СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(14–27.12)

Наступний випуск вийде 19.01.2016.

2015 № 23

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(14–27.12)
№ 23

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 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Компания Facebook заявила, что вносит изменения в свою политику, направленную на то, чтобы пользователи указывали в профиле только свои настоящие имена, передает УНН со ссылкой на BBC.

Ранее в Facebook обратились ряд различных групп и активистов, которые требовали от компании пересмотреть эту жесткую политику, которая требует от людей использовать только собственные имена.

Во вторник, 15 декабря, компания сообщила, что намерена проверить новую систему, согласно которой пользователи при наличии особых обстоятельств могут прибегнуть к использованию псевдонима.

Как уточняют в компании, смягчение политики «имени» связано с желанием помочь людям, оказавшимся в трудной ситуации, например, став жертвой домашнего насилия.

Однако компания настаивает на том, чтобы пользователи, у которых нет таких особых обстоятельств, все же указывали свое настоящее имя.

Компания утверждает, что когда люди используют свое настоящее имя, их действия и слова в социальной сети имеют больший вес, чем слова пользователя, скрывающегося под псевдонимом ***(Facebook разрешит псевдонимы // InternetUA (http://internetua.com/Facebook-razreshit-psevdonimi). – 2015. – 16.12).***

***

Компания Facebook заявила о намерении опубликовать на сайте Open Compute Project проектировочную документацию, которая даст возможность создавать аналоги сервера Big Sur, используемого Facebook для машинного обучения и работ над искусственным интеллектом.

Сервер Big Sur выполнен в форм-факторе Open Rack V2. Он содержит восемь графических ускорителей Nvidia Tesla M40 мощностью 300 Вт каждый и поддерживает установку различных вычислительных плат с шиной PCI-e.

Big Sur используется в дата-центрах Facebook для проведения экспериментов и исследования новых технологических возможностей. Big Sur служит для того, чтобы находит ответы на вопросы, для чтения рассказов, игр и решения задач на базе доступных примеров.

В компании сообщили, что со временем они пришли к выводу, что было бы эффективнее создать собственную платформу для машинного обучения и работ над искусственным интеллектом.

Big Sur – это сервер второго поколения. По сравнению с аналогичным сервером Facebook предыдущего поколения он предлагает вдвое более высокую производительность. Кроме того, как рассказали в компании, новый сервер универсальнее и эффективнее стандартных решений, которые Facebook использовала прежде.

Как рассказали в Facebook, создавая Big Sur, инженеры стремились сделать новый сервер более надежным и простым в обслуживании, чтобы сократить операционные издержки. Для этого из него были удалены необязательные компоненты. Что касается элементов, которые часто выходят из строя, инженеры сделали так, чтобы их было проще заменить. Это касается жестких дисков и DIMM-модулей.

Все детали внутри сервера, предназначенные для обслуживания техническими специалистами, выкрашены в зеленый цвет. Это правило окраски действует в целом по отношению ко всему обслуживаемому оборудованию в дата-центрах Facebook, отметили в компании.

«Не требуется ни специального обучения, ни руководства. Даже материнская плата может быть вынута за минуту, тогда как в других системах на это требуется не менее часа. Вообще, для ремонта Big Sur практически не нужны инструменты – нужна лишь отвертка, чтобы открутить радиатор процессора», – рассказали в компании ***(Facebook откроет исходники сервера для искусственного интеллекта // InternetUA (http://internetua.com/Facebook-otkroet-ishodniki-servera-dlya-iskusstvennogo-intellekta). – 2015. – 14.12).***

***

У известных пользователей соцсети «ВКонтакте» появится новая вкладка «Записи», которая будет давать информацию о просмотре той или иной записи. По оценкам специалистов компании, это будет еще один мощный инструмент для привлечения аудитории на сайт.

«Мы выпустили статистику для отдельных записей у личных профилей (как в группах). Пока она доступна только тем, у кого более 10 тыс. подписчиков и друзей», – уточнили в компании.

Наряду с закладками «Посещаемость», «Охват» и «Активность» у пользователя появится вкладка «Записи». В ней будут содержатся данные о количестве людей, просмотревших «пост» и все «репосты» – суммарно и только среди подписчиков.

Сообщается, что также можно будет узнать сколько всего «лайков» и «репостов» получила запись и общее количество комментариев к ней. Также есть данные о жалобах, переходах по записи и новых подписчиках. Обновления информации будет проходить автоматически ***(Пользователи «ВКонтакте» получат данные о просмотрах их записей // InternetUA (http://internetua.com/polzovateli--vkontakte--polucsat-dannie-o-prosmotrah-ih-zapisei). – 2015. – 15.12).***

***

…Facebook меняет правила пересылки фотографий в мобильном приложении и мессенджере – социальная сеть решила продвигать своё отдельное приложение для хранения фото. Как сообщается, после 10 января изображения, загруженные с телефона, не будут сохранятся в отдельном альбоме профиля на Facebook, а переместятся в программу Moments…

(Facebook удаляет фотографии, Bitcoin дорожает, а Apple покупает GoPro – новости утра // Блог Imena.UA (http://www.imena.ua/blog/coffee-news-192/). – 2015. – 15.12).

***

Facebook тестирует функцию уведомления о наборе комментариев в реальном времени.

Несколько недель назад некоторые пользователи iOS, использующие приложение Facebook, стали отмечать появление функции отслеживания набора сообщений: в тот момент, когда друзья набирали текстовые послания, в их новостных лентах отображалось уведомление «Друг пишет комментарий», пишет «Багнет» (http://www.bagnet.org/news/tech/274752).

На днях представители Facebook в сообщении, отправленном журналистам The Next Web, подтвердили, что тестирование новой функции действительно ведётся. В компании уверены, что подобная индикация набора текста собеседником, которая с успехом зарекомендовала себя в мессенджерах, способствует «оживлению» виртуального общения ***(Facebook тестирует функцию уведомления о наборе комментариев в реальном времени // Багнет (http://www.bagnet.org/news/tech/274752). – 2015. – 16.12).***

***

Исследователи создали самый надежный из существующих аналогов анонимный мессенджер. Система всячески запутывает следы и не позволяет наблюдателю определить, какое сообщение какому адресату предназначено, даже если он взломает более половины серверов.

Новый анонимный мессенджер

Исследователи из Массачусетского технологического института (МТИ) разработали систему для анонимного обмена сообщениями, более надежную, чем представленный в октябре 2015 г. мессенджер на базе анонимной сети Tor.

«Наша система, получившая название Vuvuzela, обладает стойкой математической гарантией анонимности пользователя, позволяя, согласно проведенным тестам, обмениваться сообщениями раз в минуту или около того», – говорится на сайте учебного заведения.

Недостаток Tor

«Работа Tor построена на предположении об отсутствии наблюдателя, который проверяет каждое соединение в сети», – заявил доцент кафедры вычислительной техники МТИ Н. Зельдович. – Однако в современных реалиях это допущение не так уж и надежно. Сегодня ничто не мешает нам предполагать, что некто может взломать более половины ваших серверов».

В июле 2015 г. исследователи МТИ продемонстрировали несовершенство конструкции анонимной сети Tor. Они смогли определить местоположение анонимного сервера и даже источник отправленных конкретному пользователю Tor данных путем анализа зашифрованного трафика, проходящего всего лишь через один узел анонимной сети.

Принцип работы системы

Система Vuvuzela, по словам создателей, лишена того недостатка, который позволил исследователям МТИ деанонимизировать пользователей Tor.

Новая система работает по принципу тайника: отправитель оставляет сообщение для адресата в секретном месте, в данном случае, по определенному адресу в памяти подключенного к интернету сервера. Адресат затем забирает это сообщение. Ряд механизмов запутывает истинное местоположение обоих участников беседы.

Ложные сообщения

Объясняя принцип работы Vuvuzela, один из ее авторов Д. Лазар предложил представить систему, в которой обмен осуществляемся между тремя пользователями. Он дал им имена Элис, Боб и Чарли. Из них Элис и Боб желают обмениваться сообщениями, но не хотят, чтобы кто-либо догадался, что они делают это.

Если Элис и Боб будут отправлять на сервер сообщения, а Чарли не будет, то наблюдатель догадается, что контактируют Элис и Боб. Поэтому клиент на компьютере пользователя регулярно отправляет на сервер сообщения вне зависимости от того, общается ли пользователь с кем-либо.

Перемешивание сообщений

Если наблюдатель взломает сервер и увидит, что Элис и Боб получают доступ к одному и тому же разделу памяти, а Чарли – к другому, он снова поймет, что контактируют между собой именно Элис и Боб.

Поэтому, вместо одного сервера, система использует сразу три. И каждое пересылаемое в системе сообщение имеет три уровня шифрования. Первый сервер, перед тем как отправить сообщение на следующий, снимает первый уровень шифрования. Второй сервер – второй уровень и т. д. На каждом сервере порядок адресатов перемешивается. То есть, например, если на него поступили сообщения сначала для Элис, потом для Боба и Чарли, то на второй они будут отправлены в ином порядке – например, сначала для Чарли, потом для Боба и Элис.

Только на третьем сервере становится известно, какие сообщения к какому адресу памяти прикреплены. Но даже если наблюдатель взломает этот последний сервер, он не сможет понять, является ли он последним.

Паразитный трафик

Допустим, наблюдатель пытается определить коммуникационную связь между двумя пользователями по временному окну, в которое от них приходят сообщения на первый сервер. Чтобы защитить пользователей от такого сценария, разработчики сделали так, чтобы сервер, в момент передачи полученных сообщений, отправлял похожие сообщения по другим различным адресам. Второй сервер делает то же самое и т. д. Таким образом, для наблюдателя становиться практически невозможным определение того, куда какие сообщения отправляются из тех, которые приходят на сервер.

Разработчики утверждают, что анонимность пользователей в системе Vuvuzela сохранится даже тогда, когда наблюдатель взломает два из трех серверов. Они доказали это во время эксперимента статистическим путем.

Практическое применение

По словам доцента Нью-Йоркского университета М. Вэлвиша, познакомившегося с работой коллег из МТИ, новая система дает лучшие результаты среди всех созданных до этого аналогов Tor в научном сообществе. Тем не менее, она пока не готова для широкого применения ввиду наличия разного рода технологических ограничений ***(Создан анонимный мессенджер надежнее Tor // InternetUA (http://internetua.com/sozdan-anonimnii-messendjer-nadejnee-Tor). – 2015. – 17.12).***

***

Facebook объявила, что теперь «мгновенные статьи» новостных изданий будут доступны всем пользователям Android-устройств. Об этом пишет searchengines.ru.

По данным компании, на сегодня в программе принимает участие более 350 издателей по всему миру, из которых свыше 100 публикуют свои материалы ежедневно.

«В течение нескольких недель мы тестировали “мгновенные статьи” для Android на небольшой группе пользователей Facebook. Во время теста мы увидели, что более быстрый и богатый опыт взаимодействия с материалами в этом формате побуждает пользователей чаще делиться ими по сравнению со стандартными статьями», – комментирует запуск менеджер по продукту М. Рекхау.

Напомним, что Facebook начала публикацию статей и видеороликов новостных изданий через новую функцию «мгновенные статьи» в мае этого года. Внедрение этого функционала было призвано ускорить загрузку мобильных страниц публикаций СМИ.

Изначально «мгновенные статьи» были запущены в США для отдельных пользователей iOS. В октябре они стали доступны пользователям iPhone во всём мире.

А в этом месяце Facebook позволила изданиям размещать больше рекламы в «мгновенных статьях»: одно объявление на каждые 350 слов. Ранее ограничение составляло 500 слов ***(Facebook запустил «мгновенные статьи» для всех пользователей Android // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45647/118/lang,ru/). – 2015. – 17.12).***

***

В социальной сети Facebook изменили функцию «Обзор года». Теперь пользователи могут убрать из автоматически генерируемой подборки опубликованных ими за год фото те, которые напоминают о грустных событиях, передает lenta.ru.

Отныне пользователи смогут проверить, какие публикации войдут в подборку, и заменить те из них, которые покажутся им неподходящими. Помимо снимков за авторством пользователя, в подборку могут войти кадры, на которых его отметили другие юзеры. Функция стала поводом для критики в адрес Facebook в 2014 г. В частности, компании пришлось извиниться перед веб-разработчиком Э. Майером за то, что автоматически сгенерированная подборка напомнила ему о погибшей от рака мозга шестилетней дочери. Тогда фотографии и записи попадали в «Обзор года» автоматически по числу отметок «Мне нравится» и комментариев. Содержание самих публикаций не учитывалось ***(Функция Facebook: начни жизнь с чистого листа // Днепропетровская Панорама (http://dnpr.com.ua/content/funkciya-facebook-nachni-zhizn-s-chistogo-lista). – 2015. – 17.12).***

***

Компания Facebook продолжает развивать свой новый сервис Facebook Messenger, в котором недавно появилась функция распознавания лиц под названием Photo Magic. Доступ к этой функции имеют все пользователи, проживающие за пределами Канады и Европейского Союза (ранее она была доступна только в Австралии).

С помощью Photo Magic можно просканировать фотографии, хранящиеся на мобильном устройстве, а затем отправить их друзьям. Facebook намеренно выпустила эту функцию сейчас, чтобы пользователи могли отправлять родным и друзьям фотографии, сделанные во время новогодних и рождественских праздников.

Включить новую функцию можно с помощью меню настроек в приложении. Также при запуске Facebook Messenger пользователь получит уведомление о возможностях Photo Magic. После обработки обнаруженных на устройстве фотографий приложение предложит разослать их друзьям. Для этого пользователю будет достаточно нажать на кнопку «Send».

Помимо этого, в Facebook Messenger появились новые возможности по изменению внешнего вида окна чата. Представитель компании С. Чудновский опубликовал уведомление, согласно которому теперь можно выбирать прозвища для друзей, менять цвета для переписки и многое другое ***(В Facebook Messenger появилась функция определения лиц // InternetUA (http://internetua.com/v-Facebook-Messenger-poyavilas-funkciya-opredeleniya-lic). – 2015. – 22.12).***

***

Facebook добавила для iOS поддержку живых фото. Увидеть ожившие картинки смогут обладатели мобильных гаджетов Apple.

Одной из самых интересных новых функций в iPhone 6s и iPhone 6s Plus стали «живые фото» (Live Photos). Камера смартфонов способна снимать 1,5 сек. видео до и после спуска затвора, дополняя обычный снимок коротким роликом со звуком. Теперь этот формат поддерживается в мобильном

приложении Facebook для iOS, но увидеть ожившие картинки смогут только обладатели мобильных гаджетов Apple. Об этом сообщает UBR.U со ссылкой на gagadget.com.

В новостной ленте Facebook «живые фото» можно опознать по метке Live в правом нижнем углу. Просмотр снимков в движении доступен в официальном клиенте социальной сети на устройствах под управлением iOS 9. В приложении для Android и на сайте будут отображаться обычные фотографии. Разработчики тестируют возможность загружать Live Photos среди небольшого процента пользователей. Масштабный запуск новой функции запланирован на 2016 г. ***(Facebook добавил для iOS поддержку живых фото // UBR.UA (http://ubr.ua/ukraine-and-world/technology/facebook-dobavil-dlia-ios-podderjku-jivyh-foto-370723). – 2015. – 22.12).***

***

Новая социальная сеть под названием Koko, приложение которой появилось на AppStore, поможет преодолеть стресс и депрессию.

Над созданием новинки работал ученый из Массачусетского технического университета Р. Моррис. Ни для кого не секрет, что в возникновении большинства депрессивных расстройств и стресса важное значение играет общество. Большинство ученых считают, что оно же и поможет преодолеть человеку тяжелое состояние. Поэтому принцип новой социальной сети построен на краудсорсинговой когнитивной терапии.

Пользователю следует зарегистрироваться и описать суть своей проблемы и уже через несколько минут он может получить множество отзывов от других пользователей. С помощью этой программы человек не только получит поддержку от других, но будет и иметь возможность взглянуть на проблему под другим углом ***(В Интернете появилась социальная сеть для людей, страдающих депрессией // «Днепр Час» (http://dpchas.com.ua/zhizn/v-internete-poyavilas-socialnaya-set-dlya-lyudey-stradayushchih-depressiey). – 2015. – 22.12).***

***

Facebook променяла Flash на HTML5

Всё больше крупных интернет-ресурсов отказываются от технологии Adobe Flash в пользу альтернативных решений. Ранее в текущем году её поддержку прекратил YouTube, а теперь примеру видеохостинга последовала социальная сеть Facebook, в которой все ролики отныне будут проигрываться с помощью HTML5 вне зависимости от используемого браузера. В компании считают, что этот стандарт намного лучше соответствует требованиям сайта с точки зрения оптимизации и безопасности, чем устаревшая Flash, по-прежнему пользующаяся популярностью у хакеров благодаря большому числу уязвимостей.

