СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(3.01–16.01)

2017 № 1

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(3.01–16.01)
№ 1

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, 2017

Київ 2017

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

3.01.2017

WhatsApp прекращает поддержку клиента для миллионов устаревших iOS и Android-устройств

Популярный мобильный мессенджер WhatsApp больше не будет работать на многих устаревших моделях смартфонов. Об этом объявили представители компании по средствам официального блога (IGate).

В ближайшее время в мессенджере появится ряд новых возможностей, с которыми уже не смогут справляться старые устройства с ограниченными аппаратными возможностями.

«Не смотря на то, что некоторые смартфоны остаются частью нашей жизни, они просто не смогут поддерживать возможности, которые мы запустим в ближайшее время. Для нас это было трудным решением, но правильным для того, чтобы предоставить людям более эффективные способы общения и поддержания связи с друзьями, семьей и близкими через WhatsApp», – отметили в компании.

WhatsApp прекращает поддержку приложения для следующих платформ:

Android 2.1, Android 2.2,

Windows Phone 7

iPhone 3GS / iOS 6.

При этом мессенджер продлевает поддержку операционных систем BlackBerry, BlackBerry 10, Nokia Symbian S60 и Nokia S40 до 30 июня 2017 г., несмотря на то, что ранее от них также хотели отказаться в начале года.

***

9.01.2017

«ВКонтакте» ввела новий сімейний стан

Адміністрація російської соціальної мережі «ВКонтакте» вирішила ввести новий статус, що звучить не інакше, як «у цивільному шлюбі». З цього моменту користувачі отримали можливість вказувати новий сімейний стан («Znaj.ua»).

Про це повідомили російські ЗМІ.

Керівництво «ВКонтакте» заявило, що новий статус уже доступний для користувачів десктопної та мобільної версій сайту.

Маркетологи також зацікавилися новим статусом. Вони активно займуться вивченням людей, для яких слово «весілля» вважається чимось незрозумілим і далеким.

***

13.01.2017

Facebook создаст технологию чтения мыслей

Facebook займется разработкой нейрокомпьютерных технологий, с помощью которых можно будет читать и передавать мысли. Об этом основатель и глава соцсети М. Цукерберг рассказал во время очередной сессии вопросов и ответов (Finance.Ua).

«Я думаю, однажды мы сможем общаться друг с другом, передавая мысли с помощью компьютерных технологий. Вы просто подумаете о чем-то, и ваши друзья смогут вас “услышать”», – сказал основатель сети.

В середине 2016 г. Facebook сформировал секретное исследовательское подразделение Building 8, которое, по слухам, занимается разработкой технологий для передачи мыслей с помощью компьютеров. Сотрудники Building 8 должны иметь опыт работы с «нейровизуализацией» и «электрофизиологическими данными».

На должность инженера нейрокомпьютерных технологий подразделению требуется доктор наук по нейробиологии, а в описании другой вакансии указано, что соискатель должен быть специалистом по разработке «алгоритмов обработки аудиосигналов» для создания «коммуникационной вычислительной платформы будущего».

С сентября 2016 г. Building 8 возглавляет М. Шевийе (Mark Chevillet) – автор образовательной программы по прикладной нейробиологии для Университета Джонса Хопкинса.

***

12.01.2017

Новая версия WhatsApp получила функцию поиска GIF-изображений

Бета-версия мессенджера WhatsApp получила поддержку поиска gif-картинок. Информацией об этом поделились разработчики (Grifonsoft).

Возможность использовать гифки в сообщениях мессенджера появилась давно, но до сих пор пользователи WhatsApp могли загружать лишь уже имеющиеся на устройствах гифки или просить помощи у сторонних приложений, которые были не очень удобны.

Теперь найти нужное gif изображение можно будет при помощи кнопки эмодзи, находящейся слева от текстового поля, и через нее пользователь получает доступ к библиотеке изображений Giphy. Кроме того представляется возможным поиск по ключевым словам.

Нововведение было анонсировано для бета-версии 2.17.6 WhatsApp. Пока неизвестно, когда именно она будет доступна для всех в постоянной версии мессенджера.

***

12.01.2017

Twitter предупреждает о закрытии своего приложения Dashboard

Компания Twitter предупреждает о закрытии своего приложения Dashboard. Известно, что оно позволяет управлять бизнес-аккаунтами, а закрытие произойдет уже в следующем месяце (Grifonsoft).

Специальная панель Dashboard появилась в социальной сети летом 2016 г., и по плану разработчиков она должна была помогать людям управлять их счетами в бизнесе. Создатели Twitter посчитали, что эта функция себя не оправдала, поэтому сейчас нужно от нее отказаться.

Представители Twitter утверждают, что переживать из-за закрытия Dashboard не нужно, ведь все функции, которые были в приложении, будут появляться в будущих проектах компании.

***

13.01.2017
Альона Мазуренко
Facebook запускає проект по боротьбі з фейками в ЗМІ

Компанія Facebook запускає проект The Facebook Journalism Project, спрямований на боротьбу з фейками в ЗМІ та інформування користувачів про способи пошуку достовірної інформації в епоху цифрових технологій. Про це повідомляє Facebook media, передає УНН (Українські Національні Новини).

Проект складатиметься з трьох напрямів: співпраця з великими ЗМІ і розробка нових продуктів, проведення спеціальних навчальних тренінгів для журналістів, допомога користувачам соцмережі в пошуку якісної та достовірної інформації.

Проект також тестуватиме нові бізнес-моделі для ЗМІ, сприятиме просуванню незалежних медіа в Facebook, організовуватиме хакатони для розробників з новинних видань.

Уже найближчим часом проект почне співпрацю з Washington Post і Vox. Надалі цей список планують розширювати.

У компанії також повідомили про те, що вже підготовлена серія навчальних курсів по продуктах Facebook, інструментах і послугах для журналістів.

Напередодні стало відомо, що Facebook тестує новий спосіб боротьби з фейковими новинами. Компанія зосередилась на повідомленнях, які задля власної вигоди поширюють спамери.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

11.01.2017

Більшість американців бажають, щоб Трамп видалив акаунт у Twitter

Про це говорить недавнє опитування, передає Depo.ua з посиланням на CNN.

Згідно з опитуванням Вінніпегського університету, 64 % громадян США виступили за закриття акаунту Д. Трампа, який був зареєстрований в 2009 р. і має понад 19 млн читачів (depo.ua).

Опитування показало, що 71 % у віці від 18 до 34 років виступають за видалення облікового запису обраного президента. Думки республіканців на цей рахунок розділилися: 49 % вважають, що Д. Трампу варто продовжувати вести запис, 45 % виступили проти цього.

Відзначають, що Д. Трамп опублікував понад 34 твіттів і з моменту обрання його президентом не подав знаку про те, що він збирається припиняти вести акаунт.

***

11.01.2017

Прощальний «твіт» Обами став найпопулярнішим на його сторінці

Прощальне повідомлення Б. Обами в ролі президента США стало найпопулярнішим за час його президентства, передає Радіо Свобода. «Твітом» поділилися понад півмільйона користувачів (LB.ua).

«Спасибі за все. Моє останнє прохання таке ж, як і перше. Я прошу вас вірити – не я в змозі щось змінювати, а ви», – написав президент у мікроблозі.

Як відзначає агентство Associated Press, до цього найпопулярнішим був пост Б. Обами, опублікований після легалізації в США одностатевих шлюбів.

Після інавгурації обраного президента Д. Трампа аккаунт глави держави перейде в його розпорядження.

***

11.01.2017

Ольга Карпенко

Киевская команда запустила поиск украинских IT-специалистов в LinkedIn

Киевская команда запустила проект TurboHiring – это онлайн-форма поиска кандидатов из Украины на IT-специальности. Пока что проект находится в бете и работает только с LinkedIn (AIN.UA).

Сейчас в команде проекта всего три человека, а самому стартапу – несколько месяцев. Идея проекта принадлежит разработчику Ю. Герасимову, она сформировалась из необходимости найти себе в команду программиста, а LinkedIn не смог с этим помочь в полной мере.

Информацию о кандидатах в выдачу поиска сервис берет из LinkedIn, но в будущем команда планирует добавить и другие источники. По словам основателей, сейчас в базе проекта – порядка 62 703 айтишников из Украины. «Если верить отчету DOU, это 60 % всего IT-рынка Украины», – говорит сооснователь проекта А. Бублиенко.

Чтобы искать кандидатов в TurboHiring, нужно зарегистрироваться, бесплатно можно искать до трех кандидатов, чтобы увидеть все результаты, нужно оплатить месячную подписку в 500 грн.

Поиск через этот сервис отличается от ручного тем, что здесь можно сразу отсеивать рекрутеров по ключевым словам. Есть фильтры по местоположению. «В LinkedIn это проблемное место, там мало кто напрямую указывает свою локацию», – говорит Александр. Есть и фильтр по опытности (он работает и для премиум-аккаунтов самой сети, но, по словам основателей стартапа, стоит дороже). Плагин TurboHiring для Chrome собирает все доступные контакты кандидата на его страницу в LinkedIn, независимо от уровня круга знакомства.

При ранжировании результатов TurboHiring учитывает тех кандидатов, кто сейчас находится в активном поиске работы. Также команда работает над автоматизацией сервиса: к примеру, чтобы можно было текст предложения о работе рассылать сразу по всем выбранным кандидатам, автоматически собрать контакты кандидатов, выслать инвайты и т. д.

