СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(15.02–28.02)

2017 № 4

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(15.02–28.02)
№ 4

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

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

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2017

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ 4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 14
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 20
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 29
Інформаційно-психологічний вплив мережевого спілкування на особистість 29
Маніпулятивні технології 41
Спецслужби і технології «соціального контролю» 43
Проблема захисту даних. DDOS та вірусні атаки 55

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

15.02.2017
Facebook начнет проигрывать видео со звуком в лентах

Социальная сеть анонсировала серию обновлений для видео. Во-первых, компания начнет автоматически проигрывать звук в видео при пролистывании ленты в мобильном приложении. При этом громкость видео будет плавно возрастать и убывать при листании ленты. Отключить функцию автоматического запуска звука для видео можно в настройках приложения. Кроме того, вертикальные видео теперь займут большую площадь экрана на Android и iOS девайсах. Пользователи также смогут активировать режим «картинка в картинке» и одновременно смотреть видео и пролистывать ленту. В случае с Android девайсами пользователь сможет продолжать смотреть видео, выйдя из приложения Facebook. Сеть также вскоре представит новое приложение для Apple TV, Amazon Fire TV и Samsung Smart TV которое позволит смотреть видео из сети (Marketing Media Review).

***

15.02.2017
1+1 Media запускает проект для соцсетей о футболе с ведущими «Профутбола»

Группа компаний 1+1 Media 15 февраля запускает новый проект для социальных сетей – FootballHub, сообщает пресс-служба холдинга (Телекритика).

В компании ожидают, что он станет новым этапом развития футбольной журналистики в Украине, поскольку объединит все виды СМИ. «Уникальность проекта заключается в том, что у проекта будет собственное видеопроизводство, онлайн-стримы, обзоры от топовых блоггеров, ежедневные эксклюзивы. Кроме того, большой акцент будет делаться на оформлении информации», – говорят в 1+1 Media.

Журналисты FootballHub будут присутствовать практически на всех матчах, поэтому зрители смогут получать уникальный контент, в том числе из-за кулис – все то, что не попадает на телевидение. Лицами проекта станут ведущие телеканала «2+2» И. Цыганык и А. Лобода.

FootballHub будет доступен в Facebook, «ВКонтакте», Twitter, Instagram и YouTube и будет состоять из 15 рубрик. Среди них, например, – рубрика «Антиексперт»: размышления о последних главных футбольных новостях «антиексперта» – человека из деревни, который увлекается футболом; «JoLiga» – авторская рубрика Лободы о «вокругфутбольном» фэшне и гламуре; рубрика спортивного комментатора «2+2» В. Кобелькова What's Up? – это откровенный

разговор со звездной личностью; рубрика блогера Р. Бебеха «Ромаріо Бебето» – обширное интервью в неформальной обстановке.

Также в проекте будет рубрика журналиста К. Андриюка и приглашенных экспертов «Суддя арбітрів» – своеобразный рейтинг судейских решений в прошлом туре; кулинарная рубрика Е. Зинченко Food Ball, в которой автор и кто-то из футболистов будут готовить различные блюда и говорить о здоровом питании.

***

17.02.2017

Цукерберг анонсував зміну формату Facebook

Засновник Facebook М. Цукерберг має намір змінити формат Facebook і зайнятися розвитком соціальної інфраструктури для формування глобального співтовариства (iPress.ua).

«Зараз по всьому світу є люди, які залишилися за бортом глобалізації, і рухи, які виступають за відхід від глобальних зв'язків», – написав М. Цукерберг у зверненні до користувачів на Facebook.

Він підкреслив, що хоче перейти від формату соцмережі для друзів і сім'ї до розвитку глобальної соціальної інфраструктури.

«У такі часи, як зараз, найважливіше, що ми в Facebook можемо зробити – це створити соціальну інфраструктуру, щоб дати людям можливість побудувати глобальне співтовариство, яке працює для всіх нас», – підкреслив М. Цукерберг.

Він виділив п'ять основних напрямів – розвиток взаємної підтримки, забезпечення безпеки, інформованості, громадянської активності та залучення представників різних культур і поглядів.

Зокрема, говорячи про поширення інформації, М. Цукерберг висловив стурбованість з приводу «бульбашок фільтрів» (персоналізація пошуку і відображення інформації, при якій користувач бачить тільки те, що йому подобається і відповідає його поглядам) і поширення фейкових новин.

На думку М. Цукерберга, проблемою є і те, що сенсаційні і прості повідомлення поширюються швидше за інші. Щоб обмежити поширення кричущих заголовків, Facebook вводить алгоритми з обліку, чи читав користувач статтю за посиланням, перш ніж їй поділитися. Ця обставина впливає на показ таких матеріалів у стрічці новин юзерів.

Крім того, М. Цукерберг зазначив, що Facebook розробив штучний інтелект, який повинен розпізнавати заборонений контент, що почне частково застосовуватися вже в 2017 р.

***

20.02.2017

Ірина Коркішко

Facebook експериментує зі сповіщеннями

Соціальна мережа Facebook експериментує з форматом «спливаючих сповіщень», що з'являються знизу сторінки подібно до чату Facebook Messenger (Watcher).

За інформацією видання iTech Post, спливаючі сповіщення – це експеримент, що дає можливість постам від друзів отримати більше уваги зі сторони користувача. Вони дозволяють обговорювати пост, не покидаючи сторінки News Feed.

Нове вікно буде відкриватися, коли хтось прокоментує пост користувача, відповість на коментар користувача під постом або ж позначить користувача у коментарях. Як і для звичайних сповіщень, спливаючі сповіщення можна вимкнути в налаштуваннях.

Як стверджує Facebook, поки що оновлення доступне невеликій кількості користувачів. Остаточної думки щодо впровадження спливаючих постів немає. Однак, є вірогідність, що оновлення стане доступним для всіх користувачів уже незабаром.

***

20.02.2017

Мессенджер WhatsApp запустил самоуничтожающиеся статусы

Команда популярного мессенджера WhatsApp добавила новую возможность в приложение. Обновленная функция Status (Статус) теперь позволяет обмениваться фотографиями и видео, а не только текстом. Эти статусы работают примерно также, как и «Истории» (Stories) в Instagram и Snapchat, самоуничтожаясь через сутки после публикации (InternetUA).

Для публикации пользователю надо использовать встроенную функцию камеры в WhatsApp для съемки фото или видео. Отснятый контент можно подписать, используя текстовые сниппеты, эмодзи и рисунки. Статусами можно делиться со всеми контактами, а также выбирать кому они будут видны. Через вкладку Статусов пользователь может наблюдать за обновлениями всех своих контактов, а также отвечать им в приватном режиме. Как и прочий контент мессенджера, статусы защищены сквозным шифрованием.

Новые Статусы начали внедряться в приложение WhatsApp с сегодняшнего дня и вскоре будут доступны всем пользователям iPhone, Android и Windows Phone.

***

20.02.2017

Базиленко Анна

Twitter блокуватиме екаунти на 12 годин за порушення правил спілкування

Сервіс мікроблогів Twitter запустив новий інструмент для боротьби з тролінгом у соцмережі. Екаунти користувачів, які порушили правила спілкування, будуть тимчасово заблоковані – на час блокування їхні публікації будуть видимі лише підписникам (Watcher).

У BuzzFeed повідомили, що заблоковані користувачі Twitter отримали від соцмережі листа, у якому йшлося про політику створення безпечного інтернет-середовища, якої дотримується компанія, а також наводились пояснення, чому їхні екаунти були заблоковані. Користувачі припускають, що тимчасові обмеження вводяться за використання ненормативної або образливої лексики. Вони також припустили, що функція працює автоматично, але офіційних підтверджень цьому немає.

На початку місяця в Twitter повідомили про запуск нових інструментів для боротьби з негативними коментарями, в тому числі, з тролінгом. Про тимчасове блокування екаунтів не йшлося, втім, повідомлялось, що заблоковані тролі більше не зможуть створювати нові екаунти, у відповідь на пошукові запити відображатимуться «безпечніші результати», повідомлення образливого змісту будуть приховуватися.

***

16.02.2017
Базиленко Анна
Facebook запустив сервіс для публікації вакансій і відправки резюме

Компанія Facebook дозволила власникам бізнес-сторінок публікувати вакансії за допомогою нового інструмента, а користувачам – безпосередньо в соцмережі відправляти резюме. Першими доступ до сервісу отримали компанії в США і Канаді, повідомляє Recode (Watcher).

Опубліковані вакансії будуть видимі в стрічці новин і в спеціальному розділі на сторінці компанії. Якщо користувача зацікавить оголошення, він зможе відгукнутися на нього, натиснувши кнопку «Apply Now».

Facebook буде автоматично вказувати в формі відгуку особисту інформацію користувача, який відгукнувся на відкриту вакансію. Ці дані будуть вилучатись з його профілю в соцмережі.

Роботодавці зможуть відповідати на отримані заявки через Messenger.

За додаткову плату компанії зможуть підвищувати видимість своїх вакансій для певних категорій користувачів.

***

21.02.2017

Пользователи Facebook смогут сами цензурировать свою ленту новостей

Facebook предоставит возможность каждому пользователю самому определять уровень цензуры в его ленте новостей. Как сообщает Adindex.ru, об этом объявил основатель соцсети М. Цукерберг (Телекритика).

По его словам, идея заключается в том, чтобы каждый мог установить свою собственную границу дозволенного в отношении, например, взрослого контента или контента, содержащего насилие.

По умолчанию пользователю будут предложены настройки, которые выбрали большинство пользователей в его стране. А Facebook периодически будет предлагать вопросы на этот счет, что избавит пользователей от самостоятельного регулирования этих настроек.

***

21.02.2017

WhatsApp запустил возможность публикации самоуничтожающихся сообщений

WhatsApp представил сервис Status, который позволяет пользователям размещать самоуничтожающиеся публикации по аналогии с Instagram Stories, Snapchat и другими сервисами. Об этом сообщает TechCrunch (IGate).

Главным отличием WhatsApp Status от похожих проектов станет шифрование размещаемых сообщений. Пользователи смогут выбрать, кто из их друзей сможет видеть публикации из Status.

Новая функция заменит «статусы», отображающиеся ранее около имен пользователей (к примеру, «Привет, я использую WhatsApp»). Как рассказал глава WhatsApp Я. Кум, основной смысл нововведения – предоставить возможность пользователям быстро рассказывать о том, что происходит в их жизни.

WhatsApp Status можно будет просматривать в специальной вкладке в мессенджере, а не над лентой обновлений, как в Instagram. Нововведение постепенно станет доступно всем пользователям сервиса на устройства Android, iOS и Windows Phone.

Отметим, что последним данным аудитория WhatsApp составляет порядка 1,2 млрд пользователей в месяц, поэтому появление новой функции может стать проблемой для дальнейшего развития Snapchat, основная «фишка» которого заключается в аналогичном функционале, отмечает TechCrunch.

Помимо WhatsApp, похожие на Snapchat Stories функции уже запустили Instagram, Facebook, «ВКонтакте», Facebook Messenger и др.

***

22.02.2017

Соцмережа «ВКонтакте» заявила про рекордну відвідуваність в Україні

На сайт «ВКонтакте» в один з лютневих днів зайшли 16 млн унікальних користувачів (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»).

Нові дані про популярність соцмережі навів у своєму блозі прес-секретар «ВКонтакте» в Україні В. Леготкин.

«“ВКонтакте” встановив новий рекорд в Україні – 16 млн унікальних відвідувачів на добу. Темпи нашого зростання прискорилися: ще в грудні ця цифра становила 15 млн», – написав В. Леготкин.

За його словами, причинами популярності соцмережі серед українців стали «зручність спілкування, свобода поширення інформації і сучасні сервіси».

Цікаво, що 16 лютого радник глави МВС З. Шкіряк запропонував ввести заборону в Україні на російські соціальні мережі «ВКонтакте» та «Одноклассники».

За словами В. Леготкина, втім, рекорд відвідуваності був встановлений до заяви політика.

***

21.02.2017
В Telegram появился редактор тем

Настольная версия Telegram обновилась до версии 1.0.12, и в ней пользователям через меню настроек стал доступен редактор тем. Помимо этого, в мессенджер была добавлена поддержка большего количества эмодзи, а также возможность с помощью курсора мыши выбирать определённый момент аудиофайла для его проигрывания. Более того, поддержка тем вместе с соответствующим редактором были впервые добавлены в Telegram для Android (InternetUA).

Ранее в этом месяце вышла бета-версия настольного клиента Telegram, из которой стало ясно, что возможность редактировать темы появятся в следующей стабильной сборке приложения. Что же касается iOS, то разработчики заявили следующее: «Если вы используете наше приложение для iOS, потерпите пару недель. В конечном итоге вы тоже получите темы, а пока мы разрабатываем для вас нечто другое – и это по-настоящему эпично».

Теперь темы в настольной версии Telegram можно выбирать двумя способами. Первый был доступен в программе ещё с момента выхода версии 1.0, состоявшегося в прошлом месяце – он позволяет просто устанавливать темы, которые были созданы другими людьми. Второй способ – это создание своего собственного варианта оформления клиента: пользователь может сам выбрать общую палитру и цвета для каждого элемента мессенджера. Раньше всё это можно было делать лишь посредством редактирования кода программы. На Android выбор тем реализован похожим образом. Поиск пользовательских вариантов оформления можно осуществлять через специальный официальный канал.

Согласно последним бета-сборкам Telegram, команда разработчиков мессенджера также собирается добавить в продукт поддержку некоей платёжной системы. Более того, генеральный директор компании П. Дуров отметил, что в сервисе вполне может появиться поддержка аудиозвонков.

***

23.02.2017
К 2019 г. мессенджеры обойдут социальные сети по популярности

Аналитики из компании Gartner уверены, что в 2019 г. мессенджеры станут более популярными нежели социальные сети. К таким выводам специалисты пришли после изучения рынка спроса на мобильные приложения (Grifonsoft).

Сотрудники компании Gartner опросили более трех тысяч жителей Великобритании, Китая и США по поводу их частоты использования социальных сетей и мессенджеров. Около 72 % пользователей заходят на серверы быстрого обмена сообщениями как минимум один раз в день.

Аналитики отметили, что раньше социальные опросы не показывали таких результатов. Людям было удобней общаться через социальные сети, так как на этих порталах с самого начала существовала возможность обмениваться медиа файлами. Теперь подобные функции стали внедрять и в мессенджеры.

В последние несколько месяцев мессенджеры начинают укреплять на рынке приложений свои позиции. Это неудивительно, ведь сами по себе программы просты в использовании и обладают всеми необходимыми функциями. В некоторых из них можно даже заказывать доставку еды и осуществлять денежные переводы.

Социальные сети и видеохостинги уже потеряли часть своей аудитории по 2 и 4 % соответственно. Компания Facebook пытается компенсировать эти утраты созданием собственного мессенджера. Примечательно то, что приложение стало намного популярнее, чем основной сервер.

***

23.02.2017
Microsoft створює на основі Windows 10 соціальну мережу

Корпорація Microsoft представила масштабне оновлення Windows 10. Зокрема, в оновленій версії операційної системи з’явиться функція MyPeople, яка дозволить розміщувати обрані контакти безпосередньо на робочому столі. У такий спосіб у Microsoft планують полегшити обмін повідомленнями як поштою, так і через додатки. Користувачі оновленої Windows 10 також зможуть обмінюватися емодзі (biznesoblast.com).

За допомогою функції MyPeople користувач може позначати важливі контакти. Іконки із зображенням цих контактів будуть знаходитися на панелі задач. Користувач зможе відправити будь-який файл, перетягнувши його на

іконку. Таким чином, файлами можна буде ділитись з іншими користувачами через імейл або Skype.

Оновлена Windows 10 також сортуватиме вхідні повідомлення з імейлу та чатів у Skype: повідомлення від обраних контактів з'являтимуться в першу чергу. MyPeople дозволяє перемикатися між додатками і відповідати в кількох з них одночасно.

***

22.02.2017

Microsoft представила «облегченную» версию Skype для пользователей с медленным Интернетом

Компания Microsoft анонсировала Android-приложение Skype Lite, являющееся «облегченной» версией мессенджера для пользователей из стран с низким качеством интернет-соединения, рассказывает TechCrunch (IGate).

На первом этапе новая программа станет доступна только в Индии, где Microsoft и представила Skype Lite в ходе конференции Future Decoded. Приложение весит всего 13 Мб и работает на мобильных устройствах под управлением Android 4.0.3 и выше, указывается в описании сервиса в Google Play. Сроки запуска приложения в других странах пока не называются.

При медленнov или нестабильнov соединение программа может адаптироваться самостоятельно, позволяя абонентам без каких-либо неудобств использовать функции обмена сообщениями и вызова, в том числе и с видео, отмечают в Microsoft.

К июню компания собирается интегрировать Skype Lite с национальной системой идентификации пользователей из Индии под названием Aadhaar, в базе которой хранятся отпечатки пальцев, а также изображения радужных оболочек глаз большинства жителей страны. При помощи этой базы пользователи мессенджера смогут быстро идентифицировать неизвестных собеседников, к примеру, при покупке товаров или собеседований при приёме на работу, говорят в Microsoft.

***

22.02.2017

«ВКонтакте» может запустить виртуального оператора VK MVNO уже летом

Популярная социальная сеть «ВКонтакте» может запустить услуги виртуального оператора VK MVNO уже в средине лета 2017 г. Об этом сообщил финансовый директор Mail.ru Group М. Хэммонд (Grifonsoft.ru).

Холдинг Mail.ru Group планирует внедрить в «ВКонтакте» функцию виртуального оператора под названием VK MVNO, что будет действовать на основе покрытия «МегаФон».

М. Хэммонд добавил, что первоначальный запуск предполагается во время VK Fest, что пройдёт 15–16 июля, но эта информация является предварительной, и может ещё измениться.

***

22.02.2017

Instagram разрешил публиковать до 10 снимков в одном посте

Instagram ввел новую функцию, которая позволит размещать до 10 элементов – фотографий и видеороликов – в одной публикации. Об этом сообщается в блоге компании (InternetUA).

Как отмечается, при публикации нового поста необходимо нажать специальный значок, после чего выбрать до 10 материалов. Снимки можно будет отредактировать в одном стиле или каждый отдельно. Также Instagram позволит выбрать порядок следования элементов. Количество фотографий и видео будет отображаться точками под публикацией.

В отличие от Stories, которые исчезают через 24 часа, эти посты будут оставаться в профиле, отмечают в Instagram.

***

28.02.2017

Найден способ скрыть свои эмоции от Facebook

В сети появилось расширение для браузеров Go Rando, не позволяющее Facebook распознать реакции пользователя под постами в ленте новостей (InternetUA).

Разработчики приложения утверждают, что социальная сеть использует информацию об эмоциональных реакциях (таких как «лайк», «вау» или «ха-ха») не только для улучшения новостной ленты, но и для таргетирования рекламы и прочих манипуляций с данными. К примеру, рекламные клиенты Facebook могут воспользоваться ситуацией, когда юзер слишком зол или, наоборот, в хорошем расположении духа.

Создатели Go Rando предлагают запутать алгоритм: расширение отправляет Facebook информацию о якобы нейтральных эмоциональных реакциях пользователя. Если юзер оставляет слишком много положительных или отрицательных эмодзи под постами, Go Rando «уравновешивает» их.

Расширение работает на браузере Google Chrome. Для других пользователей информация об инструменте доступна в блоге разработчиков.

***

27.02.2017

Google закроет мессенджер Spaces 17 апреля

В прошлом году, не дожидаясь начала конференции I/O 2016, компания Google представила мессенджер Spaces. Главной идей приложения стала организация беседы ещё до её начала: пользователи имели возможность создавать тематические чаты, где могли бы обмениваться фото- и видеофайлами, ссылками и любой другой полезной информацией, привязанной к конкретной теме. Отличительной чертой Google Spaces от аналогов стала интеграция с собственными сервисами компании: браузером Chrome, поисковиком, Google Фото и YouTube. Несмотря на расширенные возможности мессенджера, проекту так и не удалось привлечь внимание широкой аудитории. На днях разработчики сообщили о прекращении работы Google Spaces начиная с 17 апреля (InternetUA).

«Сервис Spaces задумывался как удобная площадка для обмена контентом и идеями в небольших группах, – обращаются разработчики Google к пользователям на официальной странице поддержки Google Spaces. – Накопленный опыт поможет нам улучшить другие продукты и службы Google. Благодарим вас за піддержку».

Решение о прекращении работы сервиса компания приняла всего после девяти месяцев существования мессенджера Google Spaces.

Уже 3 марта 2017 г. сервис станет доступным только для чтения, поэтому пользователи не смогут создавать темы и записи, оставлять комментарии, отправлять приглашения и добавлять участников. До 17 апреля ещё можно будет просматривать, сохранять, печатать и удалять контент, созданные темы и их участников, а также сообщать о нарушениях в Spaces и блокировать других пользователей сервиса. После 17 апреля 2017 г. сервис Google Spaces и весь контент в нём будут удалены.

***

27.02.2017

Twitter очеловечила процесс общения пользователей с компаниями

Twitter решила снова внести изменения в систему прямых сообщений – на этот раз с целью позволить клиентам общаться с компаниями и видеть, что они ведут переписку не с автоматизированным ботом, а с человеком. В сервисе появились специальные пользовательские профили для компаний, благодаря которым в переписке теперь отображается не название бренда, а имя и фотография сотрудника (InternetUA).

«Людям нравится обращаться к компаниям через Twitter, потому что они получают возможность связаться с реальным человеком, когда нуждаются в помощи, – написал руководить службы поддержки Twitter И. Кернс (Ian Cairns). – Сегодняшняя функция даёт отдельным компаниям возможность очеловечить взаимодействия. В то время как многие компании сегодня используют ботов, чтобы отвечать на запросы, до сих пор возникают случаи, когда нужен именно человек. Пользовательские профили – это способ, благодаря которому клиенты

могут избежать необходимости общаться с пресным аватаром, из-за чего становится сложно понять, говорят они с роботом или с человеком».