На самом деле HTML5-плеер присутствовал в Facebook и до этого, но воспроизведение через него по умолчанию было доступно только в самых

последних версиях некоторых обозревателей. Полномасштабному переходу на HTML5 мешало увеличенное в случае его применения время загрузки страниц, но теперь эта проблема устранена, утверждают представители соцсети. Впрочем, полностью уходить от Flash в Facebook пока не планируют, поскольку на этой технологии продолжают работать многочисленные популярные среди пользователей соцсети игры ***(Facebook променяла Flash на HTML5 // InternetUA (http://internetua.com/Facebook-promenyala-Flash-na-HTML5). – 2015. – 22.12).***

***

Google планирует выпустить мессенджер с искусственным интеллектом. Цель сервиса, согласно The Wall Street Journal, позволить пользователям взаимодействовать с чат-ботами для получения доступа к поисковым результатам и другой информации. Кроме отправления сообщений друзьям, пользователи нового мессенджера смогут получить ответы на вопросы, минуя поисковик Google. Как указано в докладе, компания будет «направлять пользователей к специальным чат-ботам, как ранее поисковик направлял их к релевантным веб-сайтам».

Кроме того, Google может открыть сервис для сторонних разработчиков, которые могут создать свои боты. Сама компания пока отказалась от комментариев. Месенджеры пользуются огромной популярностью на платформах, особенно в Азии, где такие приложения как WeChat доминируют во многих сферах повседневной жизни. И хотя Google не слишком везло с предыдущими попытками в области социальных медиа, компания надеется достичь новых пользователей и удержать существующих, так как мессенджеры становятся все более распространенными ***(Google планирует выпустить мессенджер с искусственным интеллектом // Marketing Media Review (http://mmr.ua/show/google_planiruet_vypustity_messendzher_s_iskusstvennym_intellektom). – 2015. – 23.12).***

***

Руководство соцсети Facebook запустило пилотное тестирование поиска по постам на отдельных публичных страницах.

Об этом пишет «Обозреватель» со ссылкой на портал Searchengines.

Поскольку общее количество опубликованных постов в соцсети превышает число в 2 трлн, то тестовый функционал должен облегчить поиск публикаций из одного источника. Пока он доступен только ограниченной группе пользователей в США.

В рамках тестирования на страницах этих пользователей отображается специальное окно поиска. По словам представителей Facebook, проект запущен и в мобильной, и в ПК-версии соцсети.

Если тестирование пройдет удачно, то пользователи смогут в онлайн-режиме искать нужные данные не только по своим записям и постам друзей, но и по всем публичным публикациям ***(В Facebook начали тестировать***

инновационный поиск // Обозреватель (http://tech.obozrevatel.com/news/92680-v-facebook-nachali-testirovat-poisk-po-publichnyim-postam.htm). – 2015. – 22.12).

***

По результатам исследования, 35 % украинских респондентов предпочитают читать и просматривать социальные медиа в качестве досуга. Что интересно, больше людей предпочитает читать, чем смотреть телевизор – 27 и 24 % соответственно. Исследование образа жизни поколений компании Nielsen (Nielsen Global Survey Generational Lifestyles) было проведено в рамках Исследования потребительского доверия (The Nielsen Global Consumer Confidence Survey) среди 30 тыс. онлайн-респондентов в 60 странах мира, в том числе Украине, в период с 23 февраля по 13 марта 2015 г. В Украине было опрошено 528 онлайн-респондентов ***(35 % украинцев предпочитают соцсети в качестве досуга // Marketing Media Review (http://mmr.ua/show/35_ukraintsev_predpochitayut_sotsseti_v_kachestve_dosuga). – 2015. – 22.12).***

***

Многие современные IT-компании в той или иной степени интересуются беспилотными летательными аппаратами. Twitter хоть и не имеет прямой заинтересованности в дронах, но всё-таки подал заявку на патент, связанный с управлением этим типом устройств. Он описывает способ контроля дрона, способного делать фотографии и записывать видео, а после публиковать их в ленте пользователя. Подача документов не означает наличия у Twitter планов по созданию собственного летательного устройства.

Контролироваться дрон по документам должен отправкой лайков, осуществлением ретвитов и ответов на сообщения. В зависимости от сделанного действия летательное средство сменит направление полёта, завершит фотосъёмку или видеозапись. К примеру, дроны смогут применяться для взятия интервью или освещения каких-то мероприятий. Пока сама идея кажется непривычной, но уже достаточно амбициозна и может заинтересовать в будущем ряд компаний.

Из более простых задач для дронов, управляемых твитами, можно назвать трансляции в Periscope. Представитель Twitter каналу CNBC назвал ещё более диковатую идею использования дронов, описываемую двумя словами: дрон и селфи. У этого занятия даже термин специальный появился. Селфи с беспилотника называется «дрони» ***(Twitter запатентовал управляемый твитами дрон // InternetUA (http://internetua.com/Twitter-zapatentoval-upravlyaemii-tvitami-dron). – 2015. – 23.12).***

***

Компания Facebook занимается созданием собственной корпоративной сети под названием Facebook at Work, которая будет абсолютно отдельной от всем знакомой социальной сети. Согласно задумке создателей, Facebook at

Work станет чем-то вроде Slack и Yammer и будет использоваться исключительно для работы, пишет AIN.UA (http://ain.ua/2015/12/23/623693).

Для каждой компании создается домен третьего уровня на facebook.com. Каждый сотрудник компании получает свой логин и пароль для входа. Это отдельный рабочий аккуант, который можно использовать исключительно для общения с коллегами. Посты в этом аккаунте также будут видны только сотрудникам компании. Под надписью Facebook есть место для корпоративного логотипа, а верхняя строка с поиском и уведомлениями будет темно-серого цвета.

Около 300 компаний более шести месяцев занимались тестированием сервиса, а сотрудники Facebook использовали его для внутренней коммуникации на протяжении нескольких лет. Функциональность корпоративной соцсети мало чем отличается от самого Facebook, но пользователи не найдут здесь игр.

TheDailyDot сообщает, что несмотря на отделение корпоративного Facebook от обычного, можно будет легко переключаться между личными и рабочими аккаунтами ***(Facebook готовится к запуску корпоративной версии – конкурента Slack и Yammer // AIN.UA (http://ain.ua/2015/12/23/623693). – 2015. – 23.12).***

***

В декабре уанет подводит итоги уходящего года, и социальная сеть «ВКонтакте» – не исключение. Киевский офис поделился с AIN.UA эксклюзивной статистикой за год, рассказал, чем интересовались пользователи, как и почему менялось их количество на площадке, назвал самые обсуждаемые темы года в украинском сегменте соцсети и топ-25 сообществ по популярности.

Рост аудитории

«ВКонтакте» благополучно пережил антироссийскую кампанию, когда украинцев призывали уходить из социальной сети, и на сегодня остается одним из лидеров по охвату среди всех сайтов страны, конкурируя за первое место с Google.

К концу 2015 г. количество посетителей десктопной версии возросло до 13 млн без учета мобильных пользователей. Таковы данные медиапанели Opinion Software Media от Factum Group за октябрь 2015 г.

При этом доля украинцев, которые заходят во «ВКонтакте» исключительно с мобильных устройств, в октябре 2015 г. составила 38 %, почти сравнявшись с долей десктопа.

В октябре площадкой с мобильных Android- и iOS-устройств суммарно пользовались более 5,5 млн человек.

Активность и интересы пользователей

Компания также решила развеять миф о том, что большинство людей используют «ВКонтакте» только ради бесплатной музыки. В украинском сегменте суммарные просмотры аудио- и видеоразделов составляют не более 5 % от общего количества просмотров. По словам В. Леготкина, украинцы во

«ВКонтакте» в основном переписываются, читают новости в сообществах и обмениваются фотографиями.

Так в 2015 г. украинцы загрузили в социальную сеть 11 млрд фотографий – на 4 млрд больше, чем в прошлом году.

Украинский офис работает не только с местными рекламодателями, но и с деятелями культуры и волонтерами. На площадке эксклюзивно презентовали свои клипы и альбомы такие украинские музыканты, как Sunsay, O. Скрипка, The Hardkiss, ТНМК, «Друга Ріка», Bahroma, ЯрмаК, Jamala, Pianобой. С начала декабря 2015 г. в киевском штабе «ВКонтакте» проводятся онлайн-концерты. Концерт проекта «ЯрмаК» посмотрели онлайн более 350 тыс. пользователей.

Летом социальная сеть выпустила бесплатный набор стикеров с образами из украинской истории и литературы, который добавили почти 4 млн пользователей.

Социальная сеть также представила топ сообществ в украинском сегменте и список самых обсуждаемых украинцами тем.

В рейтинге только верифицированные сообщества с данными по подписчикам на 23 декабря. Преимущественно это фан-страницы популярных украинских артистов, СМИ и медиа-проектов. Также в топ-10 входит официальная страница Президента Украины. А на первом месте новостная телепрограмма ТСН.

Топ-10 украинских сообществ по количеству подписчиков:

1. ТСН – 1 403 595 подписчиков
2. Україна ВКонтакті – 930 377 подписчиков
3. Орел и Решка – 632 214 участников
4. Канал 1+1 – 563 500 подписчиков
5. ФК «Шахтер» Донецк – 545 324 участника
6. ЯрмаК – 502 836 участников
7. Президент Петро Порошенко – 447 148 участников
8. Europa Plus Ukraine – 340 168 участников
9. Українська Вікіпедія – 328 375 подписчиков
10. STREET WORKOUT – 308 044 подписчика ***(Не музыкой единой: украинский «ВКонтакте» подвел итоги 2015 года // // AIN.UA (http://ain.ua/2015/12/24/623795). – 2015. – 24.12).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Среди официальных органов власти в мире Министерство иностранных дел Украины получило пятое место по активности в Twitter.

Об этом МИД сообщает в соцсети.

В рамках презентации «12 результатов работы МИД» в 2015 г. орган опубликовал инфографику активности в Twitter мировых лидеров. В первой пятерке – органы власти Мексики, Венесуэлы и Доминиканской республики.

Также к позитивным результатам работы в МИД относят перезагрузку Совета экспортеров и инвесторов, внедрение новых стандартов профессиональной подготовки и работы дипломатов ***(Украинский МИД занял пятое место в мире по активности в Twitter среди органов власти // Четвертая власть (http://vlada.io/vlada_news/ukrainskiy-mid-zanyal-pyatoe-mesto-v-mire-sredi-organov-vlasti-po-aktivnosti-v-twitter/). – 2015. – 22.12).***

***

Чернігівській відділ поліції ГУНП в Чернігівській області відкрив свою сторінку у Facebook.

Про це повідомляє прес-служба поліції у Чернігові.

«Тепер спілкування з керівництвом Чернігівського відділу поліції стане більш прозорим, необмеженим у часі та більш комфортним для чернігівців, журналістів, представників громадських організацій та небайдужих громадян», – ідеться у повідомленні.

Також поліціянти запрошують звертатися з повідомленнями про всі факти правопорушень, у тому числі й з боку правоохоронців, свідками яких Ви стали. Крім того, прийматиметься і оперативна інформація, яка допоможе в розкритті злочинів ***(Повідомляти поліції про правопорушення тепер можна через Фейсбук // Чернігівщина: події і коментарі (http://pik.cn.ua/19168/povidomlyati-politsiyi-pro-pravoporushennya-teper-mozhna-cherez-feysbuk/). – 2015. – 15.12).***

***

Днепропетровская облгосадминистрация завела аккаунт в Instagram. Об этом сообщает ее пресс-служба.

Кроме этого, пресс-релизы ОГА предлагают читать и в Facebook. Пользователи Facebook также заметили, что в соцсети релизы пресс-службы этой организации распространяют многочисленные спам-странички ***(Днепропетровская облгосадминистрация завела аккаунт в Инстаграм // Днепропетровская Панорама (http://dnpr.com.ua/content/dnepropetrovskaya-oblgosadministraciya-zavela-akkaunt-v-instagram). – 2015. – 22.12).***

***

Як повідомили Гал-інфо в ДМС України, міграційна служба стає доступнішою для громадян. Відтепер на гарячу лінію ДМС та на гарячі лінії територіальних органів можна зателефонувати або написати у Skype.

Також створено офіційне представництво Державної міграційної служби України у мережі Facebook. Завдяки цьому сервісу громадяни та журналісти зможуть миттєво отримувати корисну інформацію та останні новини про роботу міграційної служби.

Нові канали комунікацій створено напередодні запровадження паспорта громадянина України у формі ID-карти. Міграційна служба розуміє що у перші місяці роботи можуть виникати ускладнення, пов'язані із технічним і людським фактором, та вважає, що нові можливості швидкого інформування ДМС дозволять оперативніше реагувати на звернення, запити на інформацію та скарги громадян.

Наразі голосовий зв'язок у Skype буде можливим лише у робочі години, однак повідомлення можна надіслати у будь-який час. Для зв'язку по Skype із територіальним органом необхідно знайти на сторінці відповідного управління ім'я у сервісі. Сервіс працює у тестовому режимі, у разі виявлення ускладнень прохання повідомляти на електронну адресу hotline@dmsu.gov.ua ***(Міграційна служба тепер доступна у Skype та Facebook // Galinfo (http://galinfo.com.ua/news/migratsiyna_sluzhba_teper_dostupna_u_skype_ta_facebook_215518.html). – 2015. – 25.12).***

***

Жаловаться в мэрию кременчужане смогут через соцсети «ВКонтакте» и Facebook.

Такое предложение озвучил мэр Кременчуга В. Малецкий. Вскоре жаловаться на нарушителей порядка в городе кременчужане смогут благодаря страницам службы помощи мэра в соцсетях «ВКонтакте» и Facebook.

«Служба помощи мэра 15-63 начнет идти в ногу в интернет-технологиями. Власть Кременчуга должна быть максимально доступной для жителей города. И представительство в соцсетях является весьма удобным способом», – заявил В. Малецкий.

Также мэр сообщил, что кременчужане смогут сбрасывать туда фото- и видеодоказательства нарушений ***(Жаловаться в мэрию кременчужане смогут через соцсети «ВКонтакте» и Facebook // Кременчуг Today (http://kremen.today/2015/12/25/zhalovatsya-v-meriyu-kremenchuzhane-smogut-cherez-sotsseti-vkontakte-i-facebook/). – 2015. – 25.12).***

***

Волонтеры проекта борьбы с антиукраинской пропагандой TrolleyBust открыли общий доступ к базе из 3 млн украинофобов с «ВКонтакте», в том числе и пропагандистов.

Об этом сообщает «Луганский Радар» со ссылкой на соцсети.

Также открыт доступ к списку антиукраинских групп и страниц.

В базе – все аккаунты пользователей «ВКонтакте», активность которых можно рассматривать как направленную против Украины или украинцев.

Это как террористы из формирований так называемой «Новороссии», так и коллаборационисты из АР Крым, пропагандисты и аккаунты пользователей, которые активно поддерживают антиукраинские идеи.

В открытом доступе находятся как сама база таких аккаунтов, так и список социальных связей, их подписок и интересов ***(Волонтеры создали базу украинофобов «Вконтакте» // Луганский радар (http://lugradar.net/2015/12/110321). – 2015. – 23.12).***

***

Бурное развитие Интернета, появление «веб-гигантов» и социальных сетей произвели переворот в производстве и распределении культурных товаров. Об этом говорится в новом докладе ЮНЕСКО «О переосмыслении культурной политики».

Его авторы привлекли внимание к тому факту, что после принятия в 2005 г. Конвенции ЮНЕСКО об охране и поощрении разнообразия форм культурного самовыражения, глобальный культурный ландшафт значительно изменился. Одна из целей Конвенции – содействовать соблюдению принципа справедливости в том, что касается доступа к широкому диапазону форм культурного самовыражения во всем мире, а также сбалансированному обмену культурными товарами и услугами в глобальном масштабе.

Эксперты ЮНЕСКО полагают, что пока эту задачу не удалось выполнить в полной мере. Через десять лет после принятия Конвенции в индустрии культуры и творчества по-прежнему в значительной степени доминируют промышленно-развитые страны. Но вместе с тем в общем объеме мирового экспорта культурных товаров сегодня доля развивающихся стран уже составляет 46,7 % против 25,6 % в 2004 г. Такой резкий рост в значительной степени обусловлен культурным экспортом из Китая и Индии.

В целом мировой объем экспорта культурных товаров достиг почти 213 млрд дол. США. В ЮНЕСКО подчеркивают, что бурный рост социальных сетей, расширение интернет-контента, распространение подключенных к интернету мультимедийных устройств привели к революции в индустрии культуры и творчества. Сегодня в мире появляются новые «игроки», перекраиваются границы журналистики, к которой сегодня причастны многие пользователи социальных сетей. Эксперты обеспокоены, что такие изменения происходят частично в ущерб языковому разнообразию, а рост «веб-гигантов» угрожает культурному богатству ***(Бурный рост социальных сетей и расширение Интернет-контента изменили глобальный культурный ландшафт // «Народна Рада новости» (http://narodnarada.info/news/burnyy-rost-socialnyh-setey-rasshirenie-news-2875.html). – 2015. – 16.12).***

В рамках конференции Content Marketing Summit руководитель отдела Facebook по работе с агентствами Э. Коучман рассказал о трех главных направлениях, в сторону которых изменилось поведение онлайн-потребителей.