За несколько месяцев работы сервис привлек 550 пользователей, есть платящие клиенты. Команда развивает проект на свои средства, в свободное от работы время. «Проект мы решили строить по принципу lean startup, проверяем потребности пользователей и наши гипотезы, поэтому не тратим время на мелочи вроде логотипа… Поэтому наш проект сейчас выглядит как будто “без дизайна”», – говорит Александр.

***

11.01.2017

В Европе организована кампания «Медиа против ненависти»

Европейский форум медиа общин, Европейская федерация журналистов и Артикль 19 в партнерстве с другими организациями в декабре начали кампанию «Медиа против ненависти» (#MediaAgainstHate) (Телекритика).

Ее цель – противодействовать разжиганию ненависти и дискриминации в традиционных и онлайн средствах массовой информации путем содействия

применения этических стандартов, при этом соблюдая права на свободу выражения.

Работа организаций гражданского общества основывается на убеждении, что права на равенство и свободу выражения усиливают друг друга и имеют существенное значение для человеческого достоинства.

Кампания направлена на улучшение освещения в СМИ вопросов, связанных с миграцией, беженцами, религией и маргинальными группами в целом. Повышение потенциала журналистов, СМИ, гражданского общества и медиа-сообщества в борьбе с пропагандой ненависти, нетерпимости, расизма и дискриминации.

В январе предусмотрен запуск видеоконкурса, чтобы собрать многоязычные примеры, как страны борются против стереотипов и дискриминации.

***

13.01.2017
В Днепре стартует флешмоб музейного селфи

Уже третий год подряд все музеи мира объединяются в январе в международном флешмобе музейных селфи (Dnepr.info).

С 18 января музеи Днепра присоединяются ко всемирной акции, начатой Европейским проектом Culture Themes еще в 2015 г. Всех желающих жителей и гостей города приглашают в эти дни в исторические и художественные музеи Днепра, чтобы не только ознакомиться с собранными там коллекциями уникальных экспонатов, но и поучаствовать во флешмобе.

Для этого надо лишь выбрать наиболее интересный с вашей точки зрения экспонат и сделать ваше с ним совместное фото, после чего опубликовать его в соцсетях с тегами #MuseumSelfie (тег международной акции), #dnimSelfi (тег исторического музея Днепра) или #artmuseumdp (тег художественного музея Днепра).

Авторы самых оригинальных фото получат призы.

С 18 по 22 января, на время действия акции, фотографирование в залах исторического музея – бесплатное.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

10.01.2017
Facebook запустит рекламу в середине видеороликов

Социальная сеть Facebook начнет вставлять рекламу в середину видеороликов, которые смотрят пользователи. Об этом сообщил ресурс Recode со ссылкой на источники в индустрии (InternetUA).

По данным источника, команда соцсети вскоре начнет тестировать новый формат рекламы, предусмотривающий показ рекламных вставок через 20 секунд после начала клипа. Изменение коснется более или менее профессионально сделанных роликов и не затронет домашнее видео, которое публикуют простые пользователи.

На такой рекламе производители видео смогут зарабатывать. Facebook планирует отдавать создателям роликов 55 % от стоимости рекламы. Если проект будет запущен, это может стать первым шагом к возможности настоящего заработка с публикуемых в соцсети роликов для многих производителей видео с начала работы Facebook.

***

10.01.2017

Instagram вбудує рекламу в розділ «Історії»

Instagram збирається вбудовувати рекламні ролики в розділі Stories («Історії») і показувати їх між фото і відео користувачів (Espreso.tv).

Про це повідомляє VC.

Зазначається, що фотосервіс тестує рекламу в «Історіях» серед частини користувачів. Facebook (власник Instagram) хоче отримати якомога більше грошей, які можна вичавити з традиційної реклами.

Аналогічна система вже використовується в сервісі Snapchat, який популяризував формат «Історій». Крім того, в Instagram обговорюють можливість запуску брендованих «Історій», за допомогою яких користувач може в один клік перейти на сайт рекламодавця.

Представники Instagram не прокоментували інформацію про новий формат. При цьому вони зазначили, що компанія «планує залучити в “Історії”» рекламодавців і запустити в цьому розділі інші бізнес-можливості, не уточнюючи конкретні наміри.

Також залишається невідомим, чи можна буде пропускати рекламу в «Історіях» і як будуть ділитися рекламні доходи між сервісом і авторами фото і відео, між якими будуть з’являтися оголошення.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

3.01.2017

Большинство пользователей проверяют смартфон уже через 5 минут после пробуждения

Многие пользователи мобильных устройств, проснувшись утром, сразу же спешат взять в руки свой гаджет и проверить уведомления и почту. Согласно свежей статистике, собранной в ходе опросов Deloitte Global Mobile Consumer Survey 2016, 61 % людей берут в руки смартфон в течение 5 минут после пробуждения, 88 % проверяют его через 30 минут, а после часа это делают 96 % пользователей. Авторы опроса заявили, что такая статистика показывает массовое помешательство на использовании смартфонов, которое отвлекает от многих активностей на протяжении дня, а мобильные устройства вторгаются в личное пространство и жизнь (InternetUA).

Наиболее частым видом деятельности при этом является проверка медиа-источников и мессенджеров. Не менее интересные результаты опроса тех, кто проверяет гаджеты перед сном. За 15 минут перед тем, как уснуть, это делают 74 % владельцев смартфонов. В опросе приняли участие более 53 000 человек.

***

9.01.2017

Психологи: Соціальні мережі становлять небезпеку для психіки дитини

Група американських психологів настійно рекомендує батькам обмежити своїх дітей-підлітків у відвідуванні соціальних мереж. На думку дослідників, неконтрольована активність неповнолітніх на просторах цих ресурсів може серйозно похитнути їхню психіку (Голос українською).

Зокрема, уточнюють вчені, це стосується знущань і принижень, які часто в жартівливій формі активно застосовуються відвідувачами цих сайтів. Діти можуть ставитися до цього по-різному, проте в більшості випадків це може порушити об’єднання ефективність сприйняття реальності або істотно знизити самооцінку дитини.

Окремо психологи ставлять акцент на тому, що підлітки із-за своєї наївності можуть стати жертвами інтернет-шахраїв. Подібний вид злочинів активно поширюється в мережі. На цей факт батьків також просять звернути увагу. Третьою проблемою неконтрольованого доступу до соцмереж вчені назвали насиченість Інтернету порнографічним контентом. Сучасні ресурси в гонитві за популярністю часто зловживають розміщенням матеріалу інтимного змісту, що не може не викликати занепокоєння у батьків.

***

12.01.2017

Марта Барандій

Онлайн-юрба: чим небезпечна культура ненависті у соціальних мережах

Виступ відомої американської акторки М. Стріп на церемонії вручення щорічної кінопремії «Золотий глобус» сколихнув світову спільноту. У своїй промові акторка засудила новообраного президента США Д. Трампа за публічні прояви соціальної нетерпимості. За її словами, подібні меседжі, якщо їх дозволяє собі статусна особа, підсвідомо дають «дозвіл» решті громадскості на аналогічну поведінку, стираючи тим самим межу між добром і злом. Цей виступ набув широкого суспільного резонансу, підкреслюючи гостроту окресленої проблеми. Це перегукується із висновками дослідження, що його провели голова громадської організації Promote Ukraine (Бельгія) М. Барандій і стажер цієї організації А. Арєф'єва, результатами якого вони діляться із читачами Forbes (UAInfo).

Такі явища, як PEGIDA, Брекзіт і трампізм у 2016 р. довели, що расистські ідеї більше не є моральним табу. Різкі висловлювання, які використовуються політичними лідерами багатьох країн, поширюють культуру ненависті і стирають грань між тим, що є добре, а що зле.

Таким чином формуються неконтрольовані упередження в суспільстві. Нездатність правового механізму відкоригувати цю тенденцію провокує ланцюгову реакцію, коли послідовники цих лідерів використовують ту ж риторику і ображають своїх співрозмовників, які з ними не згодні.

Ці процеси ускладнюються наявністю нових способів обміну інформацією, якими є соціальні мережі. Тому наразі виникає нагальна потреба у визначенні етичних норм, які могли би вдало регулювати цей обмін відповідно до цінностей суспільства.

Особливої уваги потребує таке небезпечне, на наш погляд*, явище, як необережне використання соціальних мереж «статусними» публічними людьми. Насамперед – поширення власних поглядів із яскравим політичним підтекстом, але суперечливих щодо фактів.

Небезпека полягає у тому, що публічні люди, які займають високі посади, як то політики чи директори великих корпорацій, є opinion makers – формувачами чи лідерами думок, тобто творцями публічної думки. Безвідносно до того, чи є вплив на думку мас їхньою метою чи ні, публічність посту автоматично робить його таким. Водночас статус соціальних мереж, таких як Facebook, дозволяє висловлювати свою думку без підкріплення її фактами та без етичного регулювання.

Роль формувачів думок

Нещодавні дослідження показують, що соціальні мережі, і Facebook зокрема, є платформою для поширення емоційних настроїв.

Загальна ідея дослідження зводиться до того, що перевага негативно забарвлених постів у підбірці новин індивіда збільшує шанси цього індивіда створити негативний пост.

Але за браком освіти чи бажання дізнаватись особисто, або незнання англійської мови, яке є необхідним для доступу до неупереджено налаштованих західних видань, в людини виникає бажання «присвоїти» думку opinion-maker і

посилатися на нього, як на авторитет. У результаті формується аудиторія, яка сприймає надану суб'єктивну думку як об'єктивну і правомірну.

