СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(6–20.06)

2016 № 9

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(6–20.06)
№ 9

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

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

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2016

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

8.06.2016

Instagram потрапив в ТОП-25 сайтів, що відвідують українці. Російські проекти продовжують домінувати в ТОП-5

У ТОП-5 найпопулярніших сайтів, якими користувались українці в травні 2016 р., продовжують перебувати три російські – «ВКонтакте», «Яндекс» та Mail.ru. Про це свідчать дані щомісячного дослідження CMeter компанії TNS, пише Watcher.

	Сайт	Охоплення за квітень 2016, (%)	Охоплення за травень 2016, (%)
1	google.com.ua	66,8	65,2
2	vk.com	66,1	64,9
3	youtube.com	62,9	61,7
4	mail.ru	56,3	54,9
5	yandex.ua	48,8	48,6
6	olx.ua	46,6	46,2
7	facebook.com	43,9	43,1
8	wikipedia.org	43,8	42,7
9	privatbank.ua	42,1	**40,3**
10	odnoklassniki.ru	36,6	36,3
11	rozetka.com.ua	34,2	33,4
12	prom.ua	33,7	32,1
13	sinoptik.ua	30,4	29,3
14	ukr.net	24,8	23,8
15	blogspot.com	23,0	22,8
16	kinogo.net	21,3	22,4
17	gismeteo.ua	22,8	21,8
18	aliexpress.com	22,3	21,7
19	ex.ua	20,2	20,5
20	i.ua	20,0	19,7
21	segodnya.ua	16,2	17,2
22	kinopoisk.ru	16,2	16,8
23	livejournal.com	15,9	16,6
24	tsn.ua	16,9	15,9
25	instagram.com	15,0	15,7

У травні традиційно спостерігаються зниження охоплень усіх сайтів, що пов’язано з затяжними вихідними і травневими святами, під час яких люди проводять більше часу оффлайн.

У травні в ТОП-25 потрапив Instagram.com з охопленням 15,7 %, а також LiveJournal.com 16,6 %, і випали Aukro.ua з Novaposhta.ua.

***

10.06.2016

90 % українських користувачів Інтернету активно користуються принаймні однією соціальною мережею

Серед українських користувачів Інтернету 90,7 % стверджують, що активно користуються принаймні однією соціальною мережею. Серед найбільш популярних – «ВКонтакте» (59,2 %), «Одноклассники» (50 %), Facebook (38,3 %) і Google+ (33,4 %). Про це свідчать результати опитування Київського міжнародного інституту соціології, пише Watcher.

Як стало відомо, 42,5 % українців у віці 18 років і старші практично щодня користуються Інтернетом, ще 17 % – декілька разів на тиждень.

36,1 % українців зазначили, що отримують інформацію політичного характеру з Інтернету, ще 32,7 % – із соціальних мереж. Дослідження також з'ясувало рівень довіри українців до джерел отримуваної інформації. Інтернет та соціальні мережі серед лідерів джерел інформації політичного характеру, яким «повністю довіряють» – таких 17,4 % українців.

***

15.06.2016

Основним джерелом новин для молоді є соцмережі, – дослідження

Соціальні мережі витісняють телебачення як основне джерело новин у молодіжному середовищі, пише Західна інформаційна корпорація.

Про це з посиланням на доповідь Інституту журналістики Рейтер Оксфордського університету повідомляє російська служба BBC.

Під час опитування молоді люди у віці від 18 до 24 років підтвердили, що 28 % з них черпають новини в основному із соцмереж, у той час як телебачення залишається головним джерелом інформації для 24 %.

Звіт складений на основі опитування міжнародної маркетингової компанії YouGov, яке щорічно проводиться протягом останніх п'яти років у 26 країнах, включаючи Велику Британію, США, Австралію, Канаду, Бразилію, Скандинавські країни, Австрію, Чехію, Грецію, Францію, Іспанію, Італію, Туреччину, а також Південну Корею і Японію.

У ньому беруть участь 50 тис. осіб, у тому числі 2 тис. британців.

Однак жителі Росії, Китаю і деяких інших великих країн участі в опитуванні не беруть.

Автори звіту дійшли висновку, що 51 % людей, які мають доступ до Інтернету, використовують соцмережі для того, щоб дізнатися про основні події дня.

Ця тенденція, як і популярність мобільних телефонів з можливістю виходу в Інтернет, змінюють сформовані бізнес-моделі.

Автори звіту попереджають, що медійні організації зіткнулися з «другою руйнівною хвилею», яка потенційно може мати далекосяжні наслідки як для новинної індустрії, так і для видавців.

Facebook та інші соцмережі перестали бути «одним з місць, де можна дізнаватися щось нове», перетворившись на основне джерело новин.

Отримання інформації про останні події із соцмереж особливо популярно в молодіжному середовищі та серед жінок.

Водночас тиражі друкованих газет продовжують падати, а споживачі як і раніше не хочуть платити за новинний онлайн-контент.

Соціологи дійшли висновку, що Facebook є найбільш популярною платформою: 44 % опитаних використовують його для того, щоб дивитися і коментувати поточні новини, а також ділитися ними з друзями.

На другому місці – YouTube (19 %), на третьому – Twitter (10 %).

Apple News зібрали 4 % користувачів у США і 3 % у Британії, тоді як месенджером Snapchat користуються не більше 1 % опитаних у більшості країн.

***

16.06.2016

Названы самые популярные соцсети в украинских СМИ

Facebook является самой упоминаемой социальной сетью в украинских масс-медиа. Второе место занимает сервис Twitter. Такие результаты получены в рамках специализированного исследования «Самые популярные соцмедиа в СМИ», проведенного информационно-аналитическим агентством «Контекст Медиа».

В этом году Facebook в различных украинских масс-медиа упоминался 400 809 раз. Входящие в первую тройку Twitter и «ВКонтакте» отмечались в СМИ 144 502 и 70 820 раз соответственно. Несколько меньше внимания было уделено YouTube (49 758), Instagram (35 726), «Одноклассникам» (20 576) и LinkedIn (1 342). Всего о популярных социальных медиа в этом году упоминали 723 533 раз, пишет Marketing Media Review.

Чаще остальных в связи со своей работой в СМИ упоминались Twitter, YouTube, «Одноклассники» и LinkedIn. «ВКонтакте», Instagram являлись генераторами информационных поводов. Facebook оказывался в центре внимания как в связи со своей деятельностью, так и в качестве площадки для публикации важных сообщений пользователей.

Одноклассники» и LinkedIn – единственные социальные сети, не попавшие в тройку самых популярных ни в одном типе украинских СМИ. Первый сервис самые крепкие позиции занимает в региональных интернет-ресурсах, значительно обходя по популярности YouTube и Instagram. Единственным типом масс-медиа, в котором Twitter не занимает лидирующие позиции в упоминаемости, является региональная пресса.

***

6.06.2016

Услід за Facebook і Twitter Instagram змінить алгоритм формування стрічки новин

Вже цього місяця стрічка новин в Instagram стане алгоритмічною за замовчуванням, ідеться в офіційному блозі соціальної мережі, пише Watcher.

Тестування нового алгоритму новинної стрічки, яка орієнтується на уподобання користувачів, почалось у березні цього року. Раніше публікації відображались у хронологічному порядку.

У компанії заявляють, що користувачі пропускають 70 % публікацій, якщо стрічка відображається в хронологічному порядку. «Ми з'ясували, що користувачі алгоритмічної стрічки новин більш активно взаємодіють з публікаціями і спільнотою», – коментують запуск у компанії.

***

6.06.2016

Медіакомпанії втрачають аудиторію у Facebook через новий алгоритм стрічки новин

Після налаштування нового алгоритму стрічки новин у Facebook медіакомпанії, які використовують майданчик соціальної мережі, почали активно втрачати інтернет-аудиторію, повідомляє Financial Times, пише Watcher.

Кількість переглядів кожного окремого матеріалу, опублікованого на офіційних сторінках компаній, впала з початку року на 42 %. Платформа SocialFlow, яка займається просуванням різноманітних матеріалів ЗМІ, зокрема Time, AP, Tribune, зазначає зменшення кількості переглядів публікацій у Facebook зі 117 тис. у січні до 68 тис. у травні 2016 р.

Як відомо, Facebook став першою соціальною мережею, яка відмовилася від простого хронологічного формату стрічки новин. Алгоритми соціальної мережі дають можливість відбирати найбільш цікаві для користувача матеріали і виводити їх «у топ». Таким чином, різко зростає популярність публікацій на персональних сторінках окремих користувачів, у той час як офіційні сторінки втрачають інтернет-аудиторію.

***

6.06.2016

Facebook и Яндекс могут стать партнерами

Поисковая система Яндекс и соцсеть Facebook начали переговоры о возможном партнерстве. Согласно данным от приближенного к российской компании источника, стороны рассматривают различные варианты совместного продвижения некоторых сервисов Яндекса для русскоязычной аудитории

Facebook. Кроме того, компании обговаривают возможность обмена пользовательскими данными в рекламных целях. Пока что обсуждение находится на предварительном этапе, пишет IGate.

По словам источника, Facebook заинтересованы в некоторых популярных сервисах – покупкой товаров, вызовом такси, подбором билетов в кино, бронированием отелей и так далее. Яндекс может выступить оператором этих сервисов для Facebook в России, так как подобные службы у поисковой компании уже есть. В свою очередь посетители соцсети смогут использовать сервисы Яндекса прямо в Facebook.

Кроме того, стороны рассматривают различные эксклюзивные условия для подписчиков Facebook, по типу бесплатного доступа к Яндекс.Музыке или скидки на поездки в Яндекс.Такси.

***

7.06.2016

Facebook тестирует функцию экономии трафика в Android-приложении

Известной проблемой Android-приложения Facebook является относительно высокое потребление мобильного трафика и заряда батареи. Похоже, крупнейшая социальная сеть обеспокоена таким положением дел: в настоящее время, как сообщается, компания тестирует в Android-приложении функцию «использовать меньше данных», пишет InternetUA.

Некоторые пользователи сообщают о появлении соответствующего переключателя в их приложениях. Впрочем, похоже, единственное, что делает эта функция – просто загружает изображения в пониженном разрешении для последующего вывода в ленте новостей. Разумеется, это должно благотворно отразиться на скачиваемых данных и может оказаться полезно для активных пользователей социальной сети, ограниченных в потреблении мобильного трафика. Впрочем, вполне вероятно, экономия достигается также другими средствами, но об этом в описании функции ничего не сообщается.

Любопытно, что переключатель разместился в самом верху многоуровневого меню Facebook, то есть функции выделено наиболее заметное место для привлечения внимания к новой возможности и широкого тестирования среди пользователей. Впрочем, с полноценным развёртыванием режима экономии данных он может быть запрятан глубже в меню настроек.

***

7.06.2016

Facebook заставляет пользователей устанавливать Messenger

Facebook хочет принудить пользователей установить Messenger для общения в реальном времени, убрав эту функцию из основного приложения, пишет InternetUA.

Многие пользователи получили уведомление (которое можно просто закрыть), в котором говорится, что для дальнейшего общения необходимо установить Messenger. Судьба чатов внутри основного приложения остается неизвестной. Скорее всего, компания хочет отказаться от них совсем в скором будущем.

***

8.06.2016

Twitter добавил три новых способа встраивания твитов на сайты

Социальная сеть Twitter представила обновленный функционал встраивания массивов твитов на сторонние сайты и в приложения, ожидая, что это нововведение станет полезным, в частности, для СМИ, сообщает интернет-издание Cossa, пишет Телекритика.

Первый способ – это опция Factory Functions, позволяющая генерировать ленту твитов для веб-версии приложений без ограничений по количеству встраиваний. Вторая опция позволяет использовать новый интерфейс oEmbed API для быстрой интеграции профайлов или коллекций хроник твитов прямо в CMS (Content Management Software – это система управления контентом).

Третий и самый простой способ заключается в использовании сервиса publish.twitter.com, который позволяет настраивать и интегрировать массивы твитов для сайта, требуя при этом минимальных навыков программирования. По словам разработчиков, этот способ лучше всего подходит пользователям WordPress.

Кроме того, в рамках обновления Twitter отменил необходимость создавать и сохранять виджеты в аккаунте: для пользователей, у которых они уже сохранены, доступ к ним остается в настройках.

***

9.06.2016

Додатки Facebook, Instagram, Twitter та Snapchat втрачають популярність серед користувачів

Користувачі стали витрачати менше часу на додатки соціальних мереж Facebook, Instagram, Twitter та Snapchat. Про це свідчать результати дослідження SimilarWeb за I квартал 2016 р., пише Watcher.

Отримані результати показали, що користувачі Instagram стали витрачати на додаток в середньому на 23,7 % менше часу у порівнянні з минулим роком, користувачі Twitter – на 23,4 %, Snapchat – на 15,7 %, Facebook – на 8 %.

Окрім того, користувачі стали рідше встановлювати ці додатки. За перші три місяці 2016 р. кількість завантажень усіх чотирьох сервісів впала в середньому на 9 % у порівнянні з аналогічним періодом минулого року.

Аналітики SimilarWeb зазначають, що зростання популярності месенджерів є головною причиною зниження інтересу до додатків зазначених

соціальних мереж. Зокрема, кількість завантажень Facebook Messenger і WhatsApp зросла на 2 % і 5 % відповідно.

***

9.06.2016

«ВКонтакте» добавила алгоритмическую ленту в мобильное приложение

Социальная сеть «ВКонтакте» обновила мобильный клиент и внедрила алгоритмическую ленту на всех платформах. Об этом «Газете.Ru» сообщил пресс-секретарь соцсети Е. Красников, пишет InternetUA.

Режим «Сначала интересные» можно включить и отключить в настройках ленты новостей. Отмечается, что посты не будут исчезать, просто изменится их порядок показа. С включенной функцией новости будут отображаться не в хронологическом порядке и самые интересные будут выше остальных.

Также в приложении появились подсказки стикеров при наборе текста и смайликов. Например, при вводе слова «Привет» приложение покажет несколько стикеров, которые можно использовать вместо текста.

Помимо этого, приложение получило несколько незначительных изменений в анимации и дизайне. Появилась возможность сохранять и делиться GIF-анимациями, а их просмотр на iOS осуществляется теперь прямо в ленте новостей.

***

9.06.2016

Пользователям «ВКонтакте» начали принудительно менять дизайн

Социальная сеть «ВКонтакте» начала принудительно переводить пользователей на новый дизайн. В настоящее время оформление поменяли 10 процентам юзеров, выбранным случайно. Об этом сообщает 9 июня сообщество новостей соцсети LIVE Express, пишет InternetUA.

При этом пользователи, которые самостоятельно подавали заявку на смену дизайна, получат возможность менять внешний вид страницы со старого на новый, пока старый интерфейс не будет полностью отключен. Те пользователи, которым принудительно установили новый дизайн, не смогут вернуться к предыдущей версии сайта.

По данным «ВКонтакте», в социальной сети зарегистрированы более 350 млн пользователей. Таким образом, новое оформление было установлено 35 млн владельцев страниц.

Социальная сеть «ВКонтакте» представила новый дизайн 1 апреля. Практически каждый раздел соцсети подвергся существенной переработке. В левом меню стало меньше пунктов, а самые востребованные разделы переехали в верхнюю часть экрана. Также сильно изменился и раздел «Сообщения». В

новой версии дизайна в левой части экрана выводится список последних диалогов, а в правой – текущая переписка.

***

10.06.2016
Facebook запустила фото в формате 360 градусов

Социальная сеть Facebook запустила в новостной ленте функцию поддержки фотографий в формате 360 градусов. Об этом на своей странице в соцсети сообщил ее основатель Ма. Цукерберг, пишет МедиаБизнес со ссылкой на sostav.ru.

«Они аналогичны видео в формате 360 градусов – можно поворачивать телефон и чувствовать, как будто вы находитесь там», – написал М. Цукерберг.

Функция будет поддерживать фото, сделанные сферической камерой, такой как Rioch Theta S, и панорамные снимки, сделанные на смартфон. Фото также можно будет просмотреть с помощью шлемов виртуальной реальности. Таким образом, Facebook стала первой из социальных сетей, кто внедрил 360-градусные фото в свою ленту.

***

11.06.2106
В Facebook появилась возможность вставлять видео в комментарии

Теперь в комментарии к постам в Facebook можно вставлять видео, сообщает The Next Web. Чтобы загрузить запись, нужно нажать на иконку с фотоаппаратом в строке для комментариев, пишет InternetUA.

Новая возможность появилась как у пользователей десктопной версии, так в мобильных приложениях на iOS и Android. При этом видео-комментарии можно оставлять не везде, однако, на страницах друзей и организаций, а также в группах такая опция есть.

***

16.06.2016
В Twitter появилась кнопка Periscope

В сообщения в соцсети микроблогов Twitter теперь можно добавлять трансляцию из Periscope.

Как пишет Mashable, в мае Twitter тестировал новую кнопку на небольшой группе пользователей с устройствами на платформе Android, а затем и на владельцах гаджетов на iOS, пишет TRUST.UA.

Таким образом, новая функция добавится к уже существующим возможностям вставить в сообщение фото или видео. Однако при этом на устройстве должно быть установлено приложение Periscope.