Єто нововведение – очередная попытка Twitter сделать прямые сообщения более полезной функцией для брендов. Всё больше компаний переключаются на Facebook Messenger для общения с клиентами, и Twitter всеми силами старается эти компании удержать. Именно поэтому сервис не только запустил нововведение, но и заключил соглашения с рядом провайдеров технологий для обслуживания клиентов, включая Assist, Conversable, Dexter, Lithium, Sprinklr, Spredfast и Sprout Social.

Стоит отметить, что это нововведение не доступно напрямую через прямые сообщения. Вместо этого разработчикам необходимо самостоятельно встраивать соответствующую функциональность в свои предложения. На данный момент прикладной программный интерфейс, необходимый для встраивания новой возможности, находится в стадии закрытого бета-тестирования.

***

27.02.2017

В Google создали алгоритм для борьбы с гневными комментариями в Интернете

Анонимность является одной из главных проблем Интернета, так как чувствуя полную безнаказанность, некоторые пользователи оскорбляют других людей и делают всё, что им вздумается. Google решила положить этому конец и разработала алгоритм на базе машинного обучения, получивший название Perspective. Он способен анализировать и оценивать комментарии на предмет оскорблений в адрес других людей и прочих нежелательных высказываний (InternetUA).

Google выпустит набор всех необходимых инструментов, так что разработчики и платформодержатели смогут внедрить новый алгоритм в свои приложения и сайты. По мере обучения Perspective сможет распознавать разные уровни «токсичности» комментариев и выполнять соответствующие действия, запрограммированные разработчиками. Кроме этого, в перспективе алгоритм сможет распознавать комментарии, не относящиеся к теме обсуждения.

На данный момент Perspective поддерживает только английский язык, но Google исправит это в ближайшем будущем.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

15.02.2017

Євробачення-2017: у соцмережах з'явилися офіційні сторінки конкурсу

У найбільших соціальних мережах уже створили українські спільноти Євробачення-2017 (Espreso.tv).

Про це повідомляє UA:Перший.

На сторінках Євробачення оперативно надаватимуть найцікавішу офіційну й перевірену інформацію про пісенний конкурс. Також організатори хочуть таким чином об'єднати українських уболівальників.

Найближчим часом переважно інформуватимуть про перебіх підготовки травневих шоу та український національний відбір. Ближче до Єврошоу офіційні спільноти поповнюватимуться новинами про будівництво трибун та сцени в Міжнародному виставковому центрі, головними подіями з інших офіційних локацій, інформацією про спеціальних гостей шоу та бекстейджу пісенного конкурсу.

Навесні на цих сторінках для українських фанів Євробачення запускатимуться різноманітні спецпроекти, у тому числі й інтерактивні, які дозволять більше дізнатися про історію конкурсу та стати його частиною.

Адреси Євробачення-2017 у соцмережах: fb.com/eurovision2017kyiv, vk.com/eurovision2017kyiv, twitter.com/esc2017kyiv та instagram.com/eurovision2017kyiv.

***

16.02.2017

Голова Мюнхенської конференції порадив Трампу припинити писати в Twitter

Голова Мюнхенської конференції з безпеки В. Ішингер гостро розкритикував президента США Д. Трампа через непередбачуваність зовнішньої політики нової адміністрації США і некоректні висловлювання в мережі мікроблогів Twitter. Про це повідомляє DW (LB.ua).

«Той, хто так грубо озивається про медіа, судову систему та спецслужби своєї країни, той стає непередбачуваним і шкодить своїй команді», – заявив В. Ішингер в інтерв'ю газеті Bild.

«Припиніть твітити, пане президенте», – порадив Д. Трампу голова Мюнхенської конференції з безпеки. За його словами, дії Д. Трампа призвели до «максимальної невизначеності» у зовнішній політиці США. «Трампу слід вибрати один курс і дотримуватися його», – наголосив В. Ішингер. Він також розкритикував за це членів команди Д. Трампа, зазначивши, що в зовнішній політиці найважливішими є довіра і передбачуваність.

«Коли така людина, як президент США, оточує себе людьми, які їх (довіру і передбачуваність. – Ред.) підсилюють, це є запорукою успіху. Але

коли він оточує себе людьми, які викликають більше питань, аніж відповідей, тоді передбачуваність і довіра губляться», – зазначив В. Ішингер.

***

17.02.2017

До флешмобу проти афери із будівництвом ГЕС на Дністрі долучаються школярі

Рух «Вільний Дністер» проти знищення Дністровського каньйону набирає обертів. Символічно, що до протестів долучаються і діти і батьки (0352.ua – сайт міста Тернополя).

Це єднання – яке ніяким аферистам від політики і безвідповідальним політиканам та урядовцям не знищити, пише В. Ханас.

Він опублікував фото, на яких видно, як про свій протест заявляють першокласники школи ім. О. Маковея Заліщиків. Підтримують дитячий протест і їхні батьки.

***

17.02.2017

Базиленко Анна

70 % дописів у Facebook українські міністри постять на роботі

Комітет виборців України провів дослідження і з'ясував, що 70 % дописів на своїх сторінках Facebook міністри роблять у робочий час, і далеко не всі вони стосуються роботи (Watcher).

Серед членів уряду, які найактивніше користувалися Facebook на роботі, називають міністра молоді і спорту І. Жданова (83 % дописів), міністра економічного розвитку С. Кубіва (79 %), міністра оборони С. Полторака (79 %), міністра інфраструктури В. Омеляна (61 %) та міністра екології О. Семерака (61 %).

КВУ вважає, що питання медійної активності міністрів у соціальних мережах варто врегулювати шляхом внесення відповідних змін до внутрішніх документів Кабінету Міністрів і наказів Національного агентства з питань державної служби. Адже подібна практика існує в більшості держав Європи.

«Зокрема, у Великобританії діє спеціальна інструкція, яка дозволяє користуватися соцмережами в робочий час, але закликає дотримуватися певних етичних правил. Зокрема, перевіряти достовірність опублікованої інформації, утримуватися від участі в конфліктних ситуаціях, уникати публікації повідомлень щодо особистого життя тощо», – розповів аналітик Комітету виборців.

За його словами, якщо британський держслужбовець ігнорує ці правила, він отримує дисциплінарне покарання, яке може призвести до звільнення. При цьому таке правило діє незалежно від того, чи публікацію розміщено на офіційний чи особистій сторінці, у робочий чи вільний від роботи час.

***

20.02.2017

Винничане могут сообщать Муниципальной полиции о нарушениях через Viber или Facebook

Муниципальная полиция Винницы расширяет каналы коммуникации с жителями. С недавних пор эта служба стала доступна для общения через Facebook и Messenger. Еще раньше возможность сообщить о нарушении Правил благоустройства и санитарного состояния Винницы появилась у жителей через мобильное приложение Viber по номеру +380507476563 (0432.ua – Сайт города Винницы).

Зимой среди прочего Муниципальная полиция контролирует уборку территорий от снега и льда, а во время оттепели – работает с владельцами зданий, чтобы вовремя снимались сосульки с крыш кафе, магазинов и других предприятий. При таких погодных условиях для работников Муниципальной полиции важно иметь качественный обратная связь с виннитчанами, в том числе и через современные мобильные приложения – Viber и Facebook.

Сегодня, после обильных снегопадов, погода способствует тому, что на крышах зданий образуются сосульки. Над очисткой крыш многоквартирных жилых домов от льда работает более полусотни работников ЖЭКов. Также они прочищают от снега водосточные желоба и ливневые канализации.

Кроме многоэтажных домов, опасные сосульки появляются на кафе, магазинах и т. д. Согласно Правилам благоустройства и санитарного состояния Винницы, все субъекты хозяйствования должны самостоятельно убирать свою территорию от снега и льда, это же касается и физических лиц-предпринимателей (владельцы кафе, магазинов и т. д.), а также сбивать сосульки с крыш, или ограждать опасные участки улицы.

«С 6 февраля работники Муниципальной полиции проверили 4180 объектов по уборке прилегающих и придомовых территорий от снега, совершение противогололедных мероприятий для недопущения скользкости и снятия сосулек с крыш зданий. В ходе проверки было предоставлено 1575 предписаний для своевременной уборки снега в том числе 86 по снятию сосулек с крыш, а за невыполнение требований предписаний на ответственных лиц на содержание территорий было составлено 133 административных протоколов. По административным протоколом нарушители должны заплатить штраф от 850 до 1700 грн. На сегодня проверки продолжаются по уборке прилегающих и придомовых территорий, на которых в такую погоду должны быть посыпаны пешеходные дорожки, тротуары для недопущения травмирования граждан. Будем благодарны, если жители будут сообщать нам о нарушении Правил благоустройства через Интернет и мобильные приложения для смартфонов», – рассказал начальник Муниципальной полиции В. Гайовик.

***

23.02.2017

У соцмережах закликають не святкувати 23 лютого: це день окупаційної армії

Користувачі соцмереж нагадують, що 23 лютого – день окупаційної армії, й українці не мають його святкувати (Західна інформаційна корпорація).

«Якби ми були нормальною країною, 23 лютого було би не святом, а днем скорботи», – пише у Twitter користувач з ніком «тётя Роза».

Також користувачі нагадують, що день української армії – це 14 жовтня.

А 23 лютого святкує російська армія і проросійські бойовики на Донбасі.

«Уже всі успішно забули про “свято” 23 лютого. Мрію, щоб так було і з 8 березня...», – пише журналіст Н. Шутка у Facebook.

***

23.02.2017

Новости Верховной Раде появились на англоязычной странице Twitter

21 февраля 2017 г. стартовал англоязычный Twitter Верховной Рады Украины (Електронні Вісті).

Англоязычная версия позволит международным журналистам, иностранным парламентам и государственным учреждениям, посольствам иностранных государств в Украине и заинтересованным гражданам других стран получать актуальную информацию из украинского парламента на понятном для них языке.

Англоязычный Twitter-аккаунт парламента является одним из направлений развития международных коммуникаций, для введения которого используется опыт, в частности, Польши, Грузии и Литвы. В поддержку англоязычного Twitter уже осуществляется рассылка периодического ньюслеттера, на который подписались более 400 человек.

Англоязычный Twitter, с помощью которого параллельно с украинской версией осуществляется освещение событий пленарной недели, в течение нескольких часов набрал своих первых 200 подписчиков и получил положительные отзывы общественности. Страница Twitter находится по ссылке: https://twitter.com/ua_parliament.

***

22.02.2017

Ольга Стрижова

Социальные сети захватил флешмоб «Шануймо рідну мову»

В Станице Луганской школьники предложили всем желающим вспомнить и зачитать любимые стихи на украинском языке в рамках флешмоба «Шануймо рідну мову». Акция заканчивается 9 марта в день рождения Тараса

Шевченко. Уже сейчас во флешмобе приняли участие дети не только из Луганской области, но и Житомирской, Сумской, Львовской, а также Полтавской. А также волонтеры, журналисты, артисты и военные (Радіо Свобода).

По словам луганского блогера А. Фалина, неудивительно, что такая акция началась именно со Станицы Луганской, ведь этот поселок всегда был настроен проукраински.

«Если бы вы пообщались в Станице Луганской с людьми в 2013–2014 гг., они бы высказались в поддержку Украины. А сейчас они находятся на линии разграничения. В лучшем случае каждый день слышат взрывы и обстрелы, а в худшем – чувствуют их на себе и прячутся в подвалах. Они видят, кто их защищает, а кто обстреливает», – рассказывает А. Фалин.

Также блогер отметил, что флешмобы в поддержку украинского языка и литературы, как никогда сейчас нужны не только Луганщине, но и всей Украине.

«Очень важно, что такие флешмобы стартуют именно с Луганщины, с линии разграничения, из Станицы Луганской. Во-первых, это показывает, что далеко не все настроены на поддержку России и террористических группировок. Во-вторых, это свидетельствует, что у нашего государства есть будущее, ведь этот флешмоб запустили именно дети», – говорит А. Фалин.

В социальных сетях уже можно найти несколько десятков видео, на которых маленькие дети в вышиванках зачитывают стихи украинских поэтов.

***

27.02.2017

На адмінмежі з Кримом пройшла акція на підтримку опору Криму російській окупації

26 лютого в селі Чонгар, яке розташоване поблизу з адмінмежею з окупованим Кримом, відбулася акція в підтримку опору Криму російській окупації та флешмоб «Крим – це Україна» (0552.ua – Сайт города Херсона)!

Від села до контрольного пункту в'їзду-виїзду «Чонгар» відбулася піша хода, у якій взяли участь більше 300 осіб, пише Херсонская правда.

У заході, присвяченому 1096 днів опору Криму російській окупації, взяли участь керівництво Херсонської ОДА, Генічеської, Новотроїцької, Каланчацької, Чаплинської райдержадміністрацій, представники громадських організацій, релігійних конфесій, активісти громадського формування з охорони громадського порядку та державного кордону «Аскер», представники Херсонського регіонального меджлісу кримських татар та молодь.

***

27.02.20171

Херсонська ОДА закликає до міжнародної акції «Тризуб це Україна»

У зв’язку з останніми подіями в світі, постала гостра проблема у відсутності ідентифікації українських національних символів за кордоном. Через недостатню поінформованість світової спільноти про національну символіку України, виникла проблема ототожнення традиційних українських національних символів з символами ультраправих рухів. Такий стан речей дозволяє окремим політичним та громадським силам за кордоном використовувати українську символіку в цілях негативної пропаганди, що в свою чергу призводить до дезінформації громадськості за кордоном про поточний стан справ в Україні (0552.ua – Сайт города Херсона).

Про це повідомляють на сайті Херсонської Обласної Державної Адміністрації.

З цього приводу оголошується флеш-моб «Тризуб це Україна» (Trident is Ukraine), учасником якого може стати кожен, хто підтримує Україну. Основною метою флеш-мобу є поширення поінформованості закордонної спільноти стосовно українських національних символів.

Акцію організовують Світовий Конгрес Українських Молодіжних Організацій та міжфракційне депутатське об’єднання «Співпраця: Україна-Діаспора».

На кінець серпня в місті Дніпро під час проведення Форуму української молоді діаспори «Дніпро 2017» планується фото-виставка найкращих та найцікавіших фотографій.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

15.02.2017
Капитализация Twitter уступила китайскому аналогу

Капитализация сервиса микроблогов Weibo превысила Twitter, который был взят за основу при разработке китайской социальной сети. Об этом сообщает Bloomberg (InternetUA).

Рыночная стоимость компании из КНР возросла до 11,3 млрд долл. В то же время капитализация Twitter после публикации финансовой отчетности снизилась до 11,1 млрд долл.

***

15.02.2017
Глава Twitter купил акции компании на 7 млн долл.

Генеральный директор Twitter Дж. Дорси (Jack Dorsey) докупил акции компании на сумму 7 млн долл. Об этом сообщает телеканал CNBC со ссылкой на материалы, отправленные в Комиссию по ценным бумагам и биржам США (InternetUA).

Дорси приобрел около 426 тыс. ценных бумаг Twitter по цене от 15,84 до 16,6 долл. за штуку. Теперь топ-менеджеру принадлежит около 30,5 млн акций компании. Летом 2015 г. Дж. Дорси выкупил пакет ценных бумаг компании на сумму 875 тыс. долл.

За прошлую неделю котировки Twitter упали почти на 10 % после того, как компания отчиталась о самом слабом росте выручки с момента выхода на биржу. В октябре–декабре 2016 г. выручка Twitter составила 717 млн долл., что на 1 % больше относительно аналогичного периода предыдущего года.

***

16.02.2017

Как быстро набрать подписчиков в Instagram

Сегодня речь пойдёт об InstaPlus – удобном сервисе для продвижения с возможностью отложенного постинга в Instagram (Украинские реалии).

Ведёте ли вы бизнес в Instagram или просто хотите, чтобы ваши фотографии оценило как можно больше людей, без специальных методов не обойтись.

Зачем вообще нужны подписчики

Не только для повышения самооценки владельца аккаунта с помощью лайков. Чем больше аудитория, тем больше возможностей для продвижения ваших товаров и услуг. В конце концов, какая польза даже от самого интересного профиля, если на его обновления подписано лишь несколько десятков человек? Вот и получается, что без армии фолловеров все прочие усилия не приведут к хорошему результату.

Получить новых подписчиков можно с помощью массфолловинга и масслайкинга, но заниматься этим вручную – то ещё развлечение. Результат не всегда сможет оправдать затраченные усилия и время. Выход – автоматизировать процесс привлечения аудитории. Сделать это можно с помощью сервиса InstaPlus.me.

Что умеет InstaPlus

Мы неоднократно рассказывали, чем хорош InstaPlus: он взаимодействует с вашей целевой аудиторией посредством лайков, уникальных комментариев и подписок. Всего за несколько часов можно существенно увеличить количество подписчиков.

Итак, для привлечения внимания вы хотите поставить лайк или прокомментировать фотографии, отобранные по некоторому критерию. В качестве такого критерия могут выступать хештеги. Также есть возможность работать с пользователями, которые подписаны на определённый аккаунт, на тот случай, если вы захотите привлечь часть аудитории конкурентов. Наконец,

можно отмечать вниманием только те фотографии, что сделаны в определённом месте и помечены соответствующим геотегом. Вот как это делается: пишете город на карте, сервис показывает все геотеги в данном городе, а вы можете выбрать только те, которые вам подходят (рестораны, торговые центры, вузы или городские достопримечательности).

Ещё один секрет грамотного общения с аудиторией – правильно выбранное время для обращения к потенциальным клиентам. Поставили лайк ночью и ждёте, что адресат сразу же подпишется на ваш аккаунт? Скорее всего, ждёте вы зря. Мало кто любит просыпаться от внезапного уведомления, так что о лояльности тут и речи быть не может. Но неужели придётся каждый день заново настраивать задание? Вовсе нет. У InstaPlus есть умный таймер. Составляете задание, определяете дату и время его выполнения, а дальше просто копируете эти таймеры. Так можно составить расписание хоть на неделю вперёд.

Хорошая аудитория – живая аудитория. И балласт в виде «мёртвых душ»-пользователей, не проявлявших в последнее время какой-либо активности, – вам не нужен. Для избавления от них разработчики InstaPlus добавили функцию блокировки неактивных подписчиков. Также вы можете легко отписаться от взаимных и невзаимных подписчиков и вычеркнуть из перечня подписок всех, кого вы нашли с помощью InstaPlus.

Автопостинг в Instagram

Эту свежую особенность InstaPlus мы выделили в отдельный пункт. Всем известно, что фото в Instagram нельзя выложить с компьютера, а в InstaPlus теперь есть такая возможность. Пока она доступна только в английской версии сервиса, но разработчики обещают, что вскоре она появится и в русской версии. Вот тогда точно InstaPlus будет делать за вас всё. Вам даже не придётся открывать приложение, чтобы запостить фото в Instagram, – можно запланировать публикации заранее.

Особенно пригодится отложенный постинг, если вы ведёте несколько аккаунтов. И в веб-версии гораздо удобнее составлять длинные подписи к фото.

Итоги

InstaPlus по достоинству оценят все, кто хочет раскрутить свой профиль в Instagram без особых усилий. Всё действительно так просто, как мы описываем: создаёте задание, устанавливаете время его исполнения, а дальше всё происходит словно само собой.

***

20.02.2017

Популярные Instagram-блогеры зарабатывают около 300 долл. за пост

Популярные западные Instagram-блогеры зарабатывают в среднем примерно 300 долл. за пост. Такие данные опубликовал AdWeek со ссылкой на Influence.co (маркетплейс топовых блогеров), сообщает AIN.UA (Телекритика).

В большей степени их заработок зависит от количества подписчиков. Так, например, блогеры с числом фоловеров от 100 тыс. могут рассчитывать на 800 долл. за пост, а те, у кого аудитория меньше 1 тыс. человек – в лучшем случае на 100 долл.

Так, средняя цена за рекламный пост составляет примерно 300 долл., но некоторые блогеры могут зарабатывать больше в зависимости от количества подписчиков. Самые прибыльные аккаунты у моделей, вокруг них же, как правило, собирается самая большая аудитория. Также в Instagram довольно популярны фитнес-блогеры, но зарабатывают они все еще меньше, чем фотографы.

Есть также зависимость между популярностью блогера и вовлеченностью аудитории в его аккаунт: чем меньше фоловеров – тем больше вовлечение, то есть чем популярнее блогер, тем меньше вовлеченность в его посты. Но, как ни странно, большая степень вовлеченности не приносит блогеру больше денег.

Таким образом, можно сделать вывод, что на уровень заработка Instagram-блогеров влияют всего три фактора – тема, качество контента, и размер аудитории.

***

17.02.2017
Базиленко Анна
Кожен десятий інтернет-користувач у світі блокує рекламу

Компанія PageFair представила щорічний звіт щодо використання програм, що блокують рекламу. Так, за підсумками 2016 р., всього у світі такі програми були встановлені на 616 млн пристроїв – за рік ця цифра збільшилася на третину (Watcher).

11 % користувачів Інтернету в усьому світі блокують рекламу. В Україні рекламу блокують 13 % користувачів. Найвищий показник в Індонезії – 58 %.

62 % всіх блокувальників встановлені на мобільних пристроях. Найвищий показник – в Азіатсько-Тихоокеанському регіоні. За минулий рік їхня частка зросла на 40 % і зараз 94 % усіх мобільних блокувальників знаходиться саме там.

Щодо мотивів установки блокувальника реклами, то користувачі переважно вказують необхідність дотримання безпеки, подразнюючу та відволікаючу дію реклами.

Для 16 % користувачів важливо, що рекламні банери уповільнюють завантаження сторінки, а ще 14 % вважають, що реклами на сторінках занадто багато. Якщо користувачі бачать прохання відключити Adblock, то 74 % з них просто покинуть цю сторінку.

***

20.02.2017

YouTube откажется от непропускаемых 30-секундных рекламных роликов

Видеохостинг YouTube в следующем году собирается отказаться от 30-секундных рекламных роликов, которые проигрываются перед видео без возможности пропуска,сообщает The Verge (Телекритика).

Как объясняют в интернет-гиганте Google, таким образом YouTube хочет предоставить пользователям наилучший опыт взаимодействия с рекламой. Для этого сервис сосредоточится на развитии других рекламных форматах, которые будут более привлекательными как для зрителей, так и для рекламодателей.

Однако отказ от 30-секундной рекламы не означает полную отмену непропускаемых роликов. Так, например, реклама длительностью в 6, 15 и 20 секунд скорее всего останется.