Це – прошарок людей, які часто погоджуються з етично і політично некоректними твердженнями, через що, з одного боку, виникає «ефект онлайн-юрби» з наслідками конформізму – тих, хто спостерігає, а з іншого – росте сміливість автора, як лідера цієї конкретної юрби, захищати і розгортати свою позицію.

Що таке онлайн-юрба?

Соціальні мережі є своєрідним електронним простором, де люди об'єднуються за професійними інтересами чи ідейними переконаннями. Це «спляче» підгрунтя «колективної волі» неодноразово активізовувалося задля спонукання до дій, таких як маніфестації чи революції (Єгипет, Туніс, Україна). Їм передує емоційне об'єднання в онлайн-просторі, яке має характер онлайн-юрби. Хоч люди отримують у стрічці новин повідомлення, які вони не завжди очікують побачити, ці повідомлення залежать від вподобань їхніх друзів у мережі. Якщо ж вони себе з такою інформацією чи ідеями ідентифікують емоційно, то вони їх вподобують і поширюють. Таким чином створюється конкретна юрба під певну ідею.

Онлайн-юрба має багато схожого з класичним натовпом: спільність дій, сміливість, взаємна підтримка членів юрби, анонімність, безвідповідальність, некритичність, легковірність, перебільшеність та емоційність.

Ідейна спільність і стан єдності онлайн-юрби так само як і класичного натовпу, надає людині відчуття могутності і правоти. Як і класичний натовп, онлайн-юрба утворюється шляхом ланцюгової реакції та існує завдяки підтримці членами юрби один одного.

А от анонімність живого натовпу в онлайні підмінюється безпечністю віддаленого зв'язку і швидкоплинністю інформації в стрічці новин мережі. Непрямі наслідки висловів і дій у соціальних мережах породжують упевненість у відсутності моральної чи правової відповідальності.

Некритичне сприйняття закликів і дописів у Facebook є загальною проблемою сучасного інформаційного простору: люди не мають часу звертатися до фактів. Вони покладаються на доступність евристики, тобто на ті знання, які вже мають і які доповнюються першою-ліпшою інформацією. Людина не встигає думати і дозволяє це за неї робити тОму, чий допис вона вподобала чи поширила, хоча часто ці дописи також створені на основі емоцій, а не фактів. Хоча діючи спільно, поширюючи і вподобуючи дописи, люди часто не мають спільної усвідомленої мети; вони не розуміють, якими є намір і стратегія дописів і їхніх вподобань.

Як автор допису чи автор його поширення, opinion-maker є ядром чи лідером певної онлайн-юрби. Коментатори, які підтримують автора, є її активними учасниками. Також пасивними учасниками є ті, хто вподобують цей допис чи коментар. Їх активність збільшує масовість і, відповідно, ефект.

І коли хтось намагається спростувати недостовірну інформацію в дописі, члени юрби захищають оригінал і залишаються лояльними до лідера, чий пост вони вподобали, поширили чи коментували.

Тож, ті, хто критикує вподобаний допис – це перепона, яка викликає нетерпимість і гнів чи то автора, чи то учасників юрби. Захисники допису використовують два контр-аргументи проти критика – це або відсутність здібностей у нього до розуміння допису, або ж перебування на стороні противника. Юрба пристрасно захищає свою позицію, вдаючись до агресивних висловів, а моральні чесноти її не цікавлять. Захищаючи свою позицію, вона часто ображає опонента.

Серед соціальних психологів є поширеною думка, що люди мають тенденцію ненавидіти тих, кого образили. Щоби психологічно виправдати жорстокість по відношенню до супротивника, люди «деперсонізують» ворога за допомогою кличок, називаючи їх, наприклад, «японки», «хохли», «хунта», «канапи» тощо. У наш час і таке узагальнення груп людей, як «мігранти» може мати негативний відтінок і викликати ворожість.

Підхоплення ворожої риторики лідерами думок призводить до ще більшої емоційності тих, хто їх підтримує. І у певний момент може стати неможливим відрізнити факти від уяви.

Український контекст

У контексті України така ситуація може призвести до негативних наслідків. Серед них – дезінформованість населення та, як результат, суперечливість настроїв людей та офіційної політики держави.

Офіційною політикою України є курс на інтеграцію до Європейського союзу, і країна робить кроки в напрямку цього курсу, що передбачає закріплення в суспільстві європейських цінностей правової держави, демократії та прав людини. Якщо населення перебуває під впливом етично-некоректних дописів від opinion-makers, у нього створюється змінена картина реальності. Хоча лідери думок повинні бути краще поінформовані про суспільні події, ніж більшість населення, серед тих, хто поширює чи вподобує дописи, трапляються аналітики та міністри, бо ж навіть вони іноді піддаються впливові «ефекту онлайн-юрби».

Нещодавний приклад – публічний допис керівника однієї з великих корпорацій, у якому він плутає сирійців і тунісців, представляє мігрантів як загрозу Європі і порівнює їх з мавпами. Позитивна реакція на цей пост його кола друзів, серед яких також є формувачі думок, говорить про те, що люди часто несвідомі наслідків своїх дій у соціальних мережах.

Небезпека таких емоційно насичених та інформаційно бідних постів від opinion-makers полягає в тому, що думка мас буде формуватися відповідно до них. Створюється відчуття, що це тверeза оцінка ситуації, а головне, вирішення проблем є справою твердого рішення. Одночасно такі досягнення демократії і глобалізації як винайдення міжкультурного діалогу та пошук компромісних рішень відходять на другий план. Сімдесят років миру в Західному Світі

опиняються під загрозою, і риторика повертається до свого стану за часів нацистської Німеччини.

Нещодавно М. Цукерберг визнав, що Facebook повинен відповідальніше ставитися до таких висловлювань і до дезінформації, проте міжнародно-правове регулювання соціальних мереж відсутнє. Загалом Facebook стежить за расистськими висловлюваннями чи такими, що закликають до ненависті. Але, очевидно, не всі дописи перевіряються і видаляються адміністраторами. Тому відповідальність залишається на авторові.

У своїй праці «Основи геополітики» натхненник «русского мира» О. Дугін писав про необхідність створення геополітичного безладу, якому служитиме дестабілізація, дезінформація та розпалювання етнічних і расових конфліктів. Усі сучасні європейські лідери ультранаціоналістичних рухів реалізують цю стратегію, закладену О. Дугіним ще у 1997 р., і часто на російські кошти.

Ці рухи не є тими, що сприятимуть інтеграції України в ЄС, бо їхня мета той ЄС зі всіма його цінностями знищити, і для цього вони вдаються до популізму, до культури ненависті і ксенофобії. При цьому провладні проєвропейські рухи різко засуджують ці тенденції і шукають шляхи їх подолання. А всі перепони для такого подолання вважаються недружніми.

А відтак, несвідомо підхоплюючи європейську ультранаціоналістичну риторику, українські лідери думок створюють загрозу для дружніх відносин України з Європою – чи то безпосередньо через допис, чи то через його наслідки для мутації моральних принципів українського читача, і відповідно, його ставлення до формування політичного курсу держави.

* Співавтор матеріалу – Анастасія Арєф'єва, магістр філософії університету Лювен, стажер в НУО Promote Ukraine (Брюссель).

***

12.01.2017

Гонитва за лайками в соціальних мережах призводить до зневіри – дослідження

42 % користувачів соціальних мереж заздрять друзям, чиї пости викликають більше відгуків, ніж їхні власні, говорять результати дослідження, проведеного компанією Kaspersky Lab (Новое время).

Згідно з опитуванням, така ж частка респондентів засмучується, якщо їхні пости і фотографії ніхто не лайкає або лайкає менше, ніж вони розраховували.

Зазначається, що люди приходять у соцмережі з позитивними цілями: 65 % заради можливості залишатися на зв'язку з друзями і колегами, для 60 % це зручний спосіб переглядати розважальні та смішні пости.

Але насправді життя в соціальних мережах пов'язане з безліччю подразників: перше місце тут впевнено займає реклама (вона докучає 72 %). Однак багато неприємні фактори пов'язані з безпосереднім оточенням користувача. Нервувати може майже все: пости про вечірки, на які не

запросили (59 % опитаних зізналися, що через це їхній настрій погіршується), красиві фотографії друзів з відпустки (45 %), навіть власні щасливі спогади (37 % розповіли, що, переглядаючи свої попередні пости, вони схильні думати, що раніше жили щасливіше).

«Наші відносини з соціальними мережами перетворилися на порочне коло. Ми відвідуємо такі сайти, щоб розповісти про радісні події, але тим же зайняті і всі навколо. Ми опиняємося оточені фотографіями і постами щастя. Велика спокуса вирішити, що наші друзі живуть веселіше за нас самих. Через це люди відчувають себе пригніченими», – пояснює керівник управління з соціальних медіа Kaspersky Lab Є. Черешнєв.

Маніпулятивні технології

3.01.2017
Дмитро Плахта
FB vs ВК // Про інтернет-тенета впливу «русского міра»

Українське інтернет-середовище досі не може покинути тенета впливу «русского міра». Позитивна тенденція простежується, проте до остаточного видужання пацієнта ще далеко. Ілюструвати цей процес найдоречніше буде на прикладі соціальних мереж, значення яких за нинішніх реалій неможливо переоцінити. Facebook, «ВКонтакте» і «Одноклассники» – три основні середовища проживання українців у мережі. Що обирає українець: найпопулярнішу та найбільшу соцмережу в світі чи її російських клонів? Відповідь, на жаль, очевидна, і від цього ще більш сумна (День).

