом. Крошечное ядро истины в

обсуждении проблем и зависимости от технологий есть. Тем не менее, нет оснований, что наступил какой-то кризис, связанный с технологиями.

(вгору)

Додаток 10

26.06.2018

Ирина Фоменко

Apple планирует опередить Facebook в борьбе с фейковыми новостями

У Apple News появилась новая миссия: команда опытных редакторов будет анализировать политические новости вместо неконтролируемых алгоритмов, которые все преувеличивают ([InternetUA](#)).

Apple заявляет, что проверка данных людьми не является новым направлением для Apple News – компания описывает его как «главный принцип» продукта уже на протяжении трех лет.

Несмотря на тенденцию использования искусственного интеллекта для поиска фейковых новостей, в Apple News всегда была команда редакторов, которая сосредоточена на «открытии и освещении историй, основанных на фактах, чтобы предоставить читателям актуальные, правдивые новости и информацию от широкого круга издателей».

«Опытные» редакторы также оценивают политические репортажи и комментарии накануне и во время выборов в США. Только те издатели, которые компания считает «надежными», становятся политическими источниками для Apple News.

Запуск раздела ориентирован на промежуточные выборы в 2018 году в США, по крайней мере, на начальном этапе – компания обязуется предоставлять «своевременную, заслуживающую доверия информацию о промежуточных выборах», а также «наиболее важные репортажи и анализы от разных издателей».

«Сейчас, более чем когда-либо, люди хотят получать информацию из надежных источников, особенно когда речь заходит о голосовании. Выборы – это не просто конкурс. Предоставляя качественные новости из надежных источников и освещая разнообразные мнения, Apple News стремится быть ответственным за обнародование информации, а также помочь читателям понять кандидатов и главные проблемы», – заявила главный редактор Apple News Лорен Керн.

Apple явно стремится избежать обвинений в политической предвзятости, поэтому в компании подчеркивают, что раздел будет включать «разные мнения», а информацию предоставят такие предприятия, как Fox News, Vox, Washington Post, Politico и Axios. Впрочем, некоторые чиновники осуждают действия Apple News как направленные против них, сравнивая их с политической цензурой.

Запуск нового раздела Apple – безусловно, ответ на серьезные неудачи, с которыми сталкиваются технические платформы на фоне политических событий. Политики и регуляторы США по-прежнему озабочены влиянием алгоритмов на демократические процессы. Несмотря на то, что почти во всех технологических компаниях существуют фейковые новости и проблема освещения мнений, Facebook в этом плане «лидирует», учитывая президентские выборы в 2016 году в США.

После этого компания объявила о множестве изменений, направленных на борьбу с таким контентом, включая системы для проверки политических рекламодателей; работу с фактчекерами; блокирование десятков подозрительных профилей; и преуменьшение роли новостей в пользу обновлений друзей.

Однако основной алгоритмический подход к программированию иерархии контента не изменился. Хотя Facebook и приходится нанимать новых сотрудников для модерации новостей (к концу года над этим будут работать 20000 человек), методы компании все еще остаются оценочными, которые являются полной противоположностью редакторскому выбору и курированию.

Таким образом, для Apple это возможность внедрить на рынке свой новостной продукт и заполнить «пробел в доверии» надежной политической информацией.

В Apple заявляют, что новый раздел предполагает «статьи от доверенных издателей Apple News», том числе обзорные материалы «о важнейших вопросах из еще не знакомых читателям источников»; и избирательную панель Washington Post, в которой контекстуализируются «ключевые данные, такие как опрос, мнения экспертов, а также информация о выборе избирателей». Раздел также будет освещать местные новости, «предоставляя качественную информацию о проблемах, важных для избирателей на предвыборных гонках».

Раздел «2018 Midterm Elections» доступен пользователям Apple News в США с 25 июня до ноября.

[\(вгору\)](#)

Додаток 11

21.06.2018

Дмитрий Демченко

«Ужасающая» реформа авторского права в ЕС и война с мемами, в которой невозможно победить

Европейский союз 20 июня ввел в действие процесс, который может впоследствии обязать онлайн-платформы – Facebook, Reddit, 4chan и другие – цензурировать контент пользователей еще до того, как он будет опубликован. Союз хочет, чтобы компании использовали технологии распознавания контента, чтобы определять видеоролики, фото, текст и код, защищенные авторским правом. Wired рассказывает, что это положение может негативно повлиять на многих интернет-пользователей – от opensource-сообщества до

создателей мемов. Инициатива получила название «Статья 13». Еще одна проблема – «Статья 11», которую называли «налогом на ссылку» и уже говорят о создании цензуры в сети. Редакция AIN.UA рассказывает, за что критикуют инициативы ЕС (AIN.UA).