***

20.02.2017

Базиленко Анна

Google відмовляється від глобального запуску повітряних куль з Інтернетом

Компанія Google відмовляється від власної ініціативи – всесвітнього запуску бездротового Інтернету, який мав роздаватись через повітряні кулі-аеростати. Як пише Bloomberg, світове покриття більше не є обов'язковим для реалізації проекту Project Loon (Watcher).

Замість створення всесвітньої мережі, команда проекту запустить невелику кількість аеростатів в тих регіонах, які потребують інтернет-доступ. Це прискорить запуск проекту на комерційній основі, пояснюють у компанії.

«Ми можемо почати експеримент з 10-20-30 кулями. Сервіс в такому випадку отримає набагато кращі шанси стати прибутковим», – зазначив представник підрозділу материнської компанії Alphabet Inc. За його словами, компанія протестує аеростати спільно з телеком-провайдерами вже найближчими місяцями.

У 2013 р. Google провів перші тести свого амбіційного проекту. Компанія планувала покрити всю Землю дешевим Інтернетом, доступ до якого мала б забезпечити мережа аеростатів, запущена по всьому світу.

***

20.02.2017

Сервис Snapchat могут оценить в 22 млрд долл.

Компания Snap Inc., которая является владельцем сервиса моментальных сообщений Snapchat, может быть оценена более чем в 22 млрд долл. в рамках первичного публичного размещения своих акций. Об этом пишет газета The Wall Street Journal со ссылкой на информированные источники (InternetUA).

По их данным, IPO компании пройдет в ценовом диапазоне 14–16 долл. на акцию, в результате чего рыночная капитализация Snap может составить от 19,5 до 22,2 млрд долл. Это IPO на ИТ-рынке должно стать самым крупным за последние два года. Snap собирается разместить акции на Нью-Йоркской фондовой бирже в марте 2017 г.

Сервис Snapchat, начавший работу в 2011 г., позволяет обмениваться сообщениями, фотографиями и видеороликами. Особенностью проекта стала заявленная разработчиками конфиденциальность: фото- и видеосообщения после просмотра удаляются не только с устройств пользователей, но и с серверов компании.

Число пользователей Snapchat, которые запускают сервис хотя бы раз в день, составляет 158 млн человек. В 2016 г. чистый убыток компании увеличился на 35 %, достигнув 515 млн долл. При этом выручка поднялась почти в семь раз, до 404 млн долл.

***

23.02.2017

«Укрпочта» начала использовать Viber и повысила тарифы на свои услуги

С февраля «Укрпочта» начала использовать приложение для смартфонов Viber для уведомления своих клиентов о поступлении отправлений и переводов денежных средств, об этом сообщила пресс-служба фирмы, передает Еспресо (Mignews.com.ua).

На этот момент уже около половины клиентов предприятия получают сообщения от «Укрпочты» через приложение.

«В начале внедрения услуги через Viber было отправлено 24 %, а сейчас уже 44 % от общего количества тестовых сообщений. Мы рассматриваем возможности информирования клиентов с помощью других популярных мессенджеров», – отметил заместитель генерального директора по информационным технологиям «Укрпочты» С. Галаган.

Те клиенты, которые не имеют смартфона или не установили приложение, будут получать от «Укрпочты», как и прежде, СМС-сообщения. Как свидетельствует статистика, предприятие отправляет своим клиентам около 15 000 00 коротких сообщений в месяц.

***

22.02.2017

Facebook запускает сервис валютных переводов с TransferWise

Эстонская международная служба денежных переводов TransferWise сообщила о интеграции с Facebook и запуске услуги валютных переводов (fdlx.com).

Facebook запускает сервис валютных переводов с TransferWise. Вначале денежные переводы будут доступны для валютных переводов из США, Канады, Австралии, Великобритании и Европы. Позже сервис будет поддерживаться в 50 странах и 600 пунктах обмена.

Запустив бота на Facebook, TransferWise пополнила списки платежных компаний, которые экспериментируют с отправкой денег через приложения обмена сообщениями. Многие люди уверены, что именно они будут постепенно заменять автономные мобильные приложения в качестве основной платформы для электронной коммерции.

***

21.02.2017

Rozetka лидирует по количеству подписчиков в Facebook среди украинских интернет-магазинов

Socialbakers опубликовал рейтинг самых популярных интернет-магазинов Украины в Facebook (IGate).

Собственный сайт для представителей сферы e-commerce далеко не единственный инструмент продаж и привлечения новых покупателей. В наши дни ритейлеры весьма активно используют социальные сети для завлечения потребителей. Соцплатформы помогают информировать клиентов о появлении новинок, о скидках и акциях, о распродажах и прочих важных событиях.

Недавно исследователи из Socialbakers решили подсчитать, какие украинские интернет-магазины больше других преуспели в вопросе привлечения пользователей Facebook.

Так, по состоянию на февраль 2017 г., больше всего подписчиков оказалось у страницы Rozetka.ua – более 277 тыс. С отставанием более чем на 100 тыс. идет ресурс Makeup.ua – 176 тыс. На третьем месте расположился магазин Home Ideas Supply с 80 тыс.

Подробнее: http://igate.com.ua/lenta/18284-rozetka-lidiruet-po-kolichestvu-podpischikov-v-facebook-sredi-ukrainskih-internet-magazinov.

***

22.02.2017

Интернет-бизнес Yahoo! продается со скидкой в 350 млн долларов

Телекоммуникационный оператор Verizon Communications купит интернет-бизнес Yahoo! по цене, которая окажется на 350 млн долл. меньше изначально оговоренной суммы. Скидка связана с появлением информации о массовых утечках данных пользователей сервисов Yahoo (InternetUA)!

В конце июля 2016 г. было объявлено о продаже интернет-бизнеса Yahoo! (онлайн-сервисы, поисковая система, почтовая служба Yahoo Mail, агрегатор новостей Yahoo News и спортивные сайты) компании Verizon за 4,83 млрд

долл. По условиям нового соглашения, о котором Verizon объявила во вторник, 21 февраля, стоимость сделки составит 4,48 млрд долл.

В сентябре 2016 г. стало известно об утечке данных 500 млн пользователей Yahoo!. В конце 2016 г. Yahoo! сообщила об утечке информации (имена, адреса электронной почты, номера телефонов, даты рождения, контрольные вопросы и ответы), принадлежащей более 1 млрд пользователей. Руководство Verizon не раз ставило под сомнение возможность заключения сделки с Yahoo! из-за громких скандалов с кражей данных.

Verizon разделит ответственность с Yahoo! за претензии, которые могут возникнуть в связи с масштабными утечками. Под ущербом понимаются штрафы со стороны регуляторов и потенциальные выплаты по искам, поданным третьими сторонами. Yahoo! продолжит выступать ответчиком по искам акционеров, а также в расследованиях Комиссии по ценным бумагам и биржам США.

По словам исполнительного вице-президента Verizon М. Уолден (Marni Walden), новые условия сделки «обеспечивают защиту для обеих сторон и открывают путь к завершению сделки во II квартале».

Покупая интернет-бизнес Yahoo!, компания Verizon показала свою сосредоточенность на мобильном видео и рекламе в поисках нового источника выручки в условиях перенасыщенного рынка беспроводной связи.

«Мы по-прежнему рады объединению с Verizon и AOL. Эта сделка ускорит рост операционного бизнеса Yahoo!, особенно в мобильном сегменте. В то же время, она позволит эффективно отделить наши азиатские активы. Это важный шаг для разблокировки акционерной стоимости Yahoo!. Теперь мы можем двигаться вперед с уверенностью и определенностью», – сообщила глава Yahoo! М. Майер (Marissa Mayer).

Verizon и Yahoo! планируют закрыть сделку во II квартале 2017 г. Инциденты с утечками данных могут задержать процесс интеграции интернет-активов с бизнесом Verizon после закрытия сделки.

***

22.02.2017

YouTube позволит третьей стороне проверить рекламные метрики

В своем заявлении Google отметил, что позволит Media Rating Council проследить за измерениями на канале, чтобы гарантировать точность статистики просмотров роликов для рекламодателей. Facebook также позволит Media Rating Council проверить рекламные метрики после нескольких инцидентов, когда сеть признала ошибочность некоторых изменений рекламы (Marketing Media Review).

***

24.02.2017

Лисенко Юлія

Коли титри справді важливі: як створити відео для соцмереж

Журналіст і медіаактивіст із Киргизстану Б. Іскендер про секрети формату, який так любить Facebook (Watcher).

Три роки тому Facebook у черговий раз змінив алгоритм формування стрічки новин, надавши пріоритет відеороликам. Таким чином йому вдалося, по-перше, дошкулити своєму конкурентові Google, витіснивши посилання на Youtube, по-друге, дати стимул для розвитку нового жанру. Журналіст, медіаактивіст і співзасновник одного з найпопулярніших незалежних онлайн-видань Киргизстану Kloop Б. Іскендер називає короткі відеоролики з титрами – caption video – найефективнішим способом донести ідею користувачам соціальних мереж. Про те, як працювати у цьому форматі, Бектур розповів на майстер-класі у Школі журналістики Українського католицького університету.

Коли титри справді важливі: як створити відео для соцмереж

Звідки взялися cation videos. Одним із перших почав експериментувати в жанрі відео з титрами канадський сайт Vice. В Україні він здобув популярність 2014 р. завдяки серії коротких документальних роликів про окупацію Криму «Російська рулетка». Невдовзі на хвилях змін в алгоритмі Facebook набули популярності півторахвилинні ролики від американського молодіжного крила Al Jazeera – AJ+.

Чому важливі титри. Caption video дозволяє за одну-дві хвилини розповісти головне навіть глядачеві, який не може чи не хоче дивитися ролик зі звуком. Користувачі соціальних мереж дуже швидко відволікаються від будь-якого контенту, тож ролики в новинній стрічці повинні бути лаконічними. Caption video позбулось телевізійних надмірностей, таких як закадровий голос і підведення ведучих, а натомість використовує короткі титри. Споживач читає їх значно швидше, ніж слухає закадровий голос.

Як створити ефективне caption video. Головний акцент варто зробити саме на тексті, адже він передає зміст повідомлення. Найкраще, коли титри одного кольору й доповнюють композицію кадру, не затуляючи основного зображення. Навіть якщо у кадрі говорить герой, його слова обов'язково слід дублювати текстом, аби глядач міг усе прочитати. Часто титри рятують ситуацію, коли доводиться використовувати неякісний відеоматеріал або повторювати на екрані одні й ті самі кадри.

Часто до captio video додають музичний фон, який додає настрою та впливає на сприйняття. Журналісти, що звикли до принципу безсторонності, вбачають у цьому певну маніпуляцію.

Як вмістити все важливе у хвилину. Іноді автори розуміють, що в півтори хвилини неможливо запакувати всю історію, й роблять серію коротких роликів. Проте є ризик, що ці ролики почнуть поширювати окремо, і логіка оповіді буде втрачена. У такому випадку caption video краще використовувати як трейлер до розгорнутого текстового чи мультимедійного матеріалу.

Яке відео можна використовувати. Ще одна перевага caption video – для створення повноцінного ролика не потрібно мати гігабайти відзнятого

матеріалу. Розповісти новину можна, маючи кілька кадрів із камери відеоспостереження.

Стрім тривалістю в годину навряд чи переглядатиме багато глядачів, проте, якщо змонтувати найцікавіші моменти й накласти текстове пояснення, може вийти популярний ролик. Для caption video не обов'язково щось знімати: достатньо зазирнути в архівні матеріали і знайти цікавий ракурс для висвітлення подій.

***

24.02.2017
Базиленко Анна
Facebook тестує 20-секундні «рекламні паузи» у показі відео

Компанія Facebook почала тестувати так звані «рекламні паузи» як у показі звичайних відео, так і в прямих трансляціях. Як повідомляє Marketing Land, тривалість «рекламних пауз» не буде перевищувати 20 секунд: 15 секунд триватиме власне рекламний ролик і 5 секунд відводиться на інформування аудиторії про те, що у показі відео з'явиться реклама (Watcher).

Про те, що Facebook працює над запуском реклами формату mid-roll в звичайних відео, стало відомо в січні цього року. Цей формат реклами в звичайних відео поки на початковій стадії тестування. Доступ до нього отримала обмежена кількість видавців.

Разом з тим Facebook розширив доступ до mid-roll реклами в прямих трансляціях. У США власники публічних сторінок з кількістю підписників понад 2 тис. зможуть додавати «рекламні паузи» в live-відео.

Така реклама буде з'являтися щонайменше через 4 хвилини після початку трансляції за умови, що кількість глядачів перевищує 300 осіб. Наступну «рекламну паузу» можна додати не раніше, ніж через 5 хвилин після попередньої.

Як тільки будуть виконані вимоги щодо тривалості відео і кількості глядачів, автор трансляції зможе натиснути на значок «$» і вставити «рекламну паузу».

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

21.02.2017

Охота на «Синих китов»: семь советов родителям

Паника вокруг опасных игр в соцсетях, где подростков толкают к самоубийству, нарастает с каждым днем. Два дня назад полиции удалось спасти от суицида двух школьниц из Киева, которые собирались спрыгнуть с крыши многоэтажки, выполняя последнее задание игры «Синий кит», пишет Сегодня (From-UA Новости Украины).

Напомним, суть игр в том, что подросток вступает в определенные группы в соцсетях и выполняет по команде куратора несколько заданий. Задания разные и почти всегда связаны с увечьями или опасностью – вырезать лезвием на руке рисунок, пробежать перед несущимся поездом, зайти ночью в заброшенное помещение и т. д. Весь процесс снимается на видео (потом преступники продают эти записи тематическим порталам). Финальный приказ – убить себя. Часто, если ребенок отказывается, преступники вычисляют IP-адрес участника и говорят ему, что за эту трусость придется ответить его родным.

Названия игр (их гораздо больше, эти самые популярные):

«Синий кит»

«Киты плывут вверх»

«Разбуди меня в 4:20»

f57 или f58

«Тихий дом»

«Рина»

«Няпока»

«Море китов»

«50 дней до моего...»

Хэштэги: #f53 #f57 #f58 #d28 #морекитов #тихийдом #хочувигру #млечныйпуть

aa4e51f7-c718-4073-b605-b9b8194af959_w650_r0_s_01

Давят на болевые точки

«Те, кто придумывает такие игры, тонко разбираются в психологии подростков, – говорит практикующий психолог О. Перекопайко. – Они давят сразу на три болевых точки. Во-первых, берут на слабо – многие выполняют задания преступников, чтобы доказать себе и кому-то свою силу. Во-вторых, они манипулируют детьми – страх потерять родных сильнее страха собственной смерти. А в-третьих, они преподносят самоубийство как уход от всех проблем в жизни, помощь и облегчение.

Мошенники знают, что ребята помладше расскажут о таких играх взрослым. Те, кто постарше, включат критическое мышление и не поверят преступникам. А вот ученики 5-7 класса еще не понимают, что угрозы от кураторов игры, скорее всего, пустые, и из страха выполняют их приказы».

Психолог отмечает, что в популярности этой игры косвенно виноваты сами родители. В Украину эта игра пришла еще перед Новым годом. Многие дети рассказывали о ней родителям, но те только отмахивались, не

воспринимая их рассказы серьезно. Это вообще большая проблема родителей подростков – часто они настолько заняты, что уделяют слишком мало внимания детям. И те думают: «Ну что ж, может, если я умру, то хоть тогда они обратят на меня внимание». Опасность вовлечься в такие игры особенно велика у детей, чьи родители находятся в состоянии развода или в семье есть другие неурядицы.

Также проблема многих родителей в том, что они не научили детей думать самостоятельно. Они всегда все решали и выбирали за них – и на выходе получили подростка, который просто не умеет принимать решений сам. Многие дети начинают участвовать в игре с мыслью «Попробую, а потом брошу», но бросить не так легко – именно потому, что отвечать за свои действия их никто не научил.

Как вести себя родителям: 7 советов

Задайте ребенку нейтральный вопрос – мол, слышал/-а, что сейчас популярна какая-то игра «Синий кит». И послушайте, что ребенок вам расскажет. Если он ничего о ней не знает – хорошо (тут главное не вдаваться в подробности, чтобы не разбудить в нем любопытство). Если знает, внимательно слушайте рассказ. Если в нем полно подробностей и деталей, о которых не пишут в сети, то есть риск, что ваш ребенок уже в игре. Также должно насторожить, если сын или дочь ведут рассказ о подружке, участвующей в игре – вполне вероятно, что он врет и играет сам.

Нет смысла говорить, что такие игры опасны – на подростков это уже не действует. Гораздо эффективнее сказать, что ими манипулируют. Для них будет откровением, что человек, угрожающий их родным, скорее всего, больной и живет в другом городе или даже стране. И его задача – не убить родителей, а заставить ребенка выполнить его волю. Детей такое очень отрезвляет! Расскажите им, что на манипуляции «ведутся» все – сколько взрослых несут все свои сбережения мошенникам, которые звонят им среди ночи и говорят, что их близкие попали в беду! Покажите ребенку, что все уязвимы – для него очень важно услышать это от авторитетного взрослого.

Задача вашего разговора – научить подростка мыслить критично и спрашивать себя о цели того или иного поступка, обдумывать все, что с ним происходит.

Многие родители в панике решают установить тотальный контроль над ребенком – забрать телефон, закрыть дома и т. д. В этом тоже нет смысла – в XXI веке подросток, если захочет, всегда найдет гаджет и доступ в сеть. Чем больше его ограничивать – тем больше способов обойти запреты будет находиться. Ваша задача – не контролировать, а дать поддержку, чтобы ребенок пришел к вам с проблемой, а не скрывал ее до последнего.

Сейчас как никогда важна эмоциональная связь с ребенком. Больше обнимайте его, рассказывайте, что в его возрасте тоже ошибались, встревали в какие-то опасности, и вам помог кто-то из взрослых. Ребенку важно понимать, что даже его «идеальные» родители тоже оступались, и это нормально, так же как и нормально просить помощи у других. Если понимаете, что сейчас ребенок

вас не воспринимает, попросите его говорить с тем из взрослых, кому он доверяет – школьным психологом, родственником и т. д.

Даже если вы уверены, что в вашей семье все хорошо, лишняя бдительность не помешает. Подобные игры – тот случай, когда вторжение в частную жизнь сына или дочери оправданы. Просматривайте их телефоны и страницы в соцсетях – но только так, чтобы он не узнал об этом!

Если понимаете, что ребенок таки в игре, Боже вас упаси его ругать. Проявите другие эмоции – заплачьте, покажите, как сильно вы расстроены и как за него волнуетесь. Обязательно подключайте папу – в такой ситуации мужское слово сильнее «мамского». В разговоре с дочерью отцу надо найти, за что ее похвалить, а с мальчиками лучше говорить в духе «Давай поговорим как мужчина с мужчиной, что мы (именно мы!) можем сделать в этой ситуации». Если папы нет, попросите поговорить того, кому ребенок доверяет – дядю, мужа сестры и т. д.

***

19.02.2017

У Києві врятували дівчинку від самогубства в рамках гри «Синій кит»

Київські поліцейські врятували дівчинку від самогубства. Вона разом з подругою була учасницею так званих «груп смерті» у соціальних мережах. Увечері 18 лютого підлітки повинні були виконати останнє завдання – стрибнути з багатоповерхівки (LB.ua).

Про зникнення 15-річної дівчинки і залишення нею передсмертної записки правоохоронцям повідомила її мама, повідомляється на сайті Нацполіції.

«З'ясувалося, що дівчинка за кілька годин до цього вимкнула телефон, видалила свій профіль у соціальній мережі, однак при перевірці ми виявили, що вона була учасником кількох "груп смерті", які пропагують культ насильства і жорстокості, і читала книгу про самогубство», – розповів начальник Головного управління Національної поліції в Києві А. Крищенко.

Після декількох годин пошуків дівчинку з явними ознаками переохолодження та порізами рук знайшли на останньому, 16 поверсі, багатоповерхівки. Неподалік виявили навушники і ще одну записку, в якій вона написала своє останнє бажання.

Згодом поліція встановила, що дівчинка разом з подругою була учасницею групи «Синій кит», виконувала завдання, які їм давав адміністратор, зокрема наносила собі порізи на руках у вигляді кита, цифр і слова «так» – на нозі.

«Цього вечора вони повинні були виконати останнє завдання – покінчити життя самогубством, стрибнувши з багатоповерхівки, або шляхом повішення. Разом вони піднялися на верхній поверх, одна зі школярок злякалася і пішла. Саме її спочатку розшукали поліцейські, яким вона розповіла, де може бути її

подруга. Однак на місці, де вони розійшлися, втікачки не було. На її пошуки пішло кілька годин – і врешті-решт дівчинку знайшли, вона була в безпорадному стані і не могла пояснити, для чого це робить», – зазначив А. Крищенко.

Дівчинці викликали «швидку». При огляді біля неї виявили як нові, так і застарілі порізи (написи і малюнки) на руках і ногах. Їй надали необхідну медичну допомогу, і мама забрала її додому. Зараз з обома дівчатами працюють правоохоронці та поліцейські психологи.

За фактом доведення дівчинки до самогубства розпочато кримінальну справу за ст. 120 Кримінального кодексу України. Шевченківські правоохоронці з'ясовують усі обставини події, для встановлення фігурантів злочину залучили працівників кіберполіції. Зловмисникам, які штовхають дітей до самогубства, загрожує до десяти років ув'язнення.

***

20.02.2017

На Рівненщині підлітки готували масове самогубство через гру «Синій кит»

Спецслужбовці виявили підлітків у Дубні на Рівненщині, яких буто втягнуто у небезпечну гру. Про це розповіла речниця СБУ О. Гітлянська. За її словами, підлітки готували масове самогубство («Главком»).

Зокрема, спецслужбовці врятували двох 19-річних дівчат, які були учасницями небезпечних груп. Силовики прийшли до гуртожитку одного з навчальних закладів. Там вони застали одну з дівчат із порізами на руці та своєрідними написами.

Ця дівчина розповіла й про свою одногрупницю, яка теж брала участь у грі. Того вечора дівчата мали виконати чергове небезпечне завдання. Тож правоохоронці зателефонували подрузі студентки та поспілкувалися з її батьками.