Висловлюючись типовим інтернет-сленгом, необхідно надати «пруф», тобто підтвердження. Отож, відповідно до даних медіадослідження «Opinion Software Media», у листопаді 2016 р. за охопленням активності українських користувачів сімома найпопулярнішими сайтами стали «Google», «ВКонтакте», YouTube, «Яндекс», «Одноклассники», «Мейл.ру» і Facebook. Так, це перелік у порядку спадання. Так, у ньому аж чотири російські сайти. І аби не перевантажувати вас цифрами, відзначимо лише, що показник ВК був 67 %, а FB – 42 %. До слова, результати дослідження «Kantar TNS CMeter» за жовтень майже аналогічні, за винятком того, що «Одноклассники» розмістилися на 10-й позиції, що також є дуже високим показником.

Які думки з цього приводу, панове? «Та на “Одноклассники” узагалі не зважайте, там одні тільки старші сидять», – впевненим тоном скаже хтось. Цей «хтось», очевидно, виявиться відносно молодим. І постає питання якраз до молоді. Чому ж ви, такі прогресивні та інноваційні, вибираєте «ВКонтакте»? Як встановити черговий новий фоторедактор на смартфон – ви перші. Як освоїти найсвіжіше оновлення в Instagram – також перші. Ви начебто в курсі найрізноманітніших інтернет-трендів, проте досі «сидите» в примітивному та свідомо обмеженому російському клоні Facebook’у, чи не так?

«Просвіта громадян про "особливості" російських мереж зменшить їх популярність серед українців»

«Мабуть, не варто аж так узагальнювати. Молодь є різною, і, відповідно, обирає різні соцмережі. Наприклад школярі більше користуються "ВКонтакте", бо там дуже просто зареєструватись, легко закачати необхідне відео й користуватись. Хоча чимало школярів нині переходять на Viber як простий та інструментальний месенджер. Наші студенти, які вступають на перший курс, нерідко є користувачами "ВКонтакте", але поступово переходять на Facebook, не тільки тому, що там переважає викладацька та журналістська професійна спільнота, але й тому, що розуміють й оцінюють усе, що пов'язано з "національною приналежністю" ВК, – слушно відзначає доцент кафедри нових медій факультету журналістики ЛНУ ім. Івана Франка Н. Габор. – Ця тенденція вже змінюється сама. Якщо довіряти інформації бізнес-видання "Капитал" за липень 2014 р., який використовує дані лічильника "StatCounter", то за рік кількість користувачів "ВКонтакте" впала з 37 % до майже 22 %, в "Одноклассниках" з 10 до 3 %. У той самий час кількість користувачів ФБ зросла. Тобто українці, як громадяни країни, яка протистоїть російській агресивній політиці та анексії української території, свідомо відмовляються від користування російськими онлайн-сервісами.

На мою скромну думку, не варто нічого нікому забороняти, тим більше, що забороняти такі речі складно. Хоча, звичайно, дещо дивно, що приєдналися до російських мереж і досі не покинули їх, не прореагувавши на петицію української мережевої спільноти «Weua.info», Президент України та МЗС України.

Виправляти тенденцію варто, пояснюючи українським користувачам прості речі: користуючись російськими мережами, ми добровільно погоджуємось, що ФСБ отримує у своє розпорядження (згідно з прийнятим "пакетом Ярової") всі телефонні розмови, пости, записи і т. д., які будуть зберігатись упродовж півроку й надаватись на вимогу правоохоронців. Крім того, наше відвідування соцмереж – це-все-таки бізнес, а отже чи хочемо ми працювати на бізнес Росії?

Думаю, що просвіта громадян про "особливості" російських мереж зменшить їх популярність серед українців, а це, відповідно, вплине на кількість користувачів, а отже, на цінність їх акцій... Пригадуєте, була така американська мережа Myspace? Де вона тепер? Її місце посіла молодша, зорієнтована як на справу, так і відпочинок, значно інструментальніша соцмережа FB. Наші молоді люди розумні, у доброму розумінні того слова прагматичні, тому впевнена, що їх вибір буде правильним. Хоча, якщо помріяти, то було б не зле, щоб наші Weua.info стали добрими й помічними замінниками зарубіжних соцмереж. Може "не нині, не завтра, так потім!"».

«Прописка» в Інтернеті не менш важлива, ніж документ про громадянство певної держави»

Ідея з суто українськими соцмережами очікувано провалилася. І це факт. Хоча не можна заперечувати, що в майбутньому обставини складуться таким

чином, що й ця ідея вистрілить. Поки доводиться вести полеміку навколо FB і ВК. Так, 2014 р. став частково переломним моментом, адже у цей період різко збільшилася затребуваність винаходу М. Цукерберга серед українців. Утім із плином часу тенденція зросту «фейсбукізації» українців припинилася. Який ще катаклізм потрібен українцям, аби переконатися в тому, що ВК – це «русскій» шлях у нікуди? Залишається просвітницька робота. Про небезпеку російських соцмереж чимало писали ЗМІ, неодноразово на цьому наголошувала і СБУ. Свою частку в розвиток благородної справи вніс і викладач Львівського університету Б. Тихолоз, ініціюючи флеш-моб серед своїх студентів із закликом ігнорувати ВК, «Мейл.ру» і т. п. «Преподаватель из Львова запрещает использование российских соцсетей», – такими маніпулятивними заголовками наступного дня рясніли російські мас-медіа. «Живемо в добу Інтернету, у новому цифровому світі, тож ігнорувати значення новітніх форм і засобів комунікації, серед них і соціальних мереж, – усе одно, що вперто мерзнути в печері після винайдення способів видобування вогню чи переписувати книги вручну після винаходу Ґутенберґа. Водночас живемо у час тривожний і драматичний, у глобальному контексті – в ситуації загострення міжцивілізаційних конфліктів і загрози “нового варварства”, в українському ж випадку – у стані війни з Росією, у тім числі інформаційної. За цих обставин “прописка” в Інтернеті (передусім на поштовиках і в соцмережах), на мою гадку, не менш важлива, ніж документ про громадянство певної держави. Відповіді на запитання: “Де ти? Хто ти? З ким ти?” залежать і від того, на якому домені твоя поштова скринька і в яких мережах маєш особистий акаунт. Той факт, що досі величезна кількість українців (особливо молодих), нічтоже сумняшеся, “сидять” “вкантактє” чи “аднаклассніках”, а пошту отримують на скриньки із національним доменом “ru”, мене обурює й тривожить.

Свого часу один мій допис, звернений до студентів Львівського університету, в якому працюю, із закликом “покинути територію ворога”, зчинив цілу бурю в ЗМІ та соцмережах, у тому числі й російських. На жаль, із дистанції часу можу скрушно констатувати, що то була радше буря в склянці води. Себто проблема, звісно, дуже актуальна й масштабна, а її ігнорування в національних масштабах є загрозою інформаційній безпеці держави. Проте, мабуть, окремими особистими закликами її не вирішити. Потрібна системна праця з деколонізації, дерусифікації й деокупації українського інформаційного простору, а це процес тривалий і складний. На щастя, частина моїх вихованців таки дослухалася до поради позбутися інтернет-залежності від чужинських ресурсів. Одначе чимало й досі не можуть зіскочити з цієї “голки”. Мабуть, це просто справа звички, наслідок елементарних лінощів і небажання зробити бодай щось задля своєї країни. Але я переконаний, що справа варта заходу, а гра – свічок, навіть якщо бодай невелика частка української молоді звільниться від колоніального “цифрового” рабства у “русского міра”, однією з форм буття якого є так званий “Рунет”.

Певна річ, головна боротьба ще попереду. Донести ж до наших дітей, школярів і студентської молоді зміст і доцільність цих закликів – не просто

наше завдання, а наш обов'язок перед їхнім – і нашим спільним – майбутнім», – підсумовує Б. Тихолоз.

Заяви СБУ не переконують, флешмоби у Facebook також не дають належного результату

«Користуюсь ВК, оскільки з'явилася звичка», «ВК простіший у використанні, плюс уже до нього звик», «Тут багато безкоштовного (читайте: піратського) контенту», – це лише декілька зі середньостатичного переліку причин, чому українці саме «вконтактє». Незважаючи на силу-силенну попереджень, про інформаційну безпеку згадують одиниці – і то з іронічною посмішкою, мовляв, кому я в тому ФСБ потрібен. Тих, хто не вірить, у «байки про руку спецслужб у ВК», можливо, переконає історія, яка трапилася зі студенткою, кореспондентом «Громадського радіо», яка пише репортажі із зони бойових дій на Донбасі, А. Шибіко: «Відмовилася від ВК із двох простих причин: безпека персональних даних і принципи. Хто б там що не казав, що його профайл нікому не потрібен і там нічого важливого немає, ті, кому треба, можуть витягнути те, чого навіть немає на профілі. І ви про це навіть не здогадаєтеся. Та й Бог його знає, як російські спецслужби захочуть використати ваші дані. Краще таки перестрахуватися. Ну і принципи. Це російська соцмережа. Російських продуктів не купую, фільмів не дивлюся, банками не користуюся. Тоді чому ж для ВК робити виняток?

Отож, я видалилася з ВК у січні 2016 р. А у жовтні виявилося, що на сайті бойовиків "Трибунал" розмістили мої персональні дані. Використане тут фото було лише у приватних повідомленнях у ВК. Більше воно ніде не публікувалося (йдеться про фото з Майдану, у беркутівському шоломі). Тому варіант, що хтось із друзів "злив" фото, виключаю. Не знаю, чому на сайті я "каратель", а не "пропагандист", як вписують українських журналістів чи "пособник" як волонтерів. А мене от, людину, яка у житті в руках зброї не тримала, "карателем" нарекли. Однак це вже інша історія. Головне, що фото було лише ВК і потрапило на "трибунал" бойовиків».