Статья №13

Свои намерения Европейский союз описывает в Статье 13 «Директивы об авторском праве». Впрочем, ведущие техноэнтузиасты, среди которых создатель World Wide Web Тим Бернерс-Ли, основатель «Википедии» Джимми Уэйлс и другие, в открытом письме написали, что эта статья – «шаг к тому, чтобы превратить интернет из открытой платформы в инструмент для автоматического наблюдения и контроля пользователей».

Область действия

Несмотря на то, что действие статьи преимущественно направлено на борьбу с пиратским видео и музыкой, ее масштаб покрывает и другие виды контента. Интернет-мемы, которые чаще всего принимают форму вирусных изображений, могут попасть под ряд запретов. Это может создать невероятный прецедент, когда одна из самых самобытных форм общения в интернете будет запрещена.

Определения в Статье 13 слишком расплывчаты, говорит Кори Доктороу, активист в сфере цифрового права.

Система считает ограничения на свободу выражений нежелательным, но неизбежным побочным эффектом в борьбе за авторские права. Впрочем, автоматизированные системы не могут найти разницу между комментарием, критикой, сарказмом и просто копированием. Сами платформы не смогут нанять столько сотрудников, чтобы рассматривать каждый случай отдельно.

Технология фильтрации мемов – или, в этом случае, защищенных авторским правом материалов – потребует значительных инвестиций времени и денег на разработку. Это значит, что компании скорее всего будут отдавать эту задачу на аутсорс – вероятнее всего, таким компаниям, как Google и Amazon. Это в свою очередь, может создать ситуацию, когда публикации европейских пользователей будут анализировать американские компании – а это поднимает дополнительные вопросы об их защищенности.

Технология распознавания контента

У Google, Facebook и Amazon есть усовершенствованные алгоритмы распознавания изображений на основе машинного обучения. TinEye использует хеши в качестве уникальных подписей для идентификации определенных изображений целиком или частично, а Google использует подобный метод для определения копий фильмов, которые загружены на Drive.

Проверка текста более проста. Обнаружением текстового плагиата занимаются компании Grammarly и Plagiarism Checker X, хотя они ограничены объемом доступного контента. В отличие от сервиса CopyLeaks, который позволяет владельцам авторских прав видеть, была ли их работа скопирована в интернете. Система идентификации контента YouTube обнаруживает материалы, защищенные авторским правом, путем сопоставления загруженных

видео пользователей с аудиодорожками, которые владельцы авторских прав могут загружать в специальный портал для проверки.

Однако часто встречаются ложные и неточные претензии к авторскому праву, в то время как большое количество «защищенных» материалов публикуется на платформе незаметно от авторов. «Эти системы несовершенны, они будут срабатывать когда нужно и когда не нужно. Большие медиакомпании смогут быстро разблокировать контент, если неправильно попал под нарушение. Но не обычные пользователи», – говорит Доктору.

Такие автоматические системы также рискуют удалять важный контент только из-за того, что в нем случайно оказался материал, защищенный авторским правом. Они будут игнорировать принцип «честного использования», когда нарушения права допустимы. Доктору подчеркивает, что это может привести к харрасменту и даже заглушению публичных дискуссий.

Природа таких систем позволит вредительным пользователям создавать множество нерелевантных жалоб на якобы нарушение авторского права. «Создавать такие жалобы намного проще, чем их решать. Платформам, как Twitter, “Википедия” и другим, придется управлять армиями людей, чтобы сортировать жалобы и удалять нерелевантные. А если удалят законное требование об авторском праве, то столкнутся с невероятной ответственностью», – говорит Доктору.

Статья №11

Статья №11 также получила название «налога на ссылку» или «сниппет-налога». Она создана, чтобы ограничить влияние крупнейших контент-издателей, вроде Facebook и Google. Статья ужесточает закон об авторских правах и обязует платформы платить за лицензирование ссылок на источники новостей. Теоретически, это должно помочь независимым издателям и привлечь пользователей на их главные страницы, а не только на отдельные истории из новостных фидов. Однако статья даже не определяет понятие «ссылки», этот вопрос останется на рассмотрении 28 стран-членов ЕС.