Стоит отметить, что Twitter является владельцем Periscope. При этом в сообщении подчеркивается, что добавлением новой функции соцсеть микроблогов отреагировала на возможность вести трансляции в Facebook Live.

***

14.06.2016
Роман Черный
Зачем Microsoft покупает LinkedIn?

Технологический мир всколыхнула неожиданная новость. Компания Microsoft покупает социальную сеть LinkedIn за 26,2 млрд долл. Это очень большая сумма даже по меркам Кремниевой долины. За эти деньги Microsoft получает не только бренд и функционал LinkedIn, но и все 433 млн пользователей социальной сети. Обе стороны уже подтвердили сделку. Официально она будет закрыта до конца этого года, пишет IGate.

Интересно, что Д. Вейнер все так же будет руководить LinkedIn, правда, теперь его боссом станет С. Наделла. Что же в таком случае поменяется, и зачем Microsoft вообще понадобился LinkedIn?

Хотя Microsoft известен большинству пользователей как разработчик операционной системы Windows, львиную долю дохода компании приносят облачные продукты, ориентированные на крупный бизнес. Покупка социальной сети, ориентированной на профессионалов, становится еще одним логичным шагом в борьбе за клиентов из мира крупного бизнеса.

Еще одна причина, по которой Microsoft готов заплатить за LinkedIn такие огромные деньги, состоит в том, что к социальной сети ранее присматривались и другие. По слухам, покупкой LinkedIn ранее интересовались представители Salesforce, одного из главных конкурентов Microsoft на рынке облачных систем управления базами данных. В общем, кто-то социальную сеть непременно бы купил. Microsoft просто решил быть первым.

Зачем LinkedIn продается Microsoft?

Если сами по себе 26,2 млрд долл. – не очевидная причина, то существует и другая. LinkedIn является крупнейшей в мире сетью для профессионалов, но всё же это очень нишевый продукт. Как уже говорилось, количество зарегистрированных пользователей соцсети составляет 433 млн. Это много, но не идет ни в какое сравнение с полутора миллиардами душ, съеденных Facebook.

Не стоит забывать и о том, что соцсети сегодня массово сдают позиции, уступая по популярности мессенджерам. Для того, чтобы быть на коне, им приходится постоянно придумывать что-то новое. LinkedIn, будучи нишевым продуктом, не может похвастаться какими-либо яркими новшествами. А значит, появление «мессенджера для профессионалов», который переманит к себе аудиторию LinkedIn, остается лишь вопросом времени.

Чтобы выжить, социальной сети нужно преобразиться и стать чем-то большим. И в этом ей поможет Microsoft.

Судя по тому, что известно на данный момент, Microsoft приготовил для LinkedIn очень важную роль.

Для начала, социальная сеть будет интегрирована с пакетом Office 365 и другими облачными сервисами Microsoft. На выходе получится совершенная рабочая среда. С ее помощью профессионалы всего мира смогут не только связываться между собой, но и координировать выполнение самой работы. Благодаря этому LinkedIn сможет заполучить часть аудитории корпоративных мессенджеров, таких как Slack.

Само собой, в ходе интеграции данные социальной сети будут объединены с данными сервисов Microsoft. То есть, к примеру, у мессенджера Skype и LinkedIn будет единый аккаунт. Это же касается и других сервисов Microsoft. Поговаривают, что даже личный аккаунт пользователя Windows 10 может стать аккаунтом LinkedIn.

Пожалуй, самые интересные гибриды родятся в результате слияния LinkedIn и интеллектуальных систем Microsoft. Ни для кого не секрет, что в области интеллектуальных решений и машинного обучения Microsoft является одним из лидеров рынка. К примеру, искусственный интеллект Xiaoice, разработанный компанией, получился настолько совершенным, что уже несколько месяцев ведет прогноз погоды на одном из китайских телеканалов.

Интеллектуальные алгоритмы Microsoft, интегрированные в LinkedIn, позволят разработчикам экспериментировать с «умной» новостной лентой. В итоге мы увидим что-то вроде Facebook Instant Articles, ориентированных на мир бизнеса.

Со временем в LinkedIn может появиться умный помощник, который будет следить за встречами пользователя, уведомлять о важных мероприятиях и раздавать профессиональные рекомендации. Эдакий личный искусственный секретарь для каждого клиента.

Также со временем LinkedIn может превратиться в своеобразный рекомендательный сервис, через который компании смогут предлагать свои товары и услуги потенциальным покупателям. Учитывая узкий профиль LinkedIn, такая система продвижения может стать очень эффективной: предложение некоего бизнес-продукта будет идеально попадать в целевую аудиторию.

Скорее всего, масштабное слияние LinkedIn и Microsoft породит еще немало сюрпризов. Но то, что очень скоро социальная сеть превратится в нечто большее – неоспоримый факт.

***

16.06.2016

Цукерберг заявил о желании читать мысли пользователей

М. Цукерберг считает, что в будущем социальные сети позволят пользователям напрямую делиться мыслями и эмоциями. Об этом глава

Facebook заявил в ходе пресс-конференции, сообщает The Washington Post, пишет InternetUA.

М. Цукерберг отметил, что возможность мгновенно делиться информацией в форме текста, видео и фотографий – это не предел развития социальных сетей. Он также отметил, что технологии виртуальной реальности открывают впечатляющие перспективы, однако и они не исчерпывают потенциала взаимодействия человека и компьютера.

«Сегодняшние технологические достижения впечатляют, однако, я думаю, в будущем мы сможем просто фиксировать «живые» эмоции и мысли и выкладывать их прямо в Интернет», – заявил М. Цукерберг.

Он также рассказал об исследованиях правительства США, в результате которых ученые смогли проводить изменения в памяти крыс и передавать опыт одной крысы другой.

«Это прямо как в «Матрице», не так ли?» – отметил М. Цукерберг.

***

15.06.2016
Facebook Messenger начал принимать SMS

Об этом компания сообщила на своей странице в Facebook. Пока эта опция доступна для владельцев Android девайсов. Но отправленные через мессенджер SMS-сообщения смогут получить владельцы устройств на любой платформе. Кроме текстовых сообщений, функция SMS в Messenger поддерживает приём и отправку изображений, видео и аудио, местоположения, эмодзи и стикеров. При этом SMS-сообщения будут помечаться фиолетовым цветом, а переписка в Messenger – синим, пишет Marketing Media Review.

***

15.06.2016
Twitter разрешил ретвитить и цитировать собственные твиты

Социальная сеть Twitter предоставила пользователям новую возможность – ретвитить собственные твиты, а также цитировать их, пишет Телекритика.

При этом, согласно сообщению на официальной странице соцсети в микроблоге, новая функция позволяет ретвитить собственные твиты любой давности.

Большинство пользователей одобрили такое нововведение. Однако некоторые возмутились тем, что ретритить собственные посты стало возможным, а редактировать их – нет.

***

16.06.2016
В WhatsApp добавили возможность цитировать сообщения в ответах

В WhatsApp появилась возможность цитировать сообщения, на которые отвечает пользователь. Данная функция будет весьма востребованной в групповых чатах, уверенны разработчики. Сейчас нововведение доступно только группе пользователей, участвовавшей в тестировании, однако в ближайшее время обновление распространится на всех, пишет IGate.

Различные источники сообщают, что развертывание новой функциональности на самом деле уже происходит. Для того, что бы проверить, доступна ли новая функция у вас в приложении, необходимо просто нажать на цитируемое сообщение и удерживать несколько секунд, пока не появится специальная панель действий: вдобавок к традиционным функциям копирования, удаления, пересылки, а также пометки звездочкой должна появиться и новая пиктограмма, ассоциируемая с ответом. При нажатии на нее, произойдет цитирование сообщения, которое можно будет дополнить своим ответом.

***

17.06.2016
«ВКонтакте» запустил новую удобную функцию

Социальная сеть «ВКонтакте» запустила новую функцию: специалисты создали короткий адрес для сообщений vk.me, перейдя по которому можно сразу попасть в диалог или поделиться ссылкой с другими. Благодаря этому написать сообщение пользователю или задать вопрос сообществу станет еще проще, сообщают представители сети, пишет InternetUA.

Теперь любая компания может разместить на своем сайте данную ссылку наряду с другими контактными данными. Перейдя по ссылке, пользователь попадет в диалог с сообществом компании, где сможет задать свой вопрос.

Такая же система действует и с отдельными пользователями: перейдя по ссылке, можно сразу же написать сообщение своему другу или знакомому.

Таким образом, специалисты «ВКонтакте» хотят «акцентировать внимание пользователей непосредственно на коммуникации»: теперь харегистрированные в соцсети люди смогут оперативно переходить не только на страницы аккаунтов и сообществ, но и прямо в диалоги.

***

19.06.2016
Через пять лет видео полностью заменит текст в Facebook

Н. Мендельсон предсказала смерть печатного слова в ближайшую пятилетку. Вице-президент Facebook в Европе, на Ближнем Востоке и Африке заявила, что видеоконтент набирает популярность гораздо быстрее, чем можно было предположить, пишет InternetUA.

Через пять лет на Facebook может остаться исключительно видеоконтент, пишет Gizmodo. Количество просмотров роликов в социальной сети

увеличилось с одного млрд до восьми за прошедший год. Пользователи просматривают 100 млн часов видео ежедневно, заявила Н. Мендельсон.

***

19.06.2016

Записи в Facebook будут со временем исчезать

Популярная соцсеть тестирует новую функцию, при помощи которой пользователи смогут оставлять записи, не задумываясь над их содержанием.

Публикации не будут закрепляться в «Хронике», а со временем вообще будут исчезать из ленты новостей друзей, пишет iLenta со ссылкой на CNET.

Таким образом разработчики пытаются стимулировать пользователей Facebook чаще выражать свои мысли, самовыражаться, не задумываясь над смыслом и содержанием. Чтобы включить функцию, надо поставить отметку напротив фразы Hide From Your Timeline (Скрыть из Хроники).

Некоторые эксперты сравнивают нововведения Facebook с аналогичной опцией в Snapchat. Но разница в том, что в Facebook не устанавливается таймер для ликвидации записи. Так как опция проходит тестирование, она доступна не всем пользователям. Пока неизвестно, будет ли нововведение функционировать на постоянной основе.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

16.06.2016

#FollowUkraine: Мінекономіки запустило акцію на підтримку унікальних товарів і послуг з України

«Україна виробляє безліч унікальних, якісних та оригінальних товарів. На жаль, не всі про це знають. Наприклад, мало кому відомо, що канадійська збірна по хокею грає ключками, зробленими в Україні», – ідеться на сторінці відомства у Facebook, пише Watcher.

За словами організаторів, міністерство вирішило розвивати бренд #MadeinUA задля створення позитивного іміджу України як виробника. Долучитись до акції організатори закликають і українських користувачів Facebook, використовуючи хештег #FollowUkraine!

***

6.06.2016

Черновцы обзавелись официальной страницей «ВКонтакте»

Вслед за Черкассами, собственной верифицированной (подтвержденной) страницей «ВКонтакте» обзавелись Черновцы. Официальный статус сообщества дает возможность не только читать местные новости и обращаться за советами, но и жаловаться в горсовет на актуальные проблемы в жизни города, пишет AIN.UA.

Идея создать не просто развлекательное сообщество, а официальную страницу для связи жителей города с местной властью появилась у черновицкого активиста А. Жука. «Молодежь в Черновцах очень активная. Ее стоит привлечь к общественному процессу и показать, что органы местного самоуправления – не так далеко, как они думают. И что озвучить проблемы или задать вопросы городским властям можно прямо в той соцсети, которой ты активно пользуешься», – поясняет А. Жук, инициатор создания официальной группы Черновцов в «ВКонтакте».

Первое, что он сделал – обратился в пресс-службу соцсети с просьбой верифицировать сообщество. «Мы связались с пресс-секретарем киевского офиса «ВКонтакте», и нам предоставили список необходимого: получить письмо от представителя органа местного самоуправления с печатью и добавить виджет «ВКонтакте» на сайт Черновицкого городского совета», – рассказывает А. Жук.

От момента обращения в пресс-службу до подтверждения группы прошел месяц. Для официальной бюрократической машины это совсем недолго: Черновцы в лидерах по индексу публичности в стране, здесь можно запросто зайти в горсовет и пообщаться с чиновниками, напомнить о себе или узнать, что тормозит процесс.

Страница работает чуть больше месяца, пока в тестовом режиме: администратор экспериментирует, подбирает интересные пользователям рубрики и тематики. Например, в ближайшее время планируют запуск рубрики плейлистов от черновчан. Первым поделится любимыми композициями начальник черновицкой полиции.

Кроме этого, в сообществе создана специальная тема, в которой жители Черновцов могут оставить заявку об открытом люке или неработающем уличном освещении. И, конечно, страница публикует важные местные новости и информацию для туристов. Помимо этого, в сообщество часто обращаются за советами.

«Часто пишут туристы, спрашивают, что, где, куда. Однажды женщина спросила, где можно остановиться с детьми, где взять напрокат детскую коляску. Не поленился, поискал в Интернете и предоставил полный список. Мне кажется, так должно работать городское сообщество в 21 веке», – говорит А. Жук.

***

6.06.2016

Instagram запустил кампанию в поддержку разнообразия модной индустрии

На официальном аккаунте сети Instagram стартовала кампания с тегом #RunwayForAll, цель которой – расширить стандарты модной индустрии и показать, что на подиумах есть место для самых разных людей. Кампанию уже поддержиют модель плюс-сайз К. Дессо, модель с альбинизмом африканского происхождения Ш. Росс, блогер Мама Какс, правую ногу которой заменяет протез, и другие яркие личности. «Красота не всегда может опираться на обе ноги и быть нулевого размера» – пишет Мама Какс, сообщает Marketing Media Review.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

16.06.2016

YouTube позволит малому бизнесу делать дешевые рекламные ролики

Владелец крупнейшего в мире видеосервиса YouTube, инртенет-гигант Google анонсировал запуск нового приложения под названием Director, с помощью которого представители малого и среднего бизнеса со скромными рекламными бюджетами смогут сами создавать коммерческие ролики, сообщает интернет-издание Cossa, пишет Телекритика.

В Google рассказали, что один маленький парикмахерский салон в Лос-Анджелесе уже протестировал возможности нового приложения, после чего увеличил отклик на рекламную кампанию на 73 % и достиг +56 % узнаваемости бренда.

Наряду с YouTube Director компания запускает еще два сервиса, предназначенные для тех, кто сталкивается с трудностями при создании роликов. Один из них будет использовать имеющиеся у пользователя изображения (логотип, скриншоты и т. д.) для создания видео.

Кроме того, YouTube работает над новым решением, которое будет «сводить» мелких предпринимателей с теми, кто делает видео, для создания «экстремально дешевой» рекламы. Это выглядит так: через YouTube Director бизнесы в ограниченном списке городов, которые могут себе позволить потратить от 150 долл. на видеоролик, смогут обратиться к видеосервису, чтобы он подобрал для них подходящую съемочную команду, готовую выехать и снять видео.

По словам руководителя направления продуктового менеджмента Google Д. Джолли, рекламные ролики малого и среднего бизнеса значительно хуже по качеству, чем креатив крупных брендов. Кроме того, мелкие предприниматели предпочитают использовать одно и то же низкокачественное видео длительное

время в отличие от больших компаний, которые гораздо чаще придумывают и снимают новую рекламу.

***

17.06.2016

«ПриватБанк» позволил пользователям Telegram переводить деньги друг другу в один клик

Глава IT-департамента «ПриватБанка» Д. Дубилет опубликовал короткое видео, в котором рассказал о запуске бота в мессенджере Telegram, позволяющего быстро и легко переводить деньги прямо в чате сервиса, пишет IGate.

Для того, чтобы воспользоваться новой возможностью нужно подвязать свою карту «ПриватБанка» к аккаунту. После этого вы сможете переводить деньги друзьям, вызвав бота в чате командой «@paypbbot», указав необходимую сумму и нажав «отправить». Средства будут зачислены сразу. Комиссия за перевод составит 0,5 %.

***

16.06.2016

Twitter представил таргетинг по эмодзи

В преддверии Всемирного дня Emoji, который отмечается 17 июня, социальная сеть представила брендам новую возможность для таргетинга пользователей. Это означает, что если пользователь в Чикаго отправил твит с эмодзи пиццы, его пригласит локальный ресторан отведать его предложение. По данным сети, более 110 млрд эмодзи были отправлены с 2014 г., И указывая на настроение пользователя они «предоставляют уникальные возможности для маркетологов и брендов». Функция доступна для всех рекламодателей через партнеров рекламного API Twitter, включая AdParlor, Amobee, HYFN, Perion, SocialCode и 4C, пишет Marketing Media Review.

***

7.06.2016

Диана Митчелл

Как Ричард Брэнсон работает с соцсетями

Когда речь заходит о самых успешных предпринимателях в социальных сетях, многие называют Р. Брэнсона. С более чем 7 млн фоловеров в Twitter, 9 млн в LinkedIn и около 3 млн в Facebook, Р. Брэнсон на ряду с М. Кубаном и И. Маском считается одним из самых влиятельных персон в социальных медиа. Но успех здесь меряется не только лайками и количеством подписчиков. Р. Брэнсон пользуется рядом успешных практик, которые помогают ему оставаться в топе лидеров мнений и успешно развивать свой бизнес. Ими

можна воспользоваться, чтобы генерировать лиды и развивать отношения через социальные медиа, пишет AIN.UA

Он общается с людьми лично

Р. Брэнсон успешно использует платформу, чтобы рассказывать истории и органично строить вовлечение, апеллируя к чувствам максимального количества людей. Нынешние пользователи социальных сетей куда более здравомыслящие, чем раньше. Если несколько лет назад маркетинговые коммуникации могли собирать клики и вовлекать пользователей в соцсетях в свой контент, то сегодня люди ищут настоящего общения.