Серед вказівок адміністратора була вимога запросити в групу 50 друзів – цю умову дівчата виконали. Тож зараз поліція намагається встановити всіх цих осіб, щоб запобігти трагедії.

***

21.02.2017

У Луцьку від суїциду врятували дитину, яка грала у «Синього кита»

У Луцьку вдалося запобігти самогубству неповнолітньої, яка була учасником суїцидальної групи в соціальній мережі (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»).

Підлітка зупинили за крок до самогубства перед виконанням заключного завдання так званого квесту. Про це сьогодні під час брифінгу повідомив

начальник управління превентивної діяльності ГУНП у Волинській області В. Солоненко, передає власкор «Вголосу».

«Спільними зусиллями кіберполіції, співробітників ГУНП в області та патрульної поліції неповнолітню зупинили на 50 кроці інтернет-пастки, тобто наступною дією мало стати самогубство. Попередити суїцид вдалося завдяки своєчасному повідомленню в поліцію від небайдужих громадян і працівників навчального закладу. Зараз з дитиною працюють кваліфіковані психологи», – зазначив В. Солоненко. За фактом доведення до самогубства поліція відкрила кримінальне провадження за ознаками злочину, передбаченого ч. 3 ст. 120 Кримінального Кодексу України. Санкція статті, зокрема, передбачає позбавлення волі на строк від семи до десяти років.

***

21.02.2017

«Білий ведмідь»: у Інтернеті з'явилася альтернатива суїцидальним іграм

Двоє студентів-другокурсників із Придністров'я запустили інтернет-гру «Білий ведмідь», яка є повною протилежністю смертельно небезпечної гри «Синій кит». Про це повідомляє «Українська правда. Життя» (Львівський портал).

Розробники проекту – С. Іордатий та П. Доніка – заручились підтримкою правоохоронців та студентської профспілки, і створили спільноту у соцмережі «ВКонтакте».

У грі треба виконати 50 завдань. Серед них – прибирання будинку чи фото щоденника з позитивною оцінкою.

«Якщо дітям подобається виконувати завдання в реальному житті у форматі гри, чому б не дати їм таку можливість? Тим паче, що наші завдання точно кращі, ніж у "кита", хоча подекуди і складніші», – розповідає співзасновник проекту С. Йордатий.

***

23.02.2017

Instagram: подростки прячут запретные фото от родителей

Последнее время подростки стали создавать секретные инстаграм-аккаунты, в которых выкладывают свои полуобнаженные фотографии и свидетельства бурных вечеринок (podrobnosti.ua).

Такой мейнстрим связан с тем, что за их активностью в соцсетях следят не только друзья, но и родители. Что же делать, если у ребенка есть секретные профили?

Сегодня большинство Instagram-аккаунтов выглядят весьма однообразно. Подростки не стали исключением: тонны селфи, красивая еда, фото в зеркале тренажерного зала, счастливые моменты с семьей и снимки смеющихся друзей.

Как известно, в соцсетях многие идеализируют свою жизнь, именно поэтому в лентах новостей мы видим только красивые и удачные снимки.

Такие снимки не стыдно показать незнакомым людям или родственникам, ведь фильтры на фотографиях убирают несовершенства кожи, волшебным образом сбрасывают пару килограммов, добавляют шарма и романтичности.

Как оказалось, школьникам этого мало. После вечеринок у них всегда остаются фотографии, за которые несколько неловко, но не настолько, чтобы прятать их от подписчиков. Но родителям такие фото точно не покажешь.

Именно это и стало причиной того, что многие современные подростки заводят секретные аккаунты, чаще всего закрытые от посторонних глаз. Их называют finstagram или просто finsta. Под первой буквой F подразумевается фейк, но именно в «финстаграм» попадают наиболее сомнительные кадры.

В основном, такими фото в соцсетях увлекаются девушки, которые не довольны постоянным родительским контролем и слежкой за публикациями. Гораздо реже можно найти снимки парней с оголенными частями тела, но и такие встречаются.

Профиль с позитивными моментами своей жизни принято называть rinstagram (real Instagram) или rinsta – он считается реальным и, скорее всего, на него подписаны все малознакомые одноклассники, соседи, а также члены семьи. Фотографии оттуда родители публикуют у себя в Facebook, чтобы похвастаться достижениями своих детей. В «реальных» профилях приходится быть максимально сдержанным – постить туда снимки с бокалом вина и полуголыми подружками не рекомендуется.

Студентка Хана, в отличие от многих ее сверстников, ведет не один, а целых два «финстаграм»-профиля. Девушка разделила свою жизнь на три уровня, исходя из того, насколько смелой она может предстать перед разной аудиторией.

В ее «ринстрагаме» нет ничего необычного: на всех фото она улыбается, а под ними сотни лайков. Эти снимки очень милые: культурный отдых с друзьями, много щенков, цветов, скромные обеды в студенческой столовой. Основной «фистаграм» посвящен двум типам снимков: туда попадают либо слишком откровенные, либо до смешного неудачные кадры. Доступ к нему открыт для однокурсников и близких друзей.

А вот второй и самый сокровенный «фистаграм» посвящен сексуальной жизни. Туда попадают практически порнографические снимки, на которых она хвастается знакомствами на одну ночь. Девушка коллекционирует партнеров и собирает их в отдельный аккаунт, куда могут заглянуть только самые доверенные лица.

Студентка скрывает эту часть жизни сразу по нескольким причинам. Во-первых, она уверена, что в современном обществе предпочитающая свободные отношения девушка по-прежнему считается «гулящей», и не хочет навлекать на себя слишком много критики. Кроме того, Хана встречается не только с парнями, но и с девушками, а это многие могут не понять.

Пример Ханы – скорее исключение, ведь обычно «финстаграм» ведут школьницы 14-16 лет. Многие используют тайный аккаунт для того, чтобы близкие друзья знали, как девушки выглядят в неглиже, и где обычно развлекаются несовершеннолетние, которым по закону пока нельзя употреблять алкоголь.

Но некоторые подростки публикуют там фото с подписями, в которых просят совета, рассказывают о не совсем приглядных сторонах своей жизни, честно признаются в проблемах или просто болтают с близкими.

Современные школьники практически всю жизнь проводят в соцсетях. Для них ведение Instagram-аккаунта – по сути, обязанность. Стандартный набор фотографий обязательно должен соответствовать общепринятым нормам: малознакомые посетители будут лайкать только красивые лица и опрятно сложенные вещи. А лайки для подростка – один из самых важных показателей признания в обществе. «Финстаграм» – другое дело, там можно позволить себе откровенное общение.

Не исключением стала первокурсница Кэрри, которая заехала в общежитие и начала студенческую жизнь с публикации в Instagram фото алкоголя и фразы «К черту сухой закон». Хотя девушка разместила снимок в «финстаграм»-аккаунте, о нем быстро узнали в женском сообществе университета. Ее вызвали на разговор и лишили права присутствовать на женских встречах в течение месяца.

Для Кэрри это стало серьезным ударом по репутации: она, как и все, вела примерную жизнь в своем «ринстаграме» и развлекалась во втором аккаунте. Оказалось, что о ее проступке «сестрам» доложила соседка по комнате. Девушки крайне негативно отнеслись к такой развязности соратницы. Она упорно добивалась своего членства в элитном обществе, но в итоге ее репутация была разрушена одной фотографией с бокалом алкоголя.

Важно, что о «финстаграм»-профилях рассказывают на курсах повышения интернет-грамотности для родителей. Там объясняют, что современные школьники уже не просто заполняют свои ленты в Instagram, Twitter и Snapchat – они учатся прятать следы реальной жизни и крайне правдоподобно имитируют примерное поведение в публичных аккаунтах.

На тренингах взрослым чаще всего советуют шпионить за своими детьми или же напрямую задавать провокационные вопросы. Одни рекомендуют проинспектировать телефон подростка в его отсутствие и удостовериться, что тот залогинен только в одном аккаунте. Другие настаивают на том, что перед тем, как брать смартфон, нужно спросить у школьника разрешение. Сколько молодых людей с готовностью отдадут в руки мамы или папы устройство со всеми своими секретами, естественно, не уточняется.

Для особо продвинутых взрослых существует и более сложный способ – специалисты предлагают проверить аккаунты абсолютно всех друзей сына или дочери, а затем порыскать в их подписках. Редко, но все же бывает, что те не закрывают «финстаграм»-аккаунты, а просто придумывают фейковое

прозвище. Кроме того, часто подросток сам подписан на свой же секретный профиль.

Ну а для тех, кто пока не готов шпионить за собственными детьми, есть простой выход, который родители обычно игнорируют. С ребенком можно поговорить по душам, спросить о «финстаграм»-аккаунтах, вообще о его проблемах. Наверняка, узнаете много интересного.

***

23.02.2017

На Тернопільщині хлопчик з «групи смерті» вважає, що до нього застосували гіпноз

13-річного хлопця, який був у «групі смерті» в соцмережі, виявила поліція на Тернопільщині. Правоохоронці відкрили провадження за фактом схиляння до самогубства (Західна інформаційна корпорація).

Про це розповів під час брифінгу начальник обласного управління поліції О. Богомол, інформує власкор ІА ZIK.

Подряпини на руках у школяра в одному з районів області побачив учитель. Виявилося, що це малюнок у формі кита, а хлопчик виконував завдання у так званій «групі смерті».

Поліція з'ясувала, що підлітку надіслали відео на електронну пошту. Хлопець підозрює, що до нього застосовували гіпноз, оскільки помітив, що у дівчат, які вели з ним бесіду, змінювався колір очей.

«Зараз експерти вивчають це відео, щоб знайти джерело походження інформації, через яку йде схиляння до суїциду. У нас є декілька інших фактів в області, коли до дітей в соцмрежі достукувались, вони вступали в такі групи, але не шкодили своєму здоров'ю. Батьки провели бесіди з дітьми, і ті розповіли про ситуацію, попереджувальні заходи дали результати», – повідомив О. Богомол.

У поліції наголошують, що найбільш вразлива група – підлітки 5-8 класів.

«Трошки старші діти вже розуміють, що таке суїцид, і усвідомлюють наслідки. Проте, вже з'являються різновиди цієї гри, розраховані на малолітніх дітей. Є так звана гра в добру фею. Її суть у тому, що вночі треба встати, піти на кухню, відкрити газові конфорки – і до ранку, як обіцяють куратори груп, можна стати феєю», – зазначив керівник відділу комунікації обласного управління поліції С. Крета.

Тернопільські правоохоронці розпочали роботу в школах, аби запобігти трагедіям серед підлітків, яких затягують у «групи смерті». Поліція звертається до батьків із проханням більше часу проводити із дітьми, а також цікавитися їхніми справами.

***

23.02.2017

Недитячі ігри: на Закарпатті хлопчина жорстоко розіграв однокласника у соцмережі

21 лютого на службу «102» надійшло повідомлення від 15-річного хустянина, який заявив про погрози. Юнак розповів, що в одній із соцмереж з ним зв'язався чоловік на ім'я Сергій Громов та вимагає виконати завдання, погрожуючи фізичною розправою в разі непослуху. Заявник пояснив, що користувач соцмережі наказував вирізати символи на шкірі руки (InternetUA).

Працівники поліції перевірили надану інформацію та з'ясували, що дитині погрожував його однокласник. Хлопчик, який представився вигаданим ім'ям «Сергій Громов», прочитав у ЗМІ інформацію про групи смерті, матеріали про резонанс, який вони мають, та вирішив розіграти свого товариша. Юнак придумав завдання, покарання у випадку непослуху та прислав повідомлення однокласнику.

Поліція вбачає в діях дитини ознаки правопорушення, передбаченого ст. 173 Кодексом України про адміністративні правопорушення, тобто дрібне хуліганство. Оскільки підозрюваний не досяг повноліття, відповідальність понесуть його батьки, відповідно до ст. 184 Кодексу України про адміністративні правопорушення, тобто невиконання батьками або особами, що їх замінюють, обов'язків щодо виховання дітей. З батьками та дитиною проведено профілактичні бесіди. Перевірка у цій справі триває.

***

27.02.2017
Хто і навіщо створює в українському Інтернеті «групи смерті»

За рядом таких груп стоять фахівці, які свідомо доводять підлітків до суїциду. Однак до теми треба ставитись обережно і не маніпулювати нею заради цензури, пояснюють експерти (DW).

Поширення останнім часом в українських ЗМІ різної інформації та історій щодо діяльності так званих підліткових «груп смерті» в Інтернеті спонукає співробітників кіберполіції діяти на упередження. Як повідомив DW перший заступник начальника департаменту кіберполіції Національної поліції України О. Гринчак, правоохоронці знали про це явище і раніше, однак не піднімали цю тему довгий час саме через острах появи ажіотажу. Однак підвищена цікавість до теми з боку журналістів та громадськості спонукала кіберполіцейських реагувати та видати низку повідомлень щодо «груп смерті».

Слова правоохоронця підтверджує і директорка департаменту національних гарячих ліній громадської організації «Ла Страда – Україна» А. Кривуляк. «Перші дзвінки від підлітків, які стали учасниками "груп смерті", почали надходити на нашу дитячу гарячу лінію ще у вересні минулого року. Але спочатку оператори не розуміли, про що йдеться, коли діти згадували про "квести" та назви, під якими так звані "групи смерті" відомі в Інтернеті», –

розповідає А. Кривуляк. Однак справжнім каталізатором став випадок у Маріуполі наприкінці минулого року: 15-річна дівчина вистрибнула з тринадцятого поверху будинку, а перед цим вона виконувала завдання «квесту» з відповідної групи у соціальній мережі – палила руку над свічкою, проколювала опіки голкою тощо. Останнім завданням «квесту» було самогубство.

А. Кривуляк констатує, що саме після цього кількість звернень, пов'язаних із такими групами, почала стрімко зростати. Якщо за весь минулий рік їх було зафіксовано близько десятка, то менш ніж за перші два місяці нового року їхня кількість досягла 36-ти. За допомогою звертаються як родичі та друзі потенційних самогубців, так і самі учасники груп.

Страшна популярність

На відміну від українців, росіянам явище так званих «груп смерті» відоме вже доволі довго. Широкого розголосу воно набуло після розслідування російського видання «Новая газета», опублікованого весною минулого року. У матеріалі йшлося про спільноти у соціальних мережах, в яких збираються підлітки зі схильністю до самогубства, яких модератори цих груп покроково підштовхують накласти на себе руки. За даними газети, на той час через такі групи в Росії за шість місяців скоротили собі віку близько 130 молодих людей.

В Україні ж після появи публікацій про маріупольську трагедію українська поліція почала повідомляти про врятованих від самогубства жертв «груп смерті». А у п'ятницю, 24 лютого, стало відомо про затримання перших двох адміністраторів однієї із подібних онлайн-спільнот.

Правоохоронці запевняють – йдеться про справу рук професійних психологів, які схиляють підлітків до виконання завдань, що передбачають завдання тілесних ушкоджень або болю, останнім із яких є саме спроба суїциду. Виконання завдань вимагають записувати на відео, які в подальшому продаються у мережі Інтернет, зокрема у так званому «темному Інтернеті» – сегменті світової павутини, що не індексується звичайними пошуковиками.

За словами представниці «Ла Страда – Україна», в останні тижні тенденція набула загрозливих масштабів, адже тепер діти, що знаходяться у «групах смерті», не приховують цього: індивідуальні «квести» перетворюються на групові, а деякі підлітки навіть використовують це, аби шантажувати батьків, вимагаючи від батьків виконати їхні примхи.

Директор київської спеціалізованої школи № 148 ім. Івана Багряного С. Горбачов каже, що значна частина учнів його школи, із якими він обговорював цю тему, дізналася про «групи смерті» зі ЗМІ. І тепер дехто із підлітків бере участь у «квестах» із цікавості, недооцінюючи ризики потрапляння під вплив професійних маніпуляторів.

Професійні техніки

Щонайменше ряд подібних груп виглядає результатом роботи професіоналів, каже практикуючий психолог та викладач факультету психології Київського національного університету ім. Тараса Шевченка В. Романова. Таких їй траплялося близько десяти. Психолог навіть консультувала

журналістів, які у своїх розслідуваннях намагалися видати себе за користувачів відповідних груп. Попри те, що йшлося про дорослих, які робили це з метою викриття, час, проведений у спілкуванні з так званими кураторами, все одно мав чималий вплив на психіку розслідувачів, каже В. Романова. «Там використовуються трансові техніки, типові для сект, – один із журналістів дійшов до останнього завдання, і хоча, авжеж, не наклав на себе руки, але це мало певний вплив на спосіб його мислення», – розповідає психолог.

Утім, таких професійно зроблених груп не дуже багато, додає В. Романова. Величезна їх кількість створюється на тлі широко розпіареної ЗМІ теми виключно з комерційною метою: для збирання інформації про підлітків з метою продажу для поширення «реклами» відеоконтенту та комп'ютерних ігор.

Однак це не пояснює феномену справжніх «груп смерті», адже там йдеться не лише про професійних психологів, але й про спеціалістів, що створюють для них відеоконтент та просувають їх у соціальних мережах. І якщо мета сект та так званих курсів особистісного розвитку, які використовують аналогічні психотехніки, зрозуміла – викачування грошей із зазомбованих заможних адептів, – то навіщо створювати віртуальні групи, які доводять до самогубства звичайних підлітків, В. Романовій не зрозуміло.

«Можна уявити собі певну команду людей, які вирішили, що таким чином вони можуть відчути себе богами, здатними маніпулювати людськими життями, – каже психолог. – Але звідки гроші і ресурси на десятки команд таких професіоналів?»

Російський вплив

У разі, якщо адміністратори подібних груп мають достатні знання, аби забезпечити свою анонімність, вирахувати їх не так вже й легко, пояснив DW представник кіберполіції О. Гринчак. Затримання перших двох українських адміністраторів у кіберполіції не поспішають коментувати – наразі офіційно відомо лише про обшук та допит двох киян, які розповіли, що «експериментували зі свідомістю людей». За інформацією ЗМІ, йдеться про двох студентів четвертого курсу, які вчилися у київському медичному університеті.

Але у переважній більшості випадків, коли встановити місцезнаходження адміністраторів можливо, йдеться про росіян, які керують групами у російській мережі «ВКонтакте». Утім, у Кіберполіції не вдаються до спекуляцій, сухо пояснюючи, що це явище прийшло в Україну саме з Росії, тому подібна диспропорція є цілком логічною. Стрімке зростання популярності «груп смерті» в Україні О. Гринчак пояснює не «російським слідом», а тим фактом, що цю тему активно підхопили вітчизняні ЗМІ. За словами кіберполіцейського, зараз багато дітей почали реєструватися у цих групах не через схильність до самогубства, а через цікавість. «Це стало своєрідною модою», – каже О. Гринчак.

Привид цензури?

Водночас не драматизувати проблему закликає президент холдингу Internet Invest Group О. Ольшанський. Подібні «групи смерті», за його словами,

є далеко не новим явищем в Інтернеті, а схильність підлітків до самогубства була добре відомою і до його появи. Так само, як і маніпулятивні психологічні техніки, що використовуються різноманітними сектами, каже експерт, згадуючи, наприклад, про так зване «Біле братство» – тоталітарну секту, що діяла в Україна на початку 1990-х, задовго до приходу всесвітньої павутини в Україну.

Водночас тема дітей-самогубців є дуже болючою, і нею легко маніпулювати, каже О. Ольшанський, згадуючи про введення Президентом П. Порошенком у дію рішення РНБО «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації». У перспективі воно може призвести до дозволу блокувати певні сайти за рішенням суду. «Я не знаю, чи штучною є різке збільшення уваги до “груп смерті”, але це небезпечно, – каже експерт. – Якщо піддатися емоціям, можна ухвалити хибне рішення, ще й додатково розрекламувати ці групи».

Спокій та увага

У кіберполіції також закликають ставитися до теми «груп смерті» вкрай обережно, аби не спровокувати ще більшої їх популяризації. У разі виявлення подібних груп дітей та батьків просять повідомляти про це через сайт cybercrime.gov.ua, або за телефоном гарячої лінії (044) 374-37-13 з 8:45 до 18:30 у робочі дні.

Загалом же поради як кіберполіцейських, так і психологів є схожими: діти та підлітки потребують, передусім, щирої уваги та цікавості їхнім життям. Жодними погрозами та тиском убезпечити дитину від цікавості «забороненими темами» не вийде. Окрім бесід про безпеку поведінки у соціальних мережах та ризик від розголошення персональної інформації, за словами В. Романової, підліткам необхідна підтримка та довіра. «Батькам треба вчитися розмовляти із власними дітьми і у разі труднощів не боятися звертатися по допомогу спеціалістів, які допоможуть це зробити», – резюмує психолог.

Маніпулятивні технології

15.02.2017

Росія керує стотисячними «патріотичними» групами у соцмережах України

Стало відомо, що стотисячні «патріотичні» спільноти у соцмережах адмініструються з Росії (Espreso.tv).

Про це розповів керівник апарату СБУ О. Ткачук під час брифінгу, передає Еспресо.TV.

«Громадянин Росії С. Олександрович Жук 1981-го року народження приймав участь у терористичному угруповуванні ДНР під позивним “Москва” і

на даний час перебуває у Москві. Він створив профілі вигаданих людей у соцмережі – М. Гайдук та С. Мазура», – розповів О. Ткачук.

За його словами, з Росії через соцмережі від імені цих вигаданих осіб здійснюється інформаційно-психологічний вплив на українців.

«Маскуючись патріотом України, С. Жук, користуючись довірою наших громадян, намагається спровокувати масові заврушення у місті Києві», – розповіли у СБУ.

За даними служби безпеки, С. Жук безпосередньо причетний до створення та адміністрування наступних спільнот у соцмережах: «Патріоти України», «Українська Революція», «Всі на Майдан», «Продовження Революції Гідності», «Майдан три», «Ми патріоти України».

«Усі ці соціальні спільноти адмініструються із Росії саме цією особою», – сказав О. Ткачук.

За його словами, 5 лютого С. Жук розмістив у пабліку «Українська революція» заклик до масового протесту на Майдані.