Критики постановления указывают, что это создает широкие возможности для цензуры и политического давления на популярные новости. Также при наличии множества вариантов одного постановления, издателям придется равняться на самую строгую из списка.

Член Европарламента Джулия Реда, которая выступала против принятия новых статей, проиллюстрировала опасность этой ситуации в комментарии изданию The Next Web:

«Предложение “Ангела Меркель встретила с Терезой Мей”, которое может быть заголовком новостной заметки, не может защищаться законом о копирайте, потому что это утверждение факта, а не оригинальное творение. Мистер Восс (защитник Статьи №11 – прим. ред.) несколько раз заявил, что он хочет внести эти, полностью фактические заявления, под действие Статьи №11 и таким образом обеспечить издателям более широкую защиту в сравнении с той, какой обеспечены сами журналисты».

Реда также отметила, что чрезмерное цитирование или полная «кража» новостей уже находятся вне закона, а единственная цель нового закона – ограничить использование ссылок. Алекс Восс не согласен с такой трактовкой и отмечает, что благодаря принятию закона в 28 странах сразу, платформы не смогут просто так отказаться от какого-то источника новостей:

«Конечно, может случиться, что большие технологические компании заявят об уходе из Европы, если им придется платить. И они точно могут это сделать, если не хотят платить за контент из Европы. Они могут взаимодействовать с издателями, вроде Russia Today и China Daily».

Восс также не видит, как новая статья может ударить по рядовым гражданам. Он отмечает, что пользователи сохранят все нынешние возможности и смогут ссылаться, копировать информацию, но только для личных целей. Парламентарий отметил:

«Может, они не смогут получить все новости на одном сайте, но все по-прежнему будет доступна на сайтах издателей».

Рейган МакДональд, топ-менеджер и руководитель европейского отдела Mozilla, тоже высказался против новых постановлений. По его мнению, Статья №11 лишь усложнит конкуренцию на рынке и спровоцирует негативные последствия.

Копирайт должен стимулировать и поддерживать авторов, он должен подстегивать инновации и служить обществу. Но то, о чем говорят статьи №11 и, в особенности, №13 – полное непонимание работы копирайта.

([вгору](#))

Додаток 12

21.06.2018

Владимир Кондрашов

Украинские депутаты хотят ввести цензуру в Интернете

Верховная Рада Украины включила в повестку дня законопроект №6688 о внесудебной блокировке сайтов, который де-факто, устанавливает цензуру в сети Интернет ([InternetUA](#)).

Об этом на своей странице в Facebook сообщила народный депутат Украины, первый заместитель председателя Комитета ВР по вопросам свободы слова и информационной политики Ольга Червакова.

– Внесудебное блокирование сайтов – это возвращение даже не к Януковичу, а к самому Сталину! Даже законы 16 января предусматривали необходимость решения суда для блокировки интернет-ресурсов, – написала нардеп.

Включить документ в повестку дня сегодня получилось только со второй попытки – «за» проголосовали 238 человек. До этого, его также пытались включить в повестку дня парламента 13 июля прошлого года и 19 июня 2018-го, но тогда голосов не хватило.

Законопроект №6688 «О внесении изменений в некоторые законодательные акты Украины относительно противодействия угрозам национальной безопасности в информационной сфере» инициирован нардепами Иваном Винником, Дмитрием Тымчуком и Татьяной Чорновил.

– Законопроект имеет благородное название – «по противодействию угрозам национальной безопасности в информационной сфере». Такими угрозами предлагается считать «оказание воздействия на принятие решений или совершение или несовершение действий органами государственной власти или органами местного самоуправления, должностными лицами этих органов, объединениями граждан, юридическими лицами». Авторы законопроекта предлагают считать это частью «технологического терроризма», – пишет Червакова. – Службе безопасности Украины предоставляется право без решения суда с помощью провайдера блокировать доступ к любому информационному ресурсу. Основанием для этого может быть уже не только решение суда, но и решение прокурора, следователя, согласованного с прокурором, или решение СНБО.

Также документом предлагается внести изменения в законодательство, регулирующее правоохранительную деятельность в информационно-телекоммуникационной сфере, направленные на «усиление уровня ответственности и повышение размера штрафных санкций по отношению к операторам, провайдерам телекоммуникаций, предоставляющим услуги доступа в Интернет за нарушение условий и правил, регламентирующих деятельность в сфере телекоммуникаций и пользования радиочастотным ресурсом Украины, предусмотренную лицензиями, разрешениями, а также порядка и условий предоставления услуг связи в сетях общего пользования».