Несмотря на огромное количество фоловеров, Р. Брэнсон практически ежедневно отвечает на несколько твитов. Чтобы сделать свои твиты еще более личными, он часто добавляет к ним свои фотографии и изображения.

Здесь есть один очень важный элемент: Р. Брэнсон, как правило, делает посты в соцсетях самостоятельно.

Если от твоего имени вещает посторонний человек, построить настоящие отношения с аудиторией в соцсетях может быть сложно. Социально подкованные фоловеры быстро поймут, что ваш аккаунт ведут маркетологи. Р. Брэнсон понимает, что успех в соцсетях невозможен без аутентичности, поэтому обязательно находит время на них в течение дня.

На вопрос подписчика о том, как много времени Р. Брэнсон уделяет блогерству и социальным сетям, сэр Ричард ответил ему напрямую: «Зависит от того, чем я занимаюсь и где нахожусь, но я обязательно захожу хотя бы пару раз в день».

Он использует социальные сети, чтобы приводить трафик на сайт Virgin

Любой бизнес пытается завлекать людей на свой сайт, строить лояльность и увеличивать продажи через социальные сети. Посты из разряда «Будь позитивен!» могут нагнать лайков и вовлечения, но только контент, который направляет трафик на сайт компании, непосредственно конвертирует фоловеров и лайки в продажи. Facebook и Google постоянно сменяют друг друга на позиции лидера по реферальному трафику для веб-сайтов.

Р. Брэнсон понимает важность оригинального контента в блоге Virgin для его соцмедийной стратегии, поэтому пишет новый блог-пост почти каждый день. Он направляет трафик на эти посты на сайте Virgin, публикуя ссылки в Twitter, где их видят миллионы его фоловеров.

Он веселится

В своей книге Jab, Jab, Jab, Right Hook соцмедиа-эксперт и автор бестселлеров Г. Вайнерчук рекомендует сперва несколько раз предложить веселый, ценный контент, а уж потом что-то просить у своих фоловеров. Будь-то милая анимированная картинка, смешном мем или история из жизни, Р. Брэнсон вовсю делится вещами, которые ему нравятся. Более того, он делится контентом, который точно понравится его аудитории.

Направление трафика на сайт очень важно для роста вашего бизнеса, вместе с тем публикация контента, который нравится вашей аудитории,

обеспечивает некий баланс для бизнесового контента, одновременно увеличивая вероятность того, что фоловеры будут доверять вашему рекламному контенту.

Он приветствует вклад своей аудитории

Р. Брэнсон понимает, что активность в соцсетях и, как следствие, извлечение потенциальной выгоды от сильного социального присутствия подразумевает уязвимость к негативным отзывам и комментариям от клиентов. Вместо того, чтобы избегать этого типа социального фидбека, Р. Брэнсон приветствует его: «Мне нравится читать свои хроники в социальных сетях. Это отличный способ получить фидбек о своих продуктах и сервисах, и прекрасный источник новых идей».

В риал-тайм Twitter-сессиях вопросов и ответов #AskRichard и в ходе ежедневных взаимодействий, сэр Ричард вовлекает подписчиков в открытый диалог на различные темы. Он использует коллективный подход к своим фоловерам в Twitter вместо состязательного подхода, что позволяет построить высоколояльную аудиторию.

Успех в соцсетях полезен не только для известных предпринимателей с миллионом подписчиков. Сделайте шаг навстречу социальным сетям и воспользуйтесь принципами Р. Брэнсона, чтобы стать влиятельным блогером.

***

10.06.2016

Как сделать сайт из страницы в Facebook

Эти сервисы помогут сэкономить время и автоматически перенесут полезную информацию о вашем бизнесе на новую платформу – адаптивный сайт. Все сервисы в подборке позволяют настроить оплату заказов, поисковую оптимизацию, подключить аналитику и развивать дизайн и структуру сайта в простом визуальном режиме, пишет Slavpeople.

uKit Alt

Единственный проект с поддержкой русского языка. Фишка сервиса – в возможности перенести отзывы клиентов из соцсети на сайт. Сам инструмент рассчитан на создание сайтов-визиток для малого бизнеса (разместить прайс, поставить обратный звонок) и небольших витрин с товарами. Опубликовать сайт и пользоваться им можно неограниченное время, если вы разрешите проекту иметь свой промо-блок внизу ваших страниц.

Версия без промо-блока стоит от 4 долл. в месяц.

Pagevamp

Американский проект, который позволяет делать лендинги. Особенность сервиса – в возможности автоматически менять информацию на сайте, если вы изменили что-то в Facebook. Правда, ради этого приходится жертвовать встроенным редактором: тексты сайта, полученные из старого контента, нельзя изменять в самом Pagevamp. Можно лишь добавлять новые элементы и править уже их.

Встроенные виджеты ориентированы на визуалов, без работы с кодом можно добавить видео или аудио. Бесплатная версия ограничена 14 днями, дальнейшая поддержка обойдётся от 12 долл. в месяц.

Impress.ly

Голландско-американский проект, больше ориентированный на создание мобильных, а не веб-сайтов. Самое интересное в сервисе: он позволяет увидеть, как будет выглядеть ваш контент на нескольких шаблонах, прежде чем вы окончательно выберете дизайн. Виджеты ориентированы на зарубежный ресторанный сектор: есть формы предзаказа столиков и еды на вынос.

Для публикации сайта придётся заплатить от 9 до 19 долл. – и выплачивать ещё столько же ежемесячно (в зависимости от объёма рекламы, которую вы готовы видеть на своей веб-странице, и выбранного набора инструментов).

***

17.06.2016

Facebook позволит рекламодателям проанализировать эффективность рекламы до ее размещения

Социальная сеть откроет брендам доступ к данным, с помощью которых можно будет оценить эффект от рекламы до того, как ее увидят пользователи.

В преддверии Каннского фестиваля Facebook объявил, что будет предоставлять рекламодателям данные для исследования рынка, сообщает The Financial Time, пишет PRпортал.

Новый инструмент уже смогли протестировать компания Mondelez International, владелец брендов Cadbury и Oreo, а также производитель пива Stella и Budweiser – AB InBev.

Facebook будет поставлять рекламодателям данные в агрегированном и обезличенном виде, поэтому компании не смогут видеть личную информацию пользователя.

Ранее социальная сеть также объявила о том, что начнет измерять количество фактических посещений офлайн-магазинов, совершенных после просмотра рекламы. Для этого Facebook будет использовать данные о местоположении пользователей, которыми они делятся с социальной сетью, в сочетании с другими сигналами, такими как Wi-Fi. Вся информация будет доступна в режиме реального времени с разбивкой по возрасту и полу.

Главный источник доходов Facebook – реклама, доходы от которой по сравнению с аналогичным периодом в прошлом году возросли на 57 % до 5,2 млрд долл. На долю мобильной рекламы приходится 82 % от всей рекламной выручки.

***

16.06.2016

10 советов и подсказок о рекламе в Facebook

Система показа постов в Facebook устроена таким образом, что каждый пост видит только небольшой процент подписчиков вашего аккаунта или страницы. Это приводит к тому, что новости видят не все и, соответственно, важная информация может пройти незамеченной, пишет Sostav.ua.

Решением этой проблемы могут стать платные посты и реклама. Маркетинговый портал Kissmetrics опубликовал 10 советов, которые помогут использовать Facebook максимально эффективно.

1. Facebook Lead Ads

Один из новых типов кампаний в Facebook – это Lead Ads, которые позволяют рекламодателям собирать данные пользователей с помощью специальных форм, без необходимости переходить куда-либо из этой социальной сети.

Для того чтобы начать работать с Lead Ads, нужно:

– создать новую кампанию, выбрав «Lead Generation»;

– создать вашу форму Lead;

– выбрать вопросы, которые вы хотите задать пользователям.

2. Отчеты

Следует обращать особое внимание на секцию отчетов – она поможет ответить на такие вопросы, как «Происходит ли конверсия в мобильном приложении?», «Какой гендер лучше реагирует на рекламу?» и т. д.

Зная ответы на эти вопросы, вы можете лучше распределять бюджет на рекламу.

3. Модели атрибуции

Важно понимать модели атрибуции Facebook (attribution models) – как изменяются настройки, и что важно для ваших целей конверсии, поскольку существуют «правила», по которым считается каждая конверсия.

4. Тестируйте Instagram

С сентября 2015 г. с помощью Facebook Ads Dashboard можно размещать рекламу в Instagram. Для этого вам нужно просто присоединить ваш аккаунт в Instagram и выбрать размещение рекламы в этом аккаунте.

5. Похожая аудитория

Похожая аудитория – это критерий таргетирования, при котором Facebook генерирует аудиторию пользователей, похожих на ваших текущих пользователей или аудиторию. Facebook находит похожих пользователей по демографической информации, интересам, поведению и т. д. и создает лист пользователей, который вы можете использовать в своих кампаниях.

6. Используйте локацию

Еще один полезный критерий таргетирования Facebook – это опции месторасположения. Ваша целевая группа – это люди, которые живут в определенном городе или путешествуют в этот город?

7. Разговаривайте с аудиторией

Благодаря методам таргетирования Facebook вы в большинстве случаев знаете вашу аудиторию – ее интересы, поведение и т. д. Попробуйте

использовать эти знания, когда вы составляете обращения к аудитории, чтобы они были более персонализированными.

8. Ремаркетинг

Ремаркетинг позволяет повторно рекламировать определенные продукты или услуги тем пользователям, которые ранее просматривали или приобретали эти продукты. Ваша реклама будет динамически изменяться в зависимости от того, какие продукты просматривал пользователь.

9. Тестируйте

Всегда тестируйте разные варианты рекламы, чтобы понять, какой вариант работает для ваших пользователей лучше всего. Facebook оптимизирует вашу рекламу в зависимости от ее показателей и ваших целей.

Не забывайте проводить A/B-тестирование для того, чтобы определить, являются ли результаты статистически достоверными, или же это просто случайность.

10. Используйте разные размещения

Следите за результатами размещения рекламы в разных местах и выбирайте те, которые работают лучше.

При этом почти всегда имеет смысл проводить кампанию в нескольких местах, например, в десктоп-ленте и мобильной ленте Facebook.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

8.06.2016

Дослідники спробували пояснити, чому жінки частіше використовують Instagram, ніж чоловіки

Жінки активніше використовують соцмережу Instagram, ніж чоловіки. Про це пише The Atlantic, повідомляє MediaSapiens.

Згідно з даними ComScore, за квітень 2016 р. зі 108 млн унікальних відвідувачів Instagram, 42 % – це чоловіки, а 58 % – жінки. Компанія, яка займається вимірюванням інтернет-трафіку, відзначає, що такий розрив простежувався і в минулому році.

А. Марвік, дослідниця соцмереж з університету Фордхем, зазначає, що користувачі Instagram транслюють дуже різноманітні зображення – від пропаганди здорового харчування до панк-року. Але незважаючи на різноманіття тем, більшість користувачів вибудовують своє гіперболізоване зображення того, як люди мають виглядати.

«В пересічних користувачів Instagram ми бачимо звичні стандарти краси та естетики», – зазначає дослідниця. І ця орієнтація виключно на привабливий зовнішній вигляд і є фактором, який залучає більше жіночої аудиторії в соцмережу. Instagram є магнітом для моди, дизайну і beauty-брендів, які часто орієнтовані на жінок як споживачів їхньої продукції.

Основна функція Instagram – обмін фотографіями, які часто редагуються за допомогою різноманітних фільтрів, щоб зробити зображення привабливішим. Соцмережа робить надзвичайно сильний акцент на тому, як виглядають речі.

«Молоді жінки переважають серед користувачів Instagram та й візуальних платформ у цілому. Instagram дає вам можливість моделювати свій зовнішній вигляд, практично на одному рівні з косметикою та іншими подібними продуктами», – коментує розрив в аудиторії соцмережі гендерна дослідниця Р. Сіммонс.

«Кожна хоче бути найкрасивішою дівчиною в кімнаті. Instagram надає платформу, де ви можете вести цю конкуренцію щодня. Інтернет називають великим інструментом демократії, тому можливо, те, що зробив Instagram – просто надав кожному можливість взяти участь у конкурсі краси», – пояснює Р. Сіммонс.

К. Тіаденберг, соціолог та дослідниця з Талліннського університету, вважає, що перевага жінок серед користувачів Instagram може бути пов’язана з історичною традицією. «Зазвичай матері були відповідальними за сімейні фотографії в багатьох культурах. Те, що ми бачимо в Instagram, можна віднести до цієї ж сфери», – зазначає дослідниця. Ще в XIX ст. жінки із більш заможних сімей робили фото своєї сім’ї та друзів, збирали альбоми з малюнків, вирізок та фотографій.

***

9.06.2016

Facebook-зависимых будут госпитализировать

Зависимость от социальных сетей уже признана мировым сообществом как настоящее заболевание. К примеру, недавно в Алжире открылась первая в Африке частная клинка, где лечат зависимость от Facebook. Это третья по счету подобная клиника в мире. Такие клиники уже есть в Китае и Южной Корее, сообщает meddaily, пишет From-UA.

Известно: к работе в алжирской клинике привлекли специалистов, которые ранее имели дело с наркоманами и алкоголиками. Для борьбы с зависимостью от социальных сетей медики разработали специальную программу. Она призвана переключить внимание пациентов с мира виртуального на мир реальный.

Специалисты сравнивают соцсети вроде Facebook с кокаином. Такой вывод, например, делали норвежские ученые, которые доказали это в эксперименте с участием 20 добровольцев.

Анализ влияния Facebook на мозг человека показал: просмотр собственной страницы в соцсети вызывал у большинства людей появление признаков зависимости. Во время использования соцсети у человека в головном мозге повышалась активность тех же нейронных центров, что и при употреблении кокаина.

***

15.06.2016

Антисуицидальная опция Facebook появится во всех странах

Компания Facebook запускает функцию по предотвращению суицидов во всех странах присутствия социальной сети. Ранее сервис был доступен только для англоязычных пользователей, сообщает The New York Times, пишет InternetUA.

Опция позволяет сообщить администрации ресурса о тревожных постах друзей. По словам представителей Facebook, сотрудники линии поддержки круглосуточно просматривают такие сообщения.

В случае обоснованности беспокойства автор записи получит сообщение от Facebook: «Привет, друг думает, что ты, возможно, столкнулся с какими-то трудностями, и попросил нас посмотреть твой недавний пост». Пользователю будет предложено связаться с линией поддержки или написать другу.

***

16.06.2016

Ученые рассказали, зачем люди публикуют фото в социальных сетях

Гаджеты помогут запечатлеть каждую минуту жизни. Но зачем люди делятся своими снимками в социальных сетях? Это выясняли ученые, пишет 4mama.com.ua.

В современном мире появился феномен инстамама либо фэйсбукмама. Это мамы, которые часто публикуют свои фото и фото детей. Ученые говорят, что таким образом они стремятся получить согласие общества, им хочется знать, все ли они делают правильно.

В последнее время все большую популярность набирает социальная сеть Instagram, где пользователи выкладывают фото, оставляют комментарии и лайки. Если посмотреть на снимки, можно рассказать, как тот или иной человек провел свой день и отпуск. Часто это снимки достаточно личного характера, помимо еды, появляются фото до и после родов, первые минуты жизни малыша и т. д.

Ученые попытались понять, в чем заключается причина такой тяги к демонстрации своей жизни. Результаты нового исследования сообщил Journal of Personality and Social Psychology. Как выяснили американские эксперты, фотографирование является своеобразным психостимулятором, который помогает человеку ощущать более сильные эмоции.

Как это происходит в жизни: человек, который сначала фотографирует еду, а потом съедает, получает больше удовольствия от приема пищи.

Также современные люди не обходятся в путешествиях без фотокамер. Ученые говорят, что человек, который делает снимки во время своего отдыха, получает больше экстатического удовольствия, например, от снимков моря и каких-то достопримечательностей. В этом случае у него есть возможность рассмотреть мелочи и детали, то, что невооружённым взглядом сразу не увидишь.

Также исследователи заявляют о том, что фотографирование может заряжать не только позитивными эмоциями, но и негативными. Например, если человек делает снимок неприятного явления, у него, соответственно, усиливаются отрицательные эмоции.

Эксперты сделали вывод, что самые активные участники популярнейшего сервиса Instagram – это люди, которым не хватает эмоций в обычной жизни.

***

16.06.2016

Математики вычислили террористические угрозы с помощью «ВКонтакте»

Исследователи из Майамского университета разработали модель поведения сторонников «Исламского государства» в Интернете, которая может позволить следить за деятельностью боевиков и пресекать террористические угрозы. Исследование опубликовано в журнале Science, пишет InternetUA.