Facebook досконаліший, глобальніший, стабільніший і безпечніший за «ВКонтакте». У ФБ українець долучається до найбільшої спільноти людей, об'єднаних на одному ресурсі. За іронією долі, багатьох своїх співвітчизників тут він знайти не може. Це, до речі, і змушує частину українських ФБ-юзерів залишати активними їхні акаунти у «ВКонтакте», адже цей канал комунікації є часто єдиним до певної аудиторії. У ВК українець перебуває в штучно створеному просторі з декількох десятків мільйонів мешканців пострадянських республік. «ВКонтакте» – це відразу декілька діагнозів. Цей замкнений простір, як і зазвичай росіяни створили для захисту від уявних ворогів зовнішнього світу, а значна частина пострадянських людей погодилася на ці звичні правила гри. У цьому контексті можна говорити і про черговий вияв малоросійства українців – комплексу, який проявляється навіть у таких, здавалося, банальних речах. Також ВК є симптомом інших проблем, зокрема, низької медіаграмотності українського суспільства. Заяви СБУ не переконують, флешмоби у Facebook також не дають належного результату. Які ще

пропозиції? Необхідна медіавакцина – наприклад, запровадження медіаграмотності, як навчальної дисципліни у школах, де б фахово пояснювали ризики та сутність так званого «Рунету». Чим не початок системного виходу з «вконтактє»? +

***

11.01.2017

WikiLeaks вважає неправдоподібним «російське досьє» на Трампа

Поширений BuzzFeed документ, що містить інформацію про ймовірний компромат Росії на обраного президента США Д. Трампа, є неправдоподібним (LB.ua).

Таку думку оприлюднила у Twitter організація WikiLeaks.

«35-сторінковий PDF-документ про Трампа, опублікований BuzzFeed, не є доповіддю розвідки. Стиль, факти і дати неправдоподібні», – йдеться в повідомленні.

Зазначимо, що BuzzFeed не називав документ «доповіддю розвідки». Видання зазначало, що це може бути одним із матеріалів, які використовувала російська розвідка для підготовки «досьє» на Д. Трампа. При цьому такий документ, як зауважує BuzzFeed, «контролюється представником Кремля Пєсковим», який виконує прямі вказівки вищого керівництва Росії.

Також у документі, зокрема, зазначено, що російська розвідка збирала компромат на Д. Трампа під час його візиту в Москву 2013 р. з метою подальшого шантажу. Його номер у готелі Ritz Carlton, в якому зупинялися президент США Б. Обама з дружиною, прослуховувався агентами розвідки. У документі вказано, що в цей номер Д. Трамп викликав повій.

Крім того, у тексті документа вказано, що російські спецслужби контактували з помічниками Д. Трампа задовго до виборів – ці контакти тривали протягом п’яти років.

Сам Д. Трамп назвав доповідь брехливою, а новини про нього – сфабрикованими. На думку обраного президента США, подібні публікації – це «політичне полювання на відьом».

***

11.01.2017

На Facebook подали в суд за историю о поджигающем бездомных сирийском террористе

Немецкий адвокат Чань-Джо Цзюнь (Chan-jo Jun) подал в суд на социальную сеть Facebook за фейковые новости о поджигавшем бездомных сирийском беженце-террористе. Об этом сообщает The Local (InternetUA).

По словам юриста, уроженец Сирии А. Модамани (Anas Modamani) получил широкую известность после сделанного им в середине 2015 г. селфи с канцлером А. Меркель. Однако вскоре в Facebook начали распространяться

фейковые новости о том, что на самом деле А. Модамани является членом одной из сирийских террористических группировок, поджигавшим бездомных.

В ряде публикаций также сообщалось, что мужчина был одним из организаторов терактов в Брюсселе в мае 2016 г., а Меркель «сделала селфи с террористом». По мнению Цзюня, несмотря на многочисленные жалобы пользователей, Facebook не предпринял никаких мер для ограничения доступа к фейковым новостям.

Проблема фейковых новостей в Facebook широко обсуждалась во время президентских выборов в США, когда они обогнали публикации авторитетных изданий по уровню интереса читателей. 20 самых популярных фальшивок собрали 8 млн 711 тыс. шеров, лайков и комментариев, а 20 самых популярных статей СМИ – почти на полтора миллиона меньше.

***

16.01.2017
Базиленко Анна
В ЄС склали відеоінструкцію, як розпізнати прокремлівських тролів у соцмережах

Представництво Євросоюзу в Україні опублікувало у Facebook відеоінструкцію з послідовністю дій для визначення прокремлівських тролів у соціальних мережах (Watcher).

Загалом пропонується чотири кроки. В оприлюднених відеоінструкція (наразі це два відео) пояснюється, як ідентифікувати троля і як вивчити історію питання. Так, ознаками інтернет-троля, на думку авторів відео, можуть бути коментарі, які довші за чотири рядки, коментарі поза контекстом, образливі та агресивні коментарі, помилки.

Крім перших двох кроків (ідентифікація і вивчення питання), є ще два – як позначити та ігнорувати інтернет-троля. Імовірно, ці відеоінструкції будуть згодом опубліковані на Facebook-сторінці Представництва Євросоюзу в Україні.

Як відомо, в історичному районі Петербурга – Ольгино – розташовано ТОВ «Агентство Інтернет-Досліджень», яке займається інтернет-пропагандою. Сотні співробітників безперервно пишуть коментарі, розміщують картинки, обливають брудом Україну, Америку та Європу і гноблять незгодних росіян, створюючи таким чином видимість громадської думки.

***

11.01.2017
Борис Тодуров
Минздрав «изгнал» хирурга Тодурова из Facebook

Facebook заблокировал личную и публичную страницы кардиохирурга Б. Тодурова из-за кибератаки, которая была организована командой Минздрава (data.ua).

О ситуации сообщил координатор гражданской инициативы «Украинская реформа» К. Коссинский, пишет «Апостроф».

«Вначале были фейковые связки с одиозными политиками, потом манипуляция документами в ProZorro. Теперь ему вовсе перекрыли канал для трансляции своего мнения. Как происходит так называемая кибератака? Проплаченные оппонентами боты массово жалуются в администрацию ФБ на нежелательный для них аккаунт. Как известно, при накоплении достаточного количества жалоб, аккаунт блокируют», – отметил К. Коссинский.

Эксперт добавил, что если проанализировать работу основного «голоса» Минздрава Е. Закревской, то можно заметить, что ее профиль в Facebook размещает комментарии четвертые сутки без перерыва, а ссылки на ее негативные посты распространяют тысячи поддельных, по его мнению, аккаунтов по всей сети.

«Эти мощности команда У. Супрун использовала, чтобы в конце концов заставить оппонента лишиться своих площадок для выступления», – считает эксперт.

Зарубіжні спецслужби і технології «соціального контролю»

11.01.2017
Twitter обвиняют в пособничестве террористам

Родственники двух американских семей, члены которых стали жертвами террористических актов в Брюсселе и Париже, подали иск против компании Twitter, предоставляющей коммуникационную услугу. Компанию обвиняют в содействии террористам, сообщают Вести со ссылкой на BBC (News.Dneprcity).

В исковых заявлениях, которые в юриспруденции охарактеризовали как новаторские Twitter обвиняется в «сознательном предоставлении материальной поддержки и ресурсов террористам ИГИЛ в виде онлайн-сетевой платформы и коммуникационных услуг». Более того, в иске говорится, что Twitter продолжает предоставлять такие ресурсы, «несмотря на получение многочисленных жалоб». В целом иск насчитывает более 80 страниц.

Родственники жертв хотят финансовой компенсации от Twitter, однако ее размер не сообщается. В Twitter пока не прокомментировали эту ситуацию.

***

11.01.2017
Европа ужесточит правила для WhatsApp и Skype

Еврокомиссия собирается ограничить доступ интернет-компаний к данным пользователей. Помимо телекоммуникационных компаний, нововведение коснется таких сервисов как WhatsApp, Facebook Messenger, Skype, Gmail, iMessage или Viber, пишет RNS со ссылкой на Bloomberg (InternetUA).

По мнению чиновников ЕС, новый законопроект о защите электронной информации, ePrivacy, поможет пользователям усилить контроль за своими настройками онлайн. Кроме обеспечения конфиденциальности общения своих клиентов, интернет-компании должны будут запрашивать разрешения на использование персональных данных для показа таргетированной рекламы, пишет Reuters.

Помимо прочего новый законопроект предусматривает возможность использования компаниями такой личной информации, как, например, длительность разговоров или местоположение для предоставления пользователям дополнительных сервисов.

Новости об ужесточении правил для мессенджеров появились еще в августе прошлого года. Тогда Financial Times написала, что ужесточение затронет только звонки и сообщения, отправляемые на мобильные номера, и не будет затрагивать общение внутри сервисов.

Проблема захисту даних. DDOS та вірусні атаки

3.01.2017
Майя Яровая
Итоги-2016: кто и зачем кибератаковал Украину в уходящем году и что будет дальше

В 2016 г. хакерские атаки на украинские инфраструктурные объекты перестали быть чем-то сверхъестественным и уже начинают входить в привычку. Киберинцидентов с наивысшей степенью угрозы за год произошло как минимум три (из тех, которые стали достоянием общественности), благо не все закончились успехом хакеров. Однако эксперты констатируют факт: всплеска атак не было – все плохо уже давно (AIN.UA).