Основные тенденции:

1. Мобильные устройства становятся популярнее декстопов

Представитель социальной сети отметил огромные темпы роста популярности смартфонов и планшетов: «Сейчас это 26 млн. В прошлом году было 24 млн. А в позапрошлом – 20 млн. При этом четверть из 26 млн использует Facebook исключительно на мобильных устройствах».

Он также добавил, что параллельно с этим увеличивается и количество просмотров видео. На сегодня социальная сеть показывает результат в 8 млрд просмотров каждый день: 75 % из них – просмотры со смартфонов и планшетов, и этот показатель каждый год прибавляет 88 % (данные для Великобритании).

2. Визуализация коммуникаций

Сегодня люди становятся все менее восприимчивыми к тексту. На это во многом повлияли Instagram и Snapchat. По словам Э. Коучмана, изображения экономят время для восприятия, поэтому мобильные устройства становятся все более «визуализированными».

3. Мобильные пользователи хотят узнавать, а не искать

Э. Коучман заявил, что в свободное время пользователи хотят развлекаться и открывать что-то новое для себя. И конкуренция между теми, кто занимается созданием контента, только нарастает, заставляя особо думать над тем, как выделить свои посты среди множества других. Благодаря мобильным устройствам, пользователь получил круглосуточный доступ ко всему когда-либо созданному контенту.

Представитель Facebook добавил, что брендам стоит сфокусироваться на персонализации, чтобы сделать продукт более актуальным для определенных целевых групп. А на основе данных, даже делая небольшие изменения в содержании, можно значительно влиять на его воздействие на пользователей ***(Facebook рассказал о главных трендах в поведении онлайн-потребителей // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/12/15/three-trends-in-online-consumer-behaviour-according-to-facebook.html). – 2015. – 15.12).***

***

Бренды в социальных сетях иногда выглядят, как страховой агент, который пришел на вечеринку. К такому выводу пришли авторы исследования негативных реакций и насмешек, с которыми сталкиваются бренды в социальной сети. В рамках исследования было проанализировано 4284 поста, в

течение 18 месяцев опубликованных девятью брендами из четырех индустрий: упакованные продукты, рестораны, ритейл и спорт.

Авторы исследования проанализировали посты по 14 контентным характеристикам, включая что говорят бренды и как они об это говорят, а также ответы пользователей: лайки, шеры, клики на сайт, позитивные или негативные комментарии.

«Потребители ожидают, что и люди, и бизнесы будут придерживаться норм социального поведения, и склонны игнорировать или негативно реагировать на тех, кто ведет себя иначе», – говорит один из авторов, профессор Э. Стефен. Так, пользователи более склонны вовлекаться в контент, поданый в неформальном стиле, и остаются более холодны к прямой рекламе и отполированным лозунгами.

Две распространенных практики, как выяснилось, не имеют совсем никакого эффекта: привязывание постов к праздникам и рич медиа (видео, изображения).

Профессор отмечает, что бренды в соцсетях в большинстве случаев коммуницируют с людьми, которые уже проявили к ним интерес. Поэтому обезличенный тон и явно рекламный контент обижают людей, поскольку они осознают, что с ними не общаются, а пытаются что-то им продать ***(В Facebook важнее, как вы говорите, нежели о чем // Marketing Media Review (http://mmr.ua/show/issledovanie_v_facebook_vazhnee__kak_vy_govorite__nezheli_o_chem_). – 2015. – 14.12).***

***

Программное обеспечение сервиса заказа такси Uber будет интегрировано с приложением социальной сети Facebook, чтобы пользователь не переключался между платформами для заказа такси. Сервис уже доступен частично жителям США, и если будет успешным, им смогут воспользоваться и 700 млн пользователей Messenger в мире. Для продвижения услуги компании предоставят людям бесплатные первые поездки на такси на ограниченное время, с максимальной стоимостью до 20 дол. ***(Facebook позволит заказать Uber с помощью Messenger // Marketing Media Review (http://mmr.ua/show/facebook_pozvolit_zakazaty_uber_s_pomoshtyyu_messenger_). – 2015. – 17.12).***

***

Большинство маркетологов считают личные сообщения на страницах брендов мертвым каналом. Но немецкий автобренд рассказал Adweek о том, что получает сотню личных сообщений от клиентов в Facebook и Instagram. Такая постоянная коммуникация вдохновила на акцию «Секретный Санта». Mercedes с помощью личных сообщений помогает подписчикам поздравить родных, отправляя подарки от бренда. Например, часы (розничная цена 179 дол.) или Bluetooth-колонки Harmon Kardon (249 дол.).

«У нас появилась умная идея помочь нашим клиентам найти идеальный подарок от Санты», – говорит М. Аикмен, генеральный менеджер маркетинговых услуг в Mercedes-Benz USA, который работал над акцией #MBSecretSanta с агентством Razorfish. У кампании нет цели собрать данные пользователей или заставить их купить машину – это просто подарки ***(Mercedes-Benz раздал подарки через личные сообщения в Instagram // Marketing Media Review (http://mmr.ua/show/mercedes-benz_razdal_podarki_cherez_lichnye_soobshteniya_v_instagram). – 2015. – 19.12).***

***

Платежная платформа WayForPay запустили Up.Assistance – консьерж-сервис по Viber, который помогает решать любые срочные вопросы (заказать доставку еды или цветов, купить билет на самолет или поезд, забронировать номер в отеле, вызвать такси, оформить доставку из любого интернет-магазина, пополнить счет и пр.).

Все, что нужно сделать пользователю – написать свой запрос виртуальному ассистенту в Viber.

В 2016 г., согласно прогнозам eMarketer, будут популярны «виртуальные помощники» – такие как «Siri» и «Google Now». Пользователи хотят сэкономить свое время, и будут стараться решать вопросы «на ходу» при помощи своего девайса. Также eMarketer выделяет активное использование мессенджеров (Facebook Messenger и Whats App уже насчитывают более 1 млрд активных пользователей по всему миру).

Up.assistance объединяет оба эти тренда – создана служба поддержки виртуальных ассистентов, которая будет решать вопросы клиентов через Viber. Учитывая предпочтения украинцев, это наиболее популярный мессенджер на сегодня (по данным «МТС Украина» около 49 % предпочитают Viber, 28 % – Skype и 12 % – Whats App).

Вы пишете запрос в Viber, к примеру, «Добрый день. Мне нужно купить один жд билет Киев – Харьков, утро 11 декабря 2015», поддержка сервиса подбирает необходимый вариант и высылает вам инвойс (электронный счет) на email или в Viber, для оплаты стоимости билета.

В сервисе нет абонплат и нет привязки к «статусности» карт. Услуга доступна абсолютно всем. Оплата берется лишь при обработке платежа и составляет 1 % (минимум 3 грн) от заказа. То есть, при ориентировочной стоимость билета «Киев – Харьков» 293 грн, вы доплачиваете всего 3 грн за экономию своего времени.

В настоящее время через сервис можно заказать покупку билетов на мероприятия, авиа-, ЖД-билеты, билеты на автобус, заказать доставку еды, цветов или подарков, совершить ряд финансовых операций (денежные переводы, пополнение мобильного, пр.).

Проект только начинает свою работу, поэтому доступный список услуг пока ограничен. Создатели сервиса хотят проанализировать на сколько и какие услуги будут востребованы и полезны для пользователей сервиса ***(В Украине***

запустился консьерж-сервис по Viber // Itnews (http://itnews.com.ua/news/79362-v-ukraine-zapustilsya-konserzh-servis-po-viber). – 2015. – 18.12).

***

Пользователи заметили, что сервис Facebook for Business стал доступен на русском языке.

Портал Facebook for Business содержит новости о последних нововведениях для компаний; советы по маркетингу и рекламе; истории успеха; практические кейсы, демонстрирующие, как социальная сеть может помочь в достижении бизнесс-целей; и справочную информацию ***(Facebook for business добавил русский язык // IGate (http://igate.com.ua/lenta/12135-facebook-for-business-dobavil-russkij-yazyk). – 2015. – 18.12).***

***

Instagram представил пять ведущих трендов рекламы 2016 г.

Год постепенно подходит к концу, и руководитель креативных стратегий в Instagram А. Коттерилл поделился своими предположениями, какие тенденции определят развитие рекламного рынка в 2016 г.

В тренде останутся визуальные форматы сторителлинга

В 2016 г. будет наблюдаться рост использования брендами визуальных коммуникаций в различных форматах: от коротких клипов до изображений, транслируемых в режиме реального времени. Это позволит убить двух зайцев сразу: бренды смогут «прорваться» сквозь информационный шум за счет того, что создает контент, отражающий поведение и предпочтения пользователей. А рекламодатели смогут дать волю фантазии и поэкспериментировать с различными креативными форматами.

Нужно очень хорошо изучить свою аудиторию. Лучше чем когда-либо

Люди ожидают, что их новостные ленты будут наполнены тем, что им интересно, чтобы они не искали интересную информацию сами. Контент новостных лент должен быть персонализирован. Как можно привлечь внимание к своему бренду в большом потоке информации?

На нашей платформе мы можем таргетировать рекламу на основе знания о реальных людях. Это позволяет донести сообщение бренда до нужного человека в нужное время при помощи нужного устройства с учетом того, чем человек занят в данный момент. В следующем году рекламодателям важно использовать большие данные, которыми располагают, грамотно их обработать и донести нужную информацию до своих потребителей.

Грамотно выстроенный стиль продаж

Сегодня мы видим рекламу от брендов в наших новостных лентах, среди постов и фотографий наших друзей. Это дает возможность рекламодателям ненавязчиво привлечь внимание к себе. Важно, чтобы реклама была уместной, информативной и интересной. Креативные решения бренда помогают продать продукт, а Direct Response помогает построить бренд. Учитывая возможности

digital-платформ по ретаргетингу, выиграют те бренды, которые умеют последовательно рассказывать свою историю на всех уровнях воронки продаж.

В настоящее время рекламодатели, предпочитающие Direct Response, ограничиваются тем, что говорят о своем товаре или услуге. При этом крупные бренды теряют в том, что забывают рассказать о своем продукте и сервисе, сосредоточивая все внимание на большом бренде. В 2016 г. все больше компаний будут сокращать разрыв между двумя разными целями рекламных кампаний.

Мы на пороге новой информационной революции

В 2016 г. виртуальная реальность впервые станет доступна каждому. И это в корне может изменить то, как мы общаемся, а также отрасль развлечений и маркетинга.

Эта невероятная технология позволит рекламодателям стать изобретателями: все, что они будут делать с применением технологии VR будет в новинку для рынка. И хотя VR вряд ли станет мейнстрим технологией для рекламодателей в начале 2016 г., но интерес брендов очевиден.

Новые форматы видео, такие, как 360 помогут рекламодателям привлечь целевую аудиторию новыми способами, в том числе за счет того, что они позволяют людям испытать невозможное.

Просто digital – это не новость

Вне зависимости от платформы, на которой вы размещаете рекламу, самым важным остается креатив. Да, это невероятно, как всего в один клик можно просмотреть уникальный рекламный ролик компании, но это не означает, что вы должны потратить меньше времени или ресурсов на разработку идеи, креативной концепции. Потребители ценят, когда реклама органично вписывается в их поведение на этой платформе, а не когда их работа или общение прерывается всплывающими окошками с рекламой ***(Instagram представил пять ведущих трендов рекламы 2016 года // Состав (http://sostav.ua/publication/instagram-predstavil-pyat-vedushchikh-trendov-reklamy-2016-goda-69627.html). – 2015. – 23.12).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Американским ученым удалось узнать, как у людей формируется зависимость от Facebook, пишет Science Daily. По результатам исследования ученые создали тест, с помощью которого можно определить, какую роль в жизни человека играют соцсети.

Э. Феррис из университета города Акрон и ее коллега из университета города К. Холленбо наблюдали за 301 пользователем Facebook в возрасте от 18 до 68 лет. На ежегодной конференции NCA в Филадельфии они поделились результатами своего исследования.

Специалистам удалось составить тест, благодаря которому можно понять, как на человека влияют социальные сети. Если по результатам проверки ученые устанавливали, что человек пользуется Facebook, чтобы завести новых друзей или познать самого себя, то он определенно страдал интернет-зависимостью.

По мнению исследователей, пользовали популярной соцсети зачастую обладают низкой самооценкой и заходят в Facebook для того, чтобы лучше понимать себя. После того или иного поста они ждут комментариев от своих друзей, которые бы подсказали бы им, как правильно вести себя в этой ситуации.

По словам ученых, поклонники популярных соцсетей обладают мягким характером и плохой памятью. Кроме того, признаками интернет-зависимости являются потребность пользователей Facebook в получении информации или развлечений ***(Ученые разработали тест на зависимость от самой популярной социальной сети в мире // GoGetNews.info (http://www.gogetnews.info/news/society/112000-uchenye-razrabotali-test-na-zavisimost-ot-samoy-populyarnoy-socialnoy-seti-v-mire.html). – 2015. – 25.12).***

***

Вы заглядываете на свою страничку в Facebook намного чаще, чем в гости к друзьям и в магазин за обновками? Возможно, у вас развивается зависимость от социальной сети!

Что заставляет вас зайти на Facebook? Сообщения от ваших друзей, желание быть в курсе новостей или надежда встретить новых друзей? Если вы ответили утвердительно хоть на один из этих пунктов, возможно, у вас развилась зависимость от социальных сетей. Впрочем, как утверждает Я. Феррис, доктор философии из университета Акрона, это не обязательно так уж и плохо!

Доктор философии утверждает, что Facebook – это один из инструментов для достижения своих целей, и зависимость от него не так ужасна, как, скажем,

от наркотиков или алкоголя. Например, мы же ходим в магазин за продуктами, и ходим регулярно. Можно ли утверждать, что мы зависимы от супермаркета?..

Почему мы так любим Facebook?

Проект М. Цукерберга пришелся по душе огромному количеству людей, ведь эта социальная сеть позволяет нам удовлетворять свои потребности, которые так или иначе мы стремимся удовлетворить. Приведем их перечень.

– *Потребность в самоутверждении*. Каждый из нас хочет знать, что его ценят, любят, что в нем есть нечто, чем можно восхищаться. Facebook дает возможность поделиться своими оригинальными мыслями с большим количеством людей, похвастаться тем, что сделано своими руками, просто выставить на всеобщее обозрение фото себя после похудения. Такие простые действия действительно могут поднять самооценку, особенно у интровертов, которые чувствуют себя неуютно при непосредственном контакте с людьми.

– *Потребность в новых контактах*. Эта проблема всегда остро стоит перед экстравертами: где найти новых друзей и новых собеседников? Люди, ориентированные на восприятие информации извне, могут чувствовать дискомфорт, если у них ограничены возможности для контактов. Скажем, мамочки в декрете или жители небольших городков и поселков страдают от нехватки новых впечатлений и контактов. Facebook решает эту проблему.

– *Потребность в совете*. У нас как-то не принято посещать психолога, в лучшем случае мы делимся своими проблемами с подругами и родственниками, а они не всегда объективны. Сообщество Facebook дает возможность получить ответ на мучившие вас вопросы, причем для этого не обязательно спрашивать совета или делиться своими проблемами. Можно найти пользователя, который находится в схожей ситуации, и следить за тем, как он из нее выпутывается.

– *Потребность в новой информации*. Новостных сайтов сейчас огромное количество, и не всегда можно сориентироваться, какой из них объективен и непредвзят. Возможно, именно тот, который советует почитать друг по Facebook? Это сообщество – своеобразный фильтр для огромного потока информации, который ежедневно на нас выливается. Там мы можем узнать не только сами новости, но и реакцию на них большого количества людей.

– *Потребность в сопричастности.* Разнообразные группы и сообщества по интересам помогают познакомиться с людьми, которых интересует то же, что и нас. Группа любительниц вязания, группа кулинаров и собаководов – все они выполняют важную функцию: позволяют найти людей, близких нам по духу. А группы фанатов звезд, аккаунты самих звезд дают шанс ощутить себя причастным к великим и знаменитым. В самом деле: есть ли у вас возможность в повседневной жизни подойти к звезде и завязать с ней разговор? Сделать это в Facebook легче легкого: стоит только поместить комментарий под ее постом.

Как сделать, чтобы Facebook не портил вам жизнь?

Если вы вдруг заметили, что виртуальные друзья стали для вас значимее, чем реальные, если вы частенько отменяете важные встречи из-за желания «повисеть» в социальной сети, если вы пренебрегаете своими обязанностями

из-за Facebook, вам стоит напомнить себе, что реальная жизнь все-таки предпочтительнее, чем виртуальная. Придерживайтесь следующих правил.

Устраивать «разгрузочные дни». Раз в неделю вообще не открывать Facebook.

Установить тайминг. Определите, сколько времени в день вы будете посвящать Facebook, и не отступайте от своих правил.