Ученые проанализировали записи, оставленные членами 196 групп в российской социальной сети «ВКонтакте», связанных с ИГ, в течение первых восьми месяцев 2015 г. Хотя большинство из более чем 108 тыс. участников групп никогда не встречались друг с другом, в Интернете они проявляли способности к организации, увеличивая численность своих групп, восстанавливая их после блокирования, а также вдохновляя своих сторонников на террористические атаки.

По словам ученых, онлайн-деятельность ИГ похожа на растущие кристаллы. Люди организовывались вокруг социальных групп, активно участвовали в их деятельности и делились информацией. Исследователи прибегли к уравнениям физики и химии, которые применяются для описания коллективного поведения частиц. Оказалось, что перед реальными действиями кооперация между членами групп усиливается, а сами группы при этом объединяются и увеличиваются в размерах.

Ученые считают, что, если концентрировать свое внимание лишь на нескольких ключевых группах, где обсуждаются оперативные детали, каналы финансирования и меры борьбы с беспилотниками, можно эффективно предотвращать потенциальные акты насилия со стороны ИГ.

***

20.06.2016

Пользователи Twitter не читают более половины ретвитнутых новостей

На шесть из десяти ссылок, которыми делятся пользователи в Twitter, на самом деле никто не кликает. Это выяснила группа ученых из Колумбийского университета и Национального исследовательского института Inria, которая провела исследование, представленное на конференции ACM SIGMETRICS / IFIP Performance, пишет UAPARTY.

Ученые исследовали твиты, которые содержали ссылки, ведущие на пять новостных ресурсов, – BBC, CNN, and Fox News, The New York Times и The Huffington Post. Ссылки данных источников были сокращены с помощью сервиса Bit.ly, который позволяет просматривать статистику переходов. За месяц сбора данных было получено 2,8 млн постов со ссылками, которые потенциально могли быть просмотрены 75 млрд раз, и 9,6 млн кликов, которые вели на почти 60 тыс. сторонних ресурсов.

Проанализировав количество переходов по ссылкам, исследователям удалось обнаружить в поведении пользователей Twitter ряд закономерностей. Во первых, они охотнее кликали на ссылки, которые были размещены обычными пользователями, а не самими новостными ресурсами, – согласно статистике, именно размещенные в аккаунтах пользователей ссылки приходилось большее число переходов (около 61 %).

Во-вторых, люди чаще ретвитили посты, чем переходили по ссылкам, ведущим на полный текст материала. На 56 % ссылок, упомянутых в Twitter, пользователи не кликали.

В третьих, ученые заметили, что информация в Twitter «живет» достаточно долго. Пользователи переходили по ссылкам иногда спустя несколько дней после того, как они были размещены.

Таким образом, исследователи говорят о том, что влияние, которое окажет размещенная в Twitter информация, очень трудно предсказать по количеству репостов.

Недавно портал Science Post проверил результаты работы на практике, опубликовав на сайте «текст-рыбу» под заголовком «70 процентов пользователей Facebook читают только заголовок научной статьи перед тем, как ее комментировать».

Маніпулятивні технології

19.06.2016

Twitter усовершенствовала функцию блокировки троллей и обидчиков

Едва ли от агрессии и троллинга в социальных сетях можно окончательно избавиться или хотя бы спрятаться. Но попытаться всё-таки можно. Twitter, в частности, старается делать всё возможное для того, чтобы пользователи сервиса чувствовали себя комфортно, и предлагает сразу три функции, позволяющие оградиться от нежелательных комментариев и неприятных личностей. Так, твиты можно игнорировать, на неприемлемые комментарии и оскорбления можно жаловаться, а нарушающих спокойствие пользователей можно отправлять в чёрный список. Однако последняя функция до сих пор работала неидеально. В определённых условиях владельцы заблокированных учётных записей всё равно могли увидеть, например, репосты твитов пользователей, желающих ограничить с ними взаимодействие, и наоборот. Наконец, компания решила обратить внимание на эту проблему и усовершенствовала механизм блокировки аккаунтов, пишет InternetUA.

Отныне пользователи, внесённые в чёрный список, полностью исчезнут из ленты новостей и не увидят записи тех, кто их заблокировал. Правда, они всё так же могут выйти из учётной записи и посмотреть общедоступные твиты или завести новый аккаунт и продолжить досаждать своей жертве с него.

Внести учётную запись в чёрный список можно и из профиля, нажав на значок шестерёнки, и прямо из твита, нажав на значок «Ещё».

***

8.06.2016

В Запорожье разоблачили Интернет-пропагандиста боевиков

В Запорожье сотрудники СБУ разоблачили пособника боевиков ДНР, который вел активную антиукраинскую пропаганду в Интернете, пишет InternetUA.

Об этом говорится на сайте спецслужбы.

«По заданию кураторов из ДНР он за деньги размещал в соцсетях материалы с призывами к насильственному изменению конституционного строя Украины, неповиновению власти…», – отметили силовики.

Также правонарушитель должен был подготовить для очередной «прямой линии» главаря «республики» А. Захарченко «правильные» вопросы якобы от имени жителей Запорожья – «представителей разных профессий и возрастов».

***

16.06.2016

После терактов в Париже на Twitter, Google и Facebook подали в суд

Отец погибшей в ходе терактов в Париже девушки подал в суд на Twitter, Google и Facebook из-за помощи в пропаганде «Исламского государства», сообщает портал TMZ, пишет InternetUA.

Р. Гонзалес, чья дочь Нохеми погибла от рук террористов, считает, что социальные сети позволили ИГ стать самой устрашающей террористической группировкой современности.

Истец обвиняет соцсети в халатности, на его взгляд, они допускают регистрацию аккаунтов террористов и таким образом помогают им в распространении экстремистских идей. Кроме того, истец подозревает YouTube (принадлежит Google) в получении прибыли с рекламы между роликами боевиков.

***

16.06.2016

Прокуратура: Розпочато досудове розслідування стосовно черкащанина, який у соцмережах закликав до зміни державного кордону України

Прокуратурою Черкаської області спільно з управлінням СБУ в Черкаській області викрито незаконну діяльність жителя Черкащини, який в одній із соціальних мереж Інтернет розміщував на власній персональній сторінці відеоматеріали з закликами до вчинення умисних дій щодо зміни меж території або державного кордону України, маючи на меті довести цю інформацію до широкого кола осіб, пише Провінція.

Вказана особа переховується від слідства й суду та за оперативною інформацією перебуває на території Російської Федерації.

Наразі проводяться всі необхідні слідчі та процесуальні дії для повного і всебічного розслідування всіх обставин справи, завершення досудового розслідування та скерування обвинувального акта до суду.

***

11.06.2016

На Кіровоградщині СБУ заблокувала діяльність інтернет-сепаратистів

Співробітники Служби безпеки України в червні 2016 р. припинили діяльність двох адміністраторів антиукраїнських груп у популярних соціальних мережах. Про це повідомляє Перша електронна газета за інформацією прес-групи УСБУ в Кіровоградській області.

Адміністратори спільнот «Кировоград Новороссия» та «Кировоград против ЕС» активно долучали мешканців регіону до антиукраїнської діяльності та спонукали їх до наповнення груп відповідними сепаратистськими матеріалами.

Служба безпеки України оголосила офіційні застереження про неприпустимість протиправної поведінки.

***

13.06.2016

За сторінку в соцмережі «Житомирская народная дружина» терористові загрожує до 15 років ув'язнення

Житомирянин підозрюється у створенні в соціальній мережі Facebook сторінки «Житомирская народная дружина», на якій протягом 2014–2015 рр. поширював інформацію антиукраїнського характеру на підтримку «ДНР» та розміщував інші матеріали, взяті з пропагандистських російських засобів масової інформації, пише Житомир-Онлайн.

Про це йдеться в повідомленні прес-служби прокуратури області. Місцевий терорист постане перед судом.

***

16.06.2106

Гибридная война: как проукраинскими пабликами руководят из Москвы

В документах «министра информации ДНР» обнаружен список с проукраинскими пабликами. Простые читатели видят админом девушку из Винницы, которая собирает средства для солдат в АТО, пишет «АНТИКОР».

Благодаря списку, который выложили на сайте «Миротворець», мы узнаем, что настоящий куратор проукраинских пабликов М. Мамедов живет в Москве. А девушка из Винницы В. Копейко – всего навсего часть матрицы.

В пабликах сделан стандартный уклон от ФСБ на украинских националистов, которые склонны к зраде. «Порошенко всех как всегда сливает, пиар мнимых псевдо героев Хорта, Завирухи» и т.д.

Цель Кремля понятна – убеждать народ в том, что украинский Президент предатель и его нужно убирать силовым путем.

Сколько еще таких пабликов – загадка, но подобные месседжи используют в паблике «Ми патріоти України», который принадлежит партии «Свобода».

Зарубіжні спецслужби і технології «соціального контролю»

6.06.2016

«ВКонтакте» предоставляет все данные о пользователях службам ФСБ

Высшие менеджеры российской социальной сети «ВКонтакте» сотрудничают со спецслужбами РФ (ФСБ), предоставляя им всю необходимую

информацию. Об этом масс-медиа проинформировал Е. Красников, пресс-секретарь популярной социальной сети, пишет InternetUA.

Российская социальная сеть «ВКонтакте», по заявлению её менеджеров, обеспечивает сотрудников Федеральной службы безопасности (ФСБ) всей необходимой им информацией. О том, как именно это делается, в московских масс-медиа рассказал Е. Красников, занимающий должность пресс-секретаря отечественной социальной сети, являющейся крайне популярным веб-ресурсом не только среди россиян, но и среди украинцев и белорусов.

В ходе проходящего форума в Казани представитель «ВКонтакте», отвечая на вопросы журналистов, ответил, что он, как гражданин своей страны, верит в то, что российские силовые структуры, которые имеют неограниченный доступ к личной информации пользователей ВК, «делают это исключительно во благо и для защиты государства и его граждан».

***

9.06.2016

Роскомнадзор проверит «ВКонтакте» на защиту персональных данных пользователей

В течение сентября Роскомнадзор намерен провести проверку соцсети «ВКонтакте» по вопросу соблюдения законодательства касательно защиты персональной информации пользователей. Проверка, предположительно, будет завершена в течение 20 дней, однако в случае превышения прогнозируемого объема документации, подлежащей проверке, процедура может быть продлена на такой же срок, пишет HiTech-News.ru.

Проверка будет осуществляться сотрудниками управление ведомства по Северо-Западному федокругу. Ранее в текущем году Роскомнадзор проводил проверку интернет-магазинов Ozon, Lamoda, KupiVip, а также сервиса SuperJob. На сегодняшний день ведется оценка степени защищенности персональных данных пользователей сервиса HeadHunter.

***

8.06.2016

Facebook блокирует рекламные аккаунты крымских предпринимателей

Социальная сеть Facebook с начала июня начала блокировать рекламные аккаунты крымских предпринимателей, пишет InternetUA.

Скриншоты ответов от администрации сети о том, что платежи проводить нельзя, появляются в социальных сетях, сообщает Searchengines.

При попытке сделать платеж предприниматели из региона теперь получают однотипное сообщение: «Мы отключили возможность осуществления платежей для вашего аккаунта, поскольку вы находитесь в

регионе, где эта функция не поддерживается. Нам очень жаль, если это доставляет вам какие-нибудь неудобства».

Блокируются аккаунты всех пользователей, которые физически находятся на территории полуострова. Это не зависит от того, какая именно карта используется для платежей.

Для того, чтобы платежи блокировались, достаточно авторизоваться в аккаунте с любыми крымскими идентификаторами. Даже если позже подключиться с некрымского IP, доступ к платежам не восстановится.

***

10.06.2016

Власти Крыма советуют уходить из Facebook в «Одноклассники»

Вице-спикер крымского парламента А. Козенко считает, что блокировка рекламных аккаунтов жителей полуострова со стороны Facebook является боязнью выхода информации о реальной жизни в российском Крыму, пишут Новости Крыма.

«Facebook дает крымчанам определенную возможность показать свою позицию пользователям из других стран, включая западных. Мы можем говорить, что сделали осознанный выбор в пользу России и гордимся этим. Поэтому сегодня такие ограничения со стороны Facebook мы воспринимаем как определенную боязнь выхода объективной информации о реальной обстановке дел в Крыму», – сказал А. Козенко.

Вице-спикер считает, что ограничения, связанные с интернет-технологиями, являются вопиющими, но даже из этого стоит сделать вывод.

«Понятно, что Facebook – это мега-корпорация, которая смотрит на Крым свысока, но нам тоже стоит дать понять, что крымчане готовы развивать альтернативные направления. На сегодня весь интернет-контент максимально приближен к западным стандартам. Необходимо развивать свой отечественный сегмент интернет-рынка с русскими стандартами», – сказал А. Козенко.

Он подчеркнул, что аналогами Facebook по своим функциям являются российские интернет-платформы «ВКонтакте» и «Одноклассники».

***

10.06.2016

К антикрымским санкциям присоединился Instagram

Вместе с социальной сетью Facebook, рекламной деятельности крымских пользователей препятствует Instagram.

Политика этих ресурсов сделала невозможной продвижение коммерческих новостей без дополнительных капиталовложений.

Об этом сообщил учредитель крымской маркетинговой студии «Я свой» И. Морозов, передает «РИА Новости», пишет allcrimea.net.

«Мы сейчас вынуждены действовать, как говорится, в рамках импортозамещения и переводим все бюджеты на социальные сети «ВКонтакте» и «Одноклассники». Но это немного не то, поскольку целевая аудитория Facebook более деловая и представительная», – подчеркнул И. Морозов.

***

16.06.2016

Американцы решили бороться с продажей оружия через Instagram

В американском Конгрессе после массового расстрела в гей-клубе в Орландо задумались о запрете продажи оружия через социальные сети и аналогичные по функционалу онлайн-сервисы. В частности, необходимость регулирования оружейного рынка в соцсетях отметили сенаторы Э. Марки и К. Мерфи. Об этом сообщает издание Wired, пишет InternetUA.

«Нужно запретить продажу оружия через сайты вроде Facebook или Instagram. Сейчас с помощью фотосервиса пользователи с легкостью могут найти оружие, выставленное на продажу», – заявил Э. Марки.

По данным Wired, в Instagram на момент заявления политиков было опубликовано около 8 тыс. постов с хештегом #gunsforsale («оружие на продажу»).

В настоящее время посты с хештегом #gunsforsale скрыты из поиска администрацией фотосервиса. В Instagram объяснили решение об их удалении несоответствием внутренним правилам сервиса. «Это не место для поддержки терроризма, организованной преступности или ненавистнических групп. У нас запрещено предлагать сексуальные услуги, продавать и покупать оружие или наркотики, даже если они легальны в вашей стране», – пояснили в Instagram.

Однако Wired отмечает, что продавцы оружия иногда используют комбинации различных хештегов или личные сообщения, что существенно усложняет борьбу с их коммерческой деятельностью в фотосервисе. Например, снимки с хештегами #AK47 или #AR15, которые также могут использоваться для торговли оружием, удалены не были. По первому поисковому запросу фотосервис находит около 500 тыс. постов, а по второму – почти миллион.

***

16.06.2016

В Алжире на время школьных экзаменов заблокировали все соцсети

Власти Алжира временно заблокировали доступ к социальным сетям по всей стране, чтобы не дать возможность пользоваться подсказками на экзаменах в средних школах, пишет InternetUA.

Почти половина учащихся была вынуждена пересдать экзамен на аттестат о среднем образовании из-за скандала с утечкой в сеть экзаменационных заданий.

В начале июня многие пользователи Facebook и других соцсетей смогли узнать контрольные вопросы на предстоящих экзаменах.

***

16.06.2016

Российских госслужащих обяжут предоставлять данные об активности в соцсетях

Депутаты Госдумы РФ разработали законопроект, обязывающий государственных и муниципальных служащих, а также претендентов на эти должности информировать начальство о своих учетных записях в социальных сетях. Сокрытие данных о личных страницах чревато увольнением, сообщает РБК, пишет InternetUA.

16 июня соответствующие поправки в правительственный законопроект, описывающий требования к государственным и муниципальным служащим, были одобрены профильным комитетом по местному самоуправлению.

Авторами законопроекта являются представители ЛДПР А. Луговой и «Единой России» В. Бурматов. Если предложение депутатов будет принято, в законах о государственной гражданской службе и муниципальной службе появятся новые статьи, обязывающие сообщать нанимателю адреса веб-сайтов и страниц, где «служащий размещал общедоступную информацию», а также данные, позволяющие определить эти ресурсы.

Согласно поправкам, претендент на пост государственного чиновника должен предоставлять все сведения о своих публикациях в сети за три года до поступления на службу. Действующие служащие обязаны отчитываться об активности в соцсетях каждый год до 1 апреля. Об информации, опубликованной в рамках исполнения своих обязанностей, сообщать не нужно. В случае не предоставления требуемой информации служащим грозит увольнение, а устраивающийся на работу не получит должность.

***

14.06.2016

АНБ изучает способы взлома электрокардиостимуляторов

С ростом популярности «Интернета вещей» увеличивается число потенциальных векторов кибератак, что делает «умные» устройства привлекательной целью не только для хакеров, но и для спецслужб. Как сообщает издание The Intercept, Агентство национальной безопасности США изучает способы получения необходимых данных через медицинские приборы, начиная с термостатов и заканчивая электрокардиостимуляторами, пишет InternetUA.