«Я бы не сказал, что количество атак резко возросло, я бы скорее сказал, что последствия атак становятся все более печальними…», – прокомментировал генеральный директор ООО “САЙ ЕС ЦЕНТРУМ”, руководитель компании CyS-CERT Н. Коваль…

А теперь по порядку.

Удар по рубильнику, или BlackEnergy strikes again

Совсем недавно, в декабре, несколько районов Киева и области оказались обесточены на несколько часов. Причиной стал сбой автоматики управления подстанцией «Північна» в селе Новые Петровцы. Глава госпредприятия

«Укрэнерго» В. Ковальчук заявил, что причиной стало «внешнее вмешательство в системы передачи данных», то есть кибератака.

Примечательно, что атаки на энергетический комплекс страны зафиксировали еще в январе 2016 г. Хакеры воспользовались поддельными письмами от имени предприятия «Укрэнерго», которые разослали предприятиям из сферы электроэнергетики. Письма содержали вирус BlackEnergy, который проникает внутрь и уничтожает важные системные файлы. Этот же вирус использовался во время нашумевшей атаки на «Прикарпатьеоблэнерго» в конце декабря 2015 г. Тогда кибервзломщикам удалось на шесть часов обесточить половину Ивано-Франковской области и часть областного центра.

Минифильм о том, как происходила атака на «Прикарпаттяобленерго» в 2015 г., недавно опубликовало НАТО в официальном Twitter-акаунте

По данным американской компании iSight Partners, атака на «Прикарпаттяобленерго» была совершена хакерской группировкой Sandworm, базирующейся в Москве. Предположительно, все остальные атаки с использованием BlackEnergy также исходили из России...

Атаки на госреестры и сайты: под ударом бизнес и пенсионеры

Госсайты «укладывают» регулярно – например, в июле 2016 г. два дня были недоступны реестры Минюста из-за мощного DDoS, из-за чего пострадали все организации и лица, использующие электронно-цифровые подписи (ЭЦП). Именно ЭЦП могли быть целью хакеров в рамках этого инцидента, а скорее даже корневой, центральный ключ системы, который может дать злоумышленникам свободу как угодно распоряжаться вообще всеми зарегистрированными ЭЦП.

В списке Николай также упомянул кейсы, которые освещал, в частности и AIN.UA, а именно атаки на сайты Министерства финансов, Государственной казначейской службы и Пенсионного фонда Украины от 6 декабря. В этот раз хакеры не просто нарушили работу онлайн-систем ведомств – они вывели из строя сетевое оборудование. В Министерстве финансов сообщили, что атака вызвала «определенные проблемы» с полноценным выполнением платежей. В Пенсионном фонде также всполошились из-за возможных последствий, после чего Кабмин решил выделить пострадавшим ведомствам 80 млн грн из резервного фонда на обновление сетевого оборудования.

Менее вредоносной, но не менее заметной были атаки на социальные аккаунты Министерства обороны и Нацгвардии Украины, которые произошли в августе 2016 г. Пострадали Twitter-аккаунты обеих организаций и Instagram-профиль Минобороны. Так среди ночи в Twitter-аккаунтах ведомств хакеры из группировки Sprut разместили коллажи с надписью «Украины больше нет» и «Страна не найдена». Аналогичное изображение появилось и в официальном Instagram-аккаунте ведомства. Перехватить у хакеров доступ к соцаккаунтам удалось лишь днем, примерно к 14:00.

Зачем и кому это нужно

По мнению СТО украинской антивирусной компании Zillya! О. Сыча, подобные атаки преследуют очевидную цель: дестабилизировать ситуацию в Украине и продемонстрировать несостоятельность киберзащиты украинских госорганов и объектов инфраструктуры. «Для борьбы с такими атаками у нас есть соответствующие структуры и специалисты. Другое дело, что необходимо существенно повышать уровень знаний о кибербезопасности сотрудников атакуемых учреждений, поскольку возле каждого чиновника не посадишь IT-специалиста», – подчеркнул он.

Н. Коваль видит и более угрожающие сценарии, но подчеркивает, что наверняка выяснить причины атак почти невозможно. «Версия со шпионажем наиболее логична, если учесть, что этап разрушения атакованной организации зачастую наступает через 3–8 месяцев после того, как в нее проникли», – отметил експерт...

«Надо понимать, что атаки не прекращаются, просто о них узнают раньше или позже. Более того, методы атак частично совершенствуются – меняется вредоносное ПО, используются легитимные каналы для коммуникации между зараженным устройством и злоумышленником (Telegram, сервис электронной почты) и др. Тяжело ответить на вопрос “кто следующий?”, так как до конца не ясны мотивы», – заключил експерт...

«Не важно, что лежит в основе атак – бизнес-разборки, кибершпионаж, саботаж и дестабилизация, попытка повлиять на какие-то государственные процессы, ясно одно – атакуют критически важные объекты (транспорт, энергетика, финансовая система). Эта угроза перманентная и атаки будут продолжаться», – констатирует Н. Коваль.

Кибервойна и как на ней воюет Украина

По мнению О. Сыча, атаки связаны с кибервойной, которая идет в мире и в которую теперь активно втянута Украина. «По всей видимости, частота и успешность кибератак во многом будут зависеть от действий украинской стороны по организации собственной защиты. Необходимо в короткие сроки построить щит там, где его нет, или усилить там, где он недостаточно прочен. В целом наша кибербезопасность существенно повысится, если государство применит комплексный подход к защите объектов критической инфраструктуры, а не будет реагировать на совершенные атаки постфактум», – подчеркнул он…

Достижения и пробелы украинского правительства в сфере кибербезопасности

Увенчавшиеся сокрушительным успехом атаки на энергетический сектор сподвигли чиновников определиться со стратегией в области кибербезопасности, которую в марте подписал Президент Порошенко. Согласно документу, основу национальной системы кибербезопасности составят Минобороны, Госспецсвязи, СБУ, Национальная полиция Украины, НБУ и разведывательные органы.

Также Совет решил создать Национальный координационный центр кибербезопасности, который будет рабочим органом СНБО.

Впрочем, Н. Коваль скептически отзывается о предпринятых шагах. «В этом году на UISGCON было сказано о прорыве, который заключался в том, что приняли стратегию кибербезопасности… Но реформировать только Киберполицию недостаточно… В стране даже отсутствует техническая возможность видеть угрозы хотя бы на наиболее важных объектах. Я не говорю о том, что, когда появится возможность мониторить/выявлять угрозы, их надо будет тут же ликвидировать, расследовать и т. п. – а это надо кому-то делать», – заключил Н. Коваль.

По мнению О. Сыча, главные проблемы кибербезопасности еще более прозаичны – это слабая осведомленность рядовых сотрудников и халатность обслуживающего IT-персонала. «Именно разъяснительная работа среди персонала в комплексе с обновлением софта и оборудования даст возможность создать более-менее надежную защиту госучреждений. Пока на серверах будет использоваться пользовательский софт, которого там не должно быть, пока не будет понимания элементарных правил использования той же электронной почты и съемных носителей информации, каждый день любое учреждение, где сотрудники не проинформированы о таких базовых аспектах кибербезопасности, будет под угрозой», – утверждает эксперт.

***

10.01.2017

Великобритания проверит национальную систему кибербезопасности

Правительство Великобритании проведет оценку уровня национальной кибербезопасности с целью выяснить, насколько страна готова противостоять внешним кибератакам. Это решение было принято спустя два дня после публикации доклада американских спецслужб о предполагаемом вмешательстве РФ в избирательный процесс в США, сообщает Reuters (InternetUA).

«С некоторых пор все внимание сконцентрировалось на потенциальной эксплуатации киберпространства государствами и связанными с ними лицами по политическим причинам. Это только один из источников угроз, которому правительство должно противостоять», – заявила руководитель Комитета палаты общин по стратегии в области национальной безопасности М. Бекетт (Margaret Beckett).

Как отмечает Reuters, с 2014 г. по октябрь 2016 г. число атак на финансовые институты Великобритании возросло на 70 %.

В рамках исследования, британское правительство рассмотрит ряд аспектов, в том числе типы киберугроз, с которым может столкнуться Великобритания, а также численность человеческих, финансовых и технических ресурсов, необходимых для противостояния угрозам и разработки наступательных кибервозможностей.

***

10.01.2017

В опубликованный американскими спецслужбами список IP-адресов русских хакеров вошли сотни узлов сети Tor

Помимо представленного в конце декабря доклада, посвященного деятельности российских хакеров, якобы причастных ко взлому Национального комитета Демократической партии американские спецслужбы, на минувшей неделе также опубликовали обширный список IP-адресов, которые, предположительно, использовали киберпреступники, однако почти половина из них оказалась адресами выходных узлов сети Tor, сообщает The Daily Dot (InternetUA).

На это обстоятельство обратил внимание журналист издания The Intercept М. Ли, который проанализировал список из 876 «подозрительных» адресов и пришел к выводу, что 367 из них (примерно 42 %) являлись или являются адресами выходных узлов Tor, что означает, что ими пользуются тысячи людей, не имеющих никакого отношения к каким-либо хакерским атакам. Так, М. Ли обнаружил, что его блог посещали свыше 80 тыс. раз с адресов Tor, попавших в список.

«Мой блог регулярно читают пользователи Tor, и я вполне уверен, что не все из них являются русскими хакерами», – отметил М. Ли, добавив, что представленные спецслужбами аргументы в пользу причастности России к хакерским атакам во время выборов выглядят неубедительно, а неопровержимыми доказательствами могли бы стать перехваченные письма Кремля, записи разговоров или более четкие технические детали.