Выводить в реал. По возможности, переводите своих новых друзей из разряда виртуальных в разряд реальных. Например, сходите на мастер-класс, где вы можете встретиться с подругой по Facebook, или договоритесь вместе посетить концерт или выставку ***(А у вас нет зависимости от Facebook? // Домашний очаг (http://my.goodhouse.com.ua/a-u-vas-net-zavisimosti-ot-facebook/). – 2015. – 25.12).***

Маніпулятивні технології

Російські сайти поширили фейк про «затримання» Е. Згуладзе.

15 грудня російські та проросійські сайти повідомили, що заступник глави МВС України Е. Згуладзе «попалась» на вивезенні 4 млн дол. із України. Однак, у МВС це заперечили. Також у ЗМІ поширили фейкову новину про відмову супермаркетів продавати торти Roshen.

Про це пише Радіо Свобода.

Портал EurAsia Daily повідомив про буцімто вивезення 4 млн дол. із України із посиланням на екс-міністра МВС України В. Захарченка, який на своїй сторінці у Facebook написав:

«Тижнів зо два тому перший заступник міністра МВС Ека Згуладзе відбула до свого чоловіка у Францію, тому що перебуває “при надії” і повинна через пару місяців народжувати. На митниці в Борисполі її затримали з валізою грошей, в якій було – не багато, не мало – 4 млн дол. США. На запитання відповідних органів, мадам Згуладзе, не кліпнувши, і посміхаючись, пояснила, що це її особисті речі. А гроші потрібні виключно для організації медичного процесу в Парижі».

Інформацію також поширили Сегодня.ру, «Анфтифашист», «Царьград», «Украина.ру» та ін.

У прес-службі Міністерства внутрішніх справ України таку інформацію заперечили.

«Інформація щодо затримання Е. Згуладзе не відповідає дійсності. Наразі перший заступник міністра внутрішніх справ України перебуває у Києві», – наголосили в МВС.

Крім того, у митниці Борисполя повідомили, що озвучених сум ні в протоколах, ні в деклараціях не було, про це пише «Комсомольская правда в Украине».

У жартівливій формі на інформацію відреагував народний депутат України А. Геращенко.

«У соцмережах активно обговорюють питання про затримання першого заступника міністра внутрішніх справ К. Згуладзе в Борисполі зі сумкою, в якій були 14 млн дол. США. Це неправда! У сумці було не 14, а 140 000 000, і не доларів, а євро!» – написав він.

Також 15 грудня деякі російські та українські ЗМІ поширили новину, буцімто мережа супермаркетів «Ашан» відмовляється продавати торти компанії Roshen. Такий висновок зробили зі світлини оголошення у гіпермаркеті, яку опублікував у соцмережах журналіст П. Шеремет.

«Шановні покупці! ТМ "Рошен" не хоче, щоб її торти продавали дешевше, тому вони відсутні в нашій крамниці», – ідеться в оголошенні.

Пошук, за допомогою Google Images показав, що ця світлина була опублікована та актуальна ще у 2013 р.

Пізніше, у деяких ЗМІ новину видалили. Наприклад, видання «Корреспондент.нет» та InfoResist.org ***(Російські сайти поширили фейк про «затримання» Еки Згуладзе // MediaSapiens (http://osvita.mediasapiens.ua/ethics/standards/rosiyski_sayti_poshirili_feyk_pro_zatrimannya_eki_zguladze/). – 2015. – 16.12).***

Зарубіжні спецслужби і технології «соціального контролю»

Створеній глобальній мережі з протидії російській пропаганді та дезінформації, що координується групою стратегічних комунікацій Європейської служби зовнішньої діяльності, слід розширити масштаб своєю роботи та активізувати її. Таку думку під час виступу перед Парламентським комітетом асоціації ЄС – Україна європейського парламенту висловив президент Світового конгресу українців Є. Чолій, передає кореспондент ukrinform.ua.

«Створення цієї мережі є кроком у правильному напрямі, втім цю ініціативу слід посилити, розширивши масштаб діяльності за межі головної групи у Брюсселі. Команду треба збільшити та перемістити її фокус у тому числі і на Захід. Партнерство із НДО та ЗМІ країн-членів ЄС та Східного партнерства дозволить ефективніше поширювати інформацію з Євросоюзу», – сказав Є. Чолій.

Він додав, що лише минулого року Росія виділила з державного бюджету 643 млн євро на пропаганду російськими ЗМІ ідеї «русского мира».

«Міжнародна спільнота має зосередитися на найголовнішому – виробити рішення, що дозволять недвозначно визначити загрози», – підсумував Є. Чолій.

Як повідомляв Укрінформ, у жовтні ЄС почав координацію глобальної мережі із протидії російській пропаганді та дезінформації. Проект, що отримав

назву «руйнування міфів», об'єднав експертів, журналістів, дослідницькі центри, громадські неурядові організації та політиків.

Вони на добровільних засадах повідомлятимуть відповідним органам виявлені в інформаційному середовищі матеріали, які поширюються у рамках російської пропагандистської та дезінформаційної кампанії та мають за мету підривати європейські прагнення східних партнерів, компрометацію європейських цінностей, руйнування європейської єдності ***(ЄС слід посилити боротьбу з пропагандою Кремля – президент СКУ // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45655/118/lang,ru). – 2015. – 17.12).***

***

В Мариуполе вынесен приговор модератору антиукраинских групп в соцсетях. Об этом сообщает пресс-служба СБУ Донецкой области.

Вступил в силу приговор Ильичевского суда города Мариуполь в отношении местной жительницы, которая была модератором около 500 антиукраинских групп.

Злоумышленица через социальные сети агитировала вступать в ряды террористов, систематически публиковала видео в поддержку боевиков. В ее материалах содержалась информация сепаратистского характера.

Сотрудники управления СБУ Донецкой области выявили и пресекли противоправную деятельность жительницы Мариуполя. Во время обыска изъяли компьютерную технику и электронные носители с материалами, которые свидетельствуют о ее подрывной деятельности.

Суд признал женщину виновной в совершении преступления по ч. 3 ст. 109 (действия, направленные на насильственную смену или свержение конституционного строя или захват государственной власти) Уголовного кодекса Украины и назначил наказание в виде лишения свободы сроком на три года с испытательным сроком на один год ***(Модератор антиукраинских групп осуждена на три года // InternetUA (http://internetua.com/moderator-antiukrainskih-grupp-osujdena-na-tri-goda). – 2015. – 15.12).***

***

Спецслужбы могут использовать «умные» игрушки для шпионажа

Как считает заместитель гендиректора технологической торговой ассоциации Великобритании TechUK Э. Уокер, для слежки за пользователями спецслужбы могут применять не только смартфоны и другие «умные» девайсы, но и подключенные к Интернету детские игрушки. Такое мнение эксперт высказал во время выступления перед Комитетом по науке и технике палаты общин Великобритании (Science and Technology Committee).

В настоящее время британское правительство рассматривает проект «Закона о полномочиях следствия» (Investigatory Powers Bill), также известного как «Шпионский устав» (Snoopers' Charter). Документ включает ряд законопроектов, предоставляющих правоохранительным органам больше

инструментов для обеспечения безопасности граждан. В частности, новый закон обяжет интернет-провайдеров оказывать содействие властям в перехвате трафика граждан и взломе устройств.

По словам Э. Уокера, спецслужбы способны удаленно взломать любое подключенное к Интернету устройство в целях наблюдения за преступниками и подозреваемыми. Инструментами для слежки могут также стать «умные» игрушки, оснащенные встроенными модулями Wi-Fi, микрофонами и камерами. В теории, производителей подобных продуктов могут обязать обеспечивать возможности для слежки за пользователями. Правительству необходимо тщательно продумать процесс выдачи ордеров на «прослушку» электронных устройств, причем использоваться ордеры должны только в случае необходимости, подчеркнул эксперт.

«Умные» игрушки давно вызывают немало опасений по поводу потенциальной угрозы конфиденциальности данных детей. В конце ноября нынешнего года исследователь М. Якубовски продемонстрировал атаку на «говорящую» куклу Барби из серии Hello Barbie. В результате атаки М. Якубовски удалось получить имена сетей Wi-Fi, ID учетных записей и MP3-файлы. Информации оказалось достаточно для определения места жительства ребенка и многого другого. Эксперт также мог прослушивать все разговоры малыша с куклой ***(Спецслужбы могут использовать «умные» игрушки для шпионажа // InternetUA (http://internetua.com/specslujbi-mogut-ispolzovat--umnie--igrushki-dlya-shpionaja). – 2015. – 15.12).***

***

При рассмотрении запроса от иностранных граждан на получение виз в США сотрудники американских государственных учреждений будут, если сочтут необходимым, просматривать аккаунты заявителей в социальных сетях. Это подтвердил официальный представитель Госдепартамента Д. Кирби на брифинге в понедельник.

По его словам, к каждой заявке чиновники станут подходить выборочно, в индивидуальном порядке. При этом такую работу будет осуществлять не только Госдепартамент, но и Департамент внутренней безопасности.

Д. Кирби отметил, что при этом многие люди маскируют свою идентификационную информацию в соцсетях, например, используя псевдонимы. Они могут так выставить настройки приватности, что сотрудник консульства не сможет ознакомиться с содержанием персональной страницы.

Вопрос о возможной дополнительной проверке активности претендентов на американскую визу в социальных сетях был задан в связи с расследованием массового расстрела в Калифорнии. Подозреваемые в этом преступлении – этнические пакистанцы С. Фарук и его супруга Т. Малик. Непосредственно перед расстрелом Т. Малик написала в Facebook пост с восхвалением главаря террористической группировки «Исламское государство» А. аль-Багдади. Кроме того, в 2012 и 2014 гг. она отправила через Facebook два личных сообщения, предназначавшихся небольшой группе ее пакистанских друзей, где

выражала поддержку идеям джихада и заявляла, что намерена «однажды присоединиться к борьбе» ***(Власти США будут изучать аккаунты в соцсетях при подаче документов на визу // IGate (http://iqate.com.ua/lenta/12030-vlasti-ssha-budut-izuchat-akkaunty-v-sotssetyah-pri-podache-dokumentov-na-vizu). – 2015. – 15.12).***

***

Власти Германии сообщили, что Facebook, Twitter и Google готовы удалять все агрессивные высказывания в рамках своих соцсетей в течение суток. Это станет очередным шагом в борьбе с распространением и пропагандой расизма. С другой стороны, это станет шагом на пути к ужесточению контроля за информацией в сети.

Ситуация с беженцами в Европе, число которых только в одной Германии уже превысило 1 млн, вызывает шквал негативных комментариев не только по всему миру и Европе, но и в самой Германии. Некоторые из жителей, недовольные подобным положением дел и политикой страны в вопросе беженцев, пишут посты ненависти на своих страницах в соцсетях.

Это не могло не остаться без внимания со стороны германских властей. Ранее они уже предлагали социальным платформам бороться с этим явлением. Новое соглашение позволит делать это проще и быстрее.

Теперь пользователи и антирасистские группы могут сообщать о постах, содержащих разжигание межнациональной вражды, в группу специалистов социальных сетей. Об этом рассказал министр юстиции Германии Х. Маас. По его словам, контент подобного характера переходит допустимые границы свободы слова и должен удаляться из соцсетей.

Власти Германии всерьез обеспокоены реакцией собственных граждан на наплыв беженцев и стараются пресекать все агрессивные выпады в их сторону. Ранее Германия даже начала расследование в европейском офисе Facebook после того, как работники социальной сети не удалили запись, содержащую агрессивные расистские высказывания. За это, судя по всему, предстоит ответить М. Отту, управляющему директору Facebook по Северной, Центральной и Восточной Европе.

В Facebook утверждают, что работники компании не нарушают и не нарушали законов Германии.

Сегодня социальная сеть побуждает пользователей активнее сообщать о случаях публичного выражения ненависти к представителям других рас и национальностей.

В пресс-службе «Одноклассников» рассказали о своем видении ситуации. По мнению пресс-секретаря А. Жбановой, пользователей соцсетей нужно приучать к более спокойной реакции в общении, в том числе и по столь щекотливому вопросу. Что касается действий социальной сети по вопросу агрессивного контента, то «Одноклассники» (ОК) также активно мониторят все возможные проявления ненависти и удаляют подобную оскорбительную информацию в соответствии с лицензионным соглашением. Кроме того, у ОК

также имеется своя система под названием «народная модерация», когда именно пользователи сообщают об агрессивных публичных постах.

Важно также понять, насколько эффективны будут подобные меры и не вызовет ли прямая конфронтация еще большего сопротивления со стороны тех, кто является распространителем агрессивных высказываний.

Как утверждает семейный и детский психолог С. Филяева, такие действия все же принесут больше пользы, чем встречного негатива.

«С психологической точки зрения удаление экстремистских, эмоционально заряженных и несущих негативный подтекст высказываний может быть полезным по нескольким причинам. Во-первых, есть так называемый феномен “заражения эмоциями”. Люди, эмоционально лабильные, подвержены влиянию мнения других людей. Поэтому даже лояльно настроенный к теме человек может зарядиться эмоциями посланий, в которых, как правило, присутствуют яркие образы, манипулятивные и нелогичные обобщения, выводы об угрозе жизни, картины мрачного будущего.

Во-вторых, если высказывание содержит призыв к действию да к тому же имеется описание прецедента, то это может спровоцировать волну подобных действий. В психологии известна модель поведения человека, основанная на подражании. Часто преступление, описанное в СМИ, находит своих последователей и подражателей, которые или хотят стать героями на час, или находят образец для выхода своим негативным чувствам.

И в-третьих, в соцсетях большое количество детей и подростков. Их мировоззрение только формируется, они эмоционально уязвимы и могут поддаться влиянию.

Дуальность мышления, восприятие мира в черно-белом цвете, чем заряжены агрессивные, разжигающие вражду высказывания, могут дать иллюзию ответа на трудные вопросы и ложное ощущение своей силы и превосходства», – рассказала С. Филяева.

Интернет-контроль превратился в настоящий тренд последних месяцев. На фоне распространившихся сообщений о том, что боевики ИГ активно вербуют интернет-пользователей, власти многих государств озаботились принятием мер по регулированию распространяемой информации в Интернете в пользу безопасности ***(Социальные сети готовы бороться с агрессивными сообщениями в сети // InternetUA (http://internetua.com/socialnie-seti-gotovi-borotsya-s-agressivnimi-soobsxeniyami-v-seti). – 2015. – 18.12).***

***

Д. Полюдова, известная активистка из Кубани, была приговорена краснодарским судом к двум годам лишения свободы с отбыванием всего срока в колонии-поселении. Об этом передает replyua.net со ссылкой на Радио Свобода. Д. Полюдову приговорили только за то, что девушка сделала репосты картинки в социальной сети «ВКонтакте».

26-летнюю Д. Полюдову обвинили в экстремизме лишь за то, что девушка поделилась картинкой, на которой был призыв этнических украинцев с

Кубани за присоединение к Украине. На фотографии, которой поделилась Д. Полюдова, в руках она держит плакат с надписью «Украина, мы с тобой». В правоохранительных органах России посчитали такие действия экстремизмом и завели уголовное дело.

Кроме того, Д. Полюдова написала на своей странице о том, что все проблемы и теракты в России происходят из-за президента РФ. Девушка поинтересовалась, почему никто из россиян не может набраться смелости и свергнуть режим, как это сделали украинцы. Вину Д. Полюдова не признала и продолжает отрицать обвинения в том, что она призывала свергнуть российскую власть насильственным путем ***(Россиянка получила реальный срок за поддержку Украины // InternetUA (http://internetua.com/rossiyanka-polucsila-realnii-srok-za-podderjku-ukraini). – 2015. – 22.12).***

***

Путіну сподобалася ідея регулювати «погляди і думки» людей в Інтернеті.

Президент РФ В. Путін підтримав ідею регламентування захисту особистих даних інтернет-користувачів. Про це він заявив під час зустрічі з учасниками форуму «Інтернет-Економіка» у відповідь на пропозицію співзасновника «Лабораторії Касперського» Н. Касперської, повідомляє pravda.com.ua з посиланням на ТАСС.

Згідно з повідомленням, Н. Касперська запропонувала регламентувати захист не тільки персональних даних, але і так званих особистих даних, куди відносяться контакти різних людей, їхні погляди, думки тощо.

«Давайте. В умовах боротьби з терором абсолютно вірно. Тільки акуратніше треба, щоб не втручатися в особисте життя громадян», – заявив він.

Н. Касперська також запропонувала з цією метою створити єдиний центр моніторингу реагування на загрозу за аналогією зі збором цифрових загроз.

За її словами, зараз закон захищає персональні дані користувача, але абсолютно ніяк не регулюється те, що називається особистими даними. При цьому соціальні мережі містять величезну кількість інформації. Це «джерело знань» дає величезну можливість, за словами Н. Касперської, маніпулювати людьми.

На її думку, необхідно, щоб іноземні сайти, такі як Facebook передавали свої сертифікати державі в обов'язковому порядку, якщо вони хочуть працювати на території Росії.