«Ми фіксували використання ботів, штучного масового посилення цієї інформації. З Росії активно фінансується контентна реклама, яка пропагує ці заходи у соцмережах... Також росіянин закликав брати зброю на протести», – додав керівник апарату СБУ.

***

16.02.2017

Експерти назвали найбільш «гарячі» теми фейкових новин РФ проти України

З початком гібридної війни з Росією дезінформація і пропаганда стали серйозною проблемою і для України, причому останнім часом російські ЗМІ свідомо відмовилися від створення гучних історій в стилі «розіп'ятого хлопчика» і видають багато дрібних фейків на задані теми (Інформаційна агенція «Вголос»).

Про це розповів Р. Дейниченко, представник українського веб-ресурсу StopFake.org, пише «Нове время».

За словами експерта, у числі таких тем – «регіони України вимагають федералізації», «українське керівництво – корупціонери і ідіоти» і «світ втомився від України і, ось-ось, зніме антиросійські санкції».

Експерти звертають увагу на професіоналізм фейкової стратегії росіян, яка часто лише посилює і підкреслює існуючу проблему і тому сприймається однозначно – як правда.

***

20.02.2017

В Інтернеті активізувалися вербувальники на платні «протести» в Києві, – ЗМІ

Останніми днями в мережі Інтернет значно зросла кількість пропозицій, спрямованих на платне залучення громадян до протестних заходів, які заплановано на 20-22 лютого в Києві, пише ІУкрінформІ (LB.ua).

Зокрема, в соціальній мережі «ВКонтакте» активно поширюються пости – практично однакові, в яких пропонують гроші (250 грн/день, 600 грн/добу) за участь в акціях протесту в центрі столиці.

Наприклад, оголошення від 19 лютого: «Масовка на завтра. Тільки хлопці і чоловіки віком 18-45 років. Оплата 40 грн/год. Бонуси за друзів...».

Також громадян запрошують на «мирний мітинг на підтримку малого бізнесу. 21 число (з 16 років). Стояти треба добу (намет, чай). Оплата – 600 грн».

«Потрібні люди на акцію 21.02.2017. Чоловіки, жінки віком 18-65 років. Акція проходить у центрі Києва. Зустрічаємося м. «Арсенальна» о 8:30. Оплата – 8:30–18:30 – 250 грн, доба – 600 грн. Чай, кава...».

«Масовка на 21 число, оплата 500 грн добу...»

Як видно з оголошень, також проводиться збір на акцію на Майдан Незалежності на 22 лютого: «Підробіток на 22.02. Від 16 до 70 років, хлопці і дівчата. Три години 70 грн, виплата відразу після роботи!!! Робота в першій половині дня (збір о 9:00 на Майдані Незалежності)...».

«Масовка 22 лютого!!! Потрібні люди! Місць багато! Збір о 8:40 на Майдані Незалежності. (Біля Двох Гусей). Працюємо три години. Оплата 90 грн».

Акаунти, які поширюють заклики до платної участі в протестних заходах:

«Вадим Вадимович»

Спецслужби і технології «соціального контролю»

17.02.2017

«ВКонтакте» теперь блокирует тех, кто интересуется «группами смерти»

Администрация социальной сети «ВКонтакте» сообщает, что начала блокировать страницы пользователей, которые используют хэштеги, связанные с пабликами, тематика которых – самоубийства. Об этом сообщает «Медуза», ссылаясь на пресс-службу компании (Новости Донбасса).

«Мы против того, чтобы на этой теме спекулировали, распространяя связанные с ней материалы», – заявил представитель «ВКонтакте» Е. Красников.

О каких именно хэштегах идет речь, он не уточнил. Ранее пользователи сети сообщили, что аккаунты блокируются в случае многократного употребления хэштегов «4:20», «Тихий Дом», «хочу в игру» и «куратор».

После того, как пользователь связывается с администраторами «ВКонтакте», ему предлагают «сообщить о причинах публикации спорной записи». После этого в зависимости от ответа ему или предлагают помощь психологов, или просят «не увеличивать популярность “групп смерти” даже в рамках борьбы с ними», или дают «советы по безопасности страницы».

***

16.02.2017

Радник міністра МВС планує заборонити «ВКонтакте» та «Одноклассники» в Україні

Радник глави МВС З. Шкіряк пропонує ввести заборону в Україні на російські соціальні мережі «ВКонтакте» та «Одноклассники» (Украинские реалии).

За словами З. Шкіряка, 2017 р. має стати роком захисту інформаційного простору України від впливу російської пропаганди. «І одним з перших рішень (у цьому році. – Ред.) має стати блокування російських соціальних мереж “ВКонтакте” та “Одноклассники”, які сьогодні повністю підконтрольні і керуються російськими спецслужбами», – сказав радник міністра.

Він висловив сподівання, що Міністерство освіти також долучиться до цього процесу і через вчителів у школах буде пояснювати дітям шкідливість використання цих двох соцмереж.

«Ми бачимо, що вони (“Вконтакте” та “Одноклассники”. – Ред.) є основними виробниками антиукраїнського контенту, що розповсюджується в інтернеті», – заключив він.

***

17.02.2017

Как запретить «ВКонтакте» в Украине: названы варианты

Теоретически затея с блокировкой соцсетей «Вконтакте» и «Однокласники» в Украине вполне реализуема (Обозреватель).

Об этом в комментарии «Обозревателю» рассказал IT-специалист П. Нейман.

«Для того, чтобы заблокировать “ВКонтакте” на уровне дата-провайдеров Украины нужно заблокировать DNS имени Vk.com. Тогда, когда человек будет вбивать в поиске “ВКонтакте”, не будет резолвиться IP-адрес», – объяснил специалист.

Но, по словам П. Неймана, обойти этот запрет украинским пользователям будет возможно.

«Для того, чтобы обходить этот запрет пользователю нужно будет настроить для себя внешний dns-резолвер. Например, Google дает такую услугу, и, в принципе, тогда dns будет соединяться», – отметил П. Нейман.

Что же касается дополнительных возможностей для запрета, специалист выделил еще одну.

«Плюс они могут запретить трафик по украинским сетям на ip-сервера “ВКонтакте”. В таком случае туда просто не будут переходить запросы от украинских пользователей», – отметил IT-шник.

***

16.02.2017

«ВКонтакте» прокомментировали возможность закрытия соцсети в Украине

16 февраля советник министра внутренних дел З. Шкиряк заявил о том, что в Украине могут запретить социальные сети «ВКонтакте» и «Одноклассники». Информатор связался с представителями соцсетей и узнал, что они думают по этому поводу (Информатор).

Руководитель коммуникаций «ВКонтакте» по Украине В. Леготкин неохотно прокомментировал сложившуюся ситуацию.

«Мы предпочитаем не комментировать чьи-либо идеи и предложения», – отметил он.

При этом пресс-секретарь подчеркнул, что «ВКонтакте» соблюдает все законы, не прибегает к цензуре, не ограничивает ничью свободу, активно борется с мошенничеством и распространением порнографии.

«“ВКонтакте” как площадка для общения была и остаётся в стороне от политики, поэтому и претензий к нам по поводу этого просто быть не может», – резюмировал он.

Ранее в интервью AIN.UA глава Киберполиции С. Демедюк пояснил, что заблокировать такие площадки, как «ВКонтакте» или «Одноклассники» не получится: «У нас сейчас нет законодательной или технической возможности блокировать такие ресурсы, даже если к нам обратится правообладатель с жалобой на нарушение авторских прав. Их серверы находятся на территории РФ, компании входят в юрисдикцию этой страны, так что в этом случае правильно было бы использовать другие рычаги влияния – финансовые, уголовно-процессуальные и т. д. Но это возможно только в рамках международного взаимодействия, которое в отношении РФ сейчас не работает», – пояснил С. Демедюк.

***

21.02.2017

Інтернет Асоціація України висловилась щодо цензури в мережі

Інтернет Асоціації України розповсюдила офіційну позицію щодо «обмеження доступу (інтернет-цензури) до ресурсів Інтернет операторами зв'язку». МедіаБізнес наводить текст заяви без змін (МедиаБизнес).

«Інтернет Асоціація України виступає різко проти впровадження технічного механізму інтернет-цензури під будь-яким приводом, та проти всіх законопроектів, де мають місце будь-які формулювання вигляду "обмеження операторами доступу до визначених ресурсів мережі Інтернет".

Інтернет-цензура – це технічне обмеження доступу до визначених ресурсів, розміщених у мережі Інтернет операторами та провайдерами зв'язку, що надають послуги доступу до Мережі.

Україна відноситься до країн з вільним доступом до Інтернет, де відсутній технічний механізм цензури, таких як США, більшість європейських країн, Японія. У таких розвинутих країнах бізнес не несе відповідальності ні юридичної, а ні моральної за етичний вибір споживачів.

У країнах, в яких держава зобов'язує ринок інтернет-комунікацій блокувати доступ до визначених ресурсів у Мережі, вона створює для цього нормативні документі, закони та порядок виконання процедур.

Сьогодні в Україні оператори та провайдери Інтернет у своїй роботі керуються Законом України про телекомунікації від 18 листопада 2003 р. № 1280-IV, який зобов'язує операторів не втручатись у потік даних користувачів. Блокувати доступ користувачів до визначених (або не визначених) ресурсів. Інтернет-оператори не мали повноважень і як наслідок, не мали потреби для встановлення високовартісного обладнання та програмного забезпечення яке здатне блокувати доступ до ресурсів Мережі.

Не дивлячись на законодавство, що діє зараз, досі виникають та активно лобіюються законодавчі ініціативи, які мають на меті заборону на державному рівні доступ до визначених ресурсів Мережі, та/або покладення відповідальності за наявність цієї інформації у Мережі на операторів зв'язку. Припустимо, що при певних обставинах, такі ініціативи стануть законом і зглянемо можливі наслідки, що базуються на досвіді інших країн.

1. Для бізнесу та бюджету країни.

Цензура має запрацювати, а для цього потрібно розробити пакет документів та методичних матеріалів для ринку телекомунікацій України, та суміжних ринків, які визначатимуть правила роботи для галузі. Для операторів це означатиме – зміну своїх мереж: закупівля, встановлення та налаштування нового високовартісного апаратного та програмного забезпечення. Очікуваний термін та затрати на впровадження таких змін – півтора роки та 1 млрд дол. США сумарно по галузі.

2. Для визначення державних цілей.

З досвіду країн, що впровадили інтернет-цензуру відомо, що цензура завжди змінює цілі. Початкові цілі введення цензури, якими би вони не були, із часом забуваються, перелік заборонених тем розширюються. Розширити та змінити перелік заборонених тем при наявності самого механізму цензури дуже просто, як ми бачимо на прикладі цензури Мережі в Росії.

3. Для розслідування правопорушень.

Усі сучасні технічні методи інтернет-цензури, навіть китайський "Золотий Щит", дуже легко обходяться шляхом налаштування стандартного програмного забезпечення ПК (VPN, TOR, Proxy тощо). Найважливішою особливістю всіх систем цензурування, що існують є повна неспроможність заблокувати доступ тим, хто активно шукає доступу до забороненого контенту. Також усі ці механізми обходу цензури змінюють мережеві дані користувача. Для розслідування злочинів, що скоєні за допомогою Мережі, це означає значні ускладнення або навіть неможливість встановити особу, яка виконала певні дії у мережі. Наприклад, у такому разі практично неможливо буде прослідкувати розповсюджувачів і споживачів дитячої порнографії.

Єдиним напрямом, де інтернет-механізм цензури виявився ефективним – це обмеження кола розповсюдження інформації серед користувачів, які користуються популярними джерелами інформації та не бажають налаштовувати програмне забезпечення для обходу блокувань, тобто вплив на широку громадську думку та електоральні переваги населення за рахунок звуження кола розповсюдження "небажаної" інформації.

Враховуючи вищезазначене, ми схиляємося до висновку, що справжні цілі впровадження інтернет-цензури в Україні – є суто створення політичної цензури.

ІнАУ бажає бачити Україну у розвитку мережевих технологій поруч з такими країнами, як США, Японія, Німеччина, а не поруч з Росією, Іраном, Північною Кореєю. ІнАУ виступає проти впровадження технічного механізму інтернет-цензури», – йдеться на сайті ІнАУ.

***

21.02.2017

Facebook заблокував офіційний акаунт пропагандистської «Звезди»

Офіційний акаунт російського пропагандистського телеканалу «Звезда» у Facebook був заблокований у зв'язку з публікацією статті про ватажка банди «Сомалі» М. Толстих – «Гіві» (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»).

Про це ТАСС повідомив представник прес-служби «Звезды».

«Аккаунт телеканалу "Звезда" був заблокований через матеріал про загибель командира батальйону «Сомалі» М. Толстих у зв'язку з тим, що публікація нібито порушує норми спільноти соцмережі», – сказали в прес-службі.

«Ми здивовані», – додали на телеканалі.

Більш того, за словами представника «Звезды», аналогічний пост в Instagram був також вилучений.

***

27.02.2017

Росіянин отримав 160 годин виправних робіт за коментар про «ватників» у «ВКонтакте»

Жителя Саратова О. Гозенка засуджено до 160 годин обов'язкових робіт за пости у «ВКонтакте», в яких він вживав словом «ватник» (LB.ua).

Про це повідомляє ВВС.

19-річного О. Гозенка звинувачували в приниженні людської гідності, йому пред'явили звинувачення за 282 ст. Кримінального кодексу РФ.

Зокрема, прокурор К. Забєліна заявила в суді, що О. Гозенко розміщував у соцмережі «ВКонтакте» коментарі зі словами «ватники» і «кацапи».

При цьому прокуратура вбачала в цих та інших коментарях О. Гозенка «лінгвістичні та психологічні ознаки спонукання до дій насильницького характеру відносно групи осіб національної приналежності» і просила засудити його до двох років позбавлення волі умовно з випробувальним терміном на два роки.

Сам 19-річний підсудний на слідстві дав покази і визнав провину. У зв'язку з цим його справу розглядали в особливому порядку.

В останньому слові О. Гозенко просив призначити йому штраф, а його захист – обрати покарання, не пов'язане з позбавленням волі.

***

25.02.2017

Базиленко Анна

Поліція затримала адмінів груп у «ВКонтакте», в яких дітей доводили до самогубства

Поліція затримала двох адміністраторів суїцидальних груп у соціальних мережах. Про це Громадському повідомив голова Національної поліції України С. Князєв (Watcher).

«Вони (затримані. – Ред.) дають свідчення, що експериментували зі свідомістю людей», – сказав очільник Нацполіції.

За словами С. Князєва, проводяться «заходи з затримання та допиту адмінів груп "Синіх китів" та "Рожевих Фей"».

«Провели обшуки і зібрали докази. Ведемо консультації з генпрокуратурою щодо можливого затримання по справі», – повідомив С. Князєв.

***

27.02.2017

Украинцам будут принудительно отключать Интернет

Национальная комиссия по вопросам регулирования связи и информатизации утвердила изменения в правила предоставления телекоммуникационных услуг (Украинские реалии).

Они содержатся в проекте постановления Кабинета Министров «О внесении изменений в Правила предоставления и получения телекоммуникационных услуг» от 14.02.2017.

В Украине изменили порядок обслуживания абонентов, в связи с чем Нацкомиссия по вопросам регулирования связи предложила провайдерам и мобильным операторам отключать интернет пользователей, которых уличили в рассылке спама, Ddos-атаках и подозрительных звонках.

«В то же время, средств для выявления нарушителей у операторов нет. Часто поставщик услуг не в состоянии классифицировать, есть активность абонента, например, та же массовая рассылка – или спамом», – рассказал глава комитета по свободе слова и прав человека Интернет ассоциации Украины, директор компании «НетАссист» М. Тульева.

Кроме того проблема заключается в том, что пользователь может даже не знать, что с его IP-адрес компьютера или смартфона происходит вирусная рассылка. А разбираться «по ошибке» отключили или нет, абонент будет уже после блокировки.

***

27.02.2017

Как доктрина информационной безопасности повлияет на украинцев. Можно ли будет в Украине сесть за пост в сети

В Украине появилась доктрина информационной безопасности, где отражены не только актуальные угрозы нацинтересам в информационной сфере, но и предписания ведомствам и министерствам следить за Интернетом и СМИ (Украинские реалии).

Пока украинцы в сети сравнивают доктрину с аналогичным документом в России, «Сегодня» узнала, можно ли будет в Украине сесть за пост в сети, – передают «Украинские реалии» со ссылкой на МИР.

Время и цели. В СНБО доктрину утвердили еще в декабре прошлого года, однако подписал ее президент только в минувшую субботу. По словам медиаэксперта Т. Поповой, подобный документ должен был появиться еще в 2014-м, когда над ним и началась работа. Замминистра информационной политики Д. Золотухин в разговоре с «Сегодня» согласился с тем, что доктрину нужно было принимать давно: «Об этом много говорили нардепы, в том числе и в рамках коалиционного соглашения, органы нацбезопасности и обороны. Не последнюю роль в задержке сыграл разразившийся в стране год назад политический кризис, который мешал утверждению доктрины в разных ведомствах». Как отметил П. Порошенко, необходимость в таком документе продемонстрировали в РФ, используя технологии гибридной войны и превратив информационную сферу в арену противостояния.

В самом документе речь идет о предоставлении Кабмином СБУ и Министерству информполитики механизмов выявления и блокирования в Интернете информации, угрожающей украинцам. К таким данным авторы

причислили пропаганду войны, разжигание национальной и религиозной вражды, призывы к изменению конституционного строя. Также запрещены доктриной пропаганда коммунистической, нацистской и тоталитарной символики.

Мониторить на предмет нарушений чиновники будут не только блоги, посты в соцсетях и другую деятельность в Интернете украинцев, но и СМИ. Кроме того, власти хотят запустить постоянный мониторинг пропаганды со стороны государства-агрессора, чтобы оперативно отвечать на нее. Как отмечается в самой доктрине, теперь Кабмин должен посчитать, во сколько обойдется финансирование программ и координировать работу министерств и ведомств. Помогать правительству в этом будет СНБО. Конкретные наказания за нарушения правил доктрины пока не разработаны, это обещают сделать в ближайшее время.

Сесть за пост. Документ пришелся не по вкусу многим экспертам и правозащитникам. «Свобода слова? Нет, не слышали. Противодействовать пропаганде можно только одним способом – создавая качественный и объективный контент. Но если это сложно, гораздо проще идти путем запретов, хотя это и не тот путь, который нужен развивающейся стране», – говорит представитель правозащитной организации Amnesty International Украина Т. Мазур.

В свою очередь политолог Р. Бортник отмечает, что в самой доктрине нет ничего противоправного или неконституционного, и кардинально она пока ничего не поменяет. «Одно дело заявить какие-то механизмы, а другое – иметь технические или финансовые возможности для них. Но есть одна большая опасность – анализ и прочесывание Интернета на предмет неугодной информации надо было выписать более конкретно. Сейчас есть угроза, что под такую категорию данных может подпадать любая неугодная информация. В таких случаях может начаться “охота на ведьм”, когда украинцев будут привлекать к ответственности за какие-то записи в Интернете», – резюмирует эксперт.

В свою очередь в Министерстве информполитики подчеркивают, что позиций, ограничивающих гражданские права, в документе нет. «Но подобные заявления будут предохранителем. То есть у гражданского общества должна быть своя “дубина”, которая предупреждала бы: мы не позволим, чтобы госполитика использовалась для сокращения каких-то гражданских прав. Люди должны мониторить, как применяется документ и не молчать в случае нарушений», – сказал нам Д. Золотухин.

***

28.02.2017
Юрій Лапаєв
Нові інформаційні війська Росії: народжені брехати

Міністр оборони РФ С. Шойгу нещодавно заявив про створення в країні військ інформаційних операцій. Офіційно – для ведення контрпропаганди, захисту національних інтересів національної оборони та протиборства в інформаційній сфері. Цікаво, що раніше наявність таких підрозділів російські силовики намагалися заперечувати, хоча багато країн, насамперед, Україна вже встигли на собі відчути невидимий вплив «неіснуючих військ». Так що насправді стоїть за рапортами російських генералів? (Дніпроград).

Одна з причин – необхідність консолідації існуючих підрозділів і централізації управління ними. Останні події показали, що відсутність достатнього контролю вже працює проти Кремля. Лише за півроку спецслужби РФ зазнали ряд поразок на внутрішній та міжнародній аренах: виявлення участі Росії у втручанні в хід виборів в США, викриття прихованих переговорів росіян з чиновниками Трампа, виток інформації від Суркова та Фролова, яка підтверджує участь в організації «русской весны» в Україні. Це не могло залишитися без уваги російського керівництва, тому гучні відставки в адміністрації президента РФ (а за наявною інформацією саме АП РФ координувала спецслужби та групи завербованих хакерів) не були несподіванкою. Як і символічні жертви хакерів з групи «Шалтай-Болтай» та чиновників ФСБ, які показали на яку саме структуру поклали всю відповідальність.

Ще з радянських часів існувала конкуренція між головними спецслужбами країни – КГБ та ГРУ, а простіше між «комітетськими» та військовими. Інколи протистояння між ними переходило в гострі фази, інколи існував певний паритет, проте боротьба не припинялася і з розпадом СРСР. Разом з приходом до влади В. Путіна, в РФ на домінуючу роль вийшла наступниця КГБ – ФСБ, а ГРУ було вимушено піти в тінь, ставши закордонним силовим кулаком Росії в Грузії, Сирії та Україні. Проте конфлікт інтересів двох спецслужб всередині країни залишається, а С. Шойгу, здається, зовсім не проти стати в чергу до трону.

У цей контекст цілком вписується створення інформаційних військ. Об’єднання науковців, у тому числі цивільних, існуючих підрозділів інформаційно-психологічних операцій та ССО до єдиної структури, в теорії, може підняти її ефективність та керованість. А значить – підвищити і політичну цінність. Проте все має свою ціну. Скоріш за все, за кращу керованість заплатять відсутністю креативу та безініціативністю, що притаманно більшості державних відомств РФ.

Після такої «легалізації» з вуст міністра оборони, слід чекати й на певну законотворчу діяльність для офіційного розширення повноважень нових підрозділів. У такий відносно прихований спосіб можна уникнути зайвої уваги, яку могло б викликати створення окремого «міністерства правди». На думку експертів Збройних сил України, скоріш за все, російським «інформаційним бійцям» можуть надати доступ до впливових мас-медіа на однаковому рівні з ФСБ, а далі мова може йти й про початок цензури.