В прошлом году, когда данный документ только появился, Уполномоченная ВР по правам человека, руководители Украинского Хельсинского союза по правам человека и Харьковской правозащитной группы заявляли, что законопроект № 6688 посягает на права человека и подрывает саму суть права на свободу выражения мнения.

13 июля 2017 года Интернет Ассоциация Украины опубликовала открытое письмо к депутатам Верховной Рады касательно законопроектов-«близнецов» №№ 6676 та 6688, которые предусматривают радикальное расширение полномочий силовиков в сфере внесудебного блокирования информации, создание монопольной среды на рынке телекоммуникаций за счет обязательства операторов осуществлять многомиллионные закупки оборудования для анализа и блокировки трафика, предоставления чиновникам дополнительных механизмов коррупционного влияния на рынок и другие «изобретения» известных тоталитарных режимов.

– По итогам украинский пользователь получит интернет-цензуру, медленный Интернет от нескольких провайдеров-монополистов по «европейской» цене. И это под лозунгом защиты информационной безопасности государства, которая собственно и состоит из этих пользователей,

– заявляли тогдa в ИНАУ. – Интернет Ассоциация Украины призывает народных депутатов к ответственности и взвешенности и просит не допустить поддержки антидемократических, диктаторских подходов к решению вопросов безопасности в информационной сфере.

Против законопроектов №№ 6676 та 6688 направлено и совместное заявление общественных организаций «Интерньюз-Украина», «Детектор медиа», «Институт массовой информации», «Информационная безопасность», Фондации «Суспільність» и Национального союза журналистов Украины:

– В условиях военного конфликта государство имеет право накладывать определенные ограничения на свободу Интернета с точки зрения безопасности страны. Однако, предлагая законопроекты №6676 и № 6688 народные депутаты заимствуют методы и подходы агрессора – Российской Федерации по регулированию Интернета, – говорится в заявлении. – Внедрение предложенных норм способно привести к сворачиванию прав и свобод граждан и преследование политических оппонентов безотносительно к защите безопасности страны.

Однако адекватной реакции от парламентариев на эти и десятки других обращений общественности не последовало.

([вгору](#))

Додаток 13

26.06.2018

СБУ викрила адміністраторів антиукраїнських груп у соцмережах

Співробітники Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБ України та його регіональних підрозділів викрили у червні групу адміністраторів антиукраїнських спільнот в соціальних мережах, які діяли за вказівкою спецслужб РФ ([InternetUA](#)).

Службою безпеки України під час реалізації комплексу заходів із забезпечення інформаційної безпеки фіксується активізація протиправної діяльності з боку російських спецслужб через використання соціальних мереж в Інтернеті на шкоду державній безпеці нашої країни.

Фахівці спецслужби відзначають, що загострення цієї тенденції спостерігається напередодні відзначення державних свят в Україні. Відбувається активізація РФ та її спільників щодо розповсюдження інформаційних матеріалів, які поширюють ідеї «української псевдодержавності» та зміни державної влади і територіальної цілісності, намагаються загострити суспільно-політичну ситуацію в країні, розпалити міжнародну ворожнечу, а також спровокувати масові акції провокативного характеру, що можуть негативно вплинути на імідж України на міжнародній арені.

Оперативниками СБ України у червні 2018 року виявлено, локалізовано та припинено протиправну діяльність групи з п'яти громадян України, серед яких двоє мешканців Києва, а також жителі Одеси, Запоріжжя і Маріуполя, які

були адміністраторами антиукраїнських спільнот у соціальних мережах «ВКонтакте» і «Однокласники».

Зловмисники, діючи за вказівкою спецслужб РФ та отримуючи від них матеріальну винагороду, розповсюджували в соцмережах спеціально підготовлені матеріали, які містили заклики до зміни меж території України в антиконституційний спосіб, а також підтримували терористичну діяльність незаконних збройних формувань «ДНР» та «ЛНР».

У рамках відкритих кримінальних проваджень правоохоронці провели невідкладні процесуальні дії, внаслідок яких припинено протиправну діяльність адміністраторів, зокрема виявили комп'ютери та мобільні телефони, які використовувалися для розповсюдження антиукраїнського контенту.

Тривають слідчі дії.