«Треба створити правову основу для покарання за вчинення таких інформаційних атак», – заявила вона ***(Путіну сподобалася ідея регулювати «погляди і думки» людей в інтернеті // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45704/118/lang,ru/). – 2015. – 23.12).***

***

Засновник месенджера Telegram П. Дуров прокоментував заяву майбутнього радника президента Росії з питань Інтернету Г. Клименко про те, що російська влада закриє месенджер, якщо той не буде співпрацювати.

Про це П. Дуров написав на своїй сторінці «ВКонтакте».

За словами П. Дурова, «як не видавав, так і не буде видавати особисті дані та ключі шифрування третім сторонам».

«Причина проста: технічно неможливо позбавити безпечного спілкування тільки терористів, не поставивши під удар особисту переписку всіх законослухняних громадян», – написав П. Дуров.

На його думку, якщо російські правоохоронці отримають доступ до особистого листування користувачів месенджера, це призведе до виникнення чорного ринку особистих даних.

П. Дуров також зазначив, що загрози можливого блокування сервісу не вплинуть на його політику конфіденційності.

«Мессенджер популярний серед десятків мільйонів користувачів на десятках ринків, і загроза блокування на одному чи двох з них не вплине на його політику конфіденційності», – заявляє П. Дуров.

Нагадуємо, що у листопаді Telegram повідомив про блокування 78 публічних каналів, пов'язаних із забороненою в Росії терористичною організацією «Ісламська держава» ***(Дуров відмовився видавати владі особисті дані користувачів Telegram // MediaSapiens (http://osvita.mediasapiens.ua/web/social/durov_vidmovivsya_vidavati_vladi_osobisti_dani_koristuvachiv_telegram/). – 2015. – 25.12).***

***

Надзорный орган Индии в области телекоммуникаций (Telecom Regulatory Authority of India, TRAI) потребовал от сотового оператора Reliance Communications заблокировать услугу Facebook – Free Basics. Она дает бесплатный доступ ко многим популярным приложениям и сайтам. Об этом сообщает Times of India.

Уточняется, что регулятор попросил закрыть доступ на неопределенное время. По сообщению властей страны, требование было выполнено, и в настоящее время сервис недоступен. Однако, по данным газеты, запрос от властей был получен две недели назад, и услуга все еще действует.

В Facebook не подтвердили, была ли компания уведомлена о возможных проблемах. В соцсети лишь отметили: «Мы работаем с Reliance и местными властями, чтобы обеспечить Индию Интернетом при помощи нашей программы Free Basics».

Многие пользователи в Индии и эксперты отрасли критиковали эту инициативу Facebook. В частности, их не устраивал тот факт, что соцсеть не предоставляет доступ ко всей глобальной сети и разделяет юзеров на две группы: те, кто могут получить полноценный доступ к Интернету, и те, кто могут пользоваться лишь платформой соцсети бесплатно. Сама компания

активно защищает свою инициативу. Так, например, Facebook запустил кампанию, призывающую пользователей соцсети в Индии отправлять автоматические письма с поддержкой Free Basics сотрудникам TRAI.

Free Basics представляет собой платформу с примерно сотней базовых приложений для смартфона. В основном, это социальные и образовательные сервисы, такие как Wikipedia или BabyCenter (рассказывает родителям, как правильно ухаживать за малышами онлайн), сама соцсеть, а также сайты правительственных ведомств.

Услуга Free Basics является частью инициативы основателя Facebook М. Цукерберга по предоставлению бесплатного доступа к Интернету пяти миллиардам человек по всему миру (в основном, речь идет о населении бедных африканских стран). Проект получил название Internet.org, а одноименный фонд был запущен в августе 2013 г. В его рамках Facebook при помощи партнеров планирует увеличить эффективность передачи электронных данных и снизить стоимость подключения в 100 раз ***(Индия заблокировала доступ к бесплатному интернету от Facebook // InternetUA (http://internetua.com/indiya-zablokirovala-dostup-k-besplatnomu-internetu-ot-Facebook). – 2015. – 23.12).***

***

В штате Пенсильвания за пропаганду в Twitter группировки «Исламское государство» (ИГ) арестован 19-летний местный житель Д. Азиз. Об этом сообщает Reuters со ссылкой на прокуратуру штата.

Задержанный обвиняется в сговоре «с целью материальной поддержки террористической организации». Ему грозит до 20 лет тюрьмы и штраф до 250 тыс. дол. уточняет РИА Новости.

«Д. Азиз использовал по крайней мере 57 разных учетных записей в Twitter, чтобы пропагандировать насилие против США и их граждан, а также чтобы распространять пропаганду ИГ и взгляды в поддержку ИГ», – сообщается в пресс-релизе прокуратуры.

В частности, молодой человек предлагал своим фолловерам мстить сотне военнослужащих, чьи имена и адреса он распространял через соцсеть. Кроме того, он помогал желающим выехать на территории, занятые ИГ.

При обыске у Д. Азиза обнаружены четыре магазина к автомату, переделанный кухонный нож, съемный жесткий диск, лекарства и лыжная маска. Дело расследует объединенный антитеррористический центр ФБР, куда входят представители Пентагона, полиции штата Пенсильвания и местная полиция Гаррисберга ***(В США за пропаганду ИГ в Twitter арестовали 19-летнего юношу // InternetUA (http://internetua.com/v-ssha-za-propagandu-ig-v-Twitter-arestovali-19-letnego-uanoshu). – 2015. – 24.12).***

***

Правительство США хочет, что бы Apple встроила в iMessage бэкдор для спецслужб.

Американский сенатор Т. Коттон от штата Арканзас прокомментировал слова Т. Кука, сказанные в передаче «60 Minutes». Он убежден, что компанию следует обязать установить бэкдор в мессенджер iMessage, поскольку сервисом Apple пользуются не только рядовые пользователи, но и потенциальные преступники.

В последних версиях операционной системы iOS Apple внедрила полное шифрование данных, благодаря чему доступ к пользовательской информации может получить только владелец мобильного устройства. Ранее у компании хранились ключи шифрования, позволявшие разблокировать гаджеты по запросу правоохранительных органов, но в случае с iOS 8 и iOS 9 этого нет. По мнению Т. Коттона, это большая ошибка руководства сервиса.

«Apple – отличная компания, которая улучшила жизнь миллионов американцев. Но гендиректор Т. Кук рассказал несколько критических фактов о шифровании данных. Он заявил что Apple не выполняет судебные ордеры, так как не имеет технической возможности. Пусть это правда и у Apple нет доступа к зашифрованным данным, но лишь потому, что компания сама настроила таким образом работу сервиса. Наше общество не должно позволить производителям телефонов создавать системы, которые не подчиняются законным требованиям полиции.

В Купертино выступают категорически против: Apple не считает, что борьба с терроризмом может являться предлогом, под которым пользователей должны лишить приватности.

«Террористы будут шифроваться. Они знают, как это сделать. Если мы не будем шифровать данные наших пользователей, значит хорошие люди останутся без защиты. 99,999 % из них – хорошие люди», – заявил Т. Кук. Кроме того, наличие бекдора будет означать, что доступ к частным данным могут получить не только правительственные службы, но и злоумышленники ***(Правительство США хочет, что бы Apple встроила в iMessage бэкдор для спецслужб // IGate (http://igate.com.ua/lenta/12246-pravitelstvo-ssha-hochet-chto-by-apple-vstroila-v-imessage-behkdor-dlya-spetssluzhb). – 2015. – 24.12).***

***

«Власти Крыма» будут мониторить СМИ и социальные сети для противодействия «экстремизму». Об этом заявил глава госкомитета «правительства Крыма» по межнациональным отношениям и депортированным гражданам З. Смирнов, сообщает newsru.ua.

По его словам, специальная программа по противодействию «идеологии экстремизма» будет вынесена на рассмотрение «крымского правительства» в середине января.

«Основная задача программы – противодействовать распространению идеологии экстремизма и терроризма на территории республики. Особое внимание будет уделяться мониторингу средств массовой информации и социальным сетям для определения источника идей экстремизма», – подчеркнул чиновник.

«Кроме того, будут вестись профилактические работы среди школьников и студентов, так как молодежная среда является наиболее подверженной влиянию радикальных идей извне», – добавил он.

«Все данные о проявлениях экстремистских идей будут передаваться в правоохранительные органы для быстрого реагирования и правовой оценки», – сказал З. Смирнов ***(«Власти» Крыма будут мониторить СМИ и соцсети на предмет экстремизма // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45721/118/lang,ru/). – 2015. – 24.12).***

***

Редактор крымского сайта BlackSeaNews А. Клименко сообщает о том, что канал их сайта на YouTube заблокирован на территории России и в подконтрольном ей сейчас Крыму решением «Роскомнадзора» – Федеральной службой России по надзору в сфере массовых коммуникаций и связи. Об этом сообщает krymr.com.

По его словам, соответствующее сообщение он получил от компании YouTube, которую «Роскомнадзор» уведомил в том, что материалы сайта BlackSeaNews нарушают ряд федеральных законов – об информации, информационных технологиях и о защите информации.

«Я это называю “сертификат качества от ФСБ” – спасибо им за признание нашей работы», – прокомментировал А. Клименко.

В Крыму при попытке зайти на канал сайта на YouTube пользователей предупреждает сообщение: «Внимание! Вы обратились к ресурсу, который заблокирован согласно федеральному закону». Доступ к сайту BlackSeaNews раньше был заблокирован в России и Крыму из-за интервью главного редактора сайта А. Клименко «“Черный список” и морская блокада – лишь небольшой фрагмент стратегии возвращения Крыма...» ***(«Роскомнадзор» заблокировал доступ к крымскому сайту BlackSeaNews на YouTube // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45731/118/lang,ru/). – 2015. – 25.12).***

***

Система автоматического сбора и анализа контента во всех онлайн-СМИ начала работу в 19 регионах России, с ее помощью Роскомнадзор ищет противозаконные материалы на сайтах новостных изданий. В настоящее время система работает в тестовом режиме, но до конца 2016 г. проект будет полностью завершен и заработает во всей стране. Об этом «Известиям» заявил глава Роскомнадзора А. Жаров.

«Аналитическое ядро – в Главном радиочастотном центре. К концу 2016 г. проект будет полностью завершен. Информация на сегодняшний день идет из 19 регионов, – рассказывает А. Жаров. – Количество выявленных нарушений увеличилось минимум вдвое. Мы стараемся не наказывать,

поскольку эта система новая. Мы призываем устранять нарушения, и я думаю, это приведет к улучшению качества всех СМИ на всей территории РФ».

Сегодня деятельность редакций и журналистов регламентируется законом «О СМИ», где в ст. 4 есть перечисление запрещенной к публикации информации. СМИ должны не допускать материалов, содержащих «публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань». Кроме того, запрещено распространять информацию «о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ» ***(Россия запустила систему контроля за интернет-СМИ // Информационное Агентство 112.ua (http://112.ua/ato/rossiya-zapustila-sistemu-kontrolya-za-internet-smi-281200.html). – 2015. – 25.12).***

***

Министр семьи и социальной политики Турции С. Рамзаноглу рассказала журналистам о том, что Турция готовит меры, антологичные тем, что разрабатывают европейские парламентарии в отношении запрета на доступ к соцсетям Facebook, Youtube и Twitter для детей, не достигших 16 лет.

Согласно новому правилу, дети смогут пользоваться такими соцсетями, как Youtube, Facebook и Twitter, только с разрешения родителей, сообщает МК-Турция.

Если закон ратифицируют, то для таких сервисов, как соцсети, e-mail, блоги и даже поисковики, обязательным условием будет сбор персональных данных.

«Наше министерство тоже будет задействовано в этой работе. Уже начата работа над принятием закона о безопасном для детей использовании Интернета. Но до сих пор не вынесено окончательного решения по поводу пределов возрастного ценза», – сказала министр С. Рамзаоглу.

По словам министра, сколько бы и какие запреты ни ставились в Интернете, в этом вопросе очень важна линия поведения семьи.

«На самом деле, нам нужно обучить родителей. Как они проверяют портфели, так же они должны проверять сотовые телефоны и компьютеры своих детей. Вы ставите фильтры и блокировки, а они их взламывают и обходят все системы запрета», – отметила С. Рамазаноглу ***(Несовершеннолетним в Турции запретят пользоваться соцсетями // Black Sea News (http://www.blackseanews.net/read/110206). – 2015. – 25.12).***

***

Yahoo! будет предупреждать пользователей о возможных атаках спецслужб.

Компания Yahoo! решила последовать примеру Twitter и Facebook и теперь будет оповещать пользователей о возможных кибератаках. Уведомления будут получать те подписчики, чья учетная запись, по мнению сервиса, может быть взломана работающими по заказу какого-либо государства хакерами.

По словам директора по информационной безопасности Yahoo! Б. Лорда в извещениях будут предложены меры по обеспечению максимальной безопасности учетной записи. Эти меры включают двухэтапную верификацию, использование уникального ключа и создание надежного пароля. Кроме того, пользователям рекомендуется проверить информацию учетной записи, а также настройки переадресации почты и функции «ответить всем». Хакеры могут изменить данные настройки и получать всю корреспонденцию пользователя, предупреждает Б. Лорд.

По словам сотрудника Yahoo!, уведомления служат исключительно для предупреждения пользователя о возможной атаке и не указывают на компрометацию соцсети или взлом учетной записи ***(Yahoo! будет предупреждать пользователей о возможных атаках спецслужб // InternetUA (http://internetua.com/Yahoo--budet-preduprejdat-polzovatelei-o-vozmojnih-atakah-specslujb). – 2015. – 26.12).***

Проблема захисту даних. DDOS та вірусні атаки

Twitter впервые заявил о возможных взломах сервиса государственными хакерами, сообщает Financial Times.

Отмечается, что компания разослала пользователям письма с предупреждениями. В письме говорится, что взломщики могут пытаться достать номера телефонов, адреса электронной почты, и IP-адреса компьютеров.

Издание уточняет, что подобные предупреждения уже сделали компании Google и Facebook ***(Twitter предупредил пользователей об опасности взлома аккаунтов // InternetUA (http://internetua.com/Twitter-predupredil-polzovatelei-ob-opasnosti-vzloma-akkauntov). – 2015. – 14.12).***

***

Торрент-трекеры ежемесячно заражают вирусами 12 млн компьютеров.

По данным исследователей из организаций Digital Citizens Alliance и RiskIQ, торрент-трекеры, конечно, дают возможность пользователям получить доступ к пиратскому контенту, но также ставят под угрозу их безопасность. Оказалось, что 800 наиболее популярных ресурсов регулярно заражали пользовательские компьютеры вредоносным ПО: оно содержалось в загружаемых файлах, а также распространялось посредством баннеров и переходов по ссылкам.

Около 55 % зараженных инициировали загрузку самостоятельно, остальные могли даже не догадываться о заражении компьютера (речь идет о так называемых загрузках drive-by, которые не требуют дополнительных действий со стороны жертвы). Известны случаи, когда вирусы обнаруживались в «раздачах» с играми. Как пример приводится ПО, лишившее жертву накоплений в виде биткоинов на 2 тыс. дол., передает ZDNet.

Только в США ежемесячно вирусами заражается 12 млн компьютеров. Злоумышленники, в свою очередь, могут обогатиться, по подсчетам специалистов, на 70 млн дол. «Бесплатного в этом мире не существует, за все надо платить», – уверены эксперты. Они также выступают с рекомендацией пользоваться только лицензионным программным обеспечением ***(Торрент-трекеры ежемесячно заражают вирусами 12 млн компьютеров // InternetUA (http://internetua.com/torrent-trekeri-ejemesyacsno-zarajauat-virusami-12-mln-kompuaterov). – 2015. – 14.12).***

***

Разработчик утилиты MacKeeper, включающей в себя функции антивируса, допустил утечку персональных данных 13 млн пользователей компьютеров Apple Mac, сообщает Forbes со ссылкой на специалиста по компьютерной безопасности К. Викери, который обнаружил находку.

Этими персональными данными являются имена пользователей Mac, их электронные адреса, логины, хэши паролей, номера телефонов, IP-адреса, информация о системе, лицензии на программное обеспечение и коды активации.

База данных в свободном доступе

По словам эксперта, компания Kromtech Alliance, занимающаяся разработкой и поддержкой MacKeeper, оставила базу данных MongoDB с персональными данными пользователей своей утилиты на одном из своих серверов незащищенной. В результате доступ к ней можно было получить через внешнее соединение, всего лишь указав IP-адрес сервера. При этом ни логин, ни пароль вводить не требовалось.

Ситуация усугублена тем фактом, что MacKeeper использует для хранения паролей в базе данных алгоритм хэширования MD5. В Интернете можно найти множество инструментов, позволяющих получить пароль обратно из имеющейся хэш-суммы. Они позволяют за секунды узнать несложные пароли к учетным записям.

Реакция разработчика

Изначально попытка Forbes получить комментарии от Kromtech Alliance успехом не увенчалась. Позже, после того как информация об утечке была опубликована на сайте Reddit, разработчик самостоятельно вышел на связь и уведомил, что уже решил проблему неправильной конфигурации базы данных, из-за чего она была доступна. В компании добавили, что в настоящее время находятся на этапе внедрения более надежного алгоритма хэширования SHA512, но не уточнили, когда он будет запущен.