В свою очередь исполнительный директор Tor Project Ш. Стил назвала включение спецслужбами узлов Tor в список используемых хакерами адресов не лучшим способом предостеречь системных администраторов от атак русских хакеров. По ее словам, таким образом правительство пытается быть полезным, но в самих рекомендациях администраторам сетей включить адреса из списка в отдельный перечень отмечается, что проходящий через них трафик может быть и не связан с вредоносной деятельностью хакеров.

***

10.01.2017

Android возглавила рейтинг самых небезопасных операционных систем

Android был самой небезопасной ОС в 2016 г. (IGate).

Мобильная платформа Android возглавила итоговый рейтинг за 2016 г. среди операционных систем, в которых было обнаружено наибольшее число уязвимостей. «Зеленый робот» содержал в себе 523 ошибки, тогда как его главный конкурент – iOS – занял 15 строчку с показателем в 161 баг. Такие цифры приводятся в статистике аналитиков CVE Details. Любопытно, что с 2015 г. ситуация изменилась кардинальным образом. Тогда платформа Apple

отличилась 387 уязвимостями и заняла второе место в рейтинге, а Android благодаря 125 найденным ошибкам расположилась на 15 месте.

Фактически, это означает, что в ушедшем году «гугловская» ОС была более неустойчива к взломам, чем любая другая мобильная система. Под взломом в этой статистике подразумевается возможность несанкционированного получения доступа к устройству, похищение личной информации, паролей, сообщений, контроль над приложениями и др.

Интересно, что в список 2016 г. попала и другая операционная система от Apple – watchOS, заняв 35 позицию с 77 найденными багами.

***

10.01.2017

Технології часів Другої Світової війни можуть стати основою для банківських карток з високим рівнем безпеки

Запобігти шахрайству з банківськими картами дозволить впровадження нових «розумних» чіпів. Керівництво банків уже починає думати про більш витончені методи захисту, зокрема про використання модернізованого методу цифрового шифрування часів Другої Світової війни, який може бути заміною тризначного CVV-коду (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»).

Про це повідомляє dailytechinfo.org.

Таку нову систему захисту планує запровадити один з найбільших банків Великобританії, банк Barclays. Нова банківська картка буде мати вбудовану клавіатуру і маленький дисплей, а всередині чіпу цієї картки буде прошитий алгоритм шифрування, подібний алгоритму, що використовувався в німецькій шифрувальній машині Enigma. Ця система, заснована на використанні псевдовипадкових чисел, буде виробляти значення, які в сукупності з ПІН-кодом картки послужать заміною системі тризначного CVV-коду, який вже використовується впродовж 20 років.

Д. Тейлор (David Taylor) і Д. Френч (George French), винахідники цієї технології, уже отримали відповідний патент. У цьому патенті також передбачена можливість комунікацій картки з банківським обладнанням за допомогою Wi-Fi і Bluetooth. Такі опції дозволять реалізувати технології безконтактних платежів на зразок Apple Pay і Microsoft Wallet.

Утім для того, щоб запровадити нову систему, необхідна модернізація існуючого та встановлення нового програмного забезпечення і систем апаратних засобів. Технологія безконтактної оплати дозволить уникнути загрози з боку ненадійних платіжних терміналів. А введення ПІН-коду безпосередньо на клавіатурі карти дозволить уникнути його введення на клавіатурі банкоматів або терміналів, які, як добре відомо, так само є доволі вразливим місцем.

Поки навіть самі представники банку Barclays не можуть сказати точних термінів введення в експлуатацію нової системи. Але все це вказує на те, що в

банківській сфері ведуться постійні пошуки нових методів боротьби з шахрайством і зломом банківських кредитних карток.

***

11.01.2017
Самые защищенные браузеры

Safari признан самым защищенным браузером 2016 г. Об этом свидетельствуют результаты исследования компании CVE Details, оценивающей количество серьезных ошибок в ПО, которые дают возможность хакерам получить доступ к операционной системе или сети (InternetUA).

2016 г. принёс меньше всего хлопот разработчикам Apple, отвечающим за Safari. В работе «яблочного» браузера выявлено наименьшее количество брешей безопасности – всего 56.

Рекорд принадлежит обозревателю Chrome: 172 выявленные за год уязвимости. Это означает, что пользователи браузера Google подвергаются повышенной опасности, хотя компания и старается регулярно выпускать обновления с исправлениями ошибок.

Хотя Firefox не стал самым уязвимым браузером в 2016 г., флагманский продукт компании Mozilla остается антилидером в общем рейтинге. На счету этой программы 1437 идентифицированных угроз (против 1370 у Chrome).

Это, правда, неудивительно, учитывая, что CVE Details отслеживают потенциальные угрозы для Firefox с 2003 г., а для Chrome – с 2008 г.

***

12.01.2017
Объем мошенничества в e-commerce возрос на 113 %

В прошлом году количество кибератак в сфере электронной коммерции возросло на 113 %. Такие данные приводит компания Electronic Funds Transfer Association (EFTA) (Finance.Ua).

Эксперты EFTA советуют более тщательно проверять аутентификацию пользователей, что поможет минимизировать возвраты платежей, к чему, собственно, и стремятся мерчанты. Потребители, в свою очередь, ожидают удобства и более надежных систем защиты от мошенничества и кражи личных данных.

Так, в 2016 г. онлайн-торговцы потратили 23 % своего операционного бюджета на мошенничество и возврат платежей. Тем более, что при онлайн-покупках возврат платежей происходит в 49 % случаях, что в три раза выше, чем при обычных покупках.

***

12.01.2017
Константин Семенов

Хакеры смогут взламывать телефоны благодаря селфи

Профессор Национального института информатики Японии И. Эчизен рассказал, что по селфи уже возможно распознать отпечаток пальца пользователя (podrobnosti.ua).

Ученому удалось распознать отпечатки пальцев на снимке, сделанном на расстоянии трех метров от объектива.

Профессор также сообщил, что его команда разработала технологию против кражи отпечатков пальцев. В ее основе лежит использование вещества на основе окиси титана, позволяющего скрыть или даже изменить изображения любых отпечатков пальцев, снятых на фото.

Проблема особенно критична для Азии, так как местная молодежь любит делать селфи с жестом V. Поскольку все больше смартфонов, планшетов и даже ноутбуков оснащаются дактилоскопическими датчиками, злоумышленники могут без проблем получить доступ к личным данным.

***

11.01.2017

Фишеры атакуют пользователей Netflix

Эксперты компании FireEye сообщили о новой волне фишинговых атак, направленных на пользователей видеосервиса Netflix. Целью злоумышленников является похищение данных кредитных карт, номеров социального страхования и другой персональной информации жертв (InternetUA).

Эксперты рекомендуют внимательно относиться к входящим электронным письмам, поскольку хакеры используют взломанные легитимные серверы для создания поддельных страниц, по внешнему виду ничем не отличающихся от настоящих.

По словам исследователей, в большинстве случаев для обхода обнаружения HTML-код на стороне клиента обфусцирован с использованием алгоритма шифрования AES.

Как правило, жертвам рассылаются электронные уведомления о необходимости обновить подписку на Netflix. Нажав на указанную ссылку, пользователь попадает на фишинговую страницу, требующую ввести данные кредитной карты и другую персональную информацию. Полученные таким образом сведения затем передаются злоумышленникам с помощью написанной на PHP почтовой утилиты.

***

12.01.2017

Хакеры ХАМАС под видом красоток взламывают телефоны солдат Израиля

Хакеры ХАМАС взламывали телефоны израильских солдат, воруя фотографии и профили красавиц из социальных сетей. Об этом сообщила 12 января пресс-служба Армии обороны Израиля (ЦАХАЛ) в распространенном коммюнике (Главное).

«Оперативники ХАМАС создавали фальшивые профили в соцсетях и пытались убедить солдат Армии обороны Израиля подружиться с ними, – сообщили в армейской пресс-службе. – Если у них получалось войти в контакт с военнослужащими, хакеры ХАМАС хотели убедить военнослужащих загрузить содержащий вирус видео-мессенджер, который превращал мобильные телефоны в собственный источник информации террористической группировки».

Как отметили в армии, этот «видео-мессенджер» «на самом деле являлся вирусом, способным превратить мобильное устройство в открытую книгу». Вирусный мессенджер «делал доступными для ХАМАС данные контактов и географического положения, список используемых приложений, а также фотографии и файлы» на смартфонах военнослужащих. «Более того, они могли получать трансляцию видео с камеры и звука от микрофона аппарата», – добавили армейские эксперты. «На этот раз оружием ХАМАС были не бомба, не пистолет или транспортное средство, а просто запрос на дружбу в социальных сетях», – подчеркнули в ведомстве военных.

Для того, чтобы взламывать телефоны, «ХАМАС создал десятки фальшивых профилей в соцсетях, каждый из которых использовал настоящие украденные (скачанные с реально существующих профилей. – Прим. корр.) имена и фотографии ничего не подозревающих мирных жителей», сообщили в армии.

Военные отметили, что, «хотя телефоны некоторых солдат и были инфицированы вирусом до того, как он был обнаружен», армейское «Управление разведки продолжает бороться с этой новой угрозой», а также «ведет работу по идентификации поддельных профилей». Государственное радио Израиля проинформировало, что хакерская атака на телефоны солдат «не нанесла существенного ущерба безопасности Израиля».