Ще один ймовірний привід для оголошення про створення власних інформаційних військ бачать в РНБО України. Так, на думку керівника служби з питань інформаційної безпеки В. Петрова, заява С. Шойгу зроблена не для міжнародної спільноти. Адже в світі і без цього відомі спроможності цих підрозділів. Мова йде скоріше про певне самозаспокоєння для внутрішнього споживача. З екранів росіянам цілодобово кажуть про агресивний блок НАТО, який постійно створює підступні плани щодо знищення РФ. Для цього, згідно з російською теорією, використовується в тому числі й інформаційна зброя – всі довкола намагаються дискредитувати безвинну Росію. Обвинувачення в анексії Криму, допінговий скандал, війна на Донбасі, збитий МН-17, проблеми з чемпіонатом світу з футболу – все це не більш ніж вигадки ненависного Заходу. Тому, щоб показати, що Кремль здатний впоратися з цими проблемами, робиться заспокоєння для населення. Мовляв, знаємо, вміємо, переможемо. Тому в заяві С. Шойгу робиться акцент саме на контрпропаганді. Не випадковою можна вважати і дату – адже виступ міністра відбувся 22 лютого, напередодні важливого для росіян свята. Не відстають від тренду і в міністерстві закордонних справ Росії. Майже одночасно з МО, в зовнішньополітичному відомстві повідомили про розбудову власної структури, яка, начебто, буде боротися з фейками. Насправді, просто унікальна ситуація, коли за створення викривленої інформації та боротьбу з нею намагаються відповідати одні і ті ж самі люди.

Утім, це не лише «бряцання зброєю». Росії є чим похвалитися в інформаційній сфері. До справи створення та розповсюдження пропаганди та дезінформації в країні задіяна велика кількість людей, як у згаданих відомствах, так і цілком приватних організаціях. Відомий приклад – фабрика «тролів-ольгінців», а офіційно – ТОВ «Интернет-исследования» чи ТОВ «Тека», з якими пов’язується колишній кухар Путіна Є. Пригожин. Хоча, здається, що це лише верхівка айсбергу, а в Росії існують ще багато таких установ. На рахунок підрозділів ФСБ та ГРУ – звичайно, що точних даних щодо кількості персоналу немає. Хоча відомо, що лише в Центрі інформаційної безпеки ФСБ РФ до початку війни в Україні налічувалося більше 800 співробітників, а відділ інформаційної ізоляції 12 Командування резерву ЗС РФ, який займається проведенням інформаційних операції на Донбасі, складається з 60 осіб. І це без урахування російських мас-медіа на кшталт Russia Today чи Sputnik з мільярдними бюджетами, чисельної армії кишенькових «експертів», «науковців» та коментаторів по всьому світові. Наразі, попри істотний вплив антиросійських санкцій, Кремль може це собі дозволити, щоб просувати потрібні думки по всьому світу.

Чого не можна сказати про Україну. Адже на відміну від сусідів офіційний Київ значно обмежений в ресурсах. До того ж не завжди наявні кошти використовуються ефективно. Один з наочних прикладів – державне міжнародне телебачення, яке за задумом повинно розповісти всьому світові про реальний стан справ в Україні. Згідно з прийнятим наприкінці 2015 р. Закону про систему іномовлення України, щорічне фінансування платформи UA|TV

повинно складати не менше ніж 0,06 % видатків загального фонду Держбюджету за попередній рік, що для бюджету 2016 р. становить 388,3 млн грн. Звичайно, частина коштів йде на створення відеоматеріалів та на забезпечення супутникової трансляції, але кількість підписників каналу UA|TV в мережі Youtube станом на березень 2017 р. – 2664 людини, а середня кількість переглядів відео не перевищує 200. Для порівняння, Russia Today має 2 млн підписників та від 10 до 70 тис. переглядів. Не все добре і з посольствами України за кордоном. Не всі дипломатичні установи належним чином ставляться до організації інформаційної роботи в країні перебування. Частіше, все зводиться до написання звітів про, нібито, проведені заходи. Цю ситуацію повинно змінити створення ситуаційних центрів, головним завданням яких є оперативне висвітлення головних подій в державі та робота з місцевими ЗМІ.

Не дивно, що в світі часто більше вірять російській пропаганді, аніж українським спробам переконати в своїй правоті. Це підтверджують і європейські спеціалісти з виявлення дезінформації та спотворених новин. Нещодавно в Києві була проведена прес-конференція за темою «Інформаційна війна в Інтернеті. Викриття і протидія прокремлівській дезінформації в країнах Центральної та Східної Європи». Конференція, яку було організовано за сприяння української волонтерської організації StopFake, зібрала фахівців з Чехії, Польщі, Словаччини, Молдови та Угорщини. Дослідження, які були представлені під час конференції показали, що головними напрямами російського інформаційного впливу на європейців є: дискредитація НАТО (як спроможностей щодо захисту країн-членів, так і на рівні цінностей), дискредитація єдиної Європи (ЄС неодмінно чекає економічний крах та бездуховність), роздмухування проблеми мігрантів, нав’язування конспірологічних теорій (наприклад, щодо прихованої участі США чи масонів у світовій політиці), поширення проросійських думок, а в окремих випадках – заперечення права на існування держави та мови (справедливо для України та Молдови). Для цього використовуються як державні, так і альтернативні мас-медіа, блоги, соцмережі, неурядові організації та навіть російська православна церква. У цьому сенсі можна впевнено сказати, що Україна – це Європа, адже методи та тематика впливу на нашу країну та на європейських сусідів з боку Кремля однакові. Показовим є той факт, що більшість європейських спільнот з боротьби з дезінформацією виникли вже після початку війни в Україні, переважно за прикладом українського проекту StopFake.

Діяльність російських спецслужб щодо нашої країни можна розділити за такими напрямами:

Міжнародна активність. Сюди підпадає дискредитація України на світовій арені, нав’язування уявлення про провал реформ і всеосяжне проникнення корупції та переконання у необхідності припинити міжнародну підтримку. Мається на увазі як зняття санкцій з Росії так і утримання від надання летального озброєння ЗСУ. Крім того, активно використовуються історичні аспекти – як, наприклад, питання Волинської трагедії у польсько-українських відносинах.

Активність у зоні АТО та на тимчасово окупованих територіях. Головне завдання російських інформаційних спеціалістів – підрив довіри до української армії. Відомі випадки диверсій, що були скоєні саме місцевими (як вибухівка в банці з медом від мешканця Станично-Луганського району), підтверджують ефективність такої роботи. Крім обробки мозку населенню, робиться все можливе для приниження бойового духу бійців ЗСУ. Поширення панічних настроїв, чутки про зраду та загрозливі смс-повідомлення відомі ще з часів Іловайську. Переважно, така робота проводиться підрозділами ГРУ ГШ РФ.

Дестабілізація всередині країни, що є зоною відповідальності 5ої служби ФСБ РФ. Останні події на роковини Революції гідності – найсвіжішій приклад такої діяльності. А до цього – вже чисельні спроби створити «третій Майдан», виступи професійних «солдатських матерів», «тарифний геноцид», травневі марші тощо. Дуже часто як інформаційний привід для таких дій використовуються новини з фронту, переважно дрібного, тактичного рівня, але в інформаційному плані вони подаються як стратегічно важливі. Варто зазначити і вміле використання різних політичних сил. У нагоді стають не тільки відверто радянські комуністи чи регіонали, а й на перший погляд абсолютно проукраїнські сили.

Крім виключно інформаційних акцій проти України ведеться і кібервійна. За словами спікера Українського Кіберальянсу (УКА) Ш. Тансенда, російськими хакерами керує ФСБ та Адміністрація президента РФ. При чому є підтвердження наявності зв’язків російських держорганів з відомими кіберзлочинцями, що відкриває спецслужбам нові можливості. Хтось стає хакером за гроші, хтось завербований шантажем чи залякуваннями. Разом з тим, за даними УКА, російськи хакери APT28/APT29 (також відомі, як Fancy Bear та Cozy Bear), насправді не є єдиними групами і створюються ситуативно під конкретні атаки та завдання. Наявні докази вказують, що аналогічних стихійних груп ще багато, проте не всі є публічними. Крім того, через наявність різних кураторів і погану комунікацію між російськими державними органами, доволі часто ці групи працюють проти самих себе. Останні новини показали також, що ФСБ не завжди вміє тримати контроль над своїм підопічними. Чисельні витоки інформації про діяльність росіян зараз зробили більше шкоди репутації РФ ніж користі. З цим, на думку Ш. Тансенда, пов’язано і бажання російського оборонного відомства прибрати цю сферу під свій контроль.

Покращити ситуацію з протидією російському впливу повинна підписана Президентом України Доктрина інформаційної безпеки. Адже в неї нарешті прописані ролі та сфери відповідальності більшості українських державних органів, цивільних та військових. Однак, головна проблема інформаційного протиборства – це дотримання балансу між свободою слова та цензурою і чисельними заборонами. На думку Петрова, недостатньо просто зробити обмеження російським інформаційним продуктам (ЗМІ, кінофільмам чи, наприклад, пісням). Такі заходи повинні поєднуватися створенням якісної української альтернативи, щоб користувач міг самостійно, без примусу, обрати

для себе національний продукт. А з ним, і змінити свій світогляд на українській.

Проблема захисту даних. DDOS та вірусні атаки

15.02.2017
Банковский Android-троян Marcher наращивает активность

Эксперты компании Securify опубликовали доклад, посвященный деятельности банковского Android-трояна Marcher, активного с конца 2013 г. Первые версии вредоноса использовались в фишинговых атаках, направленных на хищение данных о платежных картах. В марте 2014 г. жертвами Marcher стали клиенты одного из банков в Германии (InternetUA).

Во второй половине 2016 г. Marcher атаковал десятки организаций в различных странах, включая Великобританию, США, Австралию, Францию, Польшу и Испанию. Кроме того, операторы трояна начали распространять вредонос под видом популярных приложений, в том числе WhatsApp, Netflix и версии мобильной игры Super Mario Run для Android.

За последние полгода исследователи обнаружили шесть ботнетов, включающих в общей сложности 11 049 мобильных устройств, инфицированных трояном Marcher. Более половины из них были расположены в Германии (51 %), остальные во Франции (20 %) и Великобритании (7 %).

Троян Marcher проверяет, какие приложения работают на переднем плане, и при нахождении нужного выводит поверх его окна фальшивый экран с целью хищения учетных данных и информации кредитных карт. Кроме того, вредонос использует простую, но эффективную технику для уклонения от обнаружения популярными антивирусами. Как только Marcher обнаруживает работающий процесс какого-либо антивируса, троян вынуждает устройство вернуться на главный экран. Даже если антивирус обнаружит вредоносное ПО, пользователь не сможет дать разрешение на его удаление.

По оценкам экспертов, в скором будущем ущерб от деятельности Marcher может превысить убытки, причиненные известными банковскими троянами Dyre, Dridex и Gozi.

***

15.02.2017
Базиленко Анна
Як подивитись усе, що Facebook розповідає про вас іншим людям

«Етичний» хакер з Бельгії створив онлайн-інструмент Stalkscan, що показує, яка інформація про обліковий запис користувача соцмережі доступна публічно (Watcher).

Як пише The Next Web, у 2013 р. Facebook запустив функцію Graph Search, яка дозволяє легко відшукати практично будь-яку інформацію в соцмережі.

Виявляється, більшість користувачів соцмережі не знає або забула про цей інструмент пошуку. А можливості у нього потужні. Наприклад, з його допомогою можно легко відшукати фото вашого сусіда у 20-річному віці, знайти коментарі друзів щодо події, яку вони колись відвідали, або статуси, які вони вподобали.

Використання Graph Search ускладнювалось проблемою порушення приватного життя користувачів. Тепер же подивитися все, що Facebook розповідає про вас іншим стало набагато простіше.

Усе, що потрібно зробити, це ввести URL профілю у веб-інтерфейс. За словами розробника, інструмент не порушує політику конфіденційності Facebook.

***

15.02.2017
Роман Черный
Как работает и зачем нужна двухфакторная аутентификация

Безопасность в Интернете – не то, чем можно пренебрегать. Защиты не может быть много, потому все чаще крупные интернет-сервисы вводят у себя систему двухфакторной аутентификации. Тем не менее, люди не всегда пользуются предоставленной им возможностью. Чтобы исправить это недоразумение, разберемся, что такое двухфакторная аутентификация, зачем она нужна и как работает (IGate).

Что это и зачем этим пользоваться

Двухфакторная аутентификация – это еще один способ, по которому интернет-сервис может узнать, что вы – это вы. Первым способом, как правило, является пароль. Но, как показывает практика, одного лишь пароля часто бывает недостаточно. Во-первых, пароль может быть украден или подобран. А во-вторых, сами пользователи подходят к подбору паролей крайне безответственно. Уже много лет подряд самыми популярными паролями в мире остаются комбинации «123456» и «qwerty».

Печальная реальность мира кибербезопасности

Двухфакторная аутентификация позволяет пользователю еще раз подтвердить свою личность, а потому существенно повышает степень защиты личных данных. Пожалуй, единственным ее минусом является то, что пользователь вынужден указывать на ресурсе дополнительную персональную информацию, к примеру, реальный номер своего телефона. Тем не менее, этот минус также довольно относителен.

Дело в том, что создание и поддержание системы двухфакторной аутентификации требует от ресурса больших финансовых затрат. То есть, внедрить у себя такую систему могут только самые крупные компании, вроде

поисковика Google, крупных соцсетей, банков или торговых площадок. Во всех этих случаях скрывать что-то вроде номера телефона совершенно бессмысленно. Google, наверняка, уже и так знает о вас больше, чем некоторые близкие друзья и родственники. А социальным сетям, банкингу и торговым площадкам вы сами добровольно скармливание большое количество личной информации, так как это является необходимым условием их использования. В общем, если какой-то крупный интернет-ресурс предлагает вам подключить двухфакторную аутентификацию, не стоит откладывать это на потом. В этом механизме нет ничего опасного или сложного.

Как конкретно это работает

Элементарные принципы работы двухфакторной аутентификации знакомы каждому, кто хотя бы раз пользовался электронным банкингом или оплачивал что-то карточкой через Интернет. При попытке совершить транзакцию банк высылает на ваш телефон СМС с кодом подтверждения. Этот код, введенный в соответствующее поле при оплате, доказывает, что операцию проводит владелец счета, а не постороннее лицо, завладевшее данными карты.

Подтверждение СМС-кодом – простейший способ двухфакторной аутентификации

Двухфакторная аутентификация на крупных интернет-ресурсах проходит примерно по тому же принципу. Рассмотрим этот процесс на примере аккаунта Google. Подключить двухэтапную аутентификацию можно в разделе «Мой аккаунт» – «Безопасность и вход» – «Вход в аккаунт Google» – «Двухэтапная аутентификация». Как уже говорилось, первым этапом аутентификации всегда является ваш пароль. Вторым этапом по-умолчанию для Google является СМС. Активировав эту опцию и привязав к аккаунту свой реальный номер телефона, вы будете получать СМС-сообщение с кодом всякий раз, как попытаетесь войти в аккаунт с нового устройства, будь то ПК или мобильный гаджет. Без кода система попросту не пустит вас в аккаунт, даже если вы введете правильный пароль. Таким образом, если ваш пароль будет украден, и кто-то попытается им воспользоваться, вы также получите на свой телефон СМС с кодом. Это послужит вам сигналом о том, что пароль скомпрометирован и его нужно сменить.

Также Google позволяет настраивать несколько резервных способов аутентификации. Среди них – использование одноразовых резервных кодов на случай, если телефоном воспользоваться невозможно; функция Google Prompt, которая использует в качестве ключа для входа подключенный к Интернету смартфон; приложение Authenticator; электронный ключ, записанный на флешку или резервный номер телефона.

Какие бы способы вы не выбрали, я настоятельно рекомендую использовать резервный номер телефона на случай, если ваш смартфон будет украден.

У других ресурсов правила двухфакторной аутентификации могут отличаться. К примеру, сервис цифровой дистрибуции игр Steam использует мобильный аутентификатор Steam Guard, встроенный в приложение Steam для

смартфона. Каждые 60 секунд аутентификатор генерирует уникальный пятизначный код для подтверждения каких-либо действий с аккаунтом Steam.

Так вы можете быть уверены, что никто без вашего ведома не похозяйничает в вашем инвентаре и не потратит деньги из кошелька.

Существуют и более продвинутые способы аутентификации. К примеру, пароль может подтверждаться биометрическими данными пользователя, вроде отпечатка пальца или скана радужки или сетчатки глаза. Но, так или иначе, сам принцип остается неизменным. Двухфакторная аутентификация не избавляет пользователя от необходимости использовать пароль, но, хотя бы отчасти решает извечную проблему с его недостаточной надежностью.

***

15.02.2017

Сайт коллективных петиций уличили в распространении пиратских фильмов

Сервисы наподобие Change.org считают удобным инструментом для сбора подписей под той или иной инициативой. С учетом огромной аудитории, которая превышает 100 млн пользователей, оспорить такое утверждение сложно. Однако оказалось, что не только желающие добиться истины отдают предпочтение подобным ресурсам, но также «пираты» и распространители вредоносного ПО (InternetUA).

Одна из первых «петиций», содержащих ссылку на защищенный авторским правом контент, появилась на сайте Change.org в 2013 г. Постепенно количество жалоб стало расти, запросы поступали от ряда крупных компаний, среди которых Columbia Pictures, Lionsgate, Simon & Schuster и др.

Как отмечает TorrentFreak, поиск по сайту показывает, что пиратский контент здесь появляется регулярно – или, по крайней мере, контент, который выдает себя за таковой. В описании к таким петициям (которые, правда, активно зачищаются администрацией) указываются ссылки на внешние ресурсы, посещение которых может негативно сказаться на безопасности. К удивлению некоторых пользователей, файл «[BluRay-1080p] ‘Warcraft’ On-line Movie [2016] F.ull F.r.e.e» скрывал не кодированные видеоданные, а вирус.

***

15.02.2017

Сложные пароли несут с собой опасность взлома аккаунта пользователя – Ученые

Сложные пароли несут с собой опасность взлома аккаунта пользователя в отдаленной перспективе. С таким утверждением выступили ученые из Великобритании (HiTech-News.ru).

Выступая на запланированном мероприятии, посвященном кибербезопасности в столице Шотландии Эдинбурге, исследователи отметили,

что требование придумывать сложные пароли со стороны собственников сайтов необоснованно. Речь идет о длинной последовательности символов, состоящей не только из букв, но и цифр. Такой пароль легко забывается, что в дальнейшем приводит к потере доступа к созданному профилю. А именно такие «повисшие» аккаунты, содержащие в себе достаточно пользовательской информации, становятся идеальной мишенью для кибер-преступников.

Исследователи рассказали, что уже придуман новый метод сохранения безопасности в сети Интернет. Правда, они не захотели рассказать в деталях, в чем именно состоит их новая разработка, позволяющая Британии в скором будущем выйти на первое место в мире по уровню защищенности от хакерских атак.

***

15.02.2017

Экс-сотрудник ФБР пояснил, почему хакеры побеждают в кибервойне

Правительственные и коммерческие организации пребывают в блаженном неведении по поводу того, как в действительности работает безопасность, поэтому не в состоянии должным образом противостоять киберугрозам, считает бывший ИБ-эксперт ФБР Дж. Траппи (Jason Truppi). Общество уверено в том, что правительственный и частный секторы принимают рациональные решения в вопросах информационной безопасности, однако на деле это не так (InternetUA).

«Правительство быстро реагирует на ситуации. Тем не менее, со временем мы пришли к выводу, что быстрой реакции недостаточно, нужно принимать превентивные меры», – заявил Дж. Трапп на конференции B-Sides в Сан-Франциско.

По словам эксперта, общество должно отказаться от иллюзии, будто правительство и бизнес работают сообща над обеспечением кибербезопасности. На самом деле государственные и частные организации придерживаются совершенно разных принципов.

Правительство призывает компании предоставлять ему данные о кибератаках. Однако дальнейшее расследование инцидентов может привести к предъявлению сотрудникам компаний обвинений, не связанных с кибератаками. Поэтому организации не спешат обращаться к властям с сообщениями о киберугрозах.

По словам Дж. Траппи, компании плохо справляются с обеспечением информационной безопасности и особо не беспокоятся. Они стараются нанять высококвалифицированных ИБ-специалистов, однако в итоге эксперты вынуждены заниматься неэффективной работой. Зачастую руководство не понимает всех тонкостей и вынуждает специалистов тратить целые дни на бесполезные решения малозначительных проблем.

***

15.02.2017
Мінфін планує виділити на кіберзахист більше 50 млн грн

Цьогоріч Міністерство фінансів має намір витратити 52 млн грн на забезпечення кібербезпеки державних інформаційних ресурсів (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»).

Про це повідомляє LIGA.net.

«Кошти підуть на покупку серверного та комутаційного обладнання, системи зберігання даних, антивірусного програмного забезпечення, послуг з технічного захисту інформації, послуг з надання захищеного доступу до мережі Інтернет», – йдеться в повідомленні.

***

15.02.2017
Бардусова Наталья
Опубликован рейтинг стран-лидеров по DDoS-атакам

В Сети появилась публикация рейтинга стран, которые занимают лидерские позиции по ведению с их территорий DDoS-атак. Так, детальный анализ данных позволяет экспертам делать оценку уровня обеспечения максимальной интернет-безопасности пользователей Сети (HiTech-News.ru).

Лидером рейтинга стали Соединенные Штаты, за которыми последовали Великобритания и Германия. Так, исходя из отчёта четвертого квартала прошлого года, максимальное количество IP-адресов, откуда осуществлялись хакерские атаки, было зафиксировано именно на территории США, где были выявлены 24 % киберпреступников.

Что касается других стран, не вошедших в список, по словам специалистов, на их территории DDoS-атаки не так активны, что объясняется отсутствием специально оборудованного сервера для произведения полномасштабных действий, направленных на выведение устройств из строя.