Дурная репутация

Утилита MacKeeper объединяет в себе функции антивируса и чистильщика от системного мусора. На официальном сайте приложения говорится, что оно является самым популярным в своем классе на платформе OS X, и что в общей сложности оно было загружено пользователями свыше 134 млн раз.

MacKeeper обладает дурной репутацией. На интернет-форумах можно найти множество жалоб от владельцев компьютеров Apple, что реклама MacKeeper их докучает. Дело в том, что разработчики приобрели огромное количество показов объявлений – больше, чем кто-либо до этого.

Кроме того, множество жалоб касается поведения бесплатной версии MacKeeper, которая драматизирует проблемы с компьютером и заставляет испуганных пользователей обращаться к платной версии стоимостью 40 дол., якобы способной все их решить.

Стоит также добавить, что уязвимость в некоторых версиях MacKeeper позволяет злоумышленникам исполнять на компьютере жертвы произвольный код с привилегиями администратора при посещении вредоносного сайта ***(Скандальный антивирус для Mac «слил» в Сеть данные 13 млн пользователей // InternetUA (http://internetua.com/skandalnii-antivirus-dlya-Mac--slil--v-set-dannie-13-mln-polzovatelei). – 2015. – 16.12).***

***

Как оказалось, ни одно государственное учреждение не может оставаться в безопасности вечно – даже если оно работает в космосе. Это доказала хакерская группировка Anonymous, взломавшая серверы Европейского космического агентства (ЕКА).

Хакерам удалось с помощью SQL-уязвимости взломать некоторые поддомены агентства, что позволило им получить доступ к базам данных. Злоумышленникам удалось похитить имена пользователей и пароли работников учреждения, а также имена, электронные адреса и пароли примерно восьми тысяч подписчиков поддоменов ЕКА.

Хакеры никак не объясняют свои действия, направленные на агентство – они уверяют, что взлом был произведён исключительно ради смеха (или, как выражаются сами злоумышленники, «для лулзов»). Кибератака произошла во время подготовки миссии ЕКА по отправке британского астронавта Т. Пика на Международную космическую станцию (МКС). Миссия носит название Expedition 46, целью её являются научные эксперименты и доставка припасов на МКС ***(Anonymous ради смеха взломала Европейское космическое агентство // InternetUA (http://internetua.com/Anonymous-radi-smeha-vzlomala-evropeiskoe-kosmicseskoe-agentstvo). – 2015. – 16.12).***

***

Международная антивирусная компания Eset предупредила о новом всплеске активности банковского трояна Dridex. Как сообщили CNews в Eset,

Dridex (Bugat, Cridex) – вредоносная программа, предназначенная для кражи конфиденциальной информации. Эксперты говорят о сходстве трояна с известным Zeus, но отмечают усложнение его функционала в сравнении с предшественником.

Каждые несколько недель вирусная лаборатория Eset фиксирует очередную волну распространения модификаций Dridex в разных странах мира. По данным компании, высокая активность трояна сохраняется с сентября 2015 г. В настоящее время наибольшее число заражений приходится на пользователей из Великобритании, Германии, Франции и Австралии.

Злоумышленники распространяют Dridex «по старинке» – посредством вредоносных макросов в файлах Microsoft Word и Excel. Файлы рассылаются в приложении к фишинговым сообщениям электронной почты, адресованным как частным, так и корпоративным пользователям.

После исполнения вредоносного файла Dridex заражает систему и включает ее в состав ботнета, контролируемого злоумышленниками. Троян открывает атакующим удаленный доступ к системе, позволяет устанавливать другое вредоносное ПО и следить за трафиком. Главной целью атаки является персональная информация пользователей – прежде всего, аутентификационные данные онлайн-банкинга ***(Спамеры рассылают новый опасный вирус // InternetUA (http://internetua.com/spameri-rassilauat-novii-opasnii-virus). – 2015. – 15.12).***

***

В Евросоюзе, как и в США, регистрировать аккаунт в социальных сетях без разрешения родителей дозволено только лицам, достигшим 13 лет. Уже на днях, возраст, согласно Программе защите данных, а также исследованиям специалистов в сфере защиты прав детей и образования, повысят до 16 лет. Нововведение коснется в основном таких популярных пабликов как Facebook и Instagram.

В парламенте ЕС было принято решение дать странам полномочия установить возрастной показатель самостоятельно, но в пределах все той же нормы 13–16 лет. На согласование законодательства, а также принятие всех необходимых норм и мер по контролю странам дали два года.

Принятие подобных норм остро негативно восприняли на многих интернет-ресурсах, в частности, в Facebook и Google. За счет урезания количества подростков, многие технологические компании будут терять прибыль, особенно в случае если бизнес-модель компании предполагает получение дохода только в случае набора конкретного количества клиентов (минимум подписчиков).

Как стало известно, именно технологические компании выступают с острой критикой программы и пытаются оказать давления для ее полной отмены. Основным аргументом выступает тот факт, что дети могут в сети и не сообщать свой реальный возраст и контролировать ситуацию все равно будет сложно.

В то же время, в ЕС считают, что поднятие возрастного ограничения для пользователей соцсетей позволит взять под жесткий контроль данные потребителей. В случае нарушения законодательства, компании, «пропустившие» подростка, будут штрафоваться на немалые суммы – вплоть до 4 % от суммы годового дохода.

Отметим, что специалисты в сфере образования к нововведениям отнеслись скептически. По мнению экспертов, введенный запрет никак не повлияет на положение дел и не поспособствует реализации наиболее значимого механизма образования и защиты ***(Европейским подросткам запретят использовать соцсети без разрешения родителей // Podrobnosti.mk.ua (http://podrobnosti.mk.ua/2015/12/17/evropeykim-podrostkam-zapretyat-ispol-zovat-socseti-bez-razresheniya-roditeley.html). – 2015. – 17.12).***

***

Крадущие деньги с банковских счетов троянцы в настоящее время представляют серьезную угрозу для владельцев мобильных устройств под управлением ОС Android.

Одним из таких вредоносных приложений является банкер Android.ZBot, различные модификации которого атакуют смартфоны и планшеты российских пользователей с февраля текущего года. Этот троянец интересен тем, что может похищать логины, пароли и другую конфиденциальную информацию при помощи показываемых поверх любых приложений мошеннических форм ввода, внешний вид которых генерируется по команде киберпреступников. При этом сами формы «привязываются» к атакуемым программам, создавая иллюзию того, что они настоящие и принадлежат соответствующему ПО. Полученные специалистами компании «Доктор Веб» данные говорят о том, что зараженные Android.ZBot устройства объединяются в бот-сети, при этом число последних в настоящее время составляет более десятка. Однако не исключено, что со временем их количество будет только расти, т. к. вирусописатели по-прежнему активно распространяют эту вредоносную программу.

Первая модификация банковского троянца Android.ZBot была обнаружена еще в феврале этого года и получила по классификации Dr.Web имя Android.ZBot.1.origin. Начиная с этого момента вирусные аналитики компании «Доктор Веб» стали пристально следить за активностью этого вредоносного приложения.

Как и многие другие Android-троянцы, Android.ZBot.1.origin распространяется злоумышленниками под видом безобидной программы (в данном случае – приложения Google Play), которая скачивается на мобильные устройства при посещении мошеннических или взломанных веб-сайтов, либо загружается другим вредоносным ПО. После того как жертва установит и запустит банкер, тот запрашивает у нее доступ к функциям администратора зараженного смартфона или планшета и в случае успеха выводит на экран сообщение об ошибке, предлагая перезагрузить устройство.

Если же пользователь отказывается предоставить троянцу необходимые полномочия, Android.ZBot.1.origin тут же пытается украсть у него подробные сведения о его банковской карте, включая ее номер и срок действия, трехзначный код безопасности CVV, а также имя владельца. Для этого банкер показывает жертве поддельное окно, имитирующее оригинальную форму ввода соответствующей информации настоящего приложения Google Play. Примечательно, что аналогичное окно троянец отображает и после получения требуемых функций администратора, однако лишь через некоторое время после установки на целевом устройстве.

Далее Android.ZBot.1.origin удаляет свой значок с экрана приложений, «прячась» от пользователя, и начинает контролировать системные события, связанные с загрузкой ОС. Тем самым троянец обеспечивает себе автоматический запуск при каждом включении инфицированного устройства. Как только вредоносная программа получает управление, она связывается с удаленным узлом, регистрирует на нем зараженный смартфон или планшет и ожидает дальнейших указаний злоумышленников. В зависимости от полученной директивы сервера банкер выполняет следующие действия:

– отправляет СМС с заданным текстом на указанный номер;

– совершает телефонный звонок;

– отправляет СМС по всем телефонным номерам из книги контактов;

– перехватывает входящие СМС;

– получает текущие GPS-координаты;

– показывает специально сформированное диалоговое окно поверх заданного приложения.

Например, сразу после того как на управляющем сервере регистрируется новое зараженное устройство, троянец получает команду на проверку состояния банковского баланса пользователя. Если вредоносная программа обнаруживает наличие денег, она автоматически переводит заданную злоумышленниками сумму на подконтрольные им счета. Таким образом, Android.ZBot.1.origin может получить доступ к управлению банковскими счетами владельцев мобильных Android-устройств и незаметно для пользователей похитить деньги при помощи специальных СМС-команд, предусмотренных тем или иным сервисом мобильного банкинга. При этом жертва не будет подозревать о краже, т. к. вредоносная программа перехватывает поступающие от банков сообщения с проверочными кодами транзакций.

Примечательно, что часть вредоносного функционала Android.ZBot.1.origin (например, отправка СМС-сообщений) реализована вирусописателями в виде отдельной Linux-библиотеки с именем libandroid-v7-support.so, которая хранится внутри программного пакета троянца. Это обеспечивает банкеру защиту от детектирования антивирусами и позволяет ему дольше находиться на зараженных устройствах необнаруженным.

Однако одна из главных особенностей Android.ZBot.1.origin заключается в его способности похищать логины и пароли для доступа к сервисам

мобильного банкинга при помощи поддельных форм ввода, генерируемых по указанию управляющего сервера и предназначенных для создания видимости их принадлежности к тем или иным программам. Эта атака представляет собой классический фишинг, но механизм ее любопытен. Вначале троянец получает от злоумышленников команду, содержащую название целевого приложения, после чего с определенной периодичностью начинает проверять, запущена ли пользователем соответствующая программа. В настоящее время троянец контролирует запуск следующих приложений:

ru.sberbank.ivom
ru.sberbank_sbbol
ru.raiffeisennews
ru.vtb24.mobilebanking.android
PSB.Droid
com.idamob.tinkoff.android
ru.simpls.brs2.mobbank
ru.kykyryza
com.smpbank.android
ru.ftc.faktura.sovkombank
hu.eqlsoft.otpdirektru
ru.ftc.faktura.sovkombank
uk.co.danwms.fcprem
ru.sberbankmobile
ru.alfabank.mobile.android
ru.alfabank.oavdo.amc
com.openbank
ru.ucb.android
com.idamobile.android.hcb
com.idamobile.android.ubrr
com.NGSE.Ubrir
com.citibank.mobile.ru
com.ubrir
ru.rshb.mbank
com.bssys.android.SCB
ru.bpc.mobilebank.android
ua.privatbank.ap24.old
ru.bspb
com.svyaznoybank.ui
ru.avangard
ru.minbank.android
ru.letobank.Prometheus
rusfinance.mb.client.android
com.artofweb.mkb
com.compassplus.InternetBankingJava.wscb
ru.stepup.MDMmobileBank

ru.abr
com.intervale.mobilebank.rosbank
ru.pkb
ru.stepup.vbank
ru.vbrr
com.idamobile.android.Trust
org.bms.khmb
ru.tcb.dbo.android
ru.beeline.card
ru.rocketbank.r2d2 ***(Банковский троянец Android.ZBot использует «веб-инжекты» для кражи данных // ITnews (http://itnews.com.ua/news/79336-bankovskij-troyanets-androidzbot-ispolzuet-quotveb-inzhektyquot-dlya-krazhi-dannykh). – 2015. – 16.12).***

***

Специалисты проекта Zero Day Initiative опубликовали информацию о неисправленной уязвимости в Microsoft Office Excel, позволяющей удаленному пользователю выполнить произвольный код на целевой системе.

Уязвимость существует из-за ошибки использования после высвобождения при обработке файлов XLSB. Удаленный пользователь может с помощью специально сформированного файла скомпрометировать систему. Успешная эксплуатация уязвимости требует запуска вредоносного файла жертвой.

Брешь затрагивает Microsoft Excel версий 2007, 2010 и 2013. Сведений об активной эксплуатации уязвимости не поступало. Производитель пока не планирует выпускать исправление ***(В Microsoft Excel обнаружена критическая уязвимость // InternetUA (http://internetua.com/v-Microsoft-Excel-obnarujena-kriticseskaya-uyazvimost). – 2015. – 16.12).***

***

Исследователи И. Риполл и Э. Марко обнаружили серьезную брешь (CVE-2015-8370) в загрузчике операционных систем GRUB2, позволявшую обойти парольную защиту.

Как сообщила компания Canonical, брешь затрагивает все поддерживаемые дистрибутивы Ubuntu Linux, в том числе Ubuntu 15.10 (Wily Werewolf), Ubuntu 15.04 (Vivid Vervet), Ubuntu 14.04 LTS (Trusty Tahr), и Ubuntu 12.04 LTS (Precise Pangolin), а также производные.

Уязвимыми являются версии GRUB2 1.98 (декабрь 2009 г.) – 2.02 (декабрь 2015 г.). Эксплуатация бреши в определенных обстоятельствах дает возможность локальному пользователю обойти любую парольную защиту, если она установлена для GRUB2 при загрузке.

Загрузчик ОС некорректно обрабатывает нажатия на клавишу Backspace при включенной парольной аутентификации. По словам Э. Марко, проверить систему на наличие уязвимости можно следующим способом: при вводе имени

пользователя 28 раз нажать на клавишу Backspace, если компьютер начнет перезагружаться, значит, загрузчик уязвим.

Проэксплуатировав уязвимость, злоумышленник может повысить привилегии, загрузить кастомизированное ядро или образ initramfs (например, с USB-накопителя), установить руткит или вызвать отказ в обслуживании.

Эксперты рекомендуют всем пользователям дистрибутивов GNU/Linux с установленным по умолчанию загрузчик GRUB2 в кратчайшие сроки обновиться до последней версии ПО, доступной в тестовом репозитории Arch Linux ***(В загрузчике GRUB2 обнаружена опасная уязвимость // InternetUA (http://internetua.com/v-zagruzcsike-GRUB2-obnarujena-opasnaya-uyazvimost). – 2015. – 16.12).***

***

Исследователи из команды Google Project Zero Т. Орманди и Н. Силванович обнаружили критическую уязвимость в устройствах FireEye. Брешь дает возможность злоумышленникам взламывать корпоративные сети с помощью специально сформированных сообщений электронной почты.

Ошибка получила название «666» в честь присвоенного порядкового номера. Проблема существует из-за ошибки в модуле пассивного мониторинга и затрагивает устройства FireEye NX, FX, AX и EX.

Устройства FireEye устанавливаются во внутреннюю сеть организации и проводят пассивное наблюдение за всем трафиком. Все операции по передаче файлов (например, по FTP или электронной почте) контролируются – в рамках мониторинга передаваемые файлы открываются и проверяются на предмет вредоносного ПО. Если пользователь получит письмо с вредоносным вложением, система мониторинга попытается проверить полученные файлы и будет инфицирована. Злоумышленник может получить доступ к корпоративной сети.

Уязвимость может быть проэксплуатирована на устройствах с заводскими настройками. FireEye выпустила исправления для FireEye NX, FX и AX. В связи со сложившимися обстоятельствами техническая поддержка оказывается всем клиентам, включая пользователей с истекшими контрактами на обслуживание.

В сетях с зараженными устройствами злоумышленники могут похищать конфиденциальную информацию, перехватывать либо перенаправлять трафик, устанавливать руткиты или самораспространяющиеся сетевые черви ***(В продуктах FireEye обнаружена критическая уязвимость // InternetUA (http://internetua.com/v-produktah-FireEye-obnarujena-kriticseskaya-uyazvimost). – 2015. – 17.12).***

***

«Лаборатория Касперского» представила прогноз по кибербезопасности на 2016 г., в котором предрекает смерть APT-угроз в том виде, в котором они существовали до настоящего времени. Атаки нового поколения будут более

сложны для анализа и отслеживания, и определять исполнителей экспертам станет намного труднее.

В 2015 г. специалисты центра изучения угроз GReAT «Лаборатории Касперского» смогли раскрыть 12 крупных APT-операций, организованных группировками в различных частях света. Опыт и накопленная экспертиза позволили команде сформировать наиболее вероятные сценарии развития ситуации в мире киберугроз в 2016 г.

APT-кампании станут чаще полагаться на готовые программные комплекты для заражения компьютеров, а не на разработку собственных зловредов, буткитов или руткитов. APT-атаки все больше превращаются в традиционный бизнес, и заказчикам будут в большей степени важны не навыки хакеров, а небольшие начальные инвестиции и быстрая окупаемость затрат.