Загалом з початку 2018 року Департаментом контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ та його регіональними підрозділами стосовно власників та адміністраторів спільнот у соціально орієнтованих ресурсах мережі Інтернет «ВКонтакте» та «Однокласники», котрі поширювали заклики до повалення конституційного ладу та державної влади в країні, проведення масових заворушень та інших протиправних дій, зареєстровано двадцять чотири кримінальні провадження. П'ятнадцяти особам оголошено про підозру в скоєнні злочину, винесено шість обвинувальних вироків суду за ознаками вчинення злочинів, передбачених ст. 109 (дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади), ст. 110 (посягання на територіальну цілісність і недоторканість України), ст. 258-3 (створення терористичної групи чи терористичної організації) Кримінального кодексу України.

([вгору](#))

Додаток 14

2.07.2018

Ирина Фоменко

Силовики злоупотребляют технологией распознавания лиц

Когда полиция задержала подозреваемого за стрельбу в редакции газеты The Capital Gazette 28 июня, он отказался назвать свое имя. Поэтому власти идентифицировали человека, Джаррода Рамоса, используя другой метод: технологию распознавания лиц. Об этом сообщает The New York Times ([InternetUA](#)).

За последние несколько лет технология распознавания лиц была спокойно принята властями Соединенных Штатов, в том числе полицейскими, и стала частью стандартного инструментария правоохранительных органов.

Согласно докладу Юридического центра Джорджтауна по вопросам конфиденциальности и технологий, 16 штатов позволили Федеральному бюро расследований использовать технологию для сравнения лиц подозреваемых преступников с фото на водительских правах и ID. Благодаря недавним

улучшениям в этой области некоторыми из крупнейших в мире IT-компаний, влияние технологии на полицейскую деятельность, вероятно, будет только расти.

«Технология распознавания лиц является одним из самых важных событий в борьбе с преступностью с момента обнаружения отпечатков пальцев в XIX веке. Трудно представить полицейский отдел в Соединенных Штатах с более чем 10-15 служащих в нем, у которых нет доступа к распознаванию лиц», – заявил исполнительный председатель ID4Africa Джозеф Дж. Атик.

Стоит отметить, что сторонники новой технологии считают ее серьезным инструментом для ловли преступников, но эксперты по гражданским свободам предупреждают, что это может быть инструмент массового наблюдения.

Дискуссия продолжается, поскольку такие высокотехнологичные компании, как Amazon, недавно раскритиковали за предоставление технологий распознавания лиц правоохранным органам. В прошлом месяце более двух десятков гражданских правозащитных организаций попросили Amazon прекратить продажу своей системы распознавания лиц Rekognition властям.

Члены организаций утверждали, что Rekognition может не только отслеживать людей, но и идентифицировать «до 100 лиц на сложных фотографиях», а также номерные знаки, снятые камерами движения. Так, система способна определить лица многих простых граждан, а не только преступников.

По данным экспертов в этой области, полиция не нарушала неприкосновенность частной жизни людей во время применения технологии распознавание лиц. Служащие правоохранных органов просто подтверждали личность подозреваемого, который ранее уже был под арестом.

Начальник отдела полиции округа Анн-Арандел в штате Мэриленд Тимоти Алтомаре заявил в пятницу, что полиция использовала Maryland Image Repository System, чтобы идентифицировать Рамоса, когда он отказался сотрудничать со следователями. Сначала они попытались определить личность преступника по отпечаткам пальцев, однако этот процесс довольно долгий, поэтому полиция воспользовалась новой технологией. В частности, фотографию Рамоса отправили в Центр координации и анализа штата Мэриленд.

Вычислительные системы теперь могут просматривать фотографии или видеоролики и сопоставлять их с изображениями в существующей базе данных лиц, что было невозможно еще пять лет назад. Эти системы также сканируют базы данных гораздо быстрее, чем аналитики.

Американские военные и разведывательные службы в течение многих лет пользовались новой технологией в Ираке и Афганистане для выявления потенциальных террористов. Совсем недавно она стала доступна для полицейских отделений в Соединенных Штатах.

Ожидается, что большинство компаний (например, Amazon, NEC и Cognitec) расширят свои предложения по технологии распознавания лиц.

Аппаратное и программное обеспечение также стало менее дорогостоящим, что способствовало запуску множества стартапов и других предприятий.

Полицейские отделы могут создавать подобную технологию самостоятельно. «Если бы полиция наняла меня на летнюю стажировку, я бы придумал им достойный алгоритм распознавания лиц», – заявил исследователь Массачусетского технологического института Джонатан Франкле.