В Великобритании зарегистрировано 10 %, а в Германии – только 7 % IP-адресов кибермошенников. Россия при этом находится на 5-й позиции. США является лидером атак на сервера вот уже на протяжении пяти лет. ВСогласно прошлому отчетному периоду, второе и третье месте достались Турции и Китаю соответственно.

***

16.02.2017
На Дніпропетровщині виявили групу шлюбних інтернет-шахраїв

Про це повідомляє Департамент кіберполіції Нацполіції, передає Depo.Дніпро (Depo.ua).

Кіберполіцією Дніпропетровщини задокументовано злочинну діяльність групи шахраїв, які використовували соціальні мережі та сайти онлайн-знайомств для виманювання грошей у довірливих людей. Вони реєструвалися на сайтах онлайн-знайомств та створювали фейкові сторінки в соціальній мережі «ВКонтакте» та вишукували для знайомства молодих жінок і чоловіків.

Потім шахраї імітували початок дружніх чи навіть сімейних стосунків. При встановлені довірливих відносин, фігуранти вигадували складні життєві обставини та пропонували для допомоги терміново перерахування на банківські рахунки чи на електронні гаманці WebMoney чи QIWI значні суми грошових коштів.

Встановлено, що від дій шахраїв постраждало 15 осіб, яким спричинено збитків на загальну суму більше ніж 500 тис. грн.

Групу інтернет-шахраїв було виявлено та затримано. Під час обшуку у них вилучили комп'ютерну техніку, банківські картки та телефони. Відкрито кримінальну справу за ч. 3 ст. 190 КК України (шахрайство).

***

19.02.2017

Глава МИД Франции осудил кибератаки против кандидата в президенты Макрона

Глава МИД Франции Ж.-М. Эйро в интервью Journal du Dimanche раскритиковал ситуацию с кибератаками против кандидата в президенты страны Э. Макрона (InternetUA).

Он выразил уверенность, что Россия симпатизирует правым кандидатам – Ф. Фийону и М. Ле Пен – и поэтому именно Москва совершает кибератаки против Макрона, поддерживающего ЕС-кандидата.

«Франция не допустит [вмешательства], Франция не допустит того, чтобы ей диктовали ее выбор», – заключил Ж.-М. Эйро.

Министр осудил кибератаки в отношении Э. Макрона и подчеркнул, что «подобная форма вмешательства в демократическую жизнь Франции недопустима».

***

20.02.2017

Немецкий регулятор запретил шпионящую за детьми «умную» куклу

Федеральное сетевое агентство Германии (Bundesnetzagentur) запретило линейку «умных» кукол «Моя подруга Кайла» (My Friend Cayla). Ведомство назвало игрушку шпионским устройством и рекомендовало родителям как можно скорее избавиться от нее. Согласно пресс-релизу регулятора, куклы записывают разговоры детей и передают их производителю в США (InternetUA).

Согласно описанию игрушки, представленному на официальном сайте My Friend Cayla, кукла может общаться с ребенком и отвечать на вопросы. Каждый вопрос ребенка записывается и отправляется на установленное на телефоне родителей специальное приложение. Программа конвертирует звуковой файл в текстовый и ищет ответы на заданные вопросы в Интернете. Тем не менее, как сообщает Bundesnetzagentur, приложение также отправляет записанные разговоры на серверы производителя. Согласно пользовательскому соглашению, компания имеет право использовать записи разговоров для улучшения сервиса и передавать их третьим сторонам для таргетированной рекламы.

Помимо прочего, «умную» куклу могут взломать злоумышленники, к примеру, с целью запугивания ребенка. Подключение между игрушкой и мобильным приложением защищено недостаточно, поэтому хакеры могут перехватывать разговоры.

***

20.02.2017

Microsoft патентует облачную технологию родительского контроля

Microsoft был выдан патент на новую технологию родительского контроля под названием Real-Time Parental Monitoring, позволяющую устанавливать рамки общения детей в интернете (IGate).

Виртуальный «надзиратель» сможет работать на всех устройствах. Система сможет не только отслеживать онлайн-активность ребенка, но и фиксировать адресатов, типы сообщений и прикрепленный к ним контент (аудио, видео, изображения), а также отыскивать сообщения с откровенным содержанием.

При этом родителям будет достаточно настроить сохранения или отправку сообщений в режиме реального времени и получать уведомления. В Microsoft заявляют, что сервис сможет покрыть как работу с приложениями, так и другие виды активности ребенка.

Отметим, что технология может использоваться не только для родительского контроля, но и для наблюдения за перепиской пользователей, где одно или несколько устройств являются администраторами, а остальные – подчиненными.

***

21.02.2017

Google прибрав з індексу 1 млн сайтів за порушення авторських прав

Згідно з оновленням звіту про запити на видалення контенту у зв’язку з порушенням авторських прав, за останні п’ять років Google прибрав з результатів пошуку 1,01 млн піратських сайтів і 2,15 млрд URL-адрес (Watcher).

Запит на видалення URL може бути створений власником прав на спірний матеріал. Після отримання він розглядається працівниками Google. Якщо запит буде схвалено, власник ресурса-порушника отримає сповіщення про це в Search Console.

***

20.02.2017

Число заражений вымогательским ПО растет с большой скоростью

Плата операторам вредоносного ПО за расшифровку файлов только поощряет киберпреступников к дальнейшему проведению подобных атак, уверены эксперты. Тем не менее, многие жертвы вымогателей предпочитают платить, благодаря чему количество атак с использованием троянов-шифровальщиков растет в геометрической прогрессии (InternetUA).

Согласно опубликованному в прошлом месяце отчету экспертов института Ponemon, 48 % компаний, ставших жертвами вымогательского ПО, предпочитают заплатить выкуп злоумышленникам и не искать другие решения проблемы. По данным ФБР, в 2015 г. общая сумма выкупа составила 24 млн долл., но уже в первые три месяца 2016 г. она увеличилась до 209 млн долл. (речь идет только об известных атаках и только в США). Если подобная тенденция будет продолжаться, к концу текущего года сумма выкупа достигнет 1 млрд долл.

В 2015 г. только CryptoWall3 причинил ущерб по всему миру на 325 млн долл. Убытки от обнаруженной в прошлом году версии CryptoWall4 достигли 18 млн долл. По подсчетам страховой компании Beazley, в 2016 г. число атак с использованием вымогательского ПО в четыре раза превысило показатель за 2015 г.

Как сообщили эксперты Symantec, в марте прошлого года количество заражений троянами-шифровальщиками достигло 56 тыс. – в два раза больше, чем обычно.

***

20.02.2017

Компании не уделяют должного внимания борьбе с киберугрозами – Fujitsu

Согласно исследованию Fujitsu, европейским компаниям стоит уделять особое внимание вопросам, связанным с защитой от киберпреступности (ITnews).

В опубликованном отчете «Прогноз в отношении угроз нарушения информационной безопасности в 2017 г.», подготовленном Центром операционной безопасности Fujitsu2 (Fujitsu Security Operations Center) представлен список из 10 самых опасных угроз информационной безопасности для бизнеса. Среди них авторы документа особо выделяют неспособность

компаний реализовать базовые принципы обеспечения ИТ-безопасности, атаки на банковские приложения и «умные» города.

Основываясь на результатах мониторинга угроз нарушения информационной безопасности, эксперты компании Fujitsu пришли к выводу, что наиболее опасный фактор – неспособность компаний эффективно реализовать базовые процессы обеспечения ИТ-безопасности – также является самым простым в устранении. Специалисты считают, что недостаточная защита в будущем приведет к возникновению «брешей», отмечая что: «очень многие компании не выполняют простые – при этом очень важные – задачи, которые позволяют значительно снизить риски нарушения информационной безопасности».

Согласно отчету, неотложные меры, которые все компании должны предпринять для усиления защиты своих цифровых активов, включают установку патчей для устранения уязвимостей и предоставление доступа к критически важным системам только активным существующим пользователям. Более того, многие организации слишком легко предоставляют привилегии доступа обычным пользователям без особых на то причин. В результате, как отмечается в отчете Fujitsu, компании «неоправданно подвергаются риску потери данных, кражи данных и внешнему взлому своих систем».

Одну из уязвимостей эксперты Fujitsu связывают с зашифрованными каналами, которые предоставляют доступ извне к самым важным ИТ-системам. Эти каналы используются для того, чтобы предоставить удаленным сотрудникам доступ к корпоративным сетям, но когда данные перехватываются киберпреступниками, сами компании подвергаются большому риску. Так происходит из-за явления, которое Fujitsu описывает, как «мертвая зона, где атаки на зашифрованные каналы пропускаются по причине отсутствия проверки SSL-сертификатов».

Компании должны активнее управлять банковскими приложениями, которые привлекают внимание злоумышленников. Fujitsu прогнозирует, что в 2017 г. количество атак на банковские платежные системы увеличится, и ожидает распространение банковских троянских программ, нацеленных на старые и уязвимые офисные приложения. Несмотря на то, что международные банковские сети приходят к необходимости внедрения обязательных инструментов контроля, Fujitsu констатирует, что «киберпреступники по-прежнему имеют все возможности для того, чтобы повлиять на информационную защиту бизнеса».

«Умные» города также станут целью злоумышленников – эксперты Fujitsu отметили, что «многие протоколы, созданные для управления “smart”-устройствами, имеют собственные уязвимости». В результате, хакеры могут отключить «умные» сети освещения в масштабах целых городов.

Центр операционной безопасности Fujitsu, обеспечивающий защиту заказчиков путем определения, анализа и устранения угроз, также прогнозирует, что все более активное использование искусственного интеллекта и машинного обучения коренным образом изменит традиционный

подход к корпоративной защите. Системы на основе искусственного интеллекта позволяют мгновенно определять изменения, например, в моделях интернет-трафика. Системы раннего оповещения позволят специалистам в области информационной безопасности занять проактивную позицию в работе по сокращению рисков, чтобы устранять угрозы до того, как они станут реальными проблемами. Однако в отчете также говорится, что киберпреступники в свою очередь воспользуются преимуществами технологий искусственного интеллекта для создания принципиально новых типов атак.

Р. Норрис (Rob Norris), руководитель подразделения корпоративной и информационной безопасности компании Fujitsu в регионе EMEIA, говорит: «Каждый шаг на пути к усилению кибербезопасности подразумевает экспоненциальное снижение уязвимости. Многие организации еще не осознали, что вычислительные технологии играют важную роль для поддержания бизнеса. И кража или потеря данных может привести не только к финансовым рискам, но и подрыву репутации. В нашем новом отчете описаны несколько простых рекомендаций, которые помогут компаниям предотвратить потерю и кражу данных и нарушение безопасности информационных систем».

***

21.02.2017

Google и Bing будут бороться с пиратами

Знаменитые поисковые системы Google и Bing намерены бороться с пиратами в Великобритании (Телеграф).

Дискуссии по этому поводу велись еще в середине 2016 г. Администрация по защите интеллектуальной собственности разработала комплекс мер, которые направлены на борьбу с пиратскими организациями. Крупнейшие поисковые системы намерены сократить в поисковой выдаче количество сайтов с пиратским контентом. Эта инициатива проходит параллельно с другими «антипиратскими» мероприятиями.

По словам одной из сторон, эти мероприятия помогут выяснить действенность уже существующих методов борьбы с пиратами, вместо того, чтобы вводить новые. Великобритания всерьез занялась борьбой с пиратским контентом и уже удаляет огромное количество сайтов из поисковой выдачи. По словам Э. Левитена, директора Альянса интеллектуальной собственности, люди используют такие сайты не по собственному желанию. Они просто выбирают первое, что выдает поисковая система. Сейчас сайты скрываются из поисковой ленты по запросам правообладателя. Потому большое количество музыки, кино и другого контента в бесплатном доступе начинает сокращаться.

***

20.02.2017

Небезопасные Android-приложения для автомобилей повышают риск угона

В последние несколько лет концепция connected car (автомобили с доступом в Интернет) продолжает набирать популярность. С помощью специализированных мобильных приложений можно получить координаты автомобиля, его маршрут, открыть двери, запустить двигатель, включить вспомогательные устройства. В связи с этим специалисты «Лаборатории Касперского» попытались выяснить, насколько защищены автомобильные приложения (InternetUA).

С этой целью эксперты изучили семь популярных мобильных приложений для управления различными марками автомобилей (наименования не раскрываются), в том числе одно от российского производителя. При этом рассматривался ряд аспектов: наличие потенциально опасных возможностей (т. е. позволяет ли приложение угнать авто); существование проверки на наличие прав суперпользователя на устройстве; есть ли защита от перекрытия (проверка, что после запуска устройства отображается интерфейс именно этого приложения); наличие контроля целостности (проверка на предмет изменений в коде).

Результаты оказались довольно печальными. Как выяснилось, у всех проанализированных приложений отсутствует обфускация кода, защита от перекрытия, а также нет проверок на наличие прав суперпользователя и контроля целостности. Кроме того, 6 приложений хранили учетные данные в незашифрованном виде (4 приложения – только логин, 2 – логин и пароль).

Как поясняют эксперты, теоретически после кражи учетных данных преступник сможет получить контроль над автомобилем, однако угнать транспортное средство не так просто. Для того чтобы начать движение на авто, обязательно наличие ключа. Попав в автомобиль, злоумышленники используют блок программирования и записывают в борт управления машины новый ключ. Учитывая, что все из вышеуказанных приложений позволяют разблокировать двери, угонщики могут проделать все операции быстро и скрытно.

***

21.02.2017
Українські компанії зазнали масштабного кібершпіонажу

Міжнародна компанія в сфері безпеки CyberX виявила сліди проведення масштабної операції з кібершпіонажу в Україні. За допомогою шкідливого ПО, яке експерти назвали BugDrop, хакери могли дистанційно записувати розмови в українських компаніях через мікрофони, вбудовані в ноутбуки і мобільні гаджети, повідомляє AIN.UA з посиланням на повідомлення CyberX (LB.ua).

За даними CyberX, в рамках операції BugDrop жертвами кібершпигунів стали вже як мінімум 70 компаній в різних сферах, включаючи критично важливі об’єкти інфраструктури, засоби масової інформації і науково-дослідні інститути. Метою зловмисників було здобуття конфіденційної інформації: записів розмов, скріншотів, документів і паролів, збережених у браузері.

Сліди BugDrop виявлені в Саудівській Аравії, Австрії і Росії, проте абсолютна більшість об'єктів атаки були розташовані в Україні. Відзначається, що особливо помітна активність кампанії в ДНР та ЛНР.

Вірусні файли відправлялися користувачам за допомогою фішингових електронних листів, які закликали відкривати файл Microsoft Word: саме він містив шкідливий макрос.

Якщо макроси у користувача були вимкнені, їх пропонувалося включити у діалоговому вікні, що спливало: «Увага! Файл створено в більш новій версії програми Microsoft Office. Передусім потрібно увімкнути макроси для коректного відображення вмісту документа». За допомогою декількох дій на комп'ютер користувача завантажувалося додаткове шпигунське ПЗ, яке могло красти величезний масив даних: файли форматів doc, docx, xls, xlsx, ppt, pptx, pdf, zip, rar, db, txt з самого комп'ютера і під'єднаних зовнішніх накопичувачів, а також всю інформацію про пристрій (ім'я, IP, софт і т.д.). Також зловмисники отримували доступ до мікрофона: це дозволяло їм записувати розмови користувача.

Перед тим, як файл завантажувався на Dropbox, він шифрувався за допомогою алгоритму Blowfish. Після скачування документів з Dropbox, файли зі сховища видалялись.

Точно сказати, хто стоїть за атаками і чи могли вони спонсоруватися іншою державою, в CyberX не можуть. Однак експерти відзначають, що BugDrop відрізняється своєю масштабністю і кількістю людських і матеріально-технічних ресурсів, необхідних для аналізу величезних обсягів неструктурованих даних, які були вкрадені під час операції.

Атаки BugDrop були спрямовані на компанії, які розробляють системи дистанційного моніторингу для інфраструктур нафто- і газотранспорту; міжнародні організації, які ведуть моніторинг дотримання прав людини, боротьби з тероризмом і кібератаками на критичну інфраструктуру в Україні; інжинірингові компанії, які розробляють електропідстанції, розподільні газопроводи і системи водопостачання; науково-дослідні інститути; редакторів українських газет.

На думку експертів, це був лише перший етап операції. Імовірно, хакери провели розвідку на об'єктах, щоб визначити, де вдасться організувати нові диверсії.

***

22.02.2017

Хакеры слили переписку Лещенко с наследницей Манафорта

Хакерская группа Anonymous опубликовала в сети переписку Дж. Манафорт с человеком, почта которого предположительно принадлежит нардепу С. Лещенко, передает Корреспондент (From-UA Новости Украины).

В 2016 г. С. Лещенко озвучил теневые расходы Партии регионов, согласно которым тогдашний глава предвыборного штаба Д. Трампа П.

Манафорт неофицально получил от них миллионы долларов. Позже в НАБУ признали компромат на Манафорта фальшивкой, однако к тому времени он уже уволился из штаба Д. Трампа.

«Мне нужно связаться с Полом и я должен поделиться одной важной информацией, которая касается его участия в украинском расследовании. У меня есть неопровержимые доказательства того, что он получал деньги», – пишет нардеп.

При этом С. Лещенко якобы шантажирует ее, грозя передать доказательства в ФБР.

«Если я не получу от вас никакого ответа, я передам их в ФБР и украинские органы, включая медиа. Скажите ему, что у него есть 24 часа прежде чем я опубликую всю информацию правоохранителям. Как только он свяжется со мной, я перешлю вам документы», – якобы написал С. Лещенко.

На фоне якобы полученного Джессикой сообщения от Лещенко можно заметить, как она проинформировала об этом инциденте своего отца.

«Я думала, что это спам и не обратила внимания. Что мама об этом скажет?», – написала она.

Журналист А. Дзиндзя в Twitter отмечает, что автор письма предлагает контактировать с ним по адресу leshchenko@mail.ru, который принадлежит именно С. Лещенко, что подтверждают фотографии во время заседания Верховной Рады Украины.

***

22.02.2017

Россия признала наличие у нее кибервойск

В России официально появились кибервойска. О формировании в стране так называемых «войск информационных операций» сообщил министр обороны РФ С. Шойгу, выступая сегодня в Госдуме. При этом в российском парламенте до последнего времени опровергали сообщения о том, что в стране существуют кибервойска (Главное .ua).

Так, глава комитета Совета Федерации по обороне и безопасности В. Озеров заявил 10 января агентству «Интерфакс», что кибервойск в структуре Вооруженных сил РФ не существует. «Как таковых кибервойск в структуре Вооруженных сил у нас нет. Но согласно доктрине информационной безопасности РФ, конечно, перед государством стоит задача защиты собственной информации», – сказал сенатор.

В свою очередь, газета «Коммерсант» еще 10 января опубликовала исследование международной компании Zecurion Analytics, согласно которому Россия входит в ведущую пятерку стран по численности и финансированию кибервойск, которые занимаются шпионажем, кибератаками и информационными войнами.

Согласно данным компании и источникам издания на рынке информационной безопасности, численность российских кибервойск

насчитывает примерно 1000 человек, а их финансирование может ежегодно составлять около 300 млн долл.

***

22.02.2017

Чорногорія заявила про потужні кібератаки на сайти держустанов і ЗМІ

Веб-сайти уряду Чорногорії і деякі державні установи, а також деякі проурядові ЗМІ останніми днями зазнали потужних кібератак. Про це йдеться в заяві уряду Чорногорії, повідомляє Balkan Insight (LB.ua).

«Масштаби і різноманітність атак і той факт, що вони здійснюються на професійному рівні, вказують на те, що це були синхронні дії», – йдеться в заяві.

Зазначено, що вперше офіційні веб-сайти і мережева інфраструктура зазнали серйозної кібератаки в день парламентських виборів у Чорногорії 16 жовтня 2016 р. Тоді в кібератаці було виявлено російський слід.

Нові значні атаки, які уряд визначив як інтенсивніші, ніж ті, які були в жовтні, почалися 15 лютого і сягнули свого піку наступного дня, однак тривали також і в минулі вихідні.

Уряд країни повідомив, що співпрацює з колегами з країн-партнерів над виявленням та ідентифікацією зловмисників.

«Той факт, що атака спрямована на сайти уряду й інших державних органів, а також деякі чорногорські ЗМІ, як це було зроблено в день виборів у жовтні, викликає підозру щодо мотивів. Мета таких дій полягає в тому, щоб відключити обмін інформацією між чорногорцями та міжнародною громадськістю», – зазначили в уряді.

У Чорногорії після кібератак у жовтні оголосили про плани посилити кібербезпеку, щоб захистити дані уряду.

***

23.02.2017

Программу TeamViewer снова превратили в шпионский инструмент

Занимающаяся информационной безопасностью компания Heimdal сообщает, что в выходные была зафиксирована новая кампания по распространению спама, несущая с собой вредоносное приложение TeamSpy. Эта программа способна дать хакерам полный доступ к пострадавшим от неё компьютерам (InternetUA).

Это приложение уже проявило себя в 2013 г., заразив множество ПК. Тогда злоумышленники собирали информацию относительно своих жертв, как обычных людей, так и высокопоставленных сотрудников различных компаний, организаций и даже у дипломатов. На этот раз, судя по всему, приложение TeamViewer не было скомпрометировано, так что повторное использование

паролей не несёт с собой риска, хотя делать так не рекомендуется. Хакеры используют методы социальной инженерии и заставляют пользователей установить вредоносную программу.

Пользователь получает письмо с вложенным архивом Zip, который при распаковке активирует файл .exe. TeamSpy попадает на компьютер в виде файла DLL. Заголовок письма гласит 1408581 **. Как и раньше, злоумышленники ставят на компьютер обычную версию программы TeamViewer и после этого меняют её поведение при помощи DLL, чтобы скрыть следы своей деятельности. Программа TeamSpy содержит различные компоненты приложения TeamViewer, в их число входят кейлоггер и TeamViewer VPN.

Логи сохраняются в файл, куда добавляются все имена и пароли пользователей, файл постоянно отправляется на командный сервер. Программа способна обойти двухфакторную аутентификацию и может дать доступ к зашифрованному контенту, который пользователи расшифровывают у себя на компьютере.