Киберпреступники также будут уделять больше внимания «бесфайловым» зловредам и программам, укореняющимся в памяти инфицированной машины, чтобы вызывать меньше подозрений и долго оставаться незамеченными.

В ряды кибернаемников, занимающихся APT-кампаниями, будут вливаться новые люди, и, соответственно, на рынке «труда» у хакеров станет тесно. Новым витком эволюции APT-атак может стать оказание экспресс-услуг по получению несанкционированного доступа к особо важным целям – Access-as-a-Service.

«Раз на таком прибыльном рынке, как хакерские услуги, орудует все больше кибернаемников, этот тренд обуславливает появление хорошо развитой отрасли аутсорсинга услуг, а также готовых инструментов и кампаний. Например, хакеры смогут продавать возможность несанкционированного доступа к уже взломанной цели тому, кто готов заплатить больше», – предупреждает Х. Герреро-Сааде, старший эксперт по безопасности в GReAT.

Наступающий 2016 г. станет годом расцвета банковских троянцев, которые найдут для себя новые цели в виде устройств под OS X, владельцы которых обычно являются обеспеченными людьми, а также освоят новые сегменты в виде мобильных и IoT-устройств.

Разработчики программ-вымогателей начнут учитывать набирающие популярность платежные системы – например, Apple Pay и Android Pay. Желанной целью для мошенников также станут биржевые данные.

Некоторые масштабные утечки в 2015 г. привели к шантажу или даже публичному унижению жертв атак – например, атака на сайт для неверных супругов Ashley Madison. Киберпреступники, хактивисты и даже хакерские группировки, спонсируемые правительствами, оценили влияние таких данных, как личная переписка, компрометирующие фото или информация о частной жизни, и в 2016 г. эта практика будет использоваться намного чаще.

Еще одним заметным трендом в наступающем году станет «балканизация» Интернета. Если рассматривать это явление в контексте термина «балканизация», единое глобальное информационное пространство можно будет разделять на множество «географических» сегментов благодаря

целевым атакам на крупные узлы, на которых происходит распределение трафика по географическим регионам. Эта тенденция рисует еще более мрачную перспективу: появление «черного рынка» подобных услуг.

В то же время, по мере того как технологии, используемые в дарквебе, получают все большее распространение среди обычных пользователей (например, анонимайзеры и торренты), разработчики, специализирующиеся на теневых кибертехнологиях, будут совершенствовать свои разработки, чтобы теневой Интернет продолжал оставаться в тени.

«Это будет еще один трудный год для отрасли ИБ. Мы считаем, что в этих условиях нам необходимо делиться своими прогнозами с компаниями, государственными организациями и правоохранительными органами», – добавил Х. Герреро-Сааде.

Эксперты «Лаборатории» советуют принять меры сейчас, для того чтобы избежать печальных последствий в будущем. Прежде всего организациям стоит уделять больше внимания повышению уровня осведомленности об угрозах среди сотрудников, регулярно и своевременно применять патчи, быть вдвойне осторожными с мобильными технологиями, не пренебрегать шифрованием. Многие из этих советов подойдут и конечным пользователям – им следует узнать побольше о мире кибербезопасности, применять все возможные техники защиты, включая шифрование и резервирование данных, а также думать дважды, прежде чем делиться чем-то со всем миром: Интернет помнит все.

Чтобы бороться с угрозами будущего, компаниям стоит предусмотреть отдельное подразделение, отвечающее исключительно за информационную безопасность, а также полностью продумать ИБ-стратегию ***(В 2016 году нас ждет эволюция APT // ООО Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/12/15/2016-predictions.html). – 2015. – 15.12).***

***

McAfee Labs обнародовала отчет о новых угрозах за ноябрь 2015 г., связанных с сервисами для мобильного банкинга, макросами и вредоносным ПО без файлов.

В отчете описывается, как вредоносное ПО использует индустриальную социологию для распространения в корпоративных средах – объем вредоносного ПО на основе макросов увеличился с менее чем 10 тыс. новых атак в III кв. 2015 г. до почти 45 тыс. в этом квартале. Таких темпов роста не наблюдалось с 2009 г.

Во время двухмесячного анализа практически 300 тыс. мобильных приложений специалисты обнаружили две троянские программы для мобильного банкинга, которые нарушили работу тысяч пользователей услуг мобильного банкинга в Восточной Европе. Две модификации вредоносного ПО, получившие название Android/OpFake и Android/Marry, использовали ошибки неправильного программного кода мобильных приложений, который

использовался для подключения мобильных приложений к данным управления приложениями поставщиков сервисов.

Несмотря на то, что действия этих групп злоумышленников были пресечены, они использовали имеющиеся уязвимости, чтобы незаметно установить вредоносный код и применяли схему на основе SMS-сообщений для кражи номеров кредитных карт и проведения мошеннических операций. Две троянские программы перехватили 171 256 SMS-сообщений 13 842 банковских клиентов и в удаленном режиме выполнили команды на 1645 зараженных мобильных устройствах.

McAfee Labs также зарегистрировала четырехкратное увеличение количества случаев обнаружения макросов вредоносного ПО за последний год, что приближается к самым высоким показателям с 2009 г. Это связано с атаками на основе целевого фишинга, целью которых было обмануть корпоративных пользователей при открытии вложений в письмах электронной почты. Новые макросы также продемонстрировали способность оставаться незаметными даже после того, как они загрузили вредоносный код.

За первые три квартала 2015 г. McAfee Labs зафиксировала 74 471 примеров атак без использования файлов. Три основных типа вредоносного ПО загружают вредоносный код непосредственно в разрешенную область памяти функции платформы, прячутся в интерфейсе прикладного программирования на уровне ядра или в регистре операционной системы ***(Объем вредоносного ПО на основе макросов увеличился в ноябре в 4,5 раза // Компьютерное Обозрение (http://ko.com.ua/obem_vredonosnogo_po_na_osnove_makrosov_uvelichilsya_v_noyabre_v_4_5_raza_113566). – 2015. – 18.12).***

***

Несмотря на многочисленные предупреждения правоохранительных органов и специалистов по информационной безопасности, компрометация корпоративной почты по-прежнему является одним из главных источников наживы для злоумышленников. Как правило, основной целью мошенников являются не клиенты компаний, а топ-менеджмент. По словам экспертов Symantec, у руководства проще «выманить» крупные суммы денег. В некоторых случаях суммы исчисляются в несколько сотен тысяч долларов.

По данным ФБР, за период с октября 2013 г. по август 2015 г. в результате подобных мошеннических схем компании потеряли свыше 1,2 млрд дол. Чаще всего жертвами злоумышленников становятся финансовые директоры предприятий. Для выманивания средств преступники используют разнообразные техники. Одним из распространенных методов является отправка письма якобы от гендиректора компании с просьбой перевести определенную сумму на какой-либо счет. Нередко в письме содержится указание не обсуждать транзакцию с другими сотрудниками. Мошенники могут легко получить доступ к именам и адресам электронной почты будущих жертв, просмотрев официальный веб-сайт компании или профиль в соцсети LinkedIn.

Согласно данным 18-го ежегодного опроса руководителей крупнейших компаний мира, проведенного консалтинговой компанией PwC, развитие цифровых технологий полностью изменило подходы компаний к ведению бизнеса. В 2015 г. 58 % руководителей были обеспокоены быстротой изменений в технологической сфере (против 47 % в 2014 г.). Реализация мобильных технологий в компаниях стала важной для 81 % руководителей. В список приоритетов также попали получение и анализ данных (80 %), кибербезопасность (78 %), освоение технологий социальных сетей (61 %) и облачные вычисления (60 %) ***(На компрометации корпоративной почты хакеры заработали свыше 1,2 млрд дол. // InternetUA (http://internetua.com/na-komprometacii-korporativnoi-pocsti-hakeri-zarabotali-svishe--1-2-mlrd). – 2015. – 19.12).***

***

Исследователи компании CloudSek обнаружили новую вредоносную кампанию по хищению интеллектуальной собственности у производителей программного обеспечения и правительственных организаций по всему миру. Злоумышленников интересуют как коммерческие секреты, так и информация, представляющая потенциальный интерес для правительств. По данным исследователей, кампания Santa-APT приурочена к зимним праздникам и эксплуатирует соответствующую тематику.

Эксперты проводили мониторинг активности хакерской группировки, занимающейся продажей на подпольных форумах вредоносного ПО для десктопных систем. Особенностью программ является способность обходить физически изолированные системы и похищать секретную информацию в зависимости от того, какие документы интересуют злоумышленников.

После инсталляции троян устанавливает связь с C&C-серверами в Германии и передает два типа данных – файлы и скриншоты. USB-модуль дает возможность похищать информацию даже с физически изолированных компьютеров без доступа к Интернету. Модуль сохраняет полученные данные на подключенное USB-устройство, пока не найдет инфицированный компьютер с доступом к Интернету.

Santa-APT интересует не только десктопное, но и мобильное ПО. Как выяснили исследователи CloudSek, многие работающие на группировку разработчики специализируются на приложениях для iOS- и Android-устройств. Вредоносные программы Santa-APT маскируются под игры и утилиты, посвященные новогодней тематике. В последнее время злоумышленники стали выпускать вредоносные приложения под видом игр с Санта-Клаусом. Один из C&C-серверов Santa-APT управляет мобильными программами. В общей сложности исследователи насчитали порядка 8 тыс. инфицированных смартфонов и планшетов ***(«Злой Санта» похищает конфиденциальные данные с Android-устройств // InternetUA (http://internetua.com/zloi-santa--pohisxaet-konfidencialnie-dannie-s-Android-ustroistv). – 2015. – 19.12).***

***

Носимая электроника станет целью номер один для хакеров в 2016 г.

Растущая популярность носимых устройств, таких как Fitbit и Apple Watch в этом году, может привести к тому, что их производители в гонке за первенство на рынке будут приделять недостаточно внимания вопросам безопасности этих устройств. Это, в свою очередь, может спровоцировать повышенную активность хакеров по отношению к носимой электронике.

«Носимые устройства станут следующей платформой, которую будут использовать десятки миллионов людей, количество операций с их использованием будет стремительно расти», – отметил представитель провайдера решений безопасности Good Technology Д. Херрема. «В связи с этим, после праздничного сезона носимая электроника станет очень привлекательной для хакеров».

По словам Д. Мэнки, аналитика исследовательской компании FortiGuard, кибератаки в сфере Интернета вещей впервые попали в топ-10 угроз, прогнозируемых на следующий год.

«Мы ожидаем роста количества уязвимостей на 25 % именно в сфере носимой электроники в следующем году», – отметил Д. Мэнки ***(Носимая электроника станет целью номер один для хакеров в 2016 году // InternetUA (http://internetua.com/nosimaya-elektronika-stanet-celua-nomer-odin-dlya-hakerov-v-2016-godu). – 2015. – 19.12).***

***

Производитель телекоммуникационного оборудования Juniper Networks выпустил экстренные патчи с исправлением ряда критических уязвимостей в операционной системе ScreenOS. Согласно опубликованным бюллетеням безопасности, специалисты компании обнаружили в операционной системе три проблемы, позволяющие злоумышленнику удаленно получить доступ с правами администратора к устройствам Juniper NetScreen и расшифровать VPN-трафик.

Две уязвимости (CVE-2015-7755) затрагивают версии ScreenOS 6.2.0r15-6.2.0r18 и 6.3.0r12-6.3.0r20. Первая позволяет злоумышленнику через SSH или Telnet получить к устройству удаленный доступ с правами администратора. Успешная эксплуатация проблемы может привести к компрометации целевой системы. С помощью второй уязвимости злоумышленник может расшифровать VPN-трафик.

Последняя уязвимость (CVE-2015-7754) распространяется только на версию ScreenOS 6.3.0r20. Проблема вызвана ошибкой при обработке входных данных во время обработки SSH-переговоров. Злоумышленник может с помощью специально сформированных SSH-пакетов вызвать аварийное завершение работы устройства или выполнить произвольный код на системе.

В настоящее время нет данных об активной эксплуатации вышеуказанных уязвимостей. Патчи доступны на странице поддержки производителя.

Juniper Netscreen – семейство универсальных продуктов, сочетающих функции межсетевого экрана, VPN-шлюза/концентратора, маршрутизатора и пр. Все модели межсетевых экранов серии Juniper NetScreen используют единую операционную систему ScreenOS ***(Обнаружены критические уязвимости в Juniper ScreenOS // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/12/18/Juniper-ScreenOS.html). – 2015. – 18.12).***

***

Хакеры из международной группы Anonymous взяли на себя ответственность за 97 кибератак на японские сайты за последние три месяца. Среди пострадавших ресурсов, в том числе, правительственные. Об этом в воскресенье, 20 декабря, сообщает ТАСС со ссылкой репортаж национального телеканала NHK.

В частности, 10 декабря оказался недоступен официальный сайт премьер-министра Японии С. Абэ. «Мы пока не располагаем информацией, действительно ли это дело рук группировки Anonymous», – признался тогда генеральный секретарь кабинета министров Японии Ё. Суга, подчеркнув, что «полиция уже расследует этот инцидент».

Полиция предупредила, что активность взломщиков может возрасти с приближением намеченного на конец мая саммита G7 в японской префектуре Миэ. Правоохранители призвали администраторов сайтов принять дополнительные меры безопасности ***(Хакеры Anonymous активизировали атаки на Японию // InternetUA (http://internetua.com/hakeri-Anonymous-aktivizirovali-ataki-na-yaponiua). – 2015. – 20.12).***

***

База данных 3,3 млн пользователей официального сообщества Hello Kitty (sanriotown.com) оказалась в открытом доступе. Как сообщает С. Рэгэн в своей колонке на сайте CSO со ссылкой на обнаружившего инцидент ИБ-эксперта К. Викери, в сеть утекли имена и фамилии, даты рождения, сведения о гендерной принадлежности и стране проживания, электронные адреса и хэши паролей, зашифрованные с помощью алгоритма SHA-1.

По данным эксперта, инцидент также затронул учетные записи, зарегистрированные через сайты hellokitty.com, hellokitty.com.sg, hellokitty.com.my, hellokitty.in.th и mymelody.com. Помимо основной базы данных sanriotown.com, К. Викери обнаружил в открытом доступе два дополнительных зеркальных сервера, хранящих резервные копии. Предположительно, утечка произошла 22 ноября этого года.

Эксперт уведомил об утечке компанию Sanrio, владеющую правами на бренд Hello Kitty, и хостинг-провайдеров в субботу, 19 декабря. В настоящее время в целях безопасности подробности об инциденте не раскрываются.

Этот случай стал уже вторым за последнее время, когда жертвами утечки данных являются дети ***(3,3 млн поклонников Hello Kitty стали жертвами***

утечки данных // InternetUA (http://internetua.com/3-3-mln-poklonnikov-Hello-Kitty-stali-jertvami-utecski-dannih). – 2015. – 22.12).

***

19 і 20 грудня сайти видавничої групи «Картель» «Депо» (depo.ua) і «Деловая столица» (dsnews.ua) були атаковані хакерами. Зловмисники вимагали від редакцій гроші, аби припинити DDoS-атаки.

Про це повідомляється у релізі ВГ «Картель».

Хакери погрожували у своєму листі, що атаки триватимуть далі, і їх можна буде припинити за певну винагороду. Як йдеться у повідомленні, визначити місце розташування джерела хакерської атаки на сьогодні неможливо.

Наразі видання «Депо» і «Деловая столица продовжують працювати у звичному режимі. «Атаки не нашкодили роботі наших порталів», – заявляє ВГ «Картель».

Видавнича група також повідомляє, що подаватиме заяви в Управління по боротьбі з кіберзлочинністю і в СБУна інтернет-атаки, що здійснюються на сайти ВГ «Картель» ***(Хакери вимагали гроші від двох українських сайтів за припинення DDoS-атак // MediaSapiens (http://osvita.mediasapiens.ua/web/online_media/khakeri_vimagali_groshi_vid_dvokh_ukrainskikh_saytiv_za_pripinennya_ddosatak/). – 2015. – 21.12).***

***

В распоряжении издания The Wall Street Journal оказались документы, свидетельствующие о причастности иранских хакеров к атаке на IT-инфраструктуру дамбы неподалеку от Нью-Йорка, США. Осуществленное в 2013 г. нападение не причинило ущерба, но злоумышленникам удалось раскрыть ряд важных данных.

По итогам расследования наиболее вероятным оказался вариант с иранскими киберпреступниками. Ответственная за взлом группировка также осуществила атаки на ряд объектов критической инфраструктуры, включая финансовые организации.

ИБ-эксперты неоднократно обнаруживали взлом IT-систем объектов критической инфраструктуры. Пока во время атак злоумышленники нацеливались на получение доступа к конфиденциальной информации.

Во время одной из кампаний хакеры получили доступ к 82 электростанциям, размещенным на территории США и Канады. Установить национальность злоумышленников удалось благодаря комментариям в коде используемого для взлома вредоносного ПО. Узнав об инциденте, ФБР США выпустило предупреждение о риске осуществления кибератак на объекты энергетической инфраструктуры.