Вопросы о конфиденциальности и опасения относительно потенциального злоупотребления технологией распознавания лиц также, вероятно, будут возрастать, тем более, что системам требуется большая база данных изображений. Согласно недавнему отчету Счетной палаты США, база данных ФБР охватывает 400 млн изображений.

По словам старшего юриста Electronic Frontier Foundation Дженнифер Линч, местные правоохранительные органы могут искать фото с водительских прав в государственных базах данных. Получается, что миллионы простых граждан попадут под надзор. «Люди, которые находятся в базе данных водительских прав, не согласились участвовать в уголовном розыске каждый раз, когда полиция ищет подозреваемого», – утверждает Линч.

Еще одна проблема заключается в том, что системы распознавания лиц иногда допускают ошибки, сопоставляя изображение с человеком. Это особенно важно, когда фотографии сняты на камеры слежения, которые не всегда обеспечивают четкое изображение. Даже в хороших условиях технология распознавания лиц частично не работает. По словам Франкле, количество таких ошибок может увеличиться по мере роста баз данных потенциальных подозреваемых.

«Точность этих систем зависит от многих факторов, включая размер базы данных. Технология может ухудшиться по мере увеличения базы данных», – считает Франкле.

([вгору](#))

Додаток 15

22.06.2018

Нацполиция задержала хакера, который взламывал соцсети украинцев и требовал выкуп

Правоохранители разоблачили хакера из Львовской области, занимавшегося несанкционированным вмешательством в работу учетных записей социальных сетей и распространением вредоносного программного обеспечения. Об этом сообщает пресс-служба Департамента киберполиции Нацполиции Украины ([IGate](#)).

Преступную деятельность хакера раскрыли сотрудники Карпатского управления Департамента киберполиции Национальной полиции Украины при процессуальном руководстве Львовской местной прокуратуры №1.

По информации пресс-службы, житель Львовской области, владея необходимыми навыками в сфере программирования, создал веб-сайт `hackerki-`

poslygu[.]hol.es, на котором предлагал свои услуги по взлому учетных записей, электронных ящиков и т. п. Вся переписка между ним и клиентами происходила с помощью закрытого сообщества, которое администрировал киберпреступник в этой же соцсети. При общении с клиентами он также отправлял им ссылку на якобы форму обратной связи. Однако, переходя по этой ссылке, пользователи попадали на фишинговую страницу, с помощью которой происходила компрометация (несанкционированный доступ к защищенной информации – Ред.) их логинов и паролей.

В дальнейшем хакер проверял украденные данные авторизации по всем соцсетям и популярным веб-ресурсам. Затем он блокировал доступ к учетным записям пользователей путем изменения пароля. За возвращение доступа злоумышленник требовал деньги. Суммы, которые он запрашивал, колебались в зависимости от платежеспособности жертвы.

Отмечается, что в этом же сообществе под видом приложения для взлома соцсетей, мужчина разместил для свободной загрузки вредоносное программное обеспечение, которое предназначалось для несанкционированного вмешательства в работу мобильных телефонов на базе Android. Таким образом, хакер имел возможность просматривать телефонную книжку, фотографии и записи входящих и исходящих вызовов жертвы.

Правоохранители провели санкционированный обыск по адресу фактического места проживания злоумышленника. По результатам этого обыска была изъята компьютерная техника, которую хакер использовал для противоправной деятельности, а также мобильный телефон и дополнительные носители информации.

Теперь мужчине объявлено о подозрении в совершении уголовных правонарушений, предусмотренных ч. 2 ст. 361 УК Украины и одному факту по ч.1 ст. 361-1 (создание с целью использования, распространения или сбыта вредных программных или технических средств, а также их распространения или сбыта) УК Украины.

([вгору](#))

Додаток 16

25.06.2018

Как защитить свои данные в Интернете

Адвокат рассказала, как обезопасить фотографии и другие данные в интернете авторским правом ([InternetUA](#)).

Каждый человек даже не догадывается, что может не нарочно нарушить чье-либо авторское право или кто-то другой нарушит его права, которые охраняются законом. Это статья 2 Бернской конвенции, которая охраняет права по международному законодательству, статья 8 Закона Украины «Об авторском праве и смежных правах», а также статья 433 Гражданского кодекса Украины, которая определяет объекты правовой защиты.

Такая законодательная охрана означает, что автор владеет правом, которое никто не может нарушить, и без его согласия нельзя использовать продукт творческой деятельности. Также существует так называемая презумпция авторства, а создание произведения, по сути, и является тем фактором, с которого она начинается.