Уровень обнаружения приложения антивирусами пока низкий – 15/58. Среди находящих его антивирусов можно назвать антивирус Касперского, ESET, Cyren, McAfee, Microsoft, Sophos и Symantec.

Предположительно, атака только набирает обороты. Пользователям не рекомендуется открывать файлы от неизвестных получателей, переходить по ссылкам и открывать вложенные файлы.

***

22.02.2017

Конфиденциальность пользователей Windows 10 все еще в опасности

Европейский орган надзора, обеспечивающий соблюдение законодательства о защите персональных данных, по-прежнему обеспокоен вопросами, связанными с параметрами конфиденциальности в Windows 10. По мнению регулятора, несмотря на недавние изменения, внесенные в Windows 10, настройки обработки персональных данных во время установки системы все еще не имеют надлежащих объяснений и Microsoft должна исправить это (InternetUA).

В прошлом году в Microsoft был направлен аналогичный запрос, в результате чего компания изменила процесс первичной настройки операционной системы, добавив новые опции для ограничения или запрета на сбор частной информации. По-видимому, этого оказалось недостаточно.

Теперь регулятор утверждает, что Microsoft должна объяснить более ясно, какие персональные данные обрабатываются и для каких целей. Отсутствие этих объяснений делает недействительным любое согласие пользователя, отмечает регулятор. Компания пока никак не отреагировала на новые возражения «старого континента».

Ряд национальных органов стран ЕС уже начали расследование в отношении Windows 10. К примеру, Франция еще в июле прошлого года велела Microsoft остановить чрезмерный сбор пользовательских данных.

***

22.02.2017

Українські хакери знайшли російський слід в антиукраїнських акціях у Польщі

Завдяки роботі українських «хактівістів» «Кіберхунта» і «Українського Кіберальянсу» (UCA) волонтерам InformNapalm потрапив до рук дамп пошти одного з сірих кардиналів російської зовнішньої політики в Східній Європі. З'ясувалось, що білорус активно займався організацією антиукраїнських акцій в Польщі та інших країнах Східної Європи (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»).

Волонтери нагадують, що в останні кілька місяців відносини України і Польщі несподівано почали псуватися: у Польщі пройшло кілька антиукраїнських акцій, деякі польські політики знову заговорили про Волинську різанину і почали вимагати від України перегляд своєї історії. У свою в чергу, в Україні хтось почав валити польські пам'ятники.

І ось піля кропіткої роботи волонтери InformNapalm опублікували переписку, яку отримали від українських «хактівістів» «Кіберхунти» і «Українського Кіберальянсу».

Вони зазначають, що громадянин Білорусі О. Усовський, завзятий любитель «русского мира», який неодноразово публікувався на сайті медведчуківського «Українського вибору», активно займався організацією антиукраїнських акцій в Польщі та інших країнах Східної Європи. У реалізації проектів йому допомагало офіційне прикриття – фіктивна недержавна організація «Східноєвропейська культурна ініціатива», яка була зареєстрована в столиці Словаччини в кінці 2013 р. При цьому О. Усівський шукав джерела фінансування, і навіть звертався за грошима в структури ЄС.

Також О. Усовський співпрацював із відомим українофобом К. Затуліним, а згодом – із представником польських націоналістів Dawid Berezicki (OWP, Obóz Wielkiej Polski, Табір Великої Польщі).

З наведеного хакерами листування аналітики роблять висновок, що у Східній Європі активно діють проросійські недержавні організації, які під виглядом культурних, дискусійних і аналітичних майданчиків аналізують ситуацію з метою проведення проросійських акцій.

Часто на перший погляд ці заходи не носять відверто проросійський характер. Однак, таким чином вербується і прикормлюється мережа проросійських елементів у Східній Європі.

Починається все з нешкідливих пікетів проти дій української армії на Донбасі чи зборів допомоги Новоросії, а потім переходить в обговорення з представниками різних політичних сил антиукраїнських акцій. І несподівано по

всій Польщі прокочуються антиукраїнські акції, які одночасно хтось в Україні підігріває вандалізмом польських поховань.

«Русскій мір» росіяни будуть просувати будь-яку ціну і судячи з сум, на ціні їм не залежить.

***

23.02.2017

Новая вредоносная кампания атакует пользователей Chrome

Специалист компании Malwarebytes Ж. Сегура (Jérôme Segura) сообщил о новой вредоносной кампании,затрагивающей пользователей Google Chrome. В ходе кампании злоумышленники используют всплывающие сообщения Add Extension to Leave для перенаправления жертв на web-сайт, с которого они не могут уйти, пока не загрузят и установят предлагаемое расширение Chrome (InternetUA).

После установки расширение выполняет несколько действий. Прежде всего, программа блокирует доступ пользователя к страницам chrome://extensions и chrome://settings. При попытке открыть разделы произойдет автоматическое перенаправление на страницу chrome://apps.

Также расширение перехватывает трафик и перенаправляет жертву на вредоносные сайты при обнаружении определенных ключевых слов в адресе сайта, который пользователь пытается посетить. Перенаправление происходит на различные типы ресурсов – от подозрительных сайтов, предлагающих быстрые способы обогащения до фальшивых сайтов техподдержки.

По словам Ж. Сегуры, такое поведение вызывает некоторое удивление, поскольку большинство вредоносных кампаний перенаправляют пользователей на страницы, содержащие наборы эксплоитов, которые, в свою очередь, доставляют более опасное вредоносное ПО – криптовымогателей, банковские трояны, нежелательное рекламное ПО и т. д.

***

23.02.2017

В Україні викрили групу хакерів, яких координували з Росії

СБУ спільно з поліцією припинили протиправну діяльність осередку міжнародного хакерського угруповання «кардерів», до складу якого входили чотири мешканці Дніпропетровщини (Західна інформаційна корпорація).

Про це 23 лютого інформує прес-центр СБУ.

Зловмисники отримували доступ до рахунків клієнтів іноземних та вітчизняних банківських установ та підробляли платіжні картки. Діяльність хакерів координувалася з боку Російської Федерації, а потерпілими були клієнти банків ЄС, США та України. Також зловмисники отримували несанкціонований доступ до облікових записів соціальних мереж та

електронних поштових скриньок, відомості з яких використовувались для шахрайських дій.

Під час обшуків правоохоронці вилучили спеціалізоване телекомунікаційне обладнання, що використовувалось у протиправній діяльності, персональні комп'ютери та засоби зв'язку, чимало магнітних карток з даними про банківські рахунки (так званий «білий пластик»), а також шкідливе програмне забезпечення та незаконно отримані дані банківських карток. Відкрито кримінальне провадження за ч. 2 ст. 190 (шахрайство) Кримінального кодексу України. Тривають невідкладні слідчі дії із встановлення клієнтів банків, які постраждали від протиправної діяльності.

***

23.02.2017

На Дніпропетровщині спіймали групу кардерів

Служба безпеки України затримала в Дніпропетровській області чотирьох підозрюваних у крадіжці банківських даних через Інтернет і в підробці платіжних карток. Про це повідомила прес-служба СБУ (LB.ua).

Стверджують, що затримані незаконно отримували доступ до рахунків клієнтів іноземних і вітчизняних банків і підробляли їхні картки. Діяльність хакерів координувалася з боку Росії, а потерпілими були клієнти банків Євросоюзу, США й України.

Також вони отримували несанкціонований доступ до облікових записів у соціальних мережах і до поштових скриньок, відомості з яких використовували для шахрайських дій.

Під час обшуків правоохоронці вилучили спеціалізоване телекомунікаційне обладнання, яке використовувалося у протиправній діяльності, персональні комп'ютери і засоби зв'язку, магнітні картки з даними про банківські рахунки (т. зв. «білий пластик»), а також шкідливе програмне забезпечення і незаконно отримані дані банківських карток.

Відкрито кримінальне провадження за ч. 2 ст. 190 (шахрайство) Кримінального кодексу.

***

22.02.2017

В Ровенской области арестовали торговца персональными данными через Интернет

Об этом сообщает Департамент киберполиции Нацполиции Украины в Facebook (InternetUA).

В ходе мониторинга сети Интернет, работниками отдела противодействия киберпреступности в Ровенской области выявлено, что на одном из интернет-площадок было размещено предложение по продаже баз данных

Государственного реестра физических лиц, которая содержит информацию с ограниченным доступом (конфиденциальные данные граждан).

Задержанный с целью получения прибыли сбывал базу данных со сведениями о гражданах Украины в том числе ФИО, место, дата рождения и адрес проживания. Стоимость такой базы «продавець» оценивал в 1000 грн.

В квартире у мужчины было обнаружено два ноутбука, три носителя информации и другие вещи, подтверждающие преступную деятельность.

***

27.02.2017

Крупнейший спамерский ботнет в мире обзавелся функциональностью для DDoS-атак

Мы неоднократно писали о ботнете Necurs, ведь это один из крупнейших ботнетов в мире, который, например, в одиночку способен значительно влиять на уровень спама в мировом почтовом трафике. По данным специалистов компании Cisco, многие IP-адреса, от которых исходит Necurs-спам, заражены уже более двух лет. При этом операторы ботнета стараются действовать осторожно, к примеру, хосты задействуют для рассылки писем на два-три дня, а затем не используются на протяжении двух-трех недель (InternetUA).

Аналитики AnubisNetworks Labs опубликовали отчет, согласно которому операторы Necurs ищут новые пути мотенизации имеющейся в их распоряжении мощности. Как оказалось, почти полгода назад ботнет получил новый прокси-модуль и обзавелся функциональностью, необходимой для проведения DDoS-атак. Впервые данный модуль был замечен в сентябре 2016 г., но исследователи пишут, что анализ кода позволил определить более точную дату его создания – это 23 августа 2016 г.

Модуль был классифицирован как доступный по требованию прокси-сервер, который способен перенаправлять трафик через зараженные хосты, используя для этого протоколы HTTP, SOCKSv4 и SOCKSv5. Лишь недавно исследователям удалось понять, что новая функциональность связана с DDoS-атаками. Эксперты зафиксировали странный трафик, исходящий от зараженных Necurs компьютеров: машины обращались не только стандартному для модулей 80 порту, но и к порту 5222, используя другой протокол. Расследование этой аномалии показало, что прокси-модуль может получать команды, которые приказывают ботам атаковать определенную цель посредством HTTP- или UDP-флуда.

Пока эксперты не зафиксировали ни одной DDoS-атаки, исходящей от Necurs, но специалисты AnubisNetworks Labs выражают беспокойство из-за потенциальной мощности DDoS-атак, идущих от такого ботнета.

«Все это крайне интересно, учитывая размеры Necurs (крупнейший ботнет, оснащенный данным модулем, начитывает более миллиона активных ботов в сутки). Ботнет такой величины способен осуществить крайне мощную DDoS-атаку», – пишут исследователи.

Размеры Necurs действительно впечатляют. К примеру, ответственность за мощнейшие DDoS-атаки конца 2016 г. и начала 2017 г. лежит на IoT-малвари Mirai, но самый большой известный Mirai-ботнет насчитывает лишь 400 000 устройств. Хотя, стоит учитывать, что большинство ботов Necurs – это обычные компьютеры. Операторы таких ботнетов редко устраивают разрушительные DDoS-атаки, опасаясь привлечь слишком пристальное внимание правоохранительных органов. В основном такие ботнеты используются для распространения спама, а через него малвари, к примеру, банкера Dridex или шифровальщика Locky.

При этом некоторые эксперты полагают, что модуль для DDoS-атак появился в составе Necurs вовсе не для монетизации подобных атак. Э. Шумейкер (Andy Shoemake), глава компании NimbusDDoS, которая занимается тестированием сервисов и DDoS-симуляциями говорит:

«Думаю, DDoS-функциональность могла не предназначаться для извлечения финансовой выгоды посредством вымогательства. Мотивация [операторов ботнета] могла отличаться, и функциональность предназначена для других, менее рискованных сценариев, возможно, даже для атак на других хакеров».

Независимый ИБ-исследователь MalwareTech, который много лет следит за эволюцией Necurs, тоже считает, что масштабных атак от ботнета ждать не приходится. Эксперт считает, что с учетом возраста DDoS/прокси-модуля, тот мог предназначаться для заработка, но если до сих пор не было зафиксировано ни одной атаки, значит, операторы малвари, вероятнее всего, пришли к выводу, что заниматься спамом все-таки выгоднее.

***

27.02.2017

Базиленко Анна

Через баг на сервісі Cloudflare стався масштабний витік даних користувачів

Сервіс Cloudflare, що надає послуги оптимізації і захисту трафіку, повідомив, що через випадкову помилку стався витік даних клієнтів (Watcher).

Утім, баг виявив співробітник Google Т. Орманді. Він працював над власним проектом і помітив, що при зверненні до Cloudflare сервіс повертає не тільки дані за запитом, але і дані інших ресурсів, в тому числі API-ключі, файли cookie, паролі, особисті повідомлення з великих сайтів знайомств, кадри з веб-чатів, дані кредитних карток тощо. Помітивши баг, Т. Орманді звернувся до розробників сервісу.

У Cloudflare провели розслідування і підтвердили, що баг таки є. Причина витоку – в підключенні до сервісу AMP (Accelerated Mobile Pages) – розробки Google, що поліпшує швидкість завантаження сторінок у мережі. Під час підключення відбувався збій: сторінки створювалися з помилками, оскільки деякі з функцій Cloudflare не були оптимізовані під нову технологію. У

результаті частина даних з таких сторінок відправлялася з серверів компанії в пошукові системи.

На HitHub виклали список з усіма сайтами, які могли постраждати, а це понад 4,2 млн ресурсів. Серед них є і українські. Зокрема, у AIN нарахували більше 7 тис. сайтів з доменним ім'ям .ua.

Постраждати могли і відомі компанії та бренди, зокрема Fitbit, Uber і OKCupid. Наприклад, фрагмент інформації про поїздку Uber чи пароль з цього сервісу міг потрапити в код іншого сайту, не пов'язаного із Uber.

Наразі помилка виправлена. Однак, як повідомили у Cloudflare, частина інформації встигла просочитися в кеш пошукових систем, тому представники сервісу звернулися до Google, Bing, Yahoo та інших компаній, аби в разі необхідності вручну усунути наслідки ймовірної витоку.

У компанії радять змінити паролі до електронної пошти, соцмереж та популярних онлайн-сервісів.

***

26.02.2017

Google раскрыла ещё одну уязвимость Windows

Компания Google опубликовала информацию относительно очередной незакрытой уязвимости на платформе Windows. Политика её программы поиска багов Project Zero позволяет раскрывать информацию через 90 дней после того, как разработчик программного обеспечения был поставлен в известность о существовании уязвимости (InternetUA).

Уязвимость относится к путанице типов (type confusion) в модуле браузеров Edge и Internet Explorer. Инженер Google И. Фратрич опубликовал доказательство концепции, результатом может стать падение браузеров, что открывает дверь перед получением злоумышленниками прав администратора на уязвимых системах.

И. Фратрич проанализировал 64-разрядную версию Internet Explorer на Windows Server 2012 R2, но эта же уязвимость есть в 32-разрядных Internet Explorer 11 и Edge в системах Windows 7, Windows 8.1 и Windows 10. Сообщено о ней было 25 ноября, поэтому 25 февраля в Google посчитали возможным рассказать о ней.

***

26.02.2017

Только у 3 % компаний есть необходимые средства для борьбы с кибератаками

Исследователи Tripwire и Dimensional Research провели опрос среди 403 IT-специалистов, работающих в крупных компаниях (с 1000 и более сотрудников) в США, Великобритании, Канаде и странах Европы с целью обозначить главные угрозы безопасности в 2017 г. (InternetUA).

Согласно опросу, только 3 % компаний обладают необходимыми технологиями и 10 % – необходимыми навыками для противостояния наиболее распространенным кибератакам. По мнению IT-специалистов, наибольший материальный ущерб в текущем году может причинить вымогательское ПО. Только у 44 % компаний есть нужные средства, а у 43 % – нужные навыки для борьбы с данной угрозой.

По словам 68 % респондентов, они могут эффективно противостоять фишингу, а 60 % способны успешно отражать DDoS-атаки. С проблемой инсайдерских угроз справляются 48 % участников опроса, 45 % способны отражать атаки с эксплуатацией уязвимостей, а 44 % уверены в своей возможности бороться с троянами-шифровальщиками.

Касательно наличия у компаний технологий для борьбы с вышеупомянутыми угрозами ответы IT-специалистов несколько отличаются. Лучше всего организации подготовлены к DDoS- (63 %) и фишинговым (56 %) атакам. 43 % обладают необходимыми средствами для борьбы с вымогательским ПО, 41 % – для предотвращения инсайдерских угроз и 40 % – для отражения атак с эксплуатацией уязвимостей.

По мнению 64 % опрошенных, в 2017 г. жертвами хакеров чаще остальных будут становиться финансовые сервисы. IT-специалисты американских компаний больше всего обеспокоены угрозами атак на организации здравоохранения, а европейских – на телекоммуникационные компании.

«Как показывают результаты исследования, только небольшое число организаций обладают всем необходимым для отражения наиболее распространенных типов атак. Многие компании могут противостоять одной или двум угрозам, но реальность такова, что им нужно бороться со всеми угрозами», – отметил старший директор по IT-безопасности Tripwire Т. Эрлин (Tim Erlin).

***

28.02.2017
Анна Дзюба, представник прес-служби Програми SAFE CARD
«Пастки» в мережі: шахрайські сайти крадуть гроші

Злодії вивідують карткові дані громадян, маскуючись під веб-ресурси платіжних сервісів і банків.

Наразі в Україні стрімко зростає кількість злочинних операцій в Інтернеті, пов’язаних з виманюванням реквізитів платіжних карток під виглядом надання неіснуючих послуг на шахрайських веб-ресурсах (фішингові сайти). Мета злодія – змусити користувача ввести дані своєї картки в спеціальній платіжній формі на злочинному ресурсі. У результаті обіцяні послуги не надаються, а дані картки зберігаються в шахраїв. Лише за 2016 р. кількість зафіксованих в Україні шахрайських сайтів зросла в 4,5 раза – з 38 до 174 (Утренний город).

Для крадіжок грошей з карток сьогодні кіберзлодії пропонують громадянам скористатися найрізноманітнішими «послугами» в Інтернеті (від придбання дешевих авіабілетів до онлайн-кредитування на картку). Найчастіше шахраї використовують «фейкові» сайти з поповнення мобільного рахунку (35 %), переказу грошей з картки на картку (10 %) і ресурси, які нібито надають обидві ці послуги (16 %). Ще 27 % – це сайти-підробки під Portmone, 11 % – шахрайські ресурси, що маскуються під офіційні web-сторінки інших платіжних сервісів.

Такі злочинні сайти регулярно відслідковуються й закриваються фахівцями – більшості фішингових сайтів вдається проіснувати тільки кілька тижнів, у деяких випадках – лише кілька днів. Проте за цей час шахраї встигають спіймати «на гачок» чималу кількість необачних власників карток. Лише за декілька днів роботи один такий ресурс виманює дані 800–2500 карток громадян. Для того щоб заманити жертву, злодії підвищують рейтинги своїх шахрайських сайтів, використовуючи контекстну рекламу. Таким чином, фішингові сайти можуть опинятися на перших сторінках Google або Yandex під час пошукових запитів на зразок «поповнити мобільний» чи «перевести гроші на картку».

У рамках Національної програми сприяння безпеці електронних платежів і карткових розрахунків Safe Card експертами Української міжбанківської Асоціації членів платіжних систем ЄМА створена інфографіка для громадян про те, як розпізнати такі шахрайські веб-ресурси і як діяти в разі усвідомлення, що карткові дані вже потрапили «до рук» злочинця.

Експерти виокремлюють ряд ознак, за якими можна розпізнати фішинговий сайт:

– це новий сайт, у якого відсутня репутація (немає відгуків та іншої інформації про сервіс в Інтернеті);

– вітчизняний платіжний або банківський сайт зареєстровано не на домені національного рівня (.UA). Якщо веб-ресурс зареєстрований на домені, на якому немає обмежень для реєстрації (.ru, .com.ua, .in.ua, .pp.ua, .kiev.ua, .dp.ua,. te.ua, .org , .net, .com, .info, .biz, .top, .in, .cc і т.д.), то його можна вважати потенційно небезпечним;

– сайт було створено нещодавно й зареєстровано лише на один рік;

– дані картки ніяк не маскуються під час введення (легітимні сервіси зазвичай маскують введення карткових реквізитів, наприклад, «зірочками» або використовують віртуальну клавіатуру).

Для захисту коштів від фішингових злодіїв необхідно дотримуватися наступних рекомендацій:

– користуватися лише відомими й перевіреними платіжними сайтами;

– перед введенням своїх карткових даних на сайті завжди перевіряти відгуки про нього в Інтернеті. Особливо пильно необхідно перевіряти web-ресурси з поміткою «Реклама»;

– перевіряти вік і термін реєстрації сайту. Для цього необхідно в адресному рядку браузера ввести «whois.com\whois\назва сайту» та звернути увагу на дати «created» і «expires»;

– перед користуванням послугами ресурсу впевнитися, що він не входить до списку фішингових сайтів – «Чорний список сайтів» (перелік виявлених шахрайських ресурсів, що регулярно доповнюється).

У разі підозри, що карткові реквізити могли бути перехоплені на шахрайському сайт, і необхідно негайно звернутися до банку та заблокувати картку, аби кошти не могли дістатися кіберзлодіям.

Навіть якщо громадяни не потрапили до пастки злодія, але була спроба заволодіння їхніми коштами, потрібно повідомити про інцидент у кіберполіцію, найпростіший спосіб – через форму на сайті Департаменту кіберполіції Національної поліції України.

Крім того, у разі виявлення будь-яких ознак шахрайського сайту варто повідомити про існування небезпеки, аби інші громадяни не потрапили до такої «пастки». У рамках проекту з виявлення й закриття фішингових ресурсів на сайті Асоціації ЄМА (ema.com.ua) реалізовано функціонал «Повідомити про фішинговий сайт», за допомогою якого можна проінформувати Асоціацію про підозрілий веб-сайт. Отримана інформація оперативно розглядається спеціалістами. У разі підтвердження загрози вживаються відповідні заходи для її ліквідації.

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник Терещенко Ірина

Редактор Оксана 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.