Собранная киберпреступниками информация не использовалась для выведения из строя энергетических объектов или вмешательства в рабочий процесс. Тем не менее, в случае ухудшения дипломатических отношений

между Ираном и США хакеры могут осуществить ряд разрушительных атак. Об этом заявил бывший эксперт по кибербезопасности ВВС США Р. Ли ***(Иранские хакеры атаковали дамбу в Нью-Йорке // InternetUA (http://internetua.com/iranskie-hakeri-atakovali-dambu-v-nua-iorke). – 2015. – 22.12).***

***

Киберпреступники рассылают вымогательское ПО TeslaCrypt с помощью эксплоита для Flash Player, недавно добавленного в набор эксплоитов Angler. Об этом сообщает ИБ-эксперт Kafeine.

Эксплоит использует уязвимость переполнения динамической памяти в Adobe Flash Player (CVE-2015-8446), исправленную компанией Adobe 8 декабря этого года. В понедельник, 14 декабря, вредоносный код был добавлен в Angler. Помимо TeslaCrypt, в настоящее время через набор эксплоитов Angler также распространяется вредоносное ПО Bedep.

В настоящее время TeslaCrypt практически не детектируется антивирусами. Вымогательское ПО шифрует файлы, меняет расширение на .vvv и требует выкуп в размере 500 дол. Если жертва в течение недели не выплатит преступнику требуемую сумму, размер выкупа увеличивается на 1000 дол. еженедельно.

Вредонос был впервые замечен в феврале текущего года, а первые массовые заражения начали наблюдаться в марте. Тогда вымогательское ПО инфицировало файлы сохранений компьютерных игр и требовало от геймеров выкуп, но из-за ошибки в алгоритме шифрования исследователям удалось разработать утилиту для расшифрования файлов. Вторая версия TeslaCrypt с улучшенной системой шифрования была выпущена в июле этого года ***(Злоумышленники распространяют TeslaCrypt через набор эксплоитов Angler // InternetUA (http://internetua.com/zloumishlenniki-rasprostranyauat-TeslaCrypt-cserez-nabor-eksploitov-Angler). – 2015. – 23.12).***

***

Исследователи швейцарской ИБ-компании High-Tech Bridge обнаружили серьезные уязвимости в ряде популярных веб-приложений. 21 ноября специалисты компании сообщили об ошибках в продуктах osCmax, osCommerce Online Merchant, Roundcube, Osclass и Webligo SocialEngine.

По данным High-Tech Bridge, в osCmax 2.5.4 и osCommerce Online Merchant 2.3.4 обнаружены множественные уязвимости, позволяющие удаленно выполнить код и осуществить CSRF-атаку. Эти ошибки также присутствуют в более ранних версиях продуктов.

Roundcube 1.1.3 подвержен уязвимости обхода пути, позволяющей выполнить произвольный код. В Osclass 3.5.9 и SocialEngine 489 специалисты обнаружили ошибку, позволяющую осуществить SQL-инъекцию. Уязвимостям подвержены и более ранние версии приложений.

В настоящее время подробная информация об уязвимостях отсутствует и будет обнародована после выхода исправлений. По словам эксперта High-Tech Bridge И. Колошенко, ошибки достаточно сложно проэксплуатировать, но в случае успеха злоумышленник сможет получить полный доступ к целевому веб-приложению.

«Как SQL-инъекция, так и удаленное выполнение кода позволит злоумышленнику получить полный доступ к базе данных уязвимого веб-приложения. Во втором случае атакующий сможет осуществить любые действия с системой, в том числе удалить все файлы или стереть все таблицы базы данных», – заявил И. Колошенко ***(В популярных web-приложениях обнаружены серьезные уязвимости // InternetUA (http://internetua.com/v-populyarnih-web-prilojeniyah-obnarujeni-sereznie-uyazvimosti). – 2015. – 23.12).***

***

Світова мережа готелів Hyatt знайшла вірус у системі платежів і попросила клієнтів пильнувати свої кредитки. Про це повідомляє Еспресо.TV із посиланням на The Guardian.

Компанія володіє готелями у 52 країнах світу. Компанія звернулася до клієнтів з порадою переглянути свої платежі з пластикових карток. Хакери могли заволодіти номерами кредиток або іншою чутливою інформацією.

Компанія не повідомляє, чи була викрадена інформація когось із клієнтів.

Небезпечна програма-вірус була знайдена ще 30 листопада. Чому компанія чекала три тижні, щоб повідомити про це, речниця Hyatt С. Шеппард не пояснила.

Hyatt – далеко не перша мережа готелів, яка повідомляє про хакерську атаку на їхні комп'ютери за останні кілька місяців. Раніше з такою ж проблемою стикались Hilton, Starwood, Mandarin Oriental, а також Trump Collection.

Більшість компаній не розкрила деталі атаки. Але мережа Starwood визнала, що шкідлива програма дозволила невідомим особам отримати доступ до інформації щодо платежів з карток деяких її клієнтів.

«Розслідування триває і ми матимемо більше інформації, як тільки воно завершиться», – зазначила С. Шеппард ***(Мережа готелів Hyatt повідомила про хакерську атаку // Espreso.tv (http://espreso.tv/news/2015/12/24/merezha_goteliv_hyatt_povidomyla_pro_khakersku_ataku). – 2015. – 24.12).***

***

«Лаборатория Касперского» предупреждает о волне мошеннических писем, нацеленных на клиентов служб доставки, услуги которых в настоящее время пользуются особенно высоким спросом.

Рассылки замаскированы под сообщения крупных известных курьерских компаний, таких как DHL и FedEx. Цель киберпреступников проста – убедить доверчивых пользователей скачать вредоносную программу или ввести свои

конфиденциальные данные на фишинговом сайте. Злоумышленникам играет на руку наличие таких удобных сервисов, как уведомления по электронной почте и система трекинга посылок. Именно под письма таких служб обычно маскируются вредоносные послания.

Фишинговые письма очень похожи на реальные уведомления, поскольку в них моделируются типовые ситуации. Например, киберпреступники могут попросить потенциальную жертву заполнить и подписать форму доставки для получения посылки. К письму прикрепляется документ, на деле являющийся вредоносной программой.

Другая схема обмана заключается в следующем. Жертве сообщается, что посылка уже якобы находится в офисе, но не может быть доставлена курьером, поскольку адрес написан неразборчиво. Получателю в этом случае предлагается в течение 48 часов перейти по ссылке, ведущей на фишинговый сайт, и ввести номер посылки на странице трекинга, иначе она будет возвращена обратно. Если доверчивый пользователь перейдет по ссылке, он попадет на сайт, выполненный в корпоративном стиле службы доставки, где ему будет предложено указать свои логин и пароль для входа в систему отслеживания посылки. Введенные на такой странице данные сразу же попадут в руки злоумышленников ***(Клиенты служб доставки могут стать новой целью для киберпреступников // IGate (http://igate.com.ua/lenta/12247-klienty-sluzhb-dostavki-mogut-stat-novoj-tselyu-dlya-kiberprestupnikov). – 2015. – 24.12).***

***

Компания Livestream предупредила пользователей о возможной кибератаке и попросила сменить пароли. «Недавно мы обнаружили, что неавторизованное лицо могло получить доступ к базе данных наших клиентов. Пока мы пытаемся определить масштабы инцидента, и не исключено, что злоумышленник мог похитить информацию вашей учетной записи», – говорится в письме, разосланном администрацией ресурса.

В руках неизвестного или неизвестных могли оказаться имена пользователей, адреса электронной почты, пароли в зашифрованном виде, телефонные номера и даты рождения. Каких-либо свидетельств возможной расшифровки учетных данных Livestream не фиксировала, однако в качестве меры предосторожности просит сменить пароли. По словам представителей компании, инцидент не затронул данные кредитных карт и другую платежную информацию. Подробности об атаке не разглашаются ***(Стриминговая платформа Livestream подверглась кибератаке // InternetUA (http://internetua.com/strimingovaya-platforma-Livestream-podverglas-kiberatake). – 2015. – 24.12).***

***

Индийский специалист по безопасности И. Бхайян обнаружил в популярном мессенджере WhatsApp уязвимость, которая «ломает» приложение при получении сообщения с более 4000 эмодзи. Об этом он рассказал в своем

блоге. Мессенджер зависает или «падает», единственный способ вернуть его к жизни – удалить всю переписку с отправителем, пишет AIN.UA (http://ain.ua/2015/12/25/624087?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed %3A+ainua+ %28AIN.UA %29).

И. Бхайян утверждает, что уязвимость обнаружил еще в 2014 г. Тогда он и его друг установили, что отправка сообщения длиной более 2 КБ в специальной кодировке приводит к «падению» мессенджера. Подобного эффекта можно было также добиться обычными «тяжелыми» сообщениями свыше 7 МБ, но WhatsApp устранили проблему, ограничив число символов следующим апдейтом.

Компания не учла, что длинное сообщение можно также набрать при помощи эмодзи. В декабре 2015 г. И. Бхайян проверил такую лазейку и обнаружил, что она работает. Однако ввод 4000–4500 смайлов в поле отправки в мессенджере замедляет работу приложения, поэтому, чтобы сломать кому-то WhatsApp, лучше отправлять эмодзи через веб-версию мессенджера.

По результатам опытов И. Бхайяна, при получении такого сообщения у адресата перестает работать мессенджер на ПК в браузерах Firefox и Chrome, на всех последних версиях Android (Marshmallow, Lollipop, Kitkat), а также мобильные версии на Moto E, ASUS ZenPhone 2 Laser и OnePlus Two. Уязвимость пережила лишь iOS-версия, которая не «падает», а лишь зависает на несколько секунд.

Если вам прислали такое сообщение, вы не сможете пользоваться WhatsApp до тех пор, пока не удалите всю переписку с отправителем. Таким образом, данная уязвимость – отличный способ удалить свои сообщения с чужого смартфона.

И. Бхайян сообщил об уязвимости представителям WhatsApp и надеется, что они устранят ее в следующем обновлении. А пока «под угрозой» ежемесячно находятся 800 млн человек ***(Как удалить все свои сообщения из чужого WhatsApp при помощи эмодзи // AIN.UA (http://ain.ua/2015/12/25/624087?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed %3A+ainua+ %28AIN.UA %29). – 2015. – 25.12).***

***

В среду 23 декабря из-за технических сбоев в работе «Прикарпатьеоблэнерго» без электроэнергии осталась половина Ивано-Франковской области и часть областного центра. На предприятии ни с того ни с сего начали отключаться электроподстанции. Как сообщил «ТСН», причиной стала хакерская атака: запущенный извне вирус вывел из строя систему управления телемеханикой. Возобновить подачу электроэнергии специалистам удалось лишь спустя шесть часов, пишет AIN.UA (http://ain.ua/2015/12/25/624117).

В результате атаки частично или полностью были обесточены Ивано-Франковск, Городенковский, Долинский, Коломыйский, Надвирнянский, Косовский, Калушский, Тисменицкий районы и часть Яремчанской зоны.

Энергетики не сразу поняли причины аварии. Центральная диспетчерская внезапно «ослепла». «Можно сказать, что систему фактически хакнули. Это у нас впервые за время работы», – сообщили изданию «Курс» в «Прикарпатьеоблэнерго». Восстанавливали работу станции в ручном режиме, поскольку зараженную вирусом систему пришлось отключить.

На момент включения сеть «Прикарпатьеоблэнерго» все еще была заражена вирусом, специалисты работали над тем, чтобы его обезвредить. Удалось ли это прикарпатским специалистам, пока неизвестно.

Это первая в Украине успешная кибератака на государственное предприятие снабжения населения энергоресурсами. Ранее специалисты CERT-UA в интервью AIN.UA рассказали, что такие атаки классифицируются как кибероперации. Это самый опасный вид хакерских кампаний, поскольку результатом может стать не только виртуальная, но физическая катастрофа, которая может повлечь за собой человеческие жертвы. По словам экспертов, подобные атаки, как правило, финансируются на государственном уровне в рамках киберпротивостояния между странами ***(Хакеры атаковали «Прикарпатьеоблэнерго», обесточив половину региона на 6 часов // AIN.UA (http://ain.ua/2015/12/25/624117). – 2015. – 25.12).***

***

Хакери Anonymous оголосили Анкарі кібервійну через «ІД».

Як пише Лента.ru, посилаючись на Daily Mail, за останній тиждень Anonymous вивела з ладу «до 40 тисяч інтернет-сайтів по всій Туреччині».

«Туреччина підтримує “ІД”, купує у неї нафту і лікує в госпіталях її бойовиків», – стверджує представник Anonymous, передає «ТСН».

У разі, якщо підтримка продовжиться, хакери пообіцяли масштабні атаки на весь турецький сегмент Інтернету, зокрема, на банки та сайти уряду.

Нагадаємо, що хакери Anonymous викрили компанію з Силіконової долини, яка захищає сайти бойовиків «ІД» ***(Хакери Anonymous оголосили Анкарі кібервійну // Західна інформаційна корпорація (http://zik.ua/news/2015/12/23/hakery_anonymous_ogolosyly_ankari_kiberviynu_656784). – 2015. – 23.12).***

***

Служба безопасности Украины предупредила исполнительные органы государственной власти, что на официальные электронные адреса приходят сообщения, содержащие нефиксируемый антивирусными программами и чрезвычайно вредоносный компьютерный вирус.

Сообщения имею вид деловых писем с названиями типа «Бухгалтерия» или «Рабочие документы за ноябрь месяц, ознакомьтесь с ними. Спасибо», содержащие одноименные файлы с расширением .7z.

При попытке открытия этих файлов вирус уничтожает все текстовые документы и изображения на жестком диске компьютера без возможности их восстановления. Никакие антивирусные программы его не отслеживают и не

блокируют ***(Неизлечимый компьютерный вирус уничтожает данные на компьютерах госструктур // Kherson.life. (http://kherson.life/kherson/proishestviya/neizlechimyj-kompyuternyj-virus-unichtozhaet-dannye-na-kompyuterah-gosstruktur/). – 2015. – 24.12).***

***

Microsoft анонсирует политику по защите от атак «человек посередине».

Компания Microsoft недавно объявила, что с 31 марта 2016 г. рекламное программное обеспечение с техникой «человек посередине» (man-in-the-middle) в Windows будет полностью блокироваться. За счёт этого разработчики хотят добавить новый уровень безопасности операционной системы.

Многие эксперты считают, что этот шаг давно было необходимо сделать, и в Microsoft решили, что лучше поздно, чем никогда. Такая защита поможет закрыть такие уязвимости, как Lenovo Superfish, ставшее известным в начале года приложение, которое использует технику «человек посередине» для отображения рекламы.

В своём блоге Microsoft пишет, что эта техника повышает риск для Windows-компьютеров. Она может привести к изменению настроек, которое может пройти незамеченным мимо пользователей, без уведомлений и предупреждений, оставляющих возможность блокировки. В случае с Superfish устранение угрозы стало возможным после того, как Microsoft обновила своё приложение безопасности, а следом за ней и остальные производители антивирусов. При этом уязвимость продолжала оставаться в компьютерах Lenovo и могла быть задействована другими программами.

После 31 марта все приложения с техникой «человек посередине» будут использовать модель расширений браузера, чтобы пользователи могли легко их удалить. Разработчики программного обеспечения получат оповещения, чтобы привести свои программы в соответствие с новыми требованиями. Не соответствующие требованиям приложения будут удалены ***(Microsoft анонсирует политику по защите от атак «человек посередине» // InternetUA (http://internetua.com/Microsoft-anonsiruet-politiku-po-zasxite-ot-atak--cselovek-poseredine). – 2015. – 23.12).***

***

Осторожно: телефонный номер в соцсети помогает мошенникам.

Пользователи социальных сетей нередко указывают свою контактную информацию, в том числе номер телефона. «Лаборатория Касперского» объяснила, чем опасно размещение номера в Интернете, и как защитить свои данные.

Есть мнение, что злоумышленники покупают готовые базы данных со всеми номерами телефонов. На самом деле, это не совсем так. Преступникам достаточно воспользоваться специальной программой-парсером, которая соберет всю информацию из социальной сети.

Современные кибепреступники завели в своем арсенале программы-парсеры, которые «бродят» по открытым профилям в социальной сети и структурируют собранную о пользователях информацию. Если в информации попадается телефон, то жертва «на крючке»: можно выслать спам, подделать сим-карту и похитить деньги через SMS сервисы.

Как защититься?

– удалите номер мобильного (особенно если пользуетесь мобильным банком);

– не устанавливайте приложения со сторонних источников на Android-устройствах с мобильным банком;

– определите лимиты на списание в мобильном банке;

– отключите отправку SMS на Premium-номера;

– поставьте надежный антивирус ***(Осторожно: телефонный номер в соцсети помогает мошенникам // InternetUA (http://internetua.com/ostorojno--telefonnii-nomer-v-socseti-pomogaet-moshennikam). – 2015. – 27.12).***

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.