Вместе с тем армия рекомендовала военнослужащим проявлять бдительность и не забывать про осторожность. «Выключение данных геолокации на телефоне, когда он не используется, может затруднить его отслеживание, а переход по ссылкам разумен только в том случае, если вы доверяете приславшим их контактам», – напомнили в военном командовании. Там также рекомендовали военным «не принимать запросы в друзья в социальных сетях от незнакомых людей» и «не загружать любые приложения из непроверенных источников».

***

13.01.2017
Базиленко Анна

Невідомі зламали екаунт «Дзеркала тижня» у Twitter і поширюють провокативні повідомлення на адресу українських політиків

Користувачі соціальної мережі Twitter помітили, що від імені видання «Дзеркало тижня» поширюються коментарі образливого характеру. У виданні підтвердили: Twitter-екаунт дійсно зламано (Watcher).

«Видання приносить вибачення за повідомлення, що публікуються там», – застерігають у «Дзеркалі тижня».

Від імені «Дзеркала тижня» у Twitter поширені провокативні коментарі на адресу Euromaidan Press, П. Порошенка, А. Парубія, А. Авакова, А. Яценюка.

***

15.01.2017

WhatsApp опровергает слухи о чтении пользовательских сообщений

На днях появилась информация о том, что из-за особенностей системы шифрования разработчики популярного мессенджера WhatsApp могут перехватывать и читать пользовательские сообщения без их ведома. Это вызвало шквал негодования, а Т. Болтер, специалист в области криптографии и безопасности Калифорнийского университета Беркли, обнаруживший данную уязвимость, и вовсе уверен, что разработчики WhatsApp могут при необходимости передавать переписки спецслужбам. Создатели WhatsApp незамедлительно отреагировали на такие обвинения в свой адрес и выпустили официальное заявление (InternetUA).

В сообщении представителей WhatsApp говорится следующее:

«Издание The Guardian опубликовало новость, утверждая, что намеренное решение в WhatsApp ведёт к тому, что люди могут потерять миллионы сообщений, и что это является лазейкой, позволяющей правительствам заставить WhatsApp расшифровывать потоки сообщений. Это утверждение является ложным.

WhatsApp не предоставляет правительствам “чёрный ход” в свои системы и будет бороться с любой попыткой создать такую лазейку. Дизайнерское решение, упоминаемое в истории The Guardian, предотвращает перехват сообщений. К тому же WhatsApp предлагает пользователям специальную функцию, чтобы предупредить их о возможных угрозах безопасности. Мы опубликовали технические подробности нашего шифрования и всегда были прозрачными в отношении запросов со стороны правительств, публикуя данные о них в Facebook».

Компания Facebook, являющаяся владельцем WhatsApp, отказалась сообщать, использовала ли она эту особенность системы шифрования для доступа к сообщениям пользователей и был ли хоть раз получен такой доступ по требованию государственных органов.

***

15.01.2017

Deutsche Bank запретил сотрудникам пользоваться WhatsApp

Немецкий Deutsche Bank запретил своим сотрудникам использовать мессенджеры WhatsApp, Google Talk и iMessage на корпоративных телефонах, сообщает Bloomberg (InternetUA).

Отмечается, что такая мера связана с тем, что текстовые сообщения, в отличие от писем, отправленных по электронной почте, нельзя хранить на серверах компании.

«Мы прекрасно осознаем, что такое решение изменит вашу повседневную работу, и мы сожалеем о доставленных неудобствах. Тем не менее этот шаг необходим для того, чтобы Deutsche Bank продолжал соответствовать нормативным и правовым требованиям», – говорится в обращении компании к сотрудникам.

***

16.01.2017

Базиленко Анна

Новий банківський троян може викрасти будь-який файл з Android-смартфона, маскуючись під «ВКонтакте» та «Одноклассники»

Українські кіберполіцейські виявили новий шкідливий банківський троян з root-правами, який заражає Android-смартфони. Спрямований цей троян на мешканців України, Білорусії та інших країн СНД. У Департаменті кіберполіції звітують про 500 тис. інфікованих пристроїв, при цьому щодня кількість заражених пристроїв збільшується на 30–40 тис. (Watcher).

За інформацією відомства, троян маскується під різні популярні додатки, наприклад, «ВКонтакте», «ДругВокруг», «Одноклассники», Pokemon GO, Telegram або Subway Surf.

«Мова йде про їхні копії, які поширюються через неофіційні каталоги. Впроваджений в легітимний додаток код розшифровує файл, доданий зловмисниками в ресурси програми, і запускає його. Потім запущений файл викачує з керуючого сервера основну частину шкідливого коду, який містить посилання на скачування ще декількох файлів – експлоїта для отримання рута, нових версій шкідника і так далі», – пояснюють у кіберполіції.

До функціоналу трояну входять: відправлення/крадіжка/видалення SMS, запис/переадресація/блокування дзвінків, перевірка балансу, крадіжка контактів, здійснення дзвінків, зміна керівника сервера, завантаження і запуск файлів, встановлення і видалення програм, блокування пристрою з показом веб-сторінки, заданої сервером зловмисників, складання і передача зловмисникам списку файлів, які містяться на пристрої, відправка/перейменування будь-яких файлів, перезавантаження телефону.

Кожен завантажений файл може додатково завантажити з сервера, розшифрувати і запустити нові компоненти. У результаті на заражений пристрій завантажуються кілька модулів шкідника.

Троян також завантажує і популярний пакет експлойтів для отримання прав root: встановлює один з завантажених модулів у системну папку, що ускладнює процес його деінсталяції, а за допомогою прав користувача оператори шкідливого ПЗ викрадають бази даних дефолтного браузера Android і браузера Google Chrome (якщо такий встановлений). Такі бази даних містять інформацію про збереженні логіни і паролі, історію відвідувань, файли cookie, іноді – збережені дані банківських карт. Root-права також дозволяють викрасти практично будь-який файл у системі – від фотографій і документів до файлів з даними екаунтів мобільних додатків.

***

16.01.2017

Google Key Transparency сделает шифрование более простым и доступным

С появлением большого числа онлайн-сервисов пользователи стали хранить практически всю личную информацию в Интернете. В связи с этим специалисты регулярно работают над повышением безопасности приложений и сервисов, чтобы пользовательские данные были надёжно защищены. Несмотря на это, инженеры по безопасности Google отметили, что нет единого и надёжного публичного способа обмена ключами шифрования, который бы работал с целым рядом приложений. Для решения этой проблемы поисковый гигант объявил о создании проекта Key Transparency, в рамках которого будет создан простой способ для безопасного соединения даже через ненадёжные серверы (InternetUA).

По словам Р. Херста и Г. Белвина, сотрудников Google, большинство людей сталкивается с трудностями при использовании методов шифрования, вроде PGP или зашифрованных приложений для обмена сообщениями, поскольку в случае компрометации сервера с ключами пользователям приходится вручную проверять ключи у собеседника. Идея Key Transparency заключается в том, чтобы создать прозрачный общедоступный каталог, с помощью которого разработчики смогут легко создавать системы любого вида с независимо проверяемым данными аккаунтов. Это не только позволит обеспечить защиту сообщений, но и упростит специалистам работу по обеспечению безопасности пользовательских данных.

Сейчас Key Transparency находится на начальной стадии разработки и доступен с открытым исходным кодом для всех желающих.

***

16.01.2017

Как украинцев «разводят» в социальных сетях

Чем так страшны социальные сети – точно знает криминальный эксперт С. Костыра (InternetUA).

1. Компьютер заблокирован СБУ. На ваш личный компьютер приходит письмо от неизвестного адресата. Вы переходите по ссылке, и что вы видите – ваш компьютер зависает! И посреди экрана всплывает окно о том, что вы заблокированы, потому что распространяли порно-информацию или информацию, содержащую педофилию. Это мошенники. Они скажут вам, для того, чтобы разблокировать вашу операционную систему, нужно максимум в течение 12 часов внести штраф на счет СБУ. Не верьте этому – ваши деньги попадут на счет к мошенникам.

2. «Это тебя я видел на порно видео?» – такое письмо вы получите в соцсети от какого-нибудь виртуального друга. Перейдя по ссылке, вы дадите возможность хакерам считать всю информацию с вашего компьютера. Все ваши данные, документы, и даже банковские реквизиты.

3. Wi-Fi диверсия. Вы находитесь в любом людном месте, и ваш гаджет сообщает, что здесь есть бесплатный Wi-Fi. Внимательно читайте это сообщение. Потому что нажав кнопку ОК вы разрешаете хакерам лазать по вашему компьютеру. Они с легкостью скачают всю информацию о вас и все, что будет находиться в вашем гаджете.

4. Жертвы Instagram. Часто выставляете свои фотографии с новыми приобретениями в соцсети? Не рекомендую. Это может навести воров, и вашу квартиру обнесут.

Как не стать жертвой интернет-мошенников?

1. Если вы уже пользуетесь соцсетями, никогда не выставляйте в них фотографии со своими новыми приобретениями. Никогда не фотографируйтесь на фоне сейфов, своих автомобилей и в дорогих золотых изделиях. Это может стать приманкой для преступников.

2. Если у вас на компьютере всплыло окно о том, что он заблокирован органами СБУ, не спешите пополнять счет и платить мнимый штраф. Наберите на телефон доверия органов безопасности и сообщите им об этом. Или позвоните своему провайдеру и сообщите об этой проблеме.

3. А еще не ленитесь и устанавливайте хорошие антивирусы. Они будут блокировать все спамы. И это не позволит хакерам лазить по вашему гаджету.

Соціальні мережі
як чинник інформаційної безпеки

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

Упорядник Терещенко Ірина

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

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

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