СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(2–15.11)

2015 № 20

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(2–15.11)
№ 20

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

За даними дослідження CMeter компанії TNS, список популярних сайтів серед українських інтернет-користувачів у жовтні очолили Google, «ВКонтакте» та YouTube.

«Одноклассники» за крок до вильоту з ТОП 10 найпопулярніших сайтів серед українців.

Якщо подивитися співвідношення тижневих охоплень і місячних, то у таких сайтів як Vk.com, Google.com.ua, Youtube.com вища частка регулярної аудиторії, адже приріст місячного охоплення до тижневої аудиторії відносно невеликий ***(Однокласники за крок до вильоту з ТОП-10 найпопулярніших сайтів серед українців // UkrainianWatcher (http://watcher.com.ua/2015/11/12/odnoklasnyky-za-krok-do-vylotu-z-top-10-naypopulyarnishyh-saytiv-sered-ukrayintsiv/). – 2015. – 12.11).***

***

Facebook внесе зміни до політики використання реальних імен, оскільки поточна політика сервісу не задовольняє багатьох користувачів, і соцмережа отримує численні скарги на складність процесу підтвердження імен – повідомив у своєму відкритому листі віце-президент з розвитку соціальної мережі А. Шульц.

У жовтні кілька десятків громадських організацій із США та інших країн у відкритому листі закликали керівництво Facebook внести ясність у політику реальних імен. Лист було адресовано на захист інтересів людей, що змінили стать та представників ЛГБТ-руху. Адже велика їх кількість використовують псевдоніми, щоб захистити себе від насильства.

А. Шульц повідомив, що Facebook вимагає від користувачів використовувати не реальні імена, а лише ті, за якими їх знають інші люди. Найближчим часом компанія впровадить у свою політику низку змін.

Від користувачів, які звинувачують інших у використанні фейкових імен, будуть вимагати додаткові подробиці і пояснення до скарги.

Facebook також шукає нові можливості для людей, на яких скаржаться щодо використання ними фейкових імен, щоб вони могли підтвердити свою ідентичність, яка не завжди може збігатися з їх реальним іменем у житті.

Facebook уже тестує новий, більш простий, процес підтвердження імені. Тепер користувачам не потрібно буде представляти ID (документ з фото). Замість цього можна дати посилання на блоги або інші сервіси, де у них таке саме ім’ я або псевдонім ***(Facebook суттєво пом’ якшить свою політику щодо використання реальних імен в соціальній мережі // UkrainianWatcher (http://watcher.com.ua/2015/11/02/facebook-suttyevo-pomyakshyt-svoyu-polityku-schodo-vykorystannya-realnyh-imen-v-sotsialniy-merezhi/). – 2015. – 2.11).***

***

Instagram запустил новый канал, который содержит специально отобранные фото и видео пользователей, посвящённые актуальным событиям в социальной сети. По функционалу нововведение напоминает недавно запущенный новостной сервис «Моменты» в Twitter. Об этом сообщает searchengines.ru

Новый канал доступен через вкладку Explore в мобильном приложении Instagram. Первый альбом посвящён Хэллоуину. Пока видеть его могут лишь пользователи в США.

На канале представлены «лучшие видео», опубликованные в сервисе. Их отбором занимается команда редакторов. Здесь пользователи смогут просмотреть различные видеоклипы (воспроизведение будет начато автоматически), а если их заинтересует их создатель – нажать на имя пользователя и попасть прямо на страницу его профиля или на страницу понравившейся публикации.

По данным компании, в социальной сети ежедневно публикуются 80 млн фото. Количество размещаемых видеороликов не раскрывается.

Пока на новом канале пользователи видят лишь один видеоальбом. Вероятно, в будущем в нём появятся и другие, приуроченные к актуальным событиям.

Пользователи также могут подать свой пост на рассмотрение редакционной команды. Для этого нужно присвоить ему хэштег #IGHalloween.

Компания не планирует запускать на новом канале рекламу. Об этом представитель Instagram заявил редакции Wired. Возможно, это лишь вопрос времени ***(Instagram начал освещать актуальные события в сервисе через новый канал // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45163/118/lang,ru/). – 2015. – 3.11).***

***

Десять интересных фактов о главном китайском приложении WeChat

Вы могли никогда не слышать о приложении WeChat, но в настоящее время именно оно является самым главным приложением Китая. Пользователи WeChat могут делать практически все – играть в игры, пересылать деньги, совершать видеозвонки, заказывать еду, читать новости, записываться на прием к врачу, и многое другое. По сути, это китайская версия Facebook, пишет Business Insider.

По словам представителей исследовательской компании China Skinny, едва ли возможно переоценить влияние WeChat на виртуальное пространство Китая. Оно затрагивает все, начиная от общения пользователей до покупки билетов в кино и заказов такси.

Вот несколько фактов об этом необычном приложении:

1. В августе 2015 г. аудитория WeChat составила 600 млн активных пользователей, что всего на 100 млн меньше аудитории Facebook Messenger.

При этом только 70 млн от общего числа пользователей проживает за пределами Китая.

2. На китайском языке приложение называется Weixin, что переводится как «микрософобщение».

3. Многомиллиардная компания Tencent запустила WeChat четыре года назад как сервис интернет-сообщений.

4. Сегодня приложение дает гораздо больше возможностей. Миллионы людей используют его для совершения мобильных платежей, видеовызовов, игр, вызова такси, обмена геолокационными данными и для многого другого.

5. Пользователи могут сканировать QR-коды, чтобы добавлять друзей в приложение. Это очень похоже на «снапкоды», использующиеся в приложении Snapchat для добавления друзей.

6. Случайные пользователи WeChat, которые одновременно встряхнут свои смартфоны, могут связаться друг с другом. С помощью необычного сервиса Shake WeChat позволяет людям знакомиться друг с другом. Для этого достаточно включить функцию Shake и встряхнуть телефон. Если в это же время другой пользователь также потрясет телефоном, связь будет установлена.

7. Есть и другие необычные способы повстречать в WeChat новых людей. К примеру, «радар друзей» показывает пользователей WeChat, находящихся поблизости. Чтобы эта функция работала, в смартфоне должен быть активирован доступ к геолокационным данным.

8. Еще одна необычная функция называется Drift Bottle («Послание в бутылке»). Пользователь может создать короткое сообщение (это может быть небольшая аудиозапись), а затем отправить его в виртуальное «море», где его сможет подобрать другой случайный пользователь WeChat. После того, как сообщение будет просмотрено, человек, при желании, сможет ответить отправителю и начать диалог.

9. Пользователи могут оплатить коммунальные счета или записаться на прием к врачу. В августе Tencent объявила о партнерстве с компанией Shanghai Fufeitong Information Technology, специализирующейся на онлайн-платежах за коммунальные услуги. Записываясь на прием к доктору, пациенты могут просмотреть информацию о конкретном специалисте, связаться с ним и договориться о встрече, и даже встать в очередь. Также WeChat позволяет предоплатить некоторые медицинские услуги, что избавляет пациентов от лишней волокиты.

10. Знаменитости используют WeChat для общения с поклонниками. Некоторые даже делятся эксклюзивным контентом со своими самыми преданными фанатами. Этими возможностями WeChat пользуются знаменитости всего мира, включая американскую певицу С. Гомес и актера из «Теории Большого взрыва» Д. Галэки. Китайский актер Ч. Кун даже проводил эксперименты, открывая своим фанатам доступ к эксклюзивным фото и видеоматериалам ***(10 интересных фактов о главном китайском приложении WeChat // IGate (http://igate.com.ua/news/11104-10-interesnyh-faktov-o-glavnom-kitajskom-prilozhenii-wechat). – 2015. – 3.11).***

***

Twitter заменил «звездочку» у кнопки «Избранное» на «сердечко». Об этом компания сообщила в официальном блоге.

Теперь функция получила название «Мне нравится». Как сообщается в блоге, «звездочка» у «Избранного» могла смущать пользователей, особенно новичков. «Сердечко» же – символ универсальный и понятный человеку каждой культуры. Согласно тестам, сообщает компания, пользователям больше импонировало именно «сердечко». Также вместо «Избранного» у пользователя появился раздел «Понравившееся».

По сообщению Twitter, «сердечко» перекочевало в соцсеть из другого сервиса компании под названием Periscope. Теперь оно появится во всех версиях Twitter: на iOS, Android и десктопной версии. Кроме того, «сердечко» появится и еще в одном сервисе компании под названием Vine ***(В Twitter появились «сердечки» // InternetUA (http://internetua.com/v-Twitter-poyavilis--serdecski). – 2015. – 4.11).***

***

Через два после отказа от кнопки «Избранное» в Twitter, в микроблогах развернулась целая кампания, цель которой – вернуть звездочку.

Все, кто солидарен с таким решением, публикуют посты с хэштегом TwitterHeart, который вышел в топ-10 самых популярных тегов соцсети.

«Намного значимее, когда тебя добавляют в избранное, чем когда твой твит “нравится”, “Звездочка, мы тебя не забудем”, “Остановите этот ужас, верните звезду”», – такие записи оставляют пользователи Twitter, оказавшиеся на редкость консервативными.

Пока компания официально никак не отреагировала на недовольство пользователей ***(Пользователи Twitter взбунтовались против сердечка // InternetUA (http://internetua.com/polzovateli-Twitter-vzbuntovalis-protiv-serdecska). – 2015. – 5.11).***

***

Социальная сеть Facebook планирует к 2025 г. создать технологию, которая с помощью виртуальной реальности сможет полностью телепортировать человека в желаемое им место. Об этом на конференции в Дублине заявил технический директор социальной сети М. Шрепфер.

Для достижения цели компании необходимо будет сделать три ключевых шага в данном направлении. Первый шаг – полное дублирование пользователя, включая движения рук и мимики. В таком случае пользователь не будет ощущать свою проекцию в виртуальной среде фальшивкой, как это происходит в настоящее время.