Для сохранения авторства произведения необходимо, чтобы оно приобрело предметное значение. Т.е. произведение должно быть в материальном (например, экземпляр фотографии) или цифровом виде (в интернете).

Как можно защитить фотографии авторским правом

Первое, что желательно сделать, хотя это и не требуется четко законом, – зарегистрировать такое право. Для этого автор произведения должен обратиться в Министерство экономического развития и торговли Украины с заявлением о регистрации авторского права. Нужно будет предоставить экземпляр такого произведения и оплатить небольшую госпошину.

Следует знать, что автор, например, фотографии может защитить свое произведение знаком Copyright, нанести свои инициалы, псевдоним или логотип. Также существует возможность срезать край своего фотографического произведения, уменьшить качество, сделать снимок прозрачным или расписаться на краю фото. В последствии, в случае возникновения спора можно будет доказать свое авторство.

Какие данные лучше не размещать в социальных сетях

По мнению специалистов по безопасному поведению в интернете, в социальных сетях, чатах и на сайтах знакомств ежедневно участвует около 800 тысяч (!) злоумышленников. Поэтому во всемирной паутине следует быть очень осторожным.

Во-первых, не указывайте на своих страницах дату и место Вашего рождения. Ведь очень часто эти данные используются гражданами как пароли доступа к банковским картам и другим реквизитам. Также нежелательно всем рассказывать о своих планах на путешествие или поездку: во время Вашего отсутствия квартира остается уязвимым местом перед преступниками.

Обращайте внимание на тех людей, которых добавляете себе в «друзья». Некоторые могут оказаться недоброжелателями, которые, завладев, возможно, Вашей личной информацией, могут использовать ее как компромат против Вас. При этом не стоит забывать, что размещение фотографий, на которых изображены посторонние лица, также может сулить неприятности: от такого человека необходимо получить соответствующее разрешение. Это предусмотрено статьями 307-308 Гражданского кодекса Украины.

Свободно размещать на своей «стене» Вы можете фотографии, сделанные на улице или в других публичных местах. Это право человека быть изображенным на фотографиях также охраняется авторским правом.

Можно ли защитить авторским правом фотографии на страницах социальных сетей Facebook, Instagram

И Facebook, и Instagram в своей деятельности руководствуются определенными Правилами, которые, к сожалению, мало кто читает. А эти инструкции предусматривают, что лицо имеет право размещать какой-либо контент только тогда, когда он принадлежит этому лицу, либо человек имеет на него разрешение от владельца. Поэтому Ваша публикация уже подразумевает наличие таких разрешений.

В случае нарушения Ваших прав можно обращаться с жалобой к администрации соцсети. После этого контент будет заблокирован, а нарушителю будут отправлены данные (имя и электронный адрес) настоящего владельца.

Какая предусмотрена ответственность за нарушение прав в интернете
Закон Украины «Об авторском праве и смежных правах» предусматривает гражданскую, административную и уголовную ответственность за нарушение авторского права. В последнее время были приняты изменения в законодательстве: теперь лицо, права которого были нарушены, может обратиться к собственнику сайта или представителю услуг с требованием о прекращении такого нарушения. Причем обратиться можно с помощью адвоката, который Вам поможет с написанием необходимого заявления, правильной фиксацией самого правонарушения и дальнейшими судебными разбирательствами, если они последуют.

Если Ваше обращение к владельцам ресурса, нарушившего Ваши права, будет проигнорировано в течение 3 дней, то статья 164-17 Кодекса Украины об административных правонарушениях предусматривает штраф от 500 до 1000 необлагаемых минимумов доходов граждан. Если автору произведения нанесены убытки в размере, в 20 и более раз превышающем минимальный доход, нарушитель может быть привлечен к уголовной ответственности.

В любом случае, если в добровольном порядке урегулировать спор не получается, следует обращаться в суд и требовать возмещения ущерба в сумме от 10 до 50000 минимальных зарплат.

([вгору](#))

Додаток 17

25.06.2018

Мошенники распространяют вирусы под видом информации о ЧМ-2018

Исследователи из компании Check Point выявили новую схему заражения компьютеров вирусами. Их распространяют под видом файлов с расписанием игр и турнирной таблицы Чемпионата мира по футболу 2018 ([InternetUA](#)).

В случае открытия сомнительного «футбольного» файла приложение запускает вариант вредоносного ПО под названием DownloaderGuide. Это загрузчик потенциально нежелательных программ, который чаще всего используется в качестве установщика для таких приложений, как панели инструментов, рекламное ПО или системные оптимизаторы.

Исследователи Check Point обнаружили, что в общей сложности кампания включает девять различных исполняемых файлов, все из которых были отправлены по электронной почте с использованием темы:

[World_Cup_2018_Schedule_and_Scoresheet_V1.86_CB-DL-Manager](#).

Первое сообщение о заражении поступило 30 мая 2018 года, а пика активность преступников достигла со стартом чемпионата мира.

«События, которые привлекают большое количество людей, – отличная возможность для киберпреступников, чтобы запустить вредоносную кампанию. Злоумышленники делают ставку на то, что из-за шумихи вокруг Чемпионата мира сотрудники компаний теряют бдительность и открывают подозрительные письма и вложения», – отметила руководитель группы Threat Intelligence компании Check Point Software Technologies Майя Хоровиц.

Пользователей призывают обновлять программное обеспечение, остерегаться поддельных веб-сайтов и электронных писем от неизвестных отправителей. В частности, кибер-преступники, скорее всего, «отправят множество фишинговых писем во время турнира, предлагая ряд бесплатных предложений или записей на розыгрыш билетов на матч». Отдельно эксперты просят остерегаться публичных точек Wi-Fi.

«В дополнение к этому, организации должны также принять меры для обеспечения того, чтобы фишинговые письма не попадали в почтовые ящики в первую очередь. Это должно включать использование многоуровневой стратегии кибербезопасности, которая защищает как от известных вредоносных программ, так и от новых угроз», – подчеркнули в Check Point.

[\(вгору\)](#)

Додаток 18

2.07.2018

Ирина Фоменко

Интернет вещей способствует домашнему насилию

Nest Hello прекрасно вписывается в тенденцию «умных» сетевых устройств, пишет The Guardian. Дверной звонок Nest Hello позволяет узнать, кто стоит снаружи, он также снимает HD-видео и фото. Кроме того, компания выпускает Nest Learning Thermostat – «электронный, программируемый и самообучаемый термостат с поддержкой Wi-Fi, который оптимизирует отопление и охлаждение домов и предприятий для экономии энергии» [\(InternetUA\)](#).

Такие сетевые устройства значительно упрощают жизнь: вместо того, чтобы искать в Интернете прогноз погоды или рецепт, достаточно просто попросить Алекса об этом. Если вы отправляетесь в отпуск и забываете выключить центральное отопление, то это можно сделать через Nest с помощью смартфона. Если кто-то звонит в дверь, когда вас нет дома, можно узнать, кто пришел, а также отправить предварительно записанное сообщение.

Однако существуют две вещи, на которые стоит обратить внимание. Во-первых, безопасных сетевых устройств нет. Во-вторых, с помощью «умных» гаджетов производители собирают данные о происходящем в доме пользователя. Это особенно важно для трех компаний – Google, Facebook и Amazon. Они не могут собирать данные, когда клиент отключает доступ. Таким образом, еще одно устройство, подключенное к Wi-Fi, стало для крупнейших компаний победой. Согласно McKinsey, за 2016 год в 29-метровых домах в США количество «умных» девайсов возросло на 31 %.

Главный недостаток заключается в том, что если вы можете включить душ или центральное отопление со своего смартфона, то так же хакер может проникнуть в вашу домашнюю сеть. Впрочем, это под силу не только взломщику – контролировать «умные» устройства может и бывший партнер, любовник или квартирант, зная пароль.

Согласно исследованию The New York Times, злоумышленники используют сетевые домашние устройства для контроля и преследования жертв. Преступники могут включать музыку, менять освещение или температуру для запугивания. По словам пострадавших, в их домах включались кондиционеры, менялись кодовые номера цифровых замков входной двери. Как сообщает The New York Times, эти истории говорят о новой модели поведения в случаях домашнего насилия, когда «новейшие удобства также используются в качестве средства преследования, контроля и мести».

Как и все, что связано с цифровыми технологиями, это своего рода гендерный феномен. Большинство жертв – женщины, а обидчики – преимущественно мужчины. Почему? Ответ прост: сетевые устройства в основном покупают и устанавливают мужчины. Если только они знали пароли от гаджетов, то жертвы не смогут их поменять.

[\(вгору\)](#)

Соціальні мережі

як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень

Додаток до журналу «Україна: події, факти, коментарі»

Упорядник **Терещенко Ірина Юріївна**

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, Голосіївський просп., 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
Сайт: <http://nbuviar.gov.ua/>
<http://siaz.ukr/>

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