Как сообщил заместитель директора АНБ Р. Леджетт в ходе своего выступления на конференции в Вашингтоне, посвященной военным технологиям, сотрудники спецслужбы «прямо сейчас рассматривают такую

возможность с точки зрения исследований». Р. Леджетт полностью согласен с тем, что для отслеживания террористов и иностранных шпионов существуют гораздо более простые способы. Однако, по его словам, медицинские устройства также могут предоставлять АНБ полезную информацию. На вопрос о том, чем станет для сотрудников спецслужбы обработка данных миллиардов подключенных к Интернету устройств, золотым дном или ночным кошмаром в плане безопасности, замдиректора ответил: «И тем, и другим».

В ходе конференции Р. Леджетт также объяснил, почему спецслужба не оказала содействие ФБР в разблокировке iPhone, принадлежащего террористу из Сан-Бернардино. У АНБ есть строгий список источников информации, и конкретно эта модель устройства в него не входит. Спецслужба специализируется на технологиях, которыми пользуются преступники, а не на популярных гаджетах.

«Мы не работаем с каждым телефоном и его различными моделями. Если у нас нет плохого парня, пользующегося таким телефоном, мы с ним не работаем», – заявил Р. Леджетт.

***

18.06.2016

Twitter постачає інформацію для RussiaToday, але відмовляє ЦРУ

Twitter відмовляється робити аналітичні звіти та сортувати твіти в режимі реального часу для Центрального розвідувального управління США, тоді як надає ці послуги для російської компанії Russia Today. Прокоментувати ці повідомлення попросив в очільника ЦРУ Д. Бреннана сенатор Т. Коттон, пише «Голос Америки».

«Чи ви не розчаровані, що американська компанія продає свій продукт для Russia Today, яка є пропагандистською зброєю російського уряду, і водночас не співпрацює з розвідувальним товариством у США», – запитав законодавець Т. Коттон.

Глава американської розвідки прямо не підтвердив цього, але відповів, що «не збирається з ними сперечатися».

«Я розчарований, що немає більше активної співпраці з правоохоронними органами, яка могла б бути з боку приватного сектору США», – сказав Д. Бреннан.

У директора ЦРУ законодавці також запитали, чи Russia Today є клієнтом компанії Dataminr, що спеціалізується на зборі інформації у Twitter. «Я так думаю, але до кінця не впевнений. У мене не було інформації, що для них (для Dataminr. – Ред.) перестали надавати послуги», – відповів очільник ЦРУ.

Компанія Dataminr в реальному часі аналізує мільйони загальнодоступних твітів. Коли у світі щось відбувається, спеціальна програма фіксує спалах повідомлень про подію та повідомляє про це своїх клієнтів. Це допомагає фінансовим компаніям швидше реагувати на події, медики можуть

раніше дізнаватися про спалахи хвороби, а кінокомпаніям це допомагає оцінити перспективи нових фільмів.

Коли в Парижі трапилися теракти у грудні минулого року, саме Dataminr оперативно повідомила про це спецслужби США. 5 % акцій у Dataminr належить компанії Twitter.

Проблема захисту даних. DDOS та вірусні атаки

6.06.2016
В сети опубликованы пароли 100 млн пользователей «ВКонтакте»

Сетевой злоумышленник, который ведет работу под псевдонимом Peace, выкрал и выставил на продажу личные данные, учетные записи и пароли к ним свыше 100 млн пользователей известной отечественной соцсети «ВКонтакте». Хакер получил стал обладателем данных по итогам кибератаки, совершенной в 2011–2013 гг., пишет InternetUA.

Вся информация выставлена на продажу по стоимости в 1 биткоин (эквивалентно приблизительно 570 дол.) в рамках одной из онлайн-платформ с Интернете, проинформировали на страницах американского онлайн-портала Motherboard.

Как подчеркивается в сообщении, хакер владеет личной информацией, которая принадлежит порядка 70 млн пользователей «ВКонтакте», но ее, на текущий момент, он реализовать не намерен. Иной портал – LeakedSource – проверил все представленные данные и проинформировал, что среди 100 аккаунтов, выбранных в случайном порядке, 92 оказались функционирующими.

***

6.06.2016
«ВКонтактє» запевняє, що хакерська база даних уже застаріла

Представник «ВКонтакте» Є. Красніков запевняє, що хакерська база даних не несе загрози для користувачі цієї соцмережі, пише видання Украинские реалии.

Про це він заявив, коментуючи інформацію про те, що хакер під прізвиськом Peace виставив на продаж у «дарквебі» базу з даними понад 100 млн користувачів «ВКонтакте».

За словами Є. Краснікова, виставлені на продаж паролі не актуальні з 2012 р.

«Злому бази даних «ВКонтакте» не було, йдеться про стару базу логінів/паролів, яку шахраї збирали в період з 2011 до 2012 р. Усім згаданим у ній користувачам дані для входу на сторінки змінювалися примусово», – сказав він.

«У профілактичних цілях ми б хотіли ще нагадати користувачам «ВКонтакте» про неприпустимість установки неперевіреного ПЗ на свої пристрої, можливість обрати двофакторну аутентифікацію в налаштуваннях аккаунта й застерегти від використання простих паролів, які легко підбираються», – додав Є. Красніков.

***

6.06.2016
Хакеры взломали аккаунты Цукерберга в соцсетях

Хакеры взломали аккаунты основателя Facebook М. Цукерберга в социальных сетях Instagram, Twitter, LinkedIn и Pinterest. Об этом в в понедельник, 6 июня, сообщает BBC News, пишет InternetUA.

Ответственность взяла на себя группа Ourmine, у которой более 40 тыс. подписчиков в микроблоге Twitter.

Отмечается, что в аккаунте Twitter Цукерберга, которым он не пользуется с 2012 г., появилось сообщение от хакеров, информирующее о взломе. Авторы поста заявили, что решили проверить на прочность уровень защиты системы и предложили основателю Facebook связаться с ними.

***

6.06.2016
В Facebook отрицают «микрофонный шпионаж» на смартфонах

Компания Facebook опровергла обвинения в том, что она якобы подслушивала за разговорами пользователей через микрофон, встроенный в мобильное устройство, чтобы точнее «нацеливать» на них рекламу. Как подчеркнули в пресс-службе, соцсеть «не использует микрофон вашего телефона, чтобы влиять на рекламу или менять то, что вы видите в «Хронике'», пишет InternetUA.

В Facebook настаивают, что содержимое объявлений зависит исключительно от интересов людей и другой информации, указанной в профиле. Так компания отреагировала на слова профессора по массовым коммуникациям Южно-Флоридского университета К. Бернс, заподозрившую соцсеть в «прослушке». Ранее на этой неделе она заявила изданию The Independent, что Facebook тайно слушает разговоры пользователей, однако не предоставила каких-либо доказательств.

Представители Facebook разъяснили, что приложение запрашивает доступ к микрофону и записывает звук только при использовании функций, непосредственно связанных с аудио. В качестве примера компания привела запись видео или функцию, которая распознает музыку и встраивает название песни в обновление статуса.

В любом случае, сомневающиеся в честности Facebook пользователи могут отключить приложению доступ к микрофону в любой момент. Чтобы

сделать это на iOS, зайдите в «Настройки» – «Конфиденциальность» – «Микрофон» и потяните слайдер напротив Facebook в положение выкл. На Android нужно открыть «Приватность и безопасность» в настройках, найти раздел с микрофоном и отключить его для Facebook.

***

7.06.2016

Опаснейший банковский вирус Bolik атакует Windows-пользователей

«Доктор Веб» предупреждает о появлении очень опасного полиморфного файлового вируса, способного красть деньги со счетов клиентов российских банков, похищать конфиденциальную информацию и различными способами шпионить за своей жертвой. Вредоносная программа получила название Bolik, пишет InternetUA.

Зловред наследует некоторые технические решения широко известных банковских троянов Zeus (Trojan.PWS.Panda) и Carberp, но в отличие от них умеет распространяться без участия пользователя и заражать исполняемые файлы. Функция самораспространения активируется по команде злоумышленников, после чего Bolik начинает опрашивать доступные для записи папки в сетевом окружении Windows и на подключенных USB-устройствах, ищет хранящиеся там исполняемые файлы и заражает их. При этом вирус может инфицировать как 32-х, так и 64-разрядные приложения.

Если пользователь запустит инфицированное приложение, вирус расшифрует банковского трояна и запустит его прямо в памяти атакуемого компьютера, без сохранения на диск. При этом зловред имеет специальные механизмы, затрудняющие работу антивирусов: программа, в частности, может «на лету» изменять код и структуру собственной части, а в её архитектуре предусмотрены своеобразные «замедлители», состоящие из множества циклов и повторяющихся инструкций.

Основное назначение Bolik – кража различной ценной информации у клиентов российских банков. Для этого применяются разнообразные инструменты. Например, вирус может контролировать данные, передаваемые и отправляемые браузерами Internet Explorer, Chrome, Opera и Firefox. Благодаря этому троян способен похищать информацию, которую пользователь вводит в экранные формы.

Кроме того, в шпионский арсенал банкера входит модуль для создания снимков экрана (скриншотов) и фиксации нажатий пользователем клавиш (кейлоггер). Bolik умеет создавать на заражённой машине собственный прокси-сервер и веб-сервер, позволяющий обмениваться файлами со злоумышленниками. Вирус способен организовывать так называемые «реверсные соединения»: с их помощью киберпреступники получают возможность «общаться» с заражённым компьютером, находящимся в защищённой брандмауэром сети или не имеющим внешнего IP-адреса, то есть работающим в сети с использованием NAT (Network Address Translation). Вся

информация, которой Bolik обменивается с управляющим сервером, шифруется по сложному алгоритму и сжимается.

***

8.06.2016

Хакеры научились менять отправленные сообщения в Facebook

Специалисты по интернет-безопасности компании Check Point Software Technologies обнаружили уязвимость в мессенджере от Facebook, благодаря которой хакеры могут вносить изменения в уже отправленные сообщения, сообщает Mashable, пишет InternetUA.

Чтобы обнаружить данную проблему, эксперты воспользовались уникальным идентификатором сообщения (message ID), с помощью которого можно изменять содержание отправленных посланий без ведома пользователей.

Данная брешь в системе позволяет хакерам заменять отправленный контент, например, на вредоносный код или же полностью переделывать содержание переписки извне.

Компания Check Point уже сообщила о найденной уязвимости в Facebook.

***

8.06.2016

Версии Windows от 2000 до 10 подвержены уязвимости «нулевого дня»

Специалисты исследовательской компании Trustwave SpiderLabs сообщили об обнаружении «уязвимости нулевого дня», пишет InternetUA.

Исследователи сообщили, что под угрозу попадают все версии Windows, начиная с Windows ME и заканчивая актуальной Windows 10. Владелец данного эксплойта собирается продать его за 90 000 долл.

«Дыра» скрывается в драйвере ядра win32k.sys. При превышении локальных прав компьютер можно заразить вредоносным кодом и воровать пользовательские данные, вроде банковской информации из POS-терминалов.

Компания Trustwave SpiderLabs уже сообщила Microsoft о своей находке.

***

7.06.2016

Хакеры опубликовали более 36 млн записей из баз данных MongoDB

Постепенный переход в мир BigData, где обычные реляционные базы данных не справляются с поставленной на них задачей, влечет за собой дополнительные угрозы безопасности. Еще не так давно решения для хранения огромных массивов данных не пользовались особой популярностью, и как в случае с обычным программным обеспечением, в их дизайн изначально не закладывались основные принципы безопасности, пишет InternetUA.

Ситуация с MongoDB ярко демонстрирует существующие проблемы с разработкой ранее редко используемого ПО. Заявления разработчиков, что «MongoDB не содержит уязвимостей, а пользователи просто идиоты», комментируя отсутствие включенной по умолчанию авторизации для подключения к БД, свидетельствует лишь о нежелании вендора уделять должного внимания безопасности своих пользователей.

На этой неделе стало известно о том, что хакерская группировка TeamGhostShell выложила в открытый доступ базы данных MongoDB, содержащие в общей сложности более 36 млн записей. Данные были получены с некорректно сконфигурированных серверов MongoDB, позволяющих подключение к базе данных без авторизации.

Утечка была обнаружена ИБ-специалистами из Hacked-DB Й. Мизрахи и О. Якоби. Исследователи обнаружили архив, содержащий 110 IP адресов баз данных, которые подверглись взлому. На скомпрометированных серверах хранилось много конфиденциальных данных, включая логины, пароли, имена пользователей, телефоны, физические и email адреса.

Ранее хакеры из группировки TeamGhostShell выложили в открытый доступ 700 тыс. записей с учетными данными сотрудников государственных структур, банковских учреждений, учебных заведений, индустриальных компаний и транспортных служб Южной Африки. До этого хакеры успешно атаковали 100 ведущих университетов в мире и рекрутинговые компании на Уолл-Стрит.

***

7.06.2016

Microsoft: Flash присутствует в 90 % вредоносных веб-страниц

Компания Microsoft выпустила небольшой доклад, который предлагает краткое содержание 160-страничного ежегодного доклада Security Intelligence Report, представленного в начале мая. Было выделено десять ключевых трендов кибербезопасности нынешнего года, пишет InternetUA.

Microsoft пишет, что за последние три года количество багов растёт и они становятся всё опаснее. В 2015 г. 41,8 % обнаруженных уязвимостей были признаны опасными, и по мере включения в анализ всё большего числа устройств этот процент растёт.

Microsoft говорит об уходе злоумышленников от использования уязвимостей Java. Причиной может быть добавление компанией Oracle функции безопасности Click2Play, которая затрудняет автоматическое использование объектов Java. Похожий доклад от группы NTT пришёл к тому же заключению, говоря о почти полном исчезновении Java из комплектов эксплоитов 2015 г. и большем сосредоточении на Flash.

Компании осознают опасности вредоносного ПО для своей репутации и финансов, поэтому ответственнее относятся к защите. Поэтому чаще жертвами

становятся домашние компьютеры без мощных антивирусов и прочих видов защиты.

***

8.06.2016

Взломаны форумы BitTorrent, утекли данные как минимум 34 000 пользователей

Команда проекта uTorrent, который является частью BitTorrent Inc, предупреждает своих пользователей о компрометации форумов uTorrent, на которых зарегистрировано более 388 тыс. человек. О проблемах с форумами также сообщают и представители самой компании BitTorrent. Судя по всему, дело в платформе Invision Power Board (IP.Board), на базе которой работают форумы проектов, пишет InternetUA.

Издание Torrent Freak сообщает, что ранее на этой неделе разработчиков uTorrent уведомили об уязвимости в некоем продукте стороннего производителя. Теперь команда разработчиков просит всех пользователей форумов сменить пароли, в качестве меры предосторожности, так как БД форума могла подвергнуться компрометации. Соответственное предупреждение появилось на самих форумах проекта, но индивидуально (посредством email) пользователей пока не уведомляли.

Разработчики рассказали журналистам Torrent Freak, что пока проводят расследование и не знают, сколько человек пострадало из-за уязвимости, и какие именно данные могли попасть в руки злоумышленников. Разработчики отмечают, что хеши паролей лучше считать скомпрометированными.

Издание Vice Motherboard в свою очередь сообщает, что форумы BitTorrent тоже подверглись атаке. По данным журналистов, которые сумели заполучить образец утечки, компрометации подверглись 34 тыс. пользователей. Утекли email-адреса, IP-адреса, имена пользователей и «соленые» хеши паролей (SHA1).

«Мы можем подтвердить, что возникла проблема с безопасностью, затрагивающая производителя наших форумных решений, – сообщил представитель BitTorrent К. Аверилл в письме журналистам. – Судя по всему, уязвимость возникла у одного из других клиентов производителя, но она позволила атакующим получить доступ к некоторой информации других аккаунтов, в том числе наших. В результате атакующие сумели скачать список пользователей наших форумов. Мы проводим дальнейшее расследование инцидента».

Похоже, корень проблемы кроется в форумной платформе Invision Power Board (IP.Board), с которой работали оба пострадавших проекта. Т. Хант, создатель агрегатора утечек Have I Been Pwned?, уже располагает копией утечки. Он подтверждает слова журналистов Motherboard относительно 34 тыс. пострадавших и «соленых» хешей SHA1. Также Т. Хант пишет: «Паттерн [этого случая] схож со многими утечками прошлого. Базирующиеся на PHP

форумы хранят пароли настолько ненадежно, что операторы сайтов даже не осознают того, что у них произошла утечка».

***

9.06.2016
Сайт прокремлівського «Первого канала» хакнули українці

Хакери українського кіберальянсу FalconsFlame, Trinity і Рух8 зламали корпоративний портал російського пропагандистського «Первого канала», пише InternetUA.

Про це повідомили волонтери міжнародної спільноти InformNapalm на своєму сайті й розкрили деталі злому.

За словами кіберактивістів, операція зі зламу ланок машини російської пропаганди реалізована в рамках проекту з примушення Росії до деокупації Донбасу і виконання нею зобов'язань за Мінськими угодами. «Кібератаки спрямовані виключно на ті елементи російської пропаганди, які займаються приховуванням інформації щодо військових злочинів РФ на території України», – ідеться в повідомленні волонтерів.

Внаслідок зламу були опубліковані анкетні дані всіх співробітників «Первого канала». Крім того, з'явилася можливість зламати особисті поштові скриньки і хмарні сховища працівників, які особливо відзначилися у створенні і просуванні агресивної пропаганди щодо України та її громадян, передають хакери.

***

9.06.2016
Хакер выставил на продажу 32 млн Twitter-аккаунтов

Хакер Tessa88 выставил на продажу базу данных, состоящую более чем из 32 млн учетных записей сервиса микроблогов Twitter. Об этом сообщает LeakedSource, пишет InternetUA.

Цена составляет 10 биткоинов (примерно 5800 долл.). Большая часть аккаунтов принадлежит российским пользователям. База данных включает в себя адреса электронной почты, логины и пароли.

Издание отмечает, что сам Twitter не был взломан. Предполагается, что злоумышленник получил сведения благодаря вредоносному программному обеспечению.

Выборочная проверка нескольких аккаунтов показала, что 15 из 15 паролей являются действительными.

***

13.06.2016
Как защитить себя от слежки в Интернете

Life собрал рекомендации самого известного бывшего сотрудника спецслужб США о том, как обезопасить себя в сети, пишет InternetUA.

1. Шифрование голосовых вызовов и текстовых сообщений. Е. Сноуден – абсолютный сторонник шифрования всего хранящегося и передаваемого контента. Сейчас существует множество приложений, обладающих функциями зашифровки. Причём среди них есть распространённые и известные мессенджеры, как, например, WhatsApp, Telegram, ICQ. Кстати, самый популярный – WhatsApp – в апреле 2016 г. ввёл полное сквозное шифрование.

Самым любимым мессенджером для общения сам Е. Сноуден называет Signal (есть для iOS и Android), которым, как писал в своём Twitter, он пользуется каждый день. Разработкой приложения занимается компания Open Whisper Systems, также предлагающая шифровку звонков.

2. Шифрование жёсткого диска. Вдобавок к защите мобильных устройств бывший агент ЦРУ также советует обезопасить свой компьютер, в частности, жёсткий диск. В Интернете можно найти инструкции, как это сделать. Обычно используется специальное ПО. Например, для Windows есть программа, предустановленная в расширенных версиях ОС, – BitLocker, для Mac – FileVault. Таким образом, если компьютер украдут, злоумышленник не сможет прочитать ваши данные.

3. Менеджеры паролей. Полезная вещь, о которой большинство людей даже не задумываются. Такие программы позволяют держать свои пароли в порядке – создавать уникальные ключи и хранить их. По словам Е. Сноудена, одной из самых распространённых проблем онлайн-приватности являются утечки: допустим, сервис, на котором пользователь зарегистрировался в 2007 г., подвергся атаке и данные утекли в сеть, – достаточно вспомнить недавно появившиеся сообщения о продаже миллионов паролей от аккаунтов в сетях Twitter, «ВКонтакте», MySpace, LinkedIn. На рынке есть разные менеджеры паролей, такие как 1Password, KeePassX и LastPass.

4. Двухфакторная аутентификация. Контрольные слова, ранее предлагаемые на крупных сервисах и позволяющие восстановить пароль по ним, уходят в прошлое. Сейчас все популярные онлайн-площадки – Facebook, «ВКонтакте», почтовые клиенты, Twitter, Dropbox – перешли на двуступенчатую аутентификацию. Она позволяет привязать к своему аккаунту номер телефона, с помощью которого будет происходить дополнительная авторизация при входе в учётную запись. Также она поможет восстановить утерянный пароль. Правда, придётся «засветить» свой мобильный телефон, что даёт возможность идентифицировать вас с указанным номером (как это делает, например, Facebook, позволяя найти пользователя по его телефону).

5. Tor. Анонимную сеть Tor (сокр. The Onion Router) бывший сотрудник АНБ называет «самым важным технологическим проектом для обеспечения конфиденциальности из ныне используемых». Он заявлял, что пользуется им на ежедневной основе. Tor позволяет «заметать следы» в Интернете, то есть обеспечивает анонимность, затрудняет возможность определить IP-адрес и

местоположение человека. Осуществляется это за счёт подключения через цепочку промежуточных компьютеров, принадлежащих различным пользователям сети. Проект поддерживается исключительно добровольцами. Наиболее простой способ использования системы – через одноимённый браузер (Tor Browser).

6. И ещё раз о паролях. Е. Сноуден советует использовать в качестве ключа к аккаунту не слова типа onetwothreefour («одиндватричетыре») или даже password («пароль»), а нечто более замысловатое, что не сможет подобрать даже компьютер, но при этом запоминающееся – margaretthatcheris110 %SEXY («маргареттетчерСЕКСУАЛЬНАна110 %»).

Для особых параноиков

Бывший агент АНБ продемонстрировал журналисту, как избежать тотальной слежки спецслужб, которые могут дистанционно включить микрофон или камеру на смартфоне и начать прослушивать. Ответ простой – вытащить из устройства модули микрофона и камеры. Взамен предлагается использовать внешний аксессуар и отучиться от селфи.

***

13.06.2016

Опасности соцсетей: как не стать жертвой

Излишняя откровенность может обернуться потерей денег и даже тюрьмой, пишет InternetUA.

Пользователи соцсетей, сообщающие в своем аккаунте подробную информацию о себе: имя, фамилию, электронную почту, номер телефона, сохраняющие пароли доступа к своей страничке на серверах соцсетей, могут столкнуться с серьезными неприятностями, если их страничка будет взломана хакерами. Такие случаи нередки, что показал свежий скандал со взломом сервера с информацией о пользователях популярной соцсети «ВКонтакте».

Цель хакеров

Как разъяснил нам глава Департамента киберполиции Национальной полиции Украины полковник С. Демедюк, обычно хакеры продают данные мошенникам, которые используют чужие аккаунты для зарабатывания денег. Хотя и сами не чураются заработать на обнаруженной «клубничке», которой люди, прежде всего известные, неосторожно делятся в закрытых группах «для своих», думая, что чужие этого не увидят.

«Самый популярный способ – это шантаж, например, человек в закрытой группе публикует свои интимные фото или компрометирующую переписку, после взлома все это попадает к злоумышленникам, – говорит С. Демедюк. – Хакеры требуют немалые деньги за то, что эти снимки не появятся в открытом доступе. Но куда более опасно, если от вашего имени начнут публиковать объявления о продаже оружия или наркотиков, о торговле людьми. Когда спецслужбы заинтересуются таким «бизнесом», они выйдут на человека, а он понятия не имеет, что от его имени совершается преступление.

Полицейский говорит, что спецслужбы в конечном итоге определят, что аккаунт был взломан, но «потерпевший нервов потратит немало». Что касается совершения тяжких преступлений с помощью взломанных аккаунтов – например, определить по фото в соцсети богатого человека и похитить его или его близких с целью выкупа, либо обокрасть его дом, то, по словам С. Демедюка, такие случаи чрезвычайно редки.

А IT-эксперт И. Вилков говорит, что базы данных используются в кибервойнах, например, от имени реальных пользователей публикуются записи с критикой власти, призывающие к свержению госстроя, насилию. «Также такие базы интересуют тех, кто занимается маркетингом – для рассылки рекламы и изучения рынка продаж», – добавил И. Вилков.

Как защититься

По словам И. Вилкова, в том, что их пароли и логины стали доступными, виноваты сами пользователи. «Я бы посоветовал поменьше выкладывать личных фото типа «я на Мальдивах», по минимуму ставить приложения вроде «кто был на моей странице», различные игры, так как они собирают слишком много информации о пользователе. И, конечно же, создать надежный пароль: минимум 8 символов, а лучше до 20-ти, включая большие и маленькие буквы и спецсимволы – знаки препинания, проценты, и никогда не запоминать его на компьютере», – говорит Вилков.

А вот директор IT-компании Ю. Савицкий считает, что взломать можно любой пароль, и советует привязывать аккаунт к мобильному телефону для смс-авторизации. «Это немного неудобно, но шанс потерять аккаунты снижается многократно. Также не стоит сообщать личную почту – через нее можно украсть пароль аккаунта в соцсети даже дилетанту с помощью функции «забыл пароль», и особенно не давайте номер телефона. Бывает, мошенники восстанавливали сим-карту у оператора как утерянную и потом от имени абонента совершали звонки, взламывали аккаунт и даже снимали деньги с банковского счета», – советует Ю. Савицкий.

***

13.06.2016

Хакеры пытаются обойти двухфакторную аутентификацию Google

В сети появился новый трюк, которым можно заставить пользователей выдать код двухфакторной аутентификации мошенникам, которые прикрываются заботой о безопасности пользователя. Двухфакторная аутентификация (2FA) предлагает второй уровень защиты, которую поддерживают многочисленные онлайн-сервисы – банки, государственные учреждения, Google, Facebook и Microsoft, пишет InternetUA.

2FA запрашивает у пользователя ввод пароля, который он получает на свой сотовый телефон в смс-сообщении, заходя в свою учётную запись. Если пользователь не вводит этот пароль вовремя, делается вывод о попытке взлома и пользователь лишается доступа к аккаунту.

Сооснователь Clearbit.com А. МакКау опубликовал изображение полученного им смс Неизвестный хакер отправил его якобы от имени Google.

Данный метод социальной инженерии говорит о том, что якобы имела место попытка входа в аккаунт пользователя, и что если это был не сам пользователь, он должен ответить, отправив 6-значный код. Код приходит на телефон пользователя от сервиса после того, как хакеры пытаются выполнить нелегальный вход в аккаунт. Таким образом, пользователя пытаются ввести в заблуждение и заполучить код для входа в его учётную запись.

***

12.06.2016

Приложение-вымогатель Crysis пришло на смену TeslaCrypt

Три недели назад компания ESET рассказала о прекращении операций авторами приложения-вымогателя TeslaCrypt, однако теперь появились сведения о появлении на его месте новой угрозы. Приложение под названием Crysis, первые версии которого были обнаружены в феврале, оказались далеки от идеальных, так что в ESET говорили о возможности взломать приложение и вернуть зашифрованные файлы без выкупа, пишет InternetUA.

К сожалению, того же самого столь уверенно нельзя сказать о последних версия программы. Сильный механизм шифрования Crysis охотится за локальными файлами и файлами с общим доступом, а также содержимым съёмных дисков.

Crysis не разбирается в расширениях файлов и шифрует всё подряд (даже файлы без расширений), кроме собственных файлов и системных файлов Windows. Завершив процесс шифрования, Crysis подключается к командному серверу, отсылает данные компьютера для его дальнейшей идентификации и сообщает количество зашифрованных файлов.

Далее остаётся только поместить на рабочий стол жертв текстовый файл с требованием выкупа и внести изменения в рабочий стол. Большинство вымогателей имеют сайт для внесения денег, но Crysis собственным сайтом обзавестись не успел. Вместо сайта используются два адреса электронной почты из текстового файла и изображение на обоях рабочего стола.

ESET говорит, что сумма выкупа составляет 450 до 1000 долл. Платежи производятся в биткоинах.

***

12.06.2016

«Бестелесный» троян Kovter скрывается в реестре Windows

«Доктор Веб» предупреждает о распространении вредоносной программы Kovter (Trojan.Kovter.297), особенность которой заключается в «бестелесной» архитектуре.

Троян работает в оперативной памяти инфицированного компьютера, не сохраняя собственную копию на диске в виде отдельного файла, что в определённой степени затрудняет его поиск и удаление. Зловред прячется в реестре Windows, где создаёт несколько записей: одна содержит само тело трояна в зашифрованном виде, вторая – скрипт для его расшифровки и загрузки в память компьютера. Имена этих записей включают специальные нечитаемые символы, поэтому стандартная программа regedit не может их показать, пишет InternetUA.

Kovter относится к рекламным троянам. Он незаметно для пользователя запускает в фоновом режиме несколько экземпляров браузера Microsoft Internet Explorer, «посещает» с их помощью указанные злоумышленниками сайты и накручивает количество просмотров рекламы, «нажимая» на рекламные ссылки и баннеры. Таким образом, киберпреступники получают прибыль от организаторов партнёрских программ и рекламодателей, размещающих рекламу с оплатой за нажатия и переходы.

Для распространения Kovter служит другая вредоносная программа – троян MulDrop6. Он содержит множество случайных строк и вызовов функций, чтобы усложнить его анализ, а основная вредоносная библиотека замаскирована под картинку. Этот зловред умеет показывать на экране компьютера произвольные сообщения и отключать функцию контроля учётных записей пользователя Windows (User Accounts Control, UAC). Кроме того, вредоносная программа может копировать себя в корневые папки всех подключенных к заражённой машине дисков, создавая там файл автозапуска autorun.inf, то есть, распространяться подобно червю.

***

12.06.2016

19 % аккаунтов детей подвергаются взлому

Антивирусная компания ESET представила результаты опроса, согласно которым 19 % детей столкнулись со взломом своих аккаунтов в социальных сетях, пишет InternetUA.

11 % опрошенных родителей сообщили, что дети добавляют в друзья пользователей с фейковыми аккаунтами. В ESET считают, что поддельные страницы могут быть не только развлечением одноклассников, но и «рабочим инструментом» злоумышленников.

Еще 10 % респондентов лишились денег из-за того, что дети подписывались на платные игры и дорогие сервисы.

6 % родителей рассказали, что злоумышленники присылали вредоносные ссылки, а 3 % респондентов сообщили, что их дети вступали в переписку с мошенниками. Еще 3 % назвали угрозой кибербуллинг.

По мнению 29 % респондентов, их дети никогда не сталкивались с проблемами в сети.

В опросе ESET приняли участие 1200 родителей.

***

12.06.2016

Уязвимость в беспроводной камере D-Link позволяет подглядывать в чужие дома

В беспроводной камере D-Link DCS-930L, предназначенной для видеонаблюдения за домом или офисом, обнаружена серьёзная уязвимость. С её помощью злоумышленники могут запустить на этом устройстве произвольный код, сбросить пароль и перехватить передаваемое видео, пишет InternetUA.

Камера D-Link DCS-930L рассчитана на обычных пользователей и не нуждается в сложной настройке или установке. При помощи облачного сервиса mydLink видео, которое камера передаёт по Wi-Fi, можно смотреть с любого компьютера, смартфона или планшета с доступом в Интернет. А о замеченных движении или звуке она уведомляет по электронной почта.

Уязвимость нашли специалисты компании Senrio, специализирующейся на безопасности интернета вещей. Они обнаружили, что компонент прошивки камеры, который анализирует удалённые команды, может переполнить буфер и разместить полученную по сети строку поверх стека вызовов.

Для экслуатации уязвимости достаточно прислать камере особым образом сформированную команду, которая содержит код на ассемблере и строку, которая вызовет переполнение буфера и разместит на стеке адрес этого кода.

Судя по количеству отзывов на странице камеры в интернет-магазине Amazon, D-Link DCS-930L – это очень популярный продукт, поэтому число потенциальных жертв очень велико. В Senrio не исключают, что их может оказаться ещё больше, если тот же компонент включён в прошивку других камер D-Link.

***

11.06.2016

Обнаружена опасная уязвимость в маршрутизаторах Cisco и Juniper

В маршрутизаторах известных производителей Cisco и Juniper обнаружена опасная уязвимость, позволяющая осуществить DoS-атаку, пишет InternetUA.

Уязвимость существует из-за ошибки при обработке пакетов IPv6 Neighbor Discovery (ND). Злоумышленник может отправить большое количество IPv6 ND-пакетов на уязвимое устройство и потребить все доступные ресурсы системы, тем самым вызвав отказ в обслуживании.

В настоящее время исправления к уязвимости не существует ни у одного из производителей. В качестве временного решения предлагается фильтровать

IPv6-трафик на пограничных маршрутизаторах, не чувствительных к этой проблеме.

Уязвимости присвоен идентификатор CVE-2016-1409. Производители обещают в скором времени выпустить исправления безопасности. В настоящий момент известно, что уязвимость затрагивает следующие линейки продуктов Cisco: IOS, IOS XR, IOS XE, NX-OS и ASA. Также уязвимость распространяется на линейки продуктов Juniper MX, PTX и QFX.

***

11.06.2016

Українські IT-волонтери заблокували на рахунках терористів $13 мільйонів

Волонтерська IT-організація «Українські кібервійська» діє всього два роки, проте вже заблокувала близько 13 млн дол. на 347 рахунках терористів без можливості їх відновлення, пише InternetUA.

Про це повідомив засновник організації «Українські кібервійська» Є. Докукін на своїй сторінці в соцмережі Facebook.

«За моїми підрахунками, на всіх цих рахунках було щонайменше 13 млн дол. (якщо всі гривні, рублі, євро та інші валюти конвертувати в долари). «Українські кібервійська» нанесли значного удару по фінансуванню тероризму», – написав він.

Також Є. Докукін уточнив, що деякі сепаратисти досі намагаються повернути свої кошти, проте їх рахунки більше не відновлювалися.

«Деякі із сепаратистів пишуть на своїх сайтах, що вони намагаються повернути гроші – вивести на банківську карту (рахунок залишається заблокованим). Вдалося чи ні – невідомо, тому що терористи про це не пишуть, а якщо й пишуть, то можуть збрехати. Достеменно відомо лише про факт блокування рахунків», – зазначив він.

Всього, як повідомляє Є. Докукін, за два роки свого існування «Українські кібервійська» заблокували і закрили 160 сайтів сепаратистів, зламали безліч російських електронних адрес, серверів, а також сторінок у соціальних мережах. Також українські IT-волонтери захопили понад 200 тис. мережевих пристроїв у Донецькій і Луганській областях, у Криму і в Росії. «Всього ми захопили 600 ГБ даних терористів «ДНР», «ЛНР» і Росії», – сказав Є. Докукін.

***

11.06.2016.

Утекшие учетные данные LinkedIn используются для распространения банковских троянов

Специалисты центра SANS ISC предупреждают о вредоносной кампании, направленной на пользователей из Европейских стран. В ходе атак

злоумышленники используют учетные данные, похищенные в результате взлома соцсети LinkedIn, пишет InternetUA.

По словам исследователей SANS ISC, мошенники запустили фишинговую кампанию, в ходе которой рассылают электронные письма с прикрепленным документом Microsoft Word. Файл содержит вредоносный макрос, активация которого приводит к загрузке банковского трояна Zeus Panda. Для усыпления бдительности пользователя в письме указываются его персональная информация, в частности имя, название компании и занимаемая должность.

***

11.06.2016

В мире отмечен колоссальный рост количества DDoS-атак

В течение последних полутора лет эксперты отмечают существенный рост количества хакерских атак различного рода, и наиболее активный рост демонстрируют DDoS-атаки. Согласно официальной статистике компании Akamai, в глобальном масштабе всего за год их стало больше на 125 %, пишет InternetUA.

В отчете об исследовании Akamai говорится о росте популярности DDoS-атак среди компьютерных преступников. Данный метод воздействия, пишет портал ZDNET, применяется все чаще ввиду своей эффективности и общей простоты исполнения, что и объясняет 125-процентный рост количества всего за год.

Помимо этого, увеличилось и среднее время продолжительности DDoS-атак: если в прошлом году этот параметр составлял 15 часов, то теперь он возрос до 16 часов. К тому же эксперты стали значительно чаще регистрировать случаи по-настоящему массивных атак, что связано с распространением широкополосного доступа в Интернет. Для сравнения, в I квартале 2015 г. было выявлено всего пять атак, проводившихся со скоростью 100 Гбит в секунду, а в первой четверти текущего года их было отмечено уже 19, причем их продолжительность резко увеличилась. Итого, прирост составил 137,5 %. Статистика за II квартал 2016 г. еще недоступна, поскольку он заканчивается 30 числа текущего месяца.

В общей сложности в течение первых трех месяцев текущего года Akamai зафиксировала более 4520 DDoS-атак по всему земному шару, что и дало возможность оценить рост их популярности, потому что в первой четверти 2015 г. их было чуть больше 3690. Хакеры стали все чаще атаковать не только крупные сайты и виртуальные сети предприятий, но и обычных интернет-пользователей.

В отчете об исследовании говорится и о снижении максимальной зафиксированной скорости DDoS-атаки: теперь она составляет 289 Гбит/с, хотя в последней четверти 2015 г. этот параметр был равен 309 Гбит/с. Причины снижения скорости экспертами не уточняются.

***

11.06.2016

Вирусописатели используют Microsoft BITS для повторного заражения системы

Служба фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service – BITS) используется в ОС Windows для загрузки обновлений безопасности. Именно это свойство службы злоумышленники используют для сокрытия своего присутствия на скомпрометированной системе примерно с 2007 г., пишет InternetUA.

Исследователи из компании Dell SecureWorks обнаружили опасное вредоносное ПО Zlob.Q (по классификации Symantec), использующее службу фоновой передачи данных Microsoft для связи с C&C-сервером. Во время расследования инцидента безопасности в одном из высших учебных заведений специалисты обнаружили подозрительную активность со стороны BITS после очистки системы от вредоносного ПО. В журнале событий появлялись записи о запланированных задачах, однако эти задачи не были нигде видны.

Более детальное расследование показало, что задачи были созданы в базе данных BITS. Даже после успешного удаления вредоноса на системе запускалась задача по расписанию. Запускаемый ею сценарий обращался к C&C-серверу, загружал на систему вредонос, производил его установку и удалял себя по окончании всего процесса. Таким образом злоумышленники обеспечивали постоянное присутствие вредоносного ПО на системе даже после ее очистки с помощью антивируса.

Исследователи рекомендуют пользователям, наблюдающим подозрительную активность со стороны BITS-службы, проверить задачи по расписанию внутри базы данных BITS.

***

13.06.2016

ИТ-компаниям требуется в среднем 248 дней, чтобы исправить уязвимость

Согласно новому отчёту компании WhiteHat Security, большинство веб-приложений имеют по меньшей мере две серьёзные уязвимости, а между обнаружением и устранением уязвимости проходят сотни дней – и это в лучшем случае. В худшем случае приложение останется уязвимым навсегда, пишет InternetUA.

Отчёт основан на результатах изучения десятков тысяч сайтов, использующих сервис WheteHat Sentinel для анализа своей защищённости.

От уязвимостей страдают веб-приложения всех 12 отраслей, которые описаны в отчёте, но хуже всего обстоят дела у ИТ-компаний, у образовательных учреждений и у фирм, связанных с розничной торговлей. Их

веб-приложения содержат наибольшее количество уязвимостей. Среднее значение этого показателя для ИТ, образования и розничной торговли составляет 17, 15 и 13 соответственно.

Уязвимости есть в 60 % веб-приложений ИТ-компаний, 50 % веб-приложений фирм, связанных с розничной торговлей, 47 % медицинских веб-приложений, 41 % веб-приложений финансовых сервисов и 40 % банковских веб-приложений.

Дольше всего устраняют уязвимости компании, связанные с информационными технологиями или розничной торговлей. Для того, чтобы устранить уязвимость, ИТ-компаниям требуется в среднем 248 дней. У компаний, работающих в сфере розничной торговли, этот срок составляет 205 дней.

Компании девяти из двенадцати проанализированных в отчёте отраслей не справляются с устранением более чем половины найденных уязвимостей. В частности, ИТ-компании устраняют лишь 24 % найденных уязвимостей, причём средний срок решения проблемы достигает 875 дней, то есть почти двух лет и пяти месяцев.

Доля устранённых уязвимостей сократилась для ИТ-компания (с 46 % до 24 %) и банков (с 52 % до 42 %). В то же время ситуация немного улучшилась в сфере финансовых сервисов и розничной торговли, где этот показатель возрос с 41 % до 48 % и с 42 % до 48 % соответственно.

Компании, которые работают в области производства, здравоохранения, страхования, а также в пищевой промышленности, стали прилагать для устранения уязвимостей значительные усилия, и это приносит плоды. Доля устранённых уязвимостей в этих отраслях поднялась с 34 % до 66 %, с 26 % до 42 %, с 26 % до 44 % и с 17 % до 62 % соответственно.

***

14.06.2016

Баг в Facebook позволяет увидеть ссылки, которыми пользователи делились с друзьями

Только на прошлой неделе в мессенджере Facebook была исправлена уязвимость, которая позволяла удалять и подменять любые сообщения пользователей. Теперь бельгийский исследователь Э. Сёклер рассказал о еще одной проблеме, но ее руководство социальной сети устранять не намерено. Исследователь утверждает, что приватные ссылки, которыми пользователи делятся с друзьями в частном порядке, может увидеть любой желающий, пишет Украинский телекоммуникационный портал.

Э. Сёклер всерьез рассчитывал получить солидное вознаграждение в рамках программы bug bounty, однако руководство Facebook отказалось признать его находку багом. Представители социальной сети сообщили исследователю, что возможность обращения к Facebook Graph API и последующее извлечение из БД ссылок, которыми ранее делились друг с

другом пользователи, это функция, о которой разработчикам прекрасно известно и ничего делать с ней не планируют.

Суть найденной бельгийцем проблемы заключает в том, как именно Facebook обрабатывает ссылки. Когда пользователь социальной сети отправляет кому-либо ссылку в частном порядке или постит ее открыто, платформа парсит адрес и возвращает заголовок страницы, небольшое описание ее содержимого, миниатюру изображения, а также создает идентификатор object ID. Затем вся эта информация сохраняется в базе данных.

Исследователь обнаружил, что если обратиться к Facebook Graph API напрямую и рендомно перебирать object ID, настроив фильтрацию, в ответ можно получать ссылки, в том числе те, которыми пользователи ранее приватно поделились со своими друзьями.

Хотя Э. Сёлкер пишет, что связать полученные результаты с конкретными пользователями Facebook не выйдет, это не умаляет серьезности проблемы. Дело в том, что используя обычный брутфорс и перебирая разные object ID можно составить огромную базу ссылок, многие из которых будут ссылками на личные файлы. В этих файлах могут (и будут) содержаться самые разные конфиденциальные данные людей, начиная от их имен, фамилий и адресов и заканчивая информацией о банковских счетах, медицинских записях и т. д.

Также ссылки могут вести на скрытые от посторонних глаз фотографии, документы и видеоролики, в том числе хранящиеся в облачных сервисах, или предоставлять доступ к закрытым для посторонних сервисам и ПО. В своем блоге Э. Сёлкер цитирует ответ, полученный от представителей Facebook. Исследователю сообщили, что его находка – это вовсе не уязвимость, а задокументированные функции, информация о которых представлена в документах для разработчиков. Одним словом, делиться важными данными через Facebook Messenger, само приложение или приватные группы явно не стоит. Все они потом будут одинаково доступны извне.

***

16.06.2016

В сеть утекли личные данные 45 млн пользователей свыше 1100 сайтов

Череда массовых утечек данных продолжается. В этот раз в сети оказалась персональная информация порядка 45 млн пользователей свыше тысячи ста сайтов, различных форумов и сообществ, включая спортивные, технический и автомобильные. По данным ресурса LeakedSource, каждая запись в БД включает логин, зашифрованный пароль (в некоторых случаях присутствует два пароля), адрес электронной почты и IP-адрес, пишет InternetUA.

По информации издания Motherboard, все пострадавшие сайты и форумы принадлежат канадской компании VerticalScope. По словам вице-президента по

коммерческому развитию VerticalScope Д. Орбана, компании известно об инциденте. В настоящее время ее специалисты проводят расследование инцидента. Вполне вероятно, что компания хранила все данные на объединенном сервере, из-за чего стала возможной массовая утечка информации.

Пароли, содержащиеся в БД, зашифрованы с применением алгоритма MD5 и соли, что не обеспечивает достаточной защиты от взлома. Как признался оператор LeakedSource, уже удалось взломать 74 % паролей (порядка 33 млн).

Предположительно, база данных была похищена в результате взлома серверов VerticalScope в феврале 2016 г. В настоящее время личность злоумышленников не установлена.

***

16.06.2016

Осторожно: обнаружен вирус, который ворует пароли пользователей «ВКонтакте»

В Google Play найдена опасная вредоносная программа. Она маскируется под приложение для скачивания музыки из популярной социальной сети «ВКонтакте» и, при этом, программа крадет логины и пароли пользователей, сообщается в исследовании компании «Доктор Веб», пишет InternetUA.

Троян получил название Android.PWS.Vk.3. Он прячется в приложении «Музыка из ВК», которое опубликовано в Google Play. Программа и правда дает возможность прослушивать музыку из «ВКонтакте». Однако для этого необходимо ввести свой логин и пароль из соцсети для авторизации.

Как выяснили специалисты «Доктор Веб», приложение в тайне отправляет логины и пароли пользователей на сервер злоумышленников. Таким образом они получают полный доступ к аккаунтам жертв.

На момент публикации материала приложение все еще доступно для скачивания в магазине приложений для Android. Согласно информации из Google Play, приложение уже скачали до 50 т. пользователей.

***

16.06.2016

Германия подозревает Россию во взломе данных следствия по катастрофе MH17

Федеральная служба защиты конституции Германии (BfV) заявляет, что российские спецслужбы атаковали компьютеры совета безопасности Нидерландов осенью 2015 г., перед публикацией доклада о катастрофе Boeing MH17 Malaysia Airlines на востоке Украины, сообщается в отчете BfV, пишет InternetUA.

В документе отмечается, что российские спецслужбы стоят за регулярными многолетними хакерскими атаками на аналогичные западные организации.

Среди подобных атак указывается кибернападение на совет безопасности Нидерландов «во временном контексте, связанном с обнародованием финального отчета осенью 2015 г. о причинах катастрофы самолета Malaysia Airlines MH17 17 июля 2014 г. на востоке Украины».

В отчете утверждается, что хакерские атаки могут контролироваться государством, имеют хорошее финансирование, а также обладают высоким качеством, благодаря ранее неизвестным уязвимостям. Отмечается точность и целенаправленность атак.

***

15.06.2016

Российских хакеров подозревают во взломе серверов Демократической партии США

Издание Washing Post и киберкриминалисты компании CrowdStrike сообщают, что группа так называемых «правительственных хакеров», известная под названиями Fancy Bear, Sofacy, APT28, Sednit, Pawn Storm или Strontium, взломала серверы Национального комитета Демократической партии США (Democratic National Committee, DNC). Якобы злоумышленники сумели получить доступ к множеству конфиденциальных данных, в числе которых была и информация о главном конкуренте демократов: кандидате в президенты США от Республиканской партии Д. Трампе, пишет InternetUA.

Специалисты полагают, что группа APT28 работает в тесном контакте с ГРУ. Данной группировке приписывают атаки на военные базы НАТО, польское правительство, правительство США, германский Бундестаг, французский телеканал TV5 и т. д.

Исследователи CrowdStrike, которые занимаются расследованием случившегося, пишут, что хакеры проникли в сеть DNC еще в апреле 2016 г. и использовали малварь X-Agent. По данным экспертов, внедрение вредоноса позволило злоумышленникам удаленно выполнять произвольные команды на зараженных машинах, похищать файлы и перехватывать нажатия клавиш. Благодаря использованию утилиты X-Tunnel, хакеры создали защищенное соединение со своими управляющими серверами, при помощи которого и передавались все данные.

Изданию Washing Post киберкриминалисты рассказали, что помимо прочего APT28 похитили документы, в которых содержалось аналитическое досье на Д. Трампа. Судя по всему, демократы проводили глубокое исследование бекграунда конкурента, и взломщики украли собранный ими компромат.

В ходе расследования специалисты CrowdStrike выявили в сети Национального комитета Демократической партии присутствие еще одной

группы хакеров. Исследователи утверждают, что это тоже российская «правительственная группировка», известная как Cozy Bear, CozyDuke или APT29. Данная группа якобы работает с ФСБ и ранее была замечена в атаках на почтовую систему Белого дома США, Министерство иностранных дел США и Объединенный комитет начальников штабов.

Исследователи считают, что APT29 скомпрометировала серверы DNC еще летом 2015 г. и использовала малварь SeaDaddy, тоже получив возможность удаленно выполнять произвольные команды на зараженных машинах. Хакеры похищали учетные данные при помощи малвари Mimikatz, и им удалось получить доступ к письмам сотрудников DNC и их приватным чатам.

При этом эксперты уверены, что группировки действовали порознь. Каждая из хакерских команд внедрилась в сеть самостоятельно и выполняла собственные задачи.

«Работа любой иностранной разведки заключается в сборе данных об их потенциальном противнике, – говорит Ш. Генри, глава CrowdStrike. – Для России мы является таким противником. Их работа – это просыпаться каждое утро и собирать информацию о политиках, практиках и стратегиях правительства США. Это можно делать разными способами. [Хакинг] является одним из наиболее полезных способов, так как он позволяет собрать просто кладезь данных».

Reuters сообщает, что пресс-секретарь президента РФ Д. Песков опровергает заявления Washing Post и CrowdStrike. Он уверяет, что российские власти непричастны к взлому базы данных Национального комитета.

***

15.06.2016

Ошибка в Telegram позволяет вызвать отказ в обслуживании устройства

Независимый исследователь из Ирана С. Гаф обнаружил в защищенном мессенджере Telegram любопытную уязвимость, позволяющую обойти установленное ограничение на количество символов в отправляемых сообщениях, пишет InternetUA.

Telegram разрешает отправлять сообщения, содержащие от 1 до 4096 знаков. Обнаруженная С. Гафом программная ошибка позволяет обойти данное ограничение и отправлять сообщения произвольной длины. При этом адресат будет получать всю входящую корреспонденцию вне зависимости от ее размера, что может привести к отказу в обслуживании устройства при недостаточном количестве свободной памяти.

Проэксплуатировав ошибку, исследователь смог отправить два сообщения, одно из которых содержало 30 тыс. символов, а второе было пустым. По словам С. Гафа, злоумышленник может воспользоваться данной

возможностью и отправить сообщения длиной в несколько миллионов знаков на устройство жертвы.

С. Гаф попытался связаться с администрацией Telegram, чтобы проинформировать об уязвимости, однако безуспешно. Поскольку в настоящее время ошибка остается неисправленной, эксперт отказался раскрывать подробности о ней. Тем не менее, С. Гаф опубликовал PoC-видео с демонстрацией атаки.

***

16.06.2016

Хакер взломал более 200 аккаунтов сторонников ИГИЛ, опубликовав там символику ЛГБТ

Хакер из неуловимой организации Anonymous сообщил о взломе более 200 Twitter-аккаунтов сторонников террористической группировки «Исламское государство», сообщает Newsweek, пишет Mignews.com.ua.

Вместо изображений, на которых исламисты демонстрируют казни, хакер опубликовал радужную символику и ссылки на эротические видео представителей нетрадиционной ориентации.

Несколько недель назад хакер, называющий себя WauchulaGhost, приступил к массовому взлому аккаунтов исламистов. После трагедии в клубе Pulse в Орландо, в результате которой погибли 49 человек, пользователь решил заполнить аккаунты исламистов символикой ЛГБТ-сообщества.

«Я сделал это для погибших в Орландо. Последователи ИГ распространяли и восхваляли виновника трагедии, и я решил, что буду защищать тех, для кого событие стало великой потерей», – заявил WauchulaGhost. Также хакер добавил, что продолжит свою акцию и уже заручился поддержкой еще двух анонимных взломщиков.

***

17.06.2016

Исследователи научились по номеру телефона взламывать аккаунты Facebook

Исследователи продемонстрировали возможность взлома аккаунта в социальной сети Facebook, зная лишь номер мобильного телефона, прикрепленного к этому аккаунту. Аналогичным образом можно ломать учетные записи в любых других сервисах, которые предлагают возможность восстановления пароля через смс-сообщение, пишет InternetUA.

Взлом Facebook и WhatsApp по номеру телефона

Исследователи из российской компании Positive Technologies провели успешный эксперимент по взлому аккаунтов в Facebook и WhatsApp, зная лишь номер мобильного телефона, привязанного к аккаунту.

Для этого они воспользовались уязвимостью в протоколе Signalling System No. 7 (SS7). Она позволила перенаправить смс-сообщение для восстановления пароля с номера, прикрепленного к аккаунту, на номер исследователей. Воспользовавшись полученным кодом, они смогли сбросить пароль к аккаунту Facebook, задав свой собственный.

Взлом Telegram и Twitter

Исследователи подчеркнули, что использованный ими метод может использоваться для взлома аккаунтов практически в любом сервисе – везде, где сброс пароля возможен посредством смс-сообщения. К таким сервисам, в том числе, относятся Telegram и Twitter.

Добавим, что в мае 2016 г. хакеры уже демонстрировали возможность взлома учетных записей в WhatsApp и Telegram посредством уязвимости в протоколе SS7.

Протокол SS7

SS7 – разработанный в 1975 г. один из ключевых элементов мировой инфраструктуры мобильной связи. С помощью SS7 осуществляется маршрутизация телефонных вызовов между различными центрами коммутации и различными операторами. SS7 также используется для роуминга. Например, когда абонент уезжает в другую страну, операторы в этой стране посредством протокола SS7 обмениваются данными с домашним оператором абонента для того, чтобы определить, кто его обслуживает.

«Проблема заключается в том, что в SS7 неважен источник сообщения. Все сообщения, полученные по этому протоколу, считаются безопасными по умолчанию», – поясняет Forbes.

Дверь для хакеров

Многие сервисы используют SMS для того, чтобы дополнительно обезопасить пользователей. Но на самом деле они не укрепляют безопасность. Дополнительные функции создаются на основе уязвимой инфраструктуры. Таким образом, сервисы просто указывают хакерам на дверь, через которую они могут войти, говорится в докладе Positive Technologies.

Использование в коммерческих целях

Уязвимости в SS7 оказались полезны не только для хакеров, но и коммерческих организаций. С их помощью Израильская компания Ability готова обеспечить заказчика возможностью отслеживания любого мобильного телефона в мире.

Под отслеживанием подразумевается не только определение местонахождения абонента, но также прослушивание его разговоров и перехват смс-сообщений. Для всего этого решению Ability, стоимость которого достигает 20 млн долл., необходим лишь номер мобильного телефона или международный идентификатор мобильного абонента IMSI (International Mobile Subscriber Identity).

Защита от атак

Между тем ряд операторов, включая Vodafone и Telefonica, стремятся закрыть уязвимости в протоколе. По словам эксперта по безопасности К. Ноля,

мнение которого приводит журнал Forbes, в 90 % случаях для защиты достаточно установить фаервол со специальными правилами.

Пользователям в свою очередь рекомендуется не публиковать лишний раз номер своего мобильника на любых ресурсах в Интернете.

Наконец, в компании Facebook рассказали, что пользователи могут выключить восстановление пароля через смс-сообщение. Для этого им надо активировать в настройках безопасности двухфакторную аутентификацию.

***

16.06.2016

В оборудовании Cisco обнаружена критическая уязвимость

Компания Cisco сообщила об обнаружении критической уязвимости в своих маршрутизаторах и межсетевых экранах. Проблема позволяет удаленно выполнить произвольный код с правами суперпользователя, пишет InternetUA.

Ошибка затрагивает межсетевой экран Cisco RV110W 802.11N VPN и маршрутизаторы Cisco RV130W Wireless-N Multifunction VPN, RV215W Wireless-N VPN. Уязвимость (CVE-2016-1395) получила оценку в 10 баллов по шкале CVSS.

Проблема существует из-за некорректной обработки входных данных. При помощи специально сформированного HTTP-запроса удаленный атакующий может выполнить произвольный код с привилегиями суперпользователя на целевой системе.

В настоящее время уязвимость остается неисправленной. Способов временного предотвращения эксплуатации проблемы не существует. По словам производителя, корректирующие обновления для вышеуказанной ошибки будут доступны в III квартале нынешнего года.

***

16.06.2016

Червь PhotoMiner распространяет себя через уязвимые FTP-серверы

Специалисты компании GuardiCore опубликовали подробный отчет, составленный по итогам изучения малвари PhotoMiner. Впервые этот вредонос был замечен в декабре 2015 г., но с тех пор он получил ряд обновлений и превратился в саморазмножающуюся угрозу, которая атакует FTP-серверы, компрометирует сайты, через них заражает компьютеры, работающие под управлением Windows, и майнит криптовалюту Monero, пишет InternetUA.

Исследователи пишут, что сейчас в Интернете можно обнаружить несколько версий PhotoMiner, но все они, по сути, обладают одинаковой функциональностью и различаются только несущественными мелочами.

PhotoMiner демонстрирует не совсем обычный и весьма запутанный механизм заражения. В ходе первой стадии атаки малвари нужны уязвимые FTP-серверы, где можно разместить PhotoMiner. Это вряд ли представляет

проблему, так как согласно опубликованному на днях отчету компании Rapid7, в сеть открыто «смотрят» более 20 млн FTP-серверов.

Когда червь размещен на FTP, начинается вторая стадия атаки. PhotoMiner сканирует сервер и ищет публичную директорию HTML, которая обычно присутствует на хостингах. Как только вредонос обнаруживает исходные коды сайта, он внедряется в них, чтобы распространить себя дальше. В код каждой страницы вставляется iframe, в качестве source attribute которого фигурирует «Photo.scr». Именно это дало малвари название.

Третья фаза атаки – заражение посетителей скомпрометированного сайта. Каждого попавшего на зараженную страницу пользователя спросят, не хочет ли он запустить данный файл? Если жертва наивно соглашается, PhotoMiner инфицирует ее устройство.

Проникнув на машину, работающую под управлением Windows, червь запускает два процесса. Один из них отвечает за майнинг криптовалюты Monero, а второй занимается распространением PhotoMiner на другие компьютеры сети, если таковые имеются. В поисках других ПК и FTP-серверов малварь использует ARP и NET VIEW, брутфорсит SMB, чтобы проникнуть на другие машины и использует WMI утилиты, чтобы скопировать себя.

Исследователи отмечают, что даже если антивирус замечает червя и удаляет PhotoMiner из системы, процесс Monero никуда не исчезает и продолжает выполнять свои функции. Для майнинга вредонос использует несколько разных аккаунтов MoneroPool.com, информация о которых хранится в файле конфигурации. Данный файл червь получает с управляющего сервера злоумышленников, то есть информация в нем обновляется по мере надобности.

«Заражение сайтов через незащищенные FTP-серверы – это классическая схема атак, которая, похоже, вновь набирает популярность. Создавая инфекцию, от которой так сложно избавиться, авторы PhotoMiner создали ботнет, который определенно задержится здесь надолго», – резюмируют специалисты GuardiCore.

***

17.06.2016

Дэвид Сэнджер (David E. Sanger)

У НАТО нет четкой стратегии по ведению войны в киберпространстве

Таллинн, Эстония – В течение шести месяцев после инцидента с перебоями в работе украинской электросети, спровоцированными чрезвычайно умелыми хакерами, киберсоюзники президента России В. Путина оставляли свои следы в Прибалтике, а также в Финляндии и Швеции, пишет ИноСМИ.ru.

Возможно, чтобы разубедить финнов и шведов, традиционно сохранявших нейтралитет, в необходимости сближения с НАТО – на прошлой неделе альянс впервые провел военно-морские учения на финской территории – хакеры вывели из строя официальный сайт Министерства обороны Финляндии.

Перед этим представители разведывательного агентства Германии недавно сообщили американским чиновникам, что, по их мнению, именно российские хакеры стоят за той кибератакой, которая привела к выходу из строя систем одного немецкого металлургического завода.

Здесь, в Эстонии, где НАТО создал центр по изучению слабых мест альянса перед лицом кибератак и возможных ответов на них, подавляющее большинство уверено, что западному альянсу еще только предстоит разработать стратегию противостояния все более агрессивным действиям России в киберпространстве.

Хотя в настоящее время проводится множество конференций и публикуется множество документов, у альянса пока нет никаких серьезных военных планов, помимо защиты собственных сетей. Россия, Китай и Иран непрерывно работают над созданием все более сложных сил и средств наступления в киберпространстве. У НАТО между тем нет ни подобных сил, ни утвержденного механизма по привлечению кибернетического командования США или его британского аналога.

Отсутствие стратегии ведения конфликтов в киберпространстве резко контрастирует с натовской стратегией противостояния более привычным угрозам.

Два года назад представители НАТО заявили о том, что они могут рассматривать кибератаку на одного из членов Альянса как эквивалент вооруженного нападения, в результате чего автоматически вступает в действие статья о коллективной самообороне.

Однако когда речь идет о незначительных вылазках, шпионских действиях или атаках, которым европейские компьютерные сети подвергаются каждую неделю, лидеры НАТО, по всей видимости, не готовы предпринимать никаких агрессивных действий.

Генеральный секретарь НАТО Й. Столтенберг занимает сдержанную, исключительно оборонительную позицию в вопросе о том, как альянс должен вести себя в киберпространстве. В своем интервью немецкому журналу Spiegel на прошлой неделе он говорил об обмене информацией и экспертным опытом, но ни словом не упомянул о стратегиях разведки и сдерживания на раннем этапе, которые начали разрабатывать другие крупные и более мелкие державы.

Коротко говоря, это прозвучало как стратегия из прошлого века, когда кибератаки еще не использовались регулярно в качестве оружия и средства шпионажа.

Д. Льюис из Центра стратегических и международных исследований в Вашингтоне, уже писавший о том, как НАТО может применять наступательное кибероружие, отметил «огромное нежелании обмениваться средствами». США и Великобритания почти ничего не рассказывают о своих средствах ведения наступления в киберпространстве, даже своим союзникам по НАТО.

«Россияне это понимают, – добавил Д. Льюис. – И они знают, что они могут многое сделать, не спровоцировав никакой реакции».

Отчасти это объясняется тем, что россияне умело прячут свои следы. Результаты почти всех расследований атаки на украинскую электросеть в конце 2015 г. – как секретные, так и общедоступные – указывают на хакеров из России. Однако, по словам чиновников американской разведки, им так и не удалось обнаружить непосредственную связь этого сбоя, который затронул 225 тыс. украинцев, с правительством В. Путина и, скорее всего, не удастся.

Вместо этого американские чиновники устраивают для различных компаний и фирм, занимающихся кибербезопасностью, презентации результатов анализа инцидента с электросетью, произошедшего на Украине, предупреждая их о том, что подобное может произойти и в США.

В киберкомандовании США, которое в значительной мере разрослось с момента первых кибератак, совершенных США против Ирана в 2010 г., российские сети постоянно находятся под наблюдением. К следующему году у киберкомандования будет более 130 групп по всему миру, которые будут действовать внутри ВМС, ВВС, СВ и морской пехоты – помимо тех команд, которые уже работают вместе с Агентством национальной безопасности в Форд-Мид, штат Мэриленд.

Оно уже создало обширную сеть раннего обнаружения, поместив десятки тысяч «имплантатов» – сенсоров, используемых для внедрения вредоносных программ – в сети по всему миру. Однако НАТО только начинает изучать возможности того, что альянс тактично называет «активной обороной», и его представители утверждают, что в настоящее время они не концентрируются на наступательном кибероружии.

Между тем Россию не мучают угрызения совести. Однако пока остается неясным, что именно российские хакеры хотят достичь в странах Балтии, кроме того чтобы доказать – как они сделали в 2007 г. в ходе кибератаки на Эстонию – что они способны взломать любую систему в любой момент.

«Какими бы ни были цели россиян – в основном это запугивание – им, как правило, не удается добиться своего», – сказал президент Эстонии Т. Ильвес, который вырос в Нью-джерси, а затем вернулся в Эстонию, чтобы превратить это небольшое государство в пионера по внедрению новейших технологий в систему управления страной. По его словам, кибератаки 2007 г. привели к противоположному результату, потому что они обернулись еще большим сближением Эстонии с НАТО и Евросоюзом.

В Швеции и Финляндии, которые в период холодной войны сохраняли нейтралитет, ситуация несколько сложнее. Когда на прошлой неделе в Финляндии начались военные учения НАТО, министр иностранных дел Финляндии был в Москве, где он встречался со своим российским коллегой С. Лавровым.

Чем больше Швеция и Финляндия сближаются с НАТО, тем чаще их сети, информационные сайты и сайты их министерств подвергаются атакам. В мае адмирал Д. Ричардсон, руководитель военно-морскими операциями США, сказал на одном из мероприятий в Совете по международным отношениям: «На

самом деле в настоящий момент в киберпространстве ведется довольно ожесточенная борьба».

Эта «ожесточенная борьба» во всех смыслах устраивает Россию: она является частью того, что военные стратеги называют борьбой в «серой зоне». С точки зрения В. Путина, шпионаж в киберпространстве и кибератаки выводят НАТО и его партнеров из равновесия. Нужно потратить много усилий и финансовых средств, чтобы от них защититься, и до настоящего момента они проводились на таком уровне, чтобы не провоцировать военную или экономическую реакцию.

«Они остаются в тени», – сказал М. Либики из корпорации РЭНД в ходе конференции, которая была проведена в июне в Эстонии, в Центре НАТО по обеспечению безопасности в киберпространстве.

По словам М. Либики, для россиян кибершпионаж и кибероружие – это составляющие более масштабной стратегии по распространению дезинформации и пропаганды, которая в значительной мере усложняет процесс отделения правды от вымысла – как, к примеру, в случае с крушением самолета Малазийских авиалиний на Украине. Атаки в киберпространстве также напоминают более мелким государствам Европы об их уязвимости, даже если российские войска остаются на своей стороне границы.

Пока НАТО удалось найти лишь несколько эффективных способов противостояния таким атакам.

«Самой большой проблемой в киберпространстве остается сдерживание, – считает Т. Ильвес, который сделал задачу предотвращения конфликта в киберпространстве одной из главных задач своего правительства. – В НАТО мы уже несколько лет обсуждаем необходимость решить этот вопрос».

По его словам, он боится, что Россия или какая-то другая страна может скоро подойти к новому рубежу, начав незаметно манипулировать различными данными, такими, как медицинские записи, данные о работе оружейных систем и навигационные данные.

Но пока Европа сконцентрировалась на том, чтобы защитить свои секреты и обеспечить бесперебойную работу своего оружия. В мае Германия выступила с предупреждением о возможных атаках России в киберпространстве: в прошлом году ее парламент подвергся атаке, в ходе которой хакеры попытались внедрить в его системы программу, способную предоставить им постоянный доступ к компьютерным сетям парламента. Г. Маассен, глава немецкой службы внутренней разведки, сообщил изданию Financial Times, что россияне продемонстрировали свою «готовность к саботажу».

Теперь оборонное ведомство Германии сделало то, чего не сделало НАТО: оно создало свое собственное подразделение для ведения войны в киберпространстве.

***

16.06.2016

У Чернігові хакер збирав паролі банківських рахунків громадян

Співробітники Служби безпеки України спільно з поліцією припинили протиправну діяльність студента-програміста, який збирав дані користувачів в Інтернеті. Про це повідомляє прес-служба УСБУ в Чернігівській області, інформує Garmata.tv, пише InternetUA.

Зловмисник використовував «хакерське» програмне забезпечення та атакував комп'ютери для несанкціонованого отримання даних. Він «знімав» логін-паролі електронних банківських рахунків, отримував доступ до поштових скриньок, сторінок соціальних мереж та ігрових сервісів.

У рамках кримінального провадження, передбаченого ч. 1 ст. 361-1 ККУ («створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»), у програміста проведено обшуки, на комп'ютері виявлені хакерські програми.

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Касаткіна** Тетяна

Редактори: Т. Дубас, О. Федоренко, Ю. Шлапак

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.