Второй шаг – это точное воспроизведение окружающего пользователя пространства. В таком случае пользователь не будет ощущать себя внутри виртуальной среды. Для решения этой проблемы Oculus (которую Facebook купила за 2 млрд дол.) приобрела компанию Surreal Vision,

специализирующуюся на технологиях воспроизведения реальных объектов в виртуальном пространстве.

Третьим шагом для достижения Facebook поставленной цели является возможность пользователя самому создавать виртуальные миры. На сегодняшний день для решения этой задачи Facebook планирует поставлять с контроллерами Oculus Touch, позволяющими взаимодействовать руками с виртуальным пространством, программу Medium. С её помощью пользователь может, надев очки виртуальной реальности и контроллеры для рук, начать создавать собственные трёхмерные объекты ***(Facebook раскрыл свой план «телепортации» пользователей к 2025 году // InternetUA (http://internetua.com/Facebook-raskril-svoi-plan--teleportacii--polzovatelei-k-2025-godu). – 2015. – 5.11).***

***

Социальная сеть Facebook развивает сервис видеотрансляций при помощи знаменитостей

Facebook добавила кнопку подписки на уведомления о видеотрансляциях знаменитостей и тем самым заявила свои права на рынок мобильного сервиса Meerkat и его аналога Periscope от Twitter, которые стали невероятно популярны благодаря возможности в реальном времени передавать видео с мест событий или с закрытых мероприятий. «Газета.Ru» выяснила, как за короткое время видеотрансляции стали критически важным сегментом для крупнейших интернет-компаний.

Стриминг видео в реальном времени стратегически важен для Google и ее видеосервиса YouTube, для Facebook в свете небезуспешных попыток быстро развить свою видеоплатформу и подключить к ней Instagram, для ближайших конкурентов в лице Twitter и крупнейших мобильных мессенджеров.

Ключевое значение пользовательский видеостриминг имеет для развития виртуальной реальности, в частности для функции «телепортации», объявленной Facebook и реализуемой для Oculus Rift.

Twitter, не дожидаясь развития VR-технологий, называет «телепортацией» просто выбор любого стрима в Periscope с места событий. Google пока ограничивается внедрением функций живых видеотрансляций с разрешением 4K и технологий склейки сферического стерео-видео вместе с GoPro.

Для развития всех этих технологий важно вовлечь в процесс как можно больше пользователей, и интернет-компании активно привлекают к этому знаменитостей. Twitter активно использует эту стратегию для развития на региональных рынках. Теперь его опыт перенимает Facebook.

Periscope на фоне возросшей популярности решил расширять функционал. Новая функция под названием «Телепорт» станет доступна только обладателям iPhone 6s и iPhone 6s Plus, поскольку использует технологию 3D Touch. «Телепорт» позволяет пользователю переместиться в случайную точку мира и сразу запустить одну из трансляций прямиком из нее.

Еще одним нововведением стало расширение поля возможностей для пользователей на карте. Теперь ему будет доступно гораздо большее количество стримов по всему миру. Также на карте в течение 24 часов будут отображаться уже законченные трансляции. Это позволит, например, увидеть видеозаписи пользователей с того или иного мероприятия или срочного события.

Facebook в вопросе развития видеотрансляций пока лишь делает первые шаги. Стримы доступны только верифицированным аккаунтам знаменитостей в англоязычном сегменте. Тем не менее пользователям уже активно предлагается подписаться на популярных блогеров, чтобы всегда быть в курсе текущих трансляций. Это может дать необходимый импульс для увеличения верифицированных аккаунтов знаменитостей, известных блогеров и журналистов и привлечет к сервису внимание пользователей.

Развитие трансляций видео на смартфонах во многом повторяет расцвет видеостриминга в Интернете и связано с увеличением скорости передачи данных. Если изначально сервисы видеотрансляций развивались в сфере бизнеса и предназначались для видеоконференций и удаленного обучения, то с ростом пропускной способности интернет-каналов и развитием публичных сервисов видеотрансляции стали доступны массовым пользователям и породили, например, такие явления, как стриминг компьютерных игр и видеоблоги.

Игровой стриминг стал настолько популярен, что в итоге привел к сделке по покупке сервиса игрового стриминга Twitch компанией Amazon за 970 млн дол.

Аналогично на смартфонах, где видео долгое время рассматривалось лишь в концепции видеозвонков, живые трансляции неожиданно стали новым жанром пользовательской журналистики и приобрели критически важное значение для социальных сетей и мессенджеров.

Сервисы мобильных видеотрансляций в будущем имеют возможность найти применение в целом спектре разнообразных сфер.

Так, они более широко будут использоваться в образовании для трансляции лекций, курсов, мастер-классов и других занятий. В отличие от Skype, где есть ограничение на количество участников видеоконференции, трансляции предоставят более широкий доступ, а смартфон позволяет организовать стрим без дополнительного оборудования.

Еще одно нетривиальное применение сервису трансляции в реальном времени нашел режиссер фильмов ужасов Д. Блум. Двумя неделями ранее он запустил фильм ужасов в реальном времени в Periscope.

Основной особенностью данной затеи стала возможность подписчиков трансляции влиять на происходящее на экране. Действие фильма было настолько правдоподобно, что некоторые из зрителей всерьез обеспокоились безопасностью актеров.

Приложения для мгновенных видеотрансляций также подойдут в качестве средства для оперативной передачи информации о последних

важнейших новостях с места событий. Опять же возможность обратной связи позволит зрителям влиять на происходящее на экране ***(Facebook внедряет видеостриминг // ReklaMaster.com (http://reklamaster.com/business-and-innovations/facebook-vnedrjaet-videostriming). – 2015. – 13.11).***

***

Пользователи крупнейшей в мире соцсети Facebook стали реже размещать собственный контент, ограничиваясь комментариями к чужим заметкам, пишет interfax.ru со ссылкой на The Wall Street Journal.

Как показал опрос, в III квартале 2015 г. лишь 34 % пользователей соцсети обновляли статус и 37 % делились собственными фотографиями, по сравнению с 50 и 59 % соответственно в аналогичном квартале прошлого года.

Между тем 65 % респондентов ежедневно заходили на свою страницу в первом полугодии, однако их деятельность ограничивалась просмотром чужих страниц и раздачей отметок «мне нравится».

Проводившийся ранее опрос Pew Research Center показал, что с 2010 по 2013 г. процент пользователей, обновляющих статусы ежедневно, снизился с 14 до 10 %, а доля тех, кто делает это каждые несколько недель, упала с 61 до 47 %.

Представители компании отрицают наличие проблемы, однако в текущем году Facebook начала размещать различные напоминания, которые могут вызвать интерес и стать поводом для обсуждения: это могут быть напоминания о праздниках, играх любимой спортивной команды, выходе новых серий телесериалов или сообщения о важных событиях в стране и мире.

Такие напоминания проводятся в тестовом режиме, и пока дают «отличные результаты», сказал представитель Facebook, отказавшись сообщить подробности.

Аналитики отмечают недостаточный объем данных об активности пользователей. Публикуемый ежеквартально показатель «вовлеченности» (engagement) показывает лишь долю пользователей, ежедневно заходящих на свои страницы, однако не отражает то, чем они занимаются.

Несколько лет назад Facebook приводила более подробную статистику, но прекратила такую практику после IPO в 2012 г. Так, например, по состоянию на август 2011 г. в среднем пользователи размещали 90 «единиц контента» в месяц, включая обновления статусов, фотоальбомов и т. п.

На прошлой неделе представители компании отметили, что в 2014 г. участники соцсети разместили 50 млрд «единиц контента», взятого с других ресурсов, что соответствует примерно 3 единицам в расчете на пользователя в месяц. Сравнить эти два показателя не представляется возможным.

Как подчеркивают эксперты, пока снижение активности в плане создания пользователями собственного контента не является большой проблемой для соцсети, получающей основную выручку от показа рекламных сообщений. Однако в более долгосрочной перспективе, если такая тенденция сохранится, «Facebook может показаться суховатым и скучным», сказал аналитик

GlobalWebIndex Д. Мэндер ***(Пользователи Facebook стали реже публиковать статусы и фотографии // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45184/118/lang,ru/). – 2015. – 3.11).***

***

Технический директор Facebook М. Шрепфер полагает, что, по предварительным подсчетам, объем контента, который социальная сеть сможет поставлять в ленту новостей, будет расти на 40–50 % ежегодно. Но у людей при этом не становится больше свободного времени. Это значит, что алгоритмам компании придется тщательнее отбирать материал, который следует показывать пользователю, пишет Business Insider.

«Нам необходимы системы, которые позволят лучше понимать мир и лучше фильтровать его», – сказал М. Шрепфер на Web Summit в Дублине. Потому подразделение компании, разрабатывающее искусственный интеллект, уже долгое время работает над тем, чтобы научить Facebook воспринимать мир по-человечески. Система учится понимать язык, распознавать изображения, планировать и предсказывать.

Сейчас искусственный интеллект уже умеет выделять отдельные объекты на фотографиях и называть их. В следующем месяце компания планирует представить доклад, который покажет, как система распознает фрагменты изображения, работая на 30 % быстрее и потребляя меньше ресурсов, чем раньше.

М. Шрепфер поясняет, что это может иметь практическое значение, если пользователь захочет среди сотен своих фотографий отыскать, к примеру, все те, где запечатлено море или собака. Или, к примеру, пользователь может объяснить новостной ленте, что ему нравятся фотографии с детьми, но он терпеть не может латте-арт. Также искусственный интеллект может помочь редактировать фотографии: пользователь может приказать системе сделать черно-белым всё, что изображено на фото, за исключением объекта съемки.

Вместе с визуальными, улучшаются и речевые навыки Facebook. М. Шрепфер рассказывает, что компания разрабатывает продукт, который позволит слепым и людям с плохим зрением общаться с системой. В мире насчитывается, как минимум, 285 млн человек с ограничениями зрения и 40 млн полностью слепых людей. Разработка Facebook позволит им, к примеру, попросить искусственный интеллект голосом описать все, что изображено на той или иной фотографии.

Также команда развивает возможности системы по прогнозированию, самообучению и планированию действий.

Ассистент Facebook M становится сверхмощной системой

Все эти исследования крайне важны для улучшения ассистента Facebook M, который был запущен этим летом в рамках приложения Messenger. В настоящее время ассистент проходит ограниченный бета-тест на территории

Залива Сан-Франциско, но в перспективе разработчики планируют превратить его в некую суперсилу, способную помочь любому пользователю.

На сегодняшний день все способности М контролируют люди. Тем не менее, им помогает искусственный интеллект, который оттачивает свои навыки на пользователях, участвующих в бета-тесте. Для человека это очевидно, но искусственный интеллект должен учиться задавать верные вопросы в зависимости от контекста. К примеру, если пользователь сообщает, что хочет заказать цветы, логично будет спросить «Каков ваш бюджет?» и «Куда следует их отправить?». Искусственный интеллект учится всему этому, наблюдая за работой живых операторов, приводящих в действие ассистента.

«На данный момент часть ответов уже дает сам искусственный интеллект. Мы планируем увеличивать степень его участия постепенно, чтобы дать ему возможность обучаться, – говорит М. Шрепфер. – Самое захватывающее в этой системе – то, что ее можно масштабировать. Мы не можем позволить себе нанять живых операторов для обслуживания всего мира. Но с правильно обученным искусственным интеллектом мы сможем каждому пользователю планеты предоставить персонального ассистента, который поможет управлять онлайн-средой. М станет сверхмощной системой, которая охватит весь мир».

М. Шрепфер утверждает, что за последний год команда разработки достигла больших успехов, но со временем прогресс лишь ускорится. «Я дал обещание всем специалистам по искусственному интеллекту, присоединившимся к разработке. Наш проект позволит максимально быстро продемонстрировать результаты работы миллиарду человек», – говорит М. Шрепфер ***(Facebook собирается создать идеальную новостную ленту и ассистента // IGate (http://igate.com.ua/news/11131-facebook-sobiraetsya-sozdat-idealnuyu-novostnuyu-lentu-i-assistenta). – 2015. – 4.11).***

***

В III квартале количество аккаунтов в соцсети Facebook возросло на 60 млн. По состоянию на 30 октября в мире насчитывается более 1,55 млрд пользователей этой соцсети, передает телекомпания BBC со ссылкой на сообщение компании. Это показатель измеряется ежемесячно.

На пребывание в Facebook и Instagram приходится 20 % всего времени, которое американцы тратят на Интернет, утверждают в администрации соцсети. За сентябрь число мобильных пользователей, которые обращаются к соцсети ежедневно, возросло на 27 % и составило 894 млн человек.

«В среднесрочной и долгосрочной перспективе, мы считаем, что Facebook и Instagram не конкуренты между собой. Мы станем конкурировать с другими видами средств массовой информации», – заявила главный операционный директор компании Ш. Сандберг. Ее слова приводит Reuters.

Facebook зарегистрировала 8 млрд просмотров видео в день с аудиторией около 500 млн человек ***(Число пользователей Facebook превысило полтора***

миллиарда // InternetUA (http://internetua.com/cislo-polzovatelei-Facebook-previsilo-poltora-milliarda). – 2015. – 5.11).

***

Социальная сеть Facebook запустила инструмент, который помогает пользователям делиться 30-секундными клипами с Apple Music и Spotify в своей новостной ленте. Пока функция Music Stories доступна для iOS приложений, но вскоре появится на ПК и для Android приложений. Клипы, размещенные в ленте, будут содержать ссылку на платформы и позволят пользователям проиграть всю песню на Apple Music или купить ее в iTunes, а песни со Spotify добавить в свою библиотеку, не покидая соцсеть. Тем временем, компания отметила, что думает над тем, как проигрывать весь трек ***(Facebook запустил музыкальный сервис Music Stories // Marketing Media Review (http://mmr.ua/show/facebook_zapustil_muzykalnyy_servis_music_stories). – 2015. – 6.11).***

***

Skype запустив кнопку, яка є аналогом фейсбуківської кнопки «лайк» і дає можливість ділитися контентом веб-сайтів зі своїми друзями в месенджері.

Кнопка вже інтегрована на сайтах MSN.com та Sify.com. Але розробники інших сайтів можуть додати її собі, при цьому обравши один із чотирьох наявних варіантів дизайну.

Коли користувач натисне на кнопку Skype на сайті, йому необхідно буде авторизуватись у веб-версії месенджера (ввести логін і пароль). Далі можна поділитися посиланням зі своїми друзями ***(Skype запустив свій аналог кнопки «лайк» // UkrainianWatcher (http://watcher.com.ua/2015/11/06/skype-zapustyv-sviy-analoh-knopky-layk/). – 2015. – 6.11).***

***

Крупнейшая в мире соцсеть Facebook продолжает внедрять функции, способные вызвать неоднозначную реакцию у озабоченных своей приватностью пользователей. Мессенджер Facebook научился находить друзей пользователя по соцсети в фотографиях, недавно сделанных на смартфон.

Новая функция называется Photo Magic. Она пропускает все сделанные на смартфон фотографии через алгоритм распознавания лиц. Если приложение обнаруживает на снимках кого-то похожего на ваших друзей из Facebook, оно предлагает отправить им этот снимок. Photo Magic пока доступна пользователям Android-версии Facebook Messenger в Австралии, позже добавят и поддержку iOS, а в ближайшем будущем функция доберется до США.

По словам представителей Facebook, реализовать мониторинг фотоснимков на смартфонах пользователей компанию подтолкнула популярность обмена фотографиями в Messenger. Так, только за последний месяц через чат-приложений соцсети было отправлено 9,5 млрд снимков.

Немаловажно, что именно обмен фотографиями – главная функция одного из более молодых конкурентов Facebook, мессенджера Snapchat.

При желании Photo Magic можно отключить с помощью той же настройки приватности, которая отключает предложения отметить друзей на закачиваемых в соцсеть фотографиях ***(Facebook хочет искать друзей в фотографиях на смартфоне // InternetUA (http://internetua.com/Facebook-hocset-iskat-druzei-v-fotografiyah-na-smartfone). – 2015. – 12.11).***

***

Соцсеть «ВКонтакте» запустила раздел «Актуальные темы», в котором выводится топ самых популярных на сайте хештегов. Об этом говорится в сообщении компании, поступившем в редакцию «Ленты.ру».

Самые обсуждаемые хештеги можно найти в меню «Мои Новости» во вкладке «Поиск». Они позволяют оценить самые популярные на сайте темы записей пользователей и сообществ. На момент написания материала в трендах оказались, в частности, #fallout4, #rutracker, #павленский, #янешарли, #туман.

Пока что рейтинг доступен только для жителей России, в ближайшее время функция запустят и для остальных стран присутствия соцсети. Как уточнил «Ленте.ру» пресс-секретарь «ВКонтакте» Г. Лобушкин, на данном этапе будет представлен только один общий топ. В будущем не исключено появление отдельного рейтинга для каждой страны, как это реализовано, например, в Twitter. Представитель «ВКонтакте» добавил, что раздел «Актуальные темы» станет доступен и для мобильных приложений соцсети в ближайших обновлениях.

В компании также ожидают, что новая функция будет полезна СМИ: она позволит отследить события, которые волнуют пользователей, и показать «настроения всего общества», отметил Г. Лобушкин ***(Во «ВКонтакте» появился топ популярных хештегов // InternetUA (http://internetua.com/vo--vkontakte--poyavilsya-top-populyarnih-heshtegov). – 2015. – 11.11).***

***

Facebook выпустила ранее анонсированное приложение Notify, позволяющее получать push-уведомления от более чем 70 медиапартнеров компании, включая CNN, The Weather Channel, Bloomberg, Comedy Central, Vevo и Vox Media. Сервис доступен на iOS для пользователей США.

Пользователь может выбрать одну или несколько категорий, которые ему наиболее интересны: спорт, знаменитости, новости, фильмы, музыка или шопинг. Помимо тем, в приложении есть ряд «каналов», например: «Последние новости от CNN и самые популярные публикации от Fox News», «Ежедневный дайджест знаменитостей с лучшими нарядами от Vogue», «Счет последних спортивных матчей от FOX Sports», «Новые трейлеры ожидаемых фильмов от Fandango».

Сообщения будут своевременно появляться на экране смартфона в течение дня. Чтобы увидеть более подробную информацию о новости, нужно

провести по экрану или нажать на уведомление, после чего пользователь сможет прочесть полный текст в браузере приложения.

Пользователь может делиться уведомлениями с друзьями через соцсети, email или текстовые сообщения, не покидая экран блокировки. Если человек занят, он может сохранить новость и прочесть ее позже. С помощью ленты приложения можно посмотреть все последние уведомления за 24 часа.

По словам менеджера по продукту Facebook, уведомления «становятся одним из основных способов, с помощью которых люди узнают обо всем на свете». Поэтому компания решила в «одном месте» информировать пользователей о новостях, важных для них ***(Facebook запустила новостное приложение Notify // IGate (http://igate.com.ua/lenta/11310-facebook-zapustila-novostnoe-prilozhenie-notify). – 2015. – 12.11).***

***

Согласно данным, опубликованным аналитической компанией eMarketer, к концу 2015 г. в мире мессенджерами на мобильных устройствах будут пользоваться 1,4 млрд человек, что на 31,6 % больше, чем годом ранее. Статистика также указывает на то, что к началу 2016 г. 75 % всех пользователей смартфонов будет общаться при помощи сервисов мгновенного обмена сообщениями, пишет Hyser (http://hyser.com.ua/tehnology/mobilnye-messendzhery-nabirayut-nebyvalyx-oborotov-38098).

По прогнозам экспертов eMarketer, положительная динамика роста популярности мессенджеров будет сохраняться на протяжении ближайших нескольких лет, и это, в свою очередь, приведёт к тому, что к 2018 г. их пользовательская база достигнет 2 млрд человек и составит 80 % всех владельцев смартфонов. Отметим, что наиболее востребованными мессенджерами в настоящее время являются WhatsApp, Facebook Messenger, WeChat, Line и Snapchat.

Как подчёркивает старший аналитик eMarketer К. Бойл, основным катализатором роста аудитории подобных сервисов стало появление разнообразных режимов общения и полезных возможностей вроде пиринговых платежей и электронной коммерции. При этом многие сервисы по-прежнему продолжают уделять основное внимание наращиванию аудитории, отодвигая монетизацию на второй план ***(Мобильные мессенджеры набирают небывалых оборотов популярности // Hyser (http://hyser.com.ua/tehnology/mobilnye-messendzhery-nabirayut-nebyvalyx-oborotov-38098). – 2015. – 13.11).***

***

Twitter представил новую функцию ScratchReel, которая позволяет движением мышки или касанием пальца двигать GIF-анимацию при проигрывании вперёд и назад для получения забавных эффектов.

По функционалу ScratchReel напоминает так называемый «скретчинг» – движения диджея рукой по виниловой пластинке.

Поиграть с новой возможностью можно в твите. Нововведение призвано сделать контент в Twitter более вовлекающим.

Напомним, что поддержка анимированных GIF-изображений в Twitter появилась летом 2014 г. ***(В Twitter теперь можно поиграть с GIF-анимацией как диджей // Состав.ua (http://sostav.ua/publication/v-twitter-teper-mozhno-poigrat-s-gif-animatsiej-kak-didzhej-69142.html). – 2015. – 13.11).***

***

Некоторые пользователи чат-приложения Facebook Messenger во Франции обнаружили в программе новую функцию – автоматического уничтожения переписки. Очевидно, соцсеть проводит ограниченное локальное тестирование нововведения, пишут «Экономические известия» (http://news.eizvestia.com/news_technology/full/263-facebook-testiruet-samounichtozhayushhuyusya-perepisku).

Реализация функции напоминает выпущенное Facebook в прошлом году приложение Slingshot. Slingshot позволяет снимать фото или видеоролики продолжительностью до 15 секунд, после чего накладывать на них текст, значки-эмодзи или рисовать «кистью» выбранного диаметра, а также накладывать ненавязчивую музыку и звуковые эффекты. Любопытно, что по умолчанию активируется не основная, а фронтальная камера устройства. Полученные видео и фото после просмотра исчезают.

Разумеется, новой функции не удастся избежать сравнения и с пионером жанра самоуничтожающихся посланий, мессенджером Snapchat ***(Facebook тестирует самоуничтожающуюся переписку // Экономические известия (http://news.eizvestia.com/news_technology/full/263-facebook-testiruet-samounichtozhayushhuyusya-perepisku). – 2015. – 13.11).***

***

На Pinterest появился визуальный поисковик: объекты на фото теперь можно идентифицировать

Часто бывает, что просматривая фотографию квартиры или дома, пользователю Pinterest нравится какая-либо этажерка, люстра или гаджет. Но что это и где можно купить, знают лишь люди, хорошо знакомые с современными тенденциями дизайна интерьера. Что делать остальным? Воспользоваться визуальным поисковиком сервиса, разработчики его добавили для удобства пользователей.

И действительно, все сделано довольно удобно – если выделить отдельный объект и задать поиск, то сервис покажет фотографии и описание схожих объектов. Ту же самую лампу можно выделить на фотографии, получив целый список схожих товаров.

Ссылка на визуальный поисковик размещается в углу. Можно и уточнить условия поиска, если результаты оказались слишком уж многочисленными. Фильтровать выдачу можно, например, по тегам и категориям. В этом случае

при поиске лампочки не будет высвечивать иные категории, объекты из которых могут оказаться чем-то схожими с объектом поиска.

Та же самая люстра может быть надена в категории «антиквариат» или «современный дизайн». Конечно, поиск ведется не по сети, а по базе Pinterest, но база сервиса сейчас огромна.

Визуальный поисковый сервис будет доступен для пользователей Pinterest, включая мобильное приложение и веб ***(На Pinterest появился визуальный поисковик: объекты на фото теперь можно идентифицировать // Age Of Comp (http://ageofcomp.info/wounde/42352-na-pinterest-poyavilsya-vizualnyj-poiskovik-obekty-na-foto-teper-mozhno-identificirovat.html). – 2015. – 10.11).***

***

Многие пользователи Tumblr согласятся с тем, что все это время сервису отчаянно недоставало встроенного мессенджера, который бы позволял единомышленникам в отрыве от публикации постов вести друг с другом переписку в режиме реального времени.

В итоге разработчики вняли просьбам блогеров и сообщили о запуске в Tumblr службы мгновенного обмена сообщениями, которая появилась в веб-версии, а также в сопутствующих приложениях для iOS и Android. Правда, пока только в тестовом режиме. Это означает, что в настоящее время новая функция доступна не всем, а лишь избранным счастливчикам. Они в свою очередь могут легко осчастливить других людей, просто отправив им личное сообщение при помощи мессенджера. Пользователям, получившим подобное сообщение, автоматически откроется доступ к новой возможности.

По заверениям разработчиков, встроенный мессенджер Tumblr выйдет из стадии тестирования и станет доступен всей пользовательской базе сервиса ориентировочно в декабре. В настоящее время его функциональность ограничивается обменом текстовыми сообщениями между двумя собеседниками, однако в будущем непременно появится поддержка GIF, изображений и групповых чатов ***(Сервис микроблогов Tumblr запустил собственный мессенджер // iGate (http://igate.com.ua/lenta/11361-servis-mikroblogov-tumblr-zapustil-sobstvennyj-messendzher). – 2015. – 14.11).***

***

Как развивается украинский YouTube

YouTube запустился в Украине почти три года назад. С тех пор отечественный сегмент сервиса сильно возрос по активности как аудитории, так и создателей контента. Оказывается, из всех европейских стран именно зрители из Украины проводят больше всего времени на YouTube. И между прочим, сразу два украинских канала вошли в топ-100 YouTube-каналов мира! Такие данные обнародовали на конференции «Цифровое преображение Украины» представители видеосервиса, пишет AIN (http://ain.ua/2015/11/12/615162).

Украинский сегмент YouTube на карте Европы и мира

По словам менеджера по развитию YouTube в Украине и странах СНГ А. Градиль, команда YouTube оценивает успех партнеров на платформе не только по количеству просмотров их роликов, но и по времени, которое пользователи проводят на их каналах. Данная метрика точнее показывает заинтересованность и лояльность зрителя к контенту.

Украина из года в год входит в топ-10 стран Европы по количеству часов на YouTube. Если сравнить Украину с более крупными рынками, такими как Россия, Польша, Германия, то наши зрители смотрят онлайн-видео (как на YouTube, так и на других площадках) больше и чаще. Порядка 40 % украинских онлайн-пользователей смотрят видео в Интернете каждый день.

YouTube пользуется огромной популярностью среди молодой аудитории. Но не все знают, что люди в категории 25–34 года сегодня проводят на платформе столько же времени, сколько и аудитория в возрасте 13–24 года. Для рекламодателя это возможность получить огромный охват аудитории как среди школьников и студентов, так и среди молодых профессионалов и семей.

90 % видео, которое смотрят украинцы, это развлекательный и образовательный контент. Если сравнивать Украину с другими странами, то мы чаще смотрим онлайн-видео, чтобы узнать что-то новое и оставаться в курсе событий. Очень приятно, что украинцы постоянно занимаются своим развитием.

Если говорить о глобальной статистике, то в списке топ-100 каналов YouTube есть два канала из Украины. Это каналы, которые стали популярны не только на нашем рынке, но и в целом в русскоязычном сегменте YouTube.

Также примечательно, что украинцы больше, чем другие нации, полагаются на онлайн-ресурсы, когда нужно узнать о продукте и принять решение о покупке. Соответственно неудивительно, что в украинском сегменте YouTube очень много контента посвящено техническим обзорам, распаковкам продуктов и товаров.

Видеоблогеры в Украине

Об успехах украинских видеоблогеров рассказала В. Сливинская, руководитель отдела продаж и маркетинга крупнейшей в Украине мультиканальной сети Agency of Internet Rights (AIR). В мире сеть AIR – на 17 месте, что также довольно неплохой результат.

Украинский AIR является сертифицированным партнером YouTube и занимается технической поддержкой, развитием и монетизацией YouTube-каналов. К сети подключено более 16 тыс. каналов, преимущественно из Украины и России, но есть блогеры и из других стран мира. Ежемесячно в Украине каналы сети собирают 220 млн просмотров и 1,5 млн просмотров во всем мире.

Более 7 тыс. блогеров из Украины подключены к AIR. «Это творческие личности, которым есть что сказать миру. Как правило, все начинается с хобби, которым люди делятся со своими друзьями, знакомыми, а потом и со всеми остальными. Со временем это становится постоянной, почти профессиональной

деятельностью. В результате, для многих видеоблогеров их канал превращается в основной источник дохода», – рассказала В. Сливинская.

Статистика по YouTube-каналам AIR

Аудитория украинских блогеров в гендерном смысле непропорциональная – здесь сильно больше мужчин. Зрители находятся в самых разных странах. Преимущественно в России (45 %). На Украину приходится 15 % зрителей. Интересно, что достаточно активно видео смотрят люди из США и Германии.

Что смотрят украинцы? Да то же самое, что и во всем мире. В первую очередь они приходят на YouTube за развлекательным контентом. Самая большая категория – детский контент. Также довольно популярны видео юмористического характера, компьютерные игры, обзоры технологий и гаджетов, а также общественно-политические программы на таких YouTube-каналах, как «Громадське» и Espresso.TV ***(Как развивается украинский YouTube: актуальная статистика и топ-15 отечественных видеоблогеров // AIN (http://ain.ua/2015/11/12/615162). – 2015. – 12.11).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Експерти Моніторингу якості надання послуг органами влади показали рейтинг офіційних сторінок українських державних установ у Facebook.

Рейтинг склали за кількістю лайків станом на 11 листопада 2015 р. Усього в рейтингу 33 відомства.

Перші три місця зайняли силові відомства – Міністерство оборони (майже 152 тис. лайків) і МВС (близько 34 тис. лайків), а також Генеральна прокуратура (близько 33 тис. лайків). А непопулярні серед українців сторінки Верховного Суду України (66 лайків), Національної поліції (556 лайків) і ВССУ з розгляду цивільних і кримінальних справ (799 лайків).

Рейтингові показники за кількістю уподобань офіціних сторінок державних установ України у мережі Facebook станом на 11.11.2015 р.

Назви установ	рейтинг	Кількість уподобань «лайків»
Міністерство оборони України	1	151994
МВС України	2	34243

Генеральна прокуратура України	3	33325
РНБО України. Оперативний штаб.	4	32500
Міністерство освіти і науки України	5	32439
Урядовий портал	6	28794
Адміністрація Президента України	7	28496
Міністерство фінансів України	8	25263
Міністерство соціальної політики України	9	23805
Міністерство закордонних справ України	10	22070
Міністерство економічного розвитку і торгівлі України	11	20724
Міністерство охорони здоров' я України	12	17216
Національна гвардія України	13	16241
Служба безпеки України	14	14832
Міністерство аграрної політики та продовольства України	15	11599
Міністерство інфраструктури України	16	8535
Державна прикордонна служба України	17	7943
Міністерство культури України	18	7859
Державна фіскальна служба України	19	7756
Верховна Рада України	20	7138
НАБУ	21	3816
Вищий адміністративний суд України	22	2549
Державна служба зайнятості	23	1867
ВГСУ Вищий господарський суд України	24	1829
Міністерство інформаційної політики України	25	1762
Антимонопольний комітет України	26	1481
Держслужба України з питань геодезії, картографії та кадастру	27	1226
Державна пенітенціарна служба України	28	1214
Держслужба спеціального зв' язку та захисту інформації України	29	1096
Вища рада юстиції	30	895
ВССУ з розгляду цивільних і кримінальних справ	31	799
Національна поліція України	32	556
Верховний Суд України «ВСУ»	33	66

(Яке міністерство найпопулярніше у Facebook // Телеканал новин «24» (http://24tv.ua/yake_ministerstvo_naypopulyarnishe_u_facebook_infografika_n630400). – 2015. – 13.11).

***

Министерство культуры Украины занялось своим онлайн-имиджем – представлена новая страница в социальной сети Facebook. Пользователей приглашают следить за обновлениями, участвовать в дискуссиях, задавать вопросы, отправлять жалобы и пожелания.

Репутация у специалистов, которые продвигают Минкульт в уанете, подпорчена скандалом с Twitter-аккаунтом, который случился в июле этого года. Тогда история обошла не только блогосферу, но и ряд украинских интернет-СМИ и даже попала на телеканалы ***(В украинском Минкульте***

вспомнили о Facebook – и завели официальную страницу // Блог Imena.UA (http://www.imena.ua/blog/minculturefacebook/). – 2015. – 10.11).

***

На сайті соцмережі Facebook розпочався флешмоб із закликом обладнати місця громадського користування в столиці і зробити їх доступними для людей з обмеженою мобільністю.

«В столиці проживає більше 150 тис. людей з інвалідністю, але ми не часто зустрічаємо їх на вулицях нашого міста, адже через недоступність місць громадського користування такі люди воліють не виходити з дому», – пишуть організатори.

До поняття «люди з обмеженою мобільністю» відносять не лише людей з особливими потребами – з проблемою пересування зіштовхуються мами з маленькими дітьми на візках, люди похилого віку та люди на інвалідних візках, у тому числі й ті, хто тимчасово має проблеми зі здоров'ям.

За умовами флешмобу потрібно сфотографувати місця, які не є доступними для людей на візках та людей похилого віку, викласти у своїй сторінці на Facebook та опублікувати разом з повідомленням для мера В. Кличка.

Ініціатором та організатором флешмобу є громадська організація «Підмога.інфо», яка вже не вперше звертає увагу громадськості на наявність проблеми в пересуванні людей з обмеженою мобільністю вулицями міста. Раніше організація вже проводила акцію «Один день із життя людини у візку», у якій взяли участь відомі киянки І. Карпа та С. Вітвіцька.

Громадська організація «Підмога.інфо» надає інформаційну та адвокаційну допомогу учасникам АТО і мирним громадянам, що постраждали внаслідок бойових дій на території України. Головною метою діяльності організації є захист прав людей, що потребують протезування. Акція «Один день із життя людини у візку» відбувається в рамках проекту «Безбар' єрний Київ», який організація почнереалізовувати у 2016 р. Фінансова підтримка проекту надається МБФ «Відродження» ***(У Facebook розпочався флешмоб на підтримку людей з обмеженою мобільністю // MediaSapiens (http://osvita.mediasapiens.ua/web/social/u_facebook_rozpochavsya_fleshmob_na_pidtrimku_lyudey_z_obmezhenoyu_mobilnistyu/). – 2015. – 10.11).***

***

В понедельник, 9 ноября, социальная сеть «ВКонтакте» объявила об образовательном проекте ко Дню украинского языка и письменности, созданном совместно с украинской Википедией, пишет «Обозреватель» (http://tech.obozrevatel.com/hi-tech/62947-vkontakte-obuchit-polzovatelej-ukrainskomu-yazyiku.htm**).**

В соцсете появилось сообщество «Вікіпедія про мову» с правилами и историей украинского языка, распространёнными ошибками и редкими словами. Специальная страница доступна по ссылке: vk.com/mova.

«Украинский язык – один из самых распространённых в мире. Более 11 миллионов пользователей “ВКонтакте” выбрали именно украиноязычный интерфейс сайта. Изучать украинский, говорить правильно – это лучший способ поддержать родной язык, сделать вклад в распространение грамотности. Мы позаботились, чтобы спецпроект стал удобной возможностью узнать что-то новое и полезное в привычном для интернет-пользователей формате публичной страницы в социальной сети», – сообщил пресс-секретарь «ВКонтакте» в Украине В. Леготкин.

День украинской письменности и языка отмечается 9 ноября, в день памяти Преподобного Нестора-Летописца, автора и составителя летописи «Повесть временных лет». В Украине этот праздник официально отмечается с 1997 г. и сопровождается различными мероприятиями в поддержку украинского языка ***(«ВКонтакте» обучит пользователей соцсети украинскому языку // Обозреватель (http://tech.obozrevatel.com/hi-tech/62947-vkontakte-obuchit-polzovatelej-ukrainskomu-yazyiku.htm). – 2015. – 9.11).***

***

Органы Пенсионного фонда Украины в Киеве модернизируют свою работу, активно используя ресурсы современных средств связи.

В частности, введены дистанционные формы обслуживания граждан: функционируют телефонные «горячие линии», предоставляются услуги консультирования через сеть Facebook и веб-портал Пенсионного фонда Украины, сообщается на сайте КМДА.

В частности, с сентября в органах Пенсионного фонда Украины в г. Киев заработала Skype-связь, которая предоставляет возможность гражданам пообщаться одновременно с несколькими специалистами и оперативно получить ответы на поставленные вопросы. Воспользовавшись помощью детей или внуков, сегодня пенсионеры, не выходя из дома, могут в удобный способ получить консультацию специалиста в режиме онлайн. Каждый киевлянин имеет возможность получить разъяснения по вопросам пенсионного обеспечения как непосредственно в органах фонда, так и дистанционно.

Продолжая реформирование пенсионной системы, с 2016 г. будет внедряться современная, единая, централизованная система назначения и выплаты пенсий, которая позволит быстро обслуживать людей с назначением и перерасчета пенсий ***(Пенсионеров в Киеве будут обслуживать через Skype // InternetUA (http://internetua.com/pensionerov-v-kieve-budut-obslujivat-cserez-Skype). – 2015. – 11.11).***

***

Компанія Ericsson має намір запровадити новітні технології для координації екстренних служб Львівщини. Про це йшлося під час зустрічі голови Львівської обласної державної адміністрації О. Синютки з делегацією компанії Ericsson (Королівство Швеція). За задумом шведів, поліцію,

пожежників та інші служби можна буде викликати за допомогою тегів у Twitter та Facebook, а також за допомогою вмонтованої в автомобілі системи ECall.

За допомогою нового програмно-апаратного комплексу і телекомунікаційних мереж «Система 112» повинна приймати та обробляти екстрені виклики, забезпечити передачу інформації відповідним оперативно-диспетчерським службам, які доводитимуть її до підпорядкованих підрозділів екстреної допомоги населенню.

Крім того, сторони обговорили можливості залучення фінансової допомоги від Шведського агентства міжнародного розвитку (SIDA) для реалізації цього проекту.

«Досвід показує, що повинен бути єдиний контактний центр, який координуватиме діяльність усіх екстренних служб, зокрема поліції швидкої, МНС тощо. Це буде єдина база для контролю звернень громадян, – розповів керівник ІТК проектів компанії Ericsson Ukraine І. Срібродольський. – Проект передбачає залучення новітніх технологій для швидкого реагування у випадку надзвичайних ситуації, аварії тощо. Це досягнення, які активно використовують мешканці Швеції та інших розвинених країн».

«Для нас є важливим, щоб знакові компанії приходили на Львівщину та щоб вони почували себе тут комфортно. Ми зацікавлені у реалізації цього проекту», – резюмував О. Синютка. За підсумками зустрічі, керівник області доручив підготувати всі документи, які необхідні для реалізації даного проекту ***(На Львівщині служба «112» зможе приймати виклики через Twitter та Facebook // Львівська газета (http://gazeta.lviv.ua/news/2015/11/10/50117). – 2015. – 10.11).***

***

Голова Одеської обласної державної адміністрації М. Саакашвілі повідомив на своїй сторінці у Facebook, що вже має 700 тис. читачів, передає УНН.

«Коли я перестав бути президентом Грузії, у мене було 200 тис. передплатників на Facebook, а сьогодні їх вже більше 700 тисяч. Ті півмільйона, яким за цей час сподобалася моя сторінка, це ті люди, які бачили, як я і моя команда боремося за чесні та прозорі послуги і реформи для населення України. Як це було з Державіаслужбою, чи представниками прокуратури (кожне з цих відео зібрало по 2 мільйони переглядів)», – повідомив М. Саакашвілі.

Також М. Саакашвілі наголосив, що довіра людей – показник того, наскільки правильні ті речі, які робить політик.

«Незважаючи на опір місцевих кримінальних та корупційних еліт, проплачений негатив в соціальних мережах і відкриту війну в ЗМІ, що належать олігархам, я завжди буду захищати інтереси людей», – пообіцяв М. Саакашвілі ***(Сторінка М. Сакашвілі в Facebook має вже 700 тис. читачів // Українські національні новини (http://www.unn.com.ua/uk/news/1520042-***

***storinka-m-sakashvili-v-facebook-vzhe-maye-700-tis-pidpischikiv*). – 2015. – 13.11).**

***

Российская социальная сеть «ВКонтакте» открыла собственный университет для обучения азам и секретам программирования. Проект ориентирован в первую очередь на старшеклассников и студентов.

«Мы верим в то, что большинство потрясающих талантов пока еще не раскрыты и хотим дать им возможность раскрыться. Для этого мы организуем VK University – место, где люди, интересующиеся современными технологиями, могли бы получать новые знания и общаться с единомышленниками», – говорится в сообщении администрации соцсети.

Глава пресс-службы «ВКонтакте» Г. Лобушкин не скрывает, что одна из главных задач работы университета – поиск молодых талантов. Так, на странице учебного заведения VK University планируется проводить офлайн и онлайн курсы для начинающих разработчиков. «В ближайшее время в сообществе в рамках образовательного курса будет объявлен конкурс на разработку мобильных приложений», – пишет он.

Участие в образовательных программах обещают сделать бесплатным.

В ближайших планах университета – открыть запись на курс, посвящённый созданию приложений для iOS. В него входит программирование на языках Swift и C++, обучение дизайну и UX, архитектуре приложений и использованию в них API «ВКонтакте».

Подача заявок будет происходить через личные сообщения в сообществе VK University. Из требований к участникам «ВКонтакте» предъявляет только наличие базовых навыков разработки под iOS. Курс начнется 21 ноября, подробный анонс расписания с инструкциями по участию в отборе компания обещает выпустить уже 15 ноября.

В дальнейшем компания собирается открыть аналогичный курс для разработчиков на Android, а также преподавать другие языки программирования, системное администрирование и информатику в целом. Заниматься можно будет параллельно по нескольким направлениям сразу, однако число участников каждого курса будет ограничено – не больше 50 человек.

«Живые» занятия будут проходить в петербургском офисе «ВКонтакте» раз в неделю по два часа, первые курсы будут длиться около трёх месяцев. Преподавать программирование для iOS будут разработчики официальных клиентов «ВКонтакте» и Snapster ***(«ВКонтакте» открыл собственный университет // FaceNews (http://www.facenews.ua/news/2015/297036/). – 2015. – 11.11).***

***

Президент США Б. Обама зарегистрировал аккаунт в социальной сети Facebook.

«Привет, Facebook! Я наконец-то заполучил свою собственную страничку. Я надеюсь, вы будете считать это местом, где мы можем проводить реальные разговоры о самых важных вопросах, стоящих перед нашей страной», – написал глава государства и призвал оставлять комментарии, делиться друг с другом темами с его страницы.

В своем сообщении Б. Обама заявил о необходимости «сохранить планету для детей и внуков». Для этого, по его словам, нужно решить проблему изменения климата. Данную тему с лидерами других стран президент США обсудит на 21-й Конференции ООН по вопросам изменения климата (COP21), которая пройдет с 30 ноября по 11 декабря в Париже. Под сообщением опубликовано видео, где Б. Обама гуляет по лужайке Белого дома.

На сайте администрации президента говорится, что его страница в Facebook станет новым способом прямого онлайн-общения с американцами и что все сообщения будут исходить исключительного от него самого. «Президент Обама намерен сделать свою администрацию самой открытой для общения, и его аккаунт даст возможность американцам обсуждать с ним наиболее важные для них вопросы», – отмечается в сообщении.

В выходных данных Б. Обама написал о себе: «Отец, муж и 44-й президент США». Его страница «понравилась» уже более 100 тыс. человек.

Ранее Б. Обама пользовался Twitter и официальным микроблогом Белого дома. В мае он установил мировой рекорд, получив за 5 часов после создания профиля один миллион подписчиков в личном Twitter-аккаунте @POTUS ***(Обама зарегистрировал аккаунт в Facebook // InternetUA (http://internetua.com/obama-zaregistriroval-akkaunt-v-Facebook). – 2015. – 10.11).***

***

Після терактів у Парижі модератори соціальної мережі Facebook додали корисну кнопку на випадки нападу бойовиків. Відтепер користувач зможе попередити своїх друзів про перебування в небезпечній зоні.

Таким чином користувачі, які перебувають у столиці Франції та біля неї, можуть розповісти усім, чи на безпечній території вони перебувають та побачити, хто з друзів у біді.

«Отримайте потрібну інформацію і зв’ яжіться з друзями в зоні лиха. Повідомте, в безпеці вони, якщо ви про це знаєте», – заява Facebook ***(Facebook запускає антитерористичну функцію // Znaj.ua (http://znaj.ua/news/science-and-technic/28700/facebook-zapuskaye-antiteroristichnu-funkciyu.html). – 2015. – 14.11).***

Instagram объявил, что в ближайшие недели рекламодатели смогут покупать рекламу формата «карусель» на базе модели самообслуживания – через Ads API, Power Editor и Ads Manager. Об этом пишет searchengines.ru

Кроме того, в течение последнего месяца компания работала над запуском новых способов ведения рекламных кампаний в рамках платформы. Теперь кампании могут быть настроены таким образом, чтобы презентовать бренд большему числу пользователей. Или же, чтобы доставить рекламу людям, которые наиболее склонны перейти по ссылке и купить товар. При этом одни и те же настройки могут быть использованы как для управления кампаниями в Instagram, так и в Facebook.

Напомним, что Instagram запустил рекламные объявления формата «карусель» в марте этого года ***(Instagram будет продавать рекламу формата «карусель» через систему самообслуживания // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45158/118/lang,ru/). – 2015. – 2.11).***

***

Pinterest запустил пины с кнопкой «купить» для владельцев Android девайсов. В июне такая возможность была представлена для iOS. У Pinterest уже 60 млн пинов с возможностью покупки, которые позволяют приобрести товары непосредственно у ритейлеров, таких как Nordstrom, Bloomingdale' s, Macy' s и Neiman Marcus. Компания также объявила о запуске Pinterest Shop – раздела с трендовыми коллекциями из пинов, отобранных Pinterest. Все представленные в нем товары разнесены по отдельным категориям ***(Pinterest запустил пины с кнопкой «купить» для владельцев Android девайсов // Marketing Media Review (http://mmr.ua/show/pinterest_zapustil_piny_s_knopkoy_kupity_dlya_vladelytsev_android_devaysov). – 2015. – 4.11).***

***

На чем зарабатывает Facebook

Корпорация Facebook отчиталась за III квартал 2015 г. и сообщила о рекордных финансовых показателях и росте аудитории. Крупнейшая социальная сеть остается высокодоходной, несмотря на свои масштабные неприбыльные проекты, такие, как разработки в области виртуальной реальности, подключение к Интернету населения развивающихся стран и запуск в космос спутников для обеспечения доступа в глобальную сеть в труднодоступных районах планеты.

В отчете инвесторам социальная сеть сообщила о выручке за III квартал 2015 г. в размере 4,5 млрд дол. по сравнению с 3,2 млрд дол. за этот же период годом ранее, сообщает Reuters. Это выше предсказаний аналитиков, которые оценивали этот показатель в 4,37 млрд дол.

Большую часть выручки Facebook составили рекламные доходы, которые увеличились на 45,4 % и составили 4,3 млрд дол., при этом 78 % из них получено с мобильного сегмента (в аналогичном квартале прошлого года этот показатель составлял 66 %). Это воодушевило инвесторов, и стоимость акций компании поднялась сразу на 5 % и достигла исторического максимума. Капитализация компании превысила 300 млрд дол.

Однако расходы Facebook увеличились на 68 % по сравнению с прошлым годом и составили 3 млрд дол. Тем не менее это не сильно волнует инвесторов и аналитиков.

Facebook активно инвестирует в разнообразные направления, не уступая в этом Google. Социальная сеть направляет огромные ресурсы как на приобретение различных активов – WhatsApp, Instagram и Oculus Rift, так и на собственные масштабные проекты – создание устройства «телепортации» при помощи виртуальной реальности, космические спутники, Internet.org и разработки в области искусственного интеллекта.

Компания понимает, что ждать быстрой отдачи от этих направлений быстро не стоит. Так, М. Цукерберг заявил, что виртуальная реальность – это захватывающая область для инвестиций, но он ожидает медленный рост в этом сегменте. Финансовый директор Facebook Д. Венер сообщил, что компания продолжит тратить на виртуальную реальность, искусственный интеллект и подобные проекты, чтобы подготовиться к будущему, особенно пока силен основной бизнес.

«Мы агрессивно инвестируем в будущее, – заявил Д. Венер после доклада инвесторам. – И мы видим огромные возможности впереди».

Несмотря на то что Oculus Rift, приобретенный компанией за 2 млрд дол. в середине 2014 г., пока так и не выпустил полноценный рыночный продукт, Facebook продолжает покупать компании в области 3D-моделирования, компьютерного зрения и тактильных интерфейсов.

Одним из важных направлений для Facebook, которое связано в том числе и с сегментом виртуальной реальности, остается онлайн-видео. Компания активно внедряет технологии 360-градусных роликов, собирается в скором времени создать «место для видео в Интернете», привлекать авторов качественного видеоматериала, в том числе и профессиональные медиа, и даже платить им за контент и делиться доходами.

YouTube, который в настоящее время является «местом для видео в Интернете» и тоже внедрил сферические видео, не собирается сдавать позиции. Так, создатель YouTube Х. Грин даже раскритиковал Facebook в том, что социальная сеть учитывает просмотры видео от 3 секунд, когда YouTube засчитывает в просмотр только от 30 секунд.

Однако это не отменяет интереса к видеоплатформе Facebook как со стороны пользователей, так и рекламодателей. И существенный вклад на этом направлении внесло еще одно приобретение Facebook – фото- и видеосервис Instagram, аудитория которого достигла 400 млн пользователей. Пока неясно, насколько прибыльным является этот актив, однако руководство Facebook

отчиталось о том, что оперативное внедрение рекламной платформы в Instagram было хорошо воспринято рекламодателями и привело к быстрому росту монетизации сервиса.

Еще два актива Facebook: самое дорогое его приобретение мессенджер WhatsApp и собственная разработка Messenger – также показывают отличные цифры по росту аудитории (900 млн и 700 млн пользователей соответственно), но не приносят прибыль. Facebook продолжает искать модели взаимодействия рекламодателей с аудиторией на этих платформах и пока, по словам Д. Венера, не спешит делать здесь бизнес.

Internet.org также дает свои результаты: программа Facebook уже позволила 15 млн пользователей из стран третьего мира выйти онлайн. К проекту также недавно подключилась Индия.

Однако активность Facebook в Азиатском регионе и нежелание идти на введение какой-либо цензуры привели к тому, что социальная сеть была заблокирована в Китае. Тем не менее, компания не собирается отказываться от этого рынка. «Если ваша миссия – соединить всех людей в этом мире, вы не можете отказываться от крупнейшей страны», – говорит М. Цукерберг.

Тем не менее, глава Facebook уточняет, что, если социальная сеть недоступна для населения страны, это не значит, что она не присутствует в КНР. Китайские компании-экспортеры, которым важно взаимодействовать с зарубежной аудиторией, активно наращивают свои рекламные бюджеты в Facebook ***(На чем зарабатывает Facebook // InternetUA (http://internetua.com/na-csem-zarabativaet-Facebook). – 2015. – 6.11).***

***

Фотосервис Instagram тестирует новый тип рекламы с использованием функции 3D Touch, которая появилась с выпуском iPhone 6S. Об этом сообщает gazeta.ru

Издание отмечает, что пользователи смогут не только взаимодействовать с рекламными постами при помощи нажатий, но и оплатить покупку без сторонних приложений при помощи платежной системы Apple Pay. Кнопка «Купить сейчас» появилась в фотосервисе в июне этого года. В настоящее время похожими функциями обладают также Twitter и Pinterest.

С помощью 3D Touch рекламодатели смогут размещать сразу несколько изображений внутри одного поста, которые будут показываться пользователям в случае более сильного нажатия на публикацию. Кроме того, интеграция сервиса с Apple Pay позволит избежать ввода информации о кредитных картах и воспользоваться для идентификации отпечатками пальцев.

Технология 3D Touch активно используется не только для простой разблокировки смартфона, но и для совершения покупок в App Store или пользования сервисом Apple Pay ***(Instagram тестирует интерактивную рекламу с использованием 3D Touch // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45229/118/lang,ru/). – 2015. – 9.11).***

***

Удалите это немедленно, или семь смертных грехов продвижения в Facebook

Прежде чем продвигать свой бренд на Facebook, давайте представим, что вы уже присутствуете в самой крупной и узнаваемой социальной сети мира. Вы прочли тонны руководств, советов, наняли молодых и рьяных маркетологов или все делаете сами, будучи стартапом на бутстрепинге.

Но попридержите коней. Прежде чем нажимать кнопку «Опубликовать», взвесьте все хорошенько еще раз. Неудачное фото, дурацкий хэштег или неэтичное замечание в комментарии может привести вас к провалу. Знаете ли вы, что несколько крупных компаний поплатились миллионами долларов прибыли за одну единственную оплошность на Facebook?

В среднем компании теряют до 4,3 млн дол. прибыли в год из-за SMM-ошибок. Не уделяя должного внимания деталям, вы можете обозлить своих подписчиков (читай, клиентов) и стать объектом скандала на весь Интернет, где маленькая ошибка в мгновение ока может обернуться лавиной проблем. Ниже семь самых распространенных SMM-фейлов на Facebook, которые однажды обернулись для крупных брендов настоящей катастрофой.

Не будьте роботом

Очевидно в Domino’ s Pizza не привыкли к комплиментам. Когда пользователь написал положительный отзыв на Facebook-странице бренда, то получил в ответ заготовку-шаблон с извинениями: «Простите нас за это! Пожалуйста, поделитесь подробностями инцидента и укажите ссылку # 1409193, чтобы мы могли правильно адресовать информацию».

Легким движением руки бренд превратил позитивный отзыв в фейл, который потом был добросовестно обсмеян всем Интернетом. Мораль: не используйте заготовленные ответы. Автоматизация – это круто с точки зрения эффективности и экономии ресурсов, но есть области, в которых человека заменить нельзя.

Не удаляйте посты

Если вы хотите, чтобы ваши пользователи как можно скорее отвернулись от вас, давайте, удаляйте их сообщения с ваших Facebook-просторов. Когда пользователи начали писать производителю фруктовых джемов и топингов Smuckers вопросы, содержится ли ГМО в их продуктах, компания просто удаляла эти посты из Facebook и делала вид, будто их никогда не существовало.

Эти вопросы были для Smuckers возможностью заявить о позиции компании и получить живой фидбек. Иногда можно затушить волну негатива еще до того, как она наберет силу, просто общаясь с людьми, вместо того, чтобы удалять их вопросы.

Не пойте себе дифирамбы

Современных потребителей нервирует традиционная реклама в социальных сетях. Более половины подписчиков отписались от страниц в

Facebook из-за того, что их администраторы слишком часто пытались им что-то продать, бесконечно нахваливали компанию или просто вели станицу скучно.

General Motors – пример Facebook-страницы, на которой компания предпочитает транслировать рекламу вместо того, чтобы вовлекать пользователей в общение. Не нужно засыпать своих фанов пресс-релизами. Это выглядит так, будто вы пришли поговорить об Иисусе, а люди опрометчиво открыли дверь. Нужно показать им, что именно делает компанию уникальной и полезной для них. Но ненавязчиво.

Не забывайте, что Facebook-контент глобален

За день до того как шведы победили португальцев в решающем матче Чемпионата мира по футболу, на шведской странице Pepsi в Facebook появилась реклама, в которой кукла вуду португальского нападающего Криштиану Рональдо была представлена в разнообразных «убийственных» позициях.

Шведы и все остальные народы отреагировали на рекламу спокойно, однако португальские болельщики были вне себя. За один единственный день они умудрились собрать группу анти-фанов Pepsi в Facebook на 100 000+ подписчиков и заставили Pepsi принести публичные извинения.

Даже если ваша компания не глобальна, вы должны помнить: то, что попадает в Интернет, сразу становится доступным всему миру. Поэтому постарайтесь не отмочить нечто такое, что может ранить чувства представителей даже самых дальних от вас стран.

#Не #перебарщивайте #с #хэштегами

Использовать хэштеги на Facebook или нет? Это извечный вопрос. Проанализировав более 200 тыс. постов эксперты из SocialBackers пришли к выводу, что идеальное количество хэштегов в Facebook – один или два. Использование большего количества хэштегов чревато резким провалом во взаимодействии с аудиторией. Перебор с хэштегами заставляет вашу компанию выглядеть отчаявшейся привлечь внимание и набрать лайков.

С этим реально перебарщивает Starbucks – буквально каждый пост компании напичкан хэштегами. Правда, в последнее время они исправились и не вставляют в одну запись больше двух.

Наш вам совет: не путайте Instagram и Facebook, #эторазныевещи.

Не устраивайте «петросянщину»

Все шутки делятся на два вида: смешные и нет. SMMщики сети минимаркетов 7-Eleven считали себя очень остроумными, поэтому отважились пошутить на скользкую тему. В месяц психического здоровья (в США в этом году им объявили май) он опубликовали такой пост: «Май – месяц психического здоровья… или так заставляют вас думать КОНСПИРАТОРЫ, КОТОРЫЕ КОНТРОЛИРУЮТ МИР!»

Некоторые пользователи, возможно, и улыбнулись, но большинство подписчиков сообщества восприняли пост как насмешку над больными психическими расстройствами. 7-Eleven вынуждена была публично принести

извинения. Урок усвоен, но какой ценой! Долгое время компанию гнобили в медиапространстве, что не могло не сказаться на ее доходах.

Так что если вы приготовились сострить, еще раз подумайте, а не выйдет ли вам это боком.

Не попрошайничайте

Что-то у кого-то выпрашивать нельзя. И лайки/шеры – в том числе, потому что это просто цифровая форма попрошайничества. Это все-равно что написать в Facebook: «У нас нет стратегии и мы до конца не уверены, кто мы и зачем мы здесь». Производитель чистящих средств Oxiclean однажды нарушил это табу. Они не просто попросили лайков, но зачем-то присовокупили этот пост к сезону заполнения налоговых деклараций.

«Лайкни, если заполнил!»

В итоге никто так и не понял, что это было (хотя 623 лайка им все-таки отсыпали). Ясно одно – не нужно выпрашивать одобрение или умолять людей подписаться на вас. Так вы будете выглядеть жалко ***(Удалите это немедленно или 7 смертных грехов продвижения в Facebook // AIN (http://ain.ua/2015/11/07/614188). – 2015. – 7.11).***

***

Екперт сайту blog.newswhip.com Л. Коркоран проаналізував, які відео збирають на Facebook найбільше переглядів, та виокремив п’ять факторів спільних для найбільш поширюваних відео.

Короткі

Цю ознаку помітно з рейтингу відео шести різних ЗМІ, які у вересні зібрали найбільшу кількість репостів.

Квадратні

У BuzzFeed виявили, що 75 % найбільш поширюваних відео мали квадратний формат. Просто глядачі рідко хочуть повертати телефон, щоб подивитись коротке відео. За даними newswhip, 90 % найрейтинговіших відео у вересні були у квадратому форматі. Така звичка прийшла до Facebook з Instagram, Vine і Snapchat.

Важлива дія

Люди репостять приголомшливу картинку, де є багато дій і рухів. Тут рідко трапляються відео, де лише розмовляють.

Без звуку

Саме через таку опцію кліпи про їжу є серед найбільш популярних відео на Facebook. Картинки розповідають історію. Зараз багато найпопулярніших відео на Facebook можна дивитися незалежно від звуку. Великі і зручні для читання субтитри – простий спосіб трансформувати відеоряд у когерентну розповідь.

Запрошення до дії

Найбільш успішні відеорозповсюджувачі у Facebook додають короткий заклик до дії в кінці своїх відео, або на самих Facebook-сторінках. Розміщення кнопки «Дивитись відео» на сторінці – один із способів скерувати людей

ознайомитися з відеопродуктом. Також можна додати запрошення до перегляду в кінці відео через пункт меню «Редагувати відео» і Call To Action ***(5 ознак відео, які наберуть репости у Facebook // Телекритика (http://www.telekritika.ua/go_telek/2015-11-11/112630). – 2015. – 11.11).***

***

Как добиться успеха на Pinterest?

Секрет, как всегда, – качественный контент. Если обычно упор идёт на текстовую составляющую, здесь важна визуальная. Это статья об эффективности инфографики. Всего лишь шесть правил – шагов к графическому совершенству вашего контента для Pinterest. Этот путь приведёт вас к эффективному продвижению на ресурсе, стремительно набирающем популярность.

1. Тема. Ориентируйтесь на массовые популярные тренды Еда, маркетинг, и…

Перечислим всё, что привлекает публику, для чего стоит сделать инфографику.

Тема путешествий. Её любят все. Даже те, у кого нет времени сходить на обед. В мечтах люди могут находиться хоть на Багамах. И да, они с радостью будут просматривать инфографику об этом.

Еда. Взгляните на миллионы кулинарных сайтов, групп, пабликов. На Instagram, наконец! Вопросы отпадут сами собой.

О маркетинге читают. А когда текст «сдобрен» разного рода визуальной информацией, целевая аудитория воспринимает его лучше.

Наука, природа. Человек всегда хочет казаться себе умным и образованным. Кроме, разумеется, асоциальных и маргинальных особей. Потому, статьи/инфографика научной, экологической направленности остаются востребованными.

Life Style. Та же история, что с путешествиями. Людям нравится смотреть на это, мечтать. Даже завидовать.

Бизнес. Куда же без него? Ведь именно бизнес сегодня остаётся в топе факторов ментальной эволюции общества. Развивайся, становись успешным, или… смотри инфографику о чужих успехах.

Технологии. Вышел новый iГаджет! Техпроцессы Intel стали ещё совершенней, а процессоры – миниатюрней. Тебе не интересна статья? Вот инфографика. Лучше? Спасибо. Теперь можешь её расшарить.

Дизайн. Тематика, интересная в равной мере специалисту/ простому пользователю. Рассказы о том, как сделать визитку/оформить сайт/офис/кофейню в современном стиле – вчерашний день. А вот инфографика по топ-трендам может пригодиться.

О здоровье читают даже заядлые курильщики, люди, открыто смеющиеся над ЗОЖ – идеологией.

2. Веселим, информируем, мотивируем.

Три основных потребности, на которых стоит играть – потребность в развлечениях, полезной информации, мотивации к какой-либо активности.

Смешной контент. Люди любят веселиться. Такая информация, если она оригинально оформлена, воспринимается легко, быстро распространяется самими пользователями.

Побуждение/мотивация. Даже самый ленивый юзер в глубине души отчаянный активист, борец с чем угодно. Сам для себя, он – Нео, борющийся с Матрицей – системой, пролистывая инфографику.

Практическое. Люди любят красиво подаваемую, но реально применимую информацию. Создайте же её.

Желаемое. Чего хотят массы? Не делайте вид, будто не знаете.

Удивительные факты. Или не совсем факты. Удивлять, восхищать людей становится всё сложнее. Но нет ничего невозможного.

Интересное. Самый сложный пункт. Наравне с предыдущим.

3. Создаём простую информативную инфографику.

Повышая качество, информативность инфографики, вы автоматически повышаете её привлекательность для потенциального читателя. Списки, выводы, красивые постеры – путь к успеху.

Перечислим, выстроив список по популярности:

Информативность.

Оформление.

Сравнение и сопоставление.

Стилизация.

Временная линейка.

Иерархия.

Этот список показывает, что привлекает посетителя в первую очередь.

Статистика показала, что эффективнее всего в Pinterest работает текстовая инфографика. Далее идёт комбинированная, с изображениями, иллюстрациями, диаграммами.

4. Шрифты с засечками по-прежнему эффективны.

Большая часть инфографики для Pinterest выполняется при помощи шрифтов без засечек. Напрасно. Статистика всё так же неумолима, демонстрирует, что шрифты с засечками для инфографики эффективнее. Впрочем, можете экспериментировать – поймёте, какой вариант лучше работает.

5. Спектр. Красное и жёлтое.

Избегайте использования в цветовой схеме более двух цветов. Иначе восприятие осложняется. Если цветов больше трёх, шансы привлечь внимание меньше. Больше пяти – вы близки к провалу.

Практика показывает, что популярности добивается инфографика с красным и жёлтым цветами. Почётное третье место досталось синему. Комбинации также бывают успешны.

6. Длинноформатная инфографика популярна.

Оптимальная длина инфографики – миф. Но для успеха она должна быть больше ширины примерно в 5–9 раз. Такой формат оказывается эффективнее. Пусть пользователь использует вертикальную прокрутку. В наше время это стало одним из веб-рефлексов ***(Как сделать инфографику для Pinterest привлекательной // Sostav.ua (http://sostav.ua/publication/kak-sdelat-infografiku-dlya-pinterest-privlekatelnoj-69152.html). – 2015. – 13.11).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Відсутність соціальних мереж позитивно впливає на моральний стан людини, пише «Корреспондент.net» (http://ua.korrespondent.net/lifestyle/3588366-eksperty-ziasuvaly-scho-vidbuvaietsia-pislia-tyzhnevoi-vidmovy-vid-Facebook).

Психологи з Данії з' ясували, що відмова від використання соціальних мереж зменшує відчуття самотності і підвищує рівень задоволеності від власного життя, пише The Guardians.

Згідно з останнім дослідженням Happiness Research Institute в Копенгагені, навіть сім днів утримання від Facebook може позитивно позначитися на людині.

Таких висновків учені дійшли під час аналізу більше тисячі активних користувачів соціальних мереж від 16 до 76 років. Частина з них продовжувала використовувати Facebook, решта – на час відмовилися від цієї звички.

У підсумку з'ясувалося, що по закінченні тижня друга частина добровольців пережили на 55 % менше стресових і негативних емоцій. При цьому середній показник задоволення життям респондентів зріс із 7,56 до 8,12.

Також добровольці, що відмовилися від Facebook, зізналися, що стали більш соціально активними в реальному світі і перестали відчувати почуття самотності.

Експерти пояснюють це тим, що люди бачать у своїй стрічці оновлень «відретушовані» варіанти життя їхніх близьких і друзів – новини про досягнення, відпустках і подарунках.

За словами організатора дослідження М. Вайкінга, це тільки перша частина експерименту – надалі вчені планують вивчити вплив тривалої відмови від соціальних мереж.

Зокрема, у планах дослідників вивчити психологічний вплив року без Facebook у минулому активних його користувачів ***(Експерти з'ясували, що відбувається після тижневої відмови від Facebook // Корреспондент.net***

(http://ua.korrespondent.net/lifestyle/3588366-eksperty-ziasuvaly-scho-vidbuvaietsia-pislia-tyzhnevoi-vidmovy-vid-Facebook). – 2015. – 11.11).

***

Користувачі соцмережі в тій же мірі схильні до емоційного зараження, як і люди в натовпі. Емоції можуть передаватися і без безпосередньої фізичної присутності людей, показали дані дослідження, пише «Корреспондент.net» (http://ua.korrespondent.net/world/3588022-korystuvachi-Twitter-skhylni-emotsiinomu-zarazhennui-vcheni).

Дослідники з Індіанського університету в Блумінгтоні і Університету Південної Каліфорнії виявили, що кількість негативних чи позитивних твітів у стрічці користувача Twitter здатна вплинути на емоційне забарвлення його наступних твітів, повідомив сайт N+1 з посиланням на журнал PLoS ONE.

Іншими словами, користувачі цієї соціальної мережі в тій же мірі схильні до емоційного зараження, як і люди в натовпі, а для виникнення цього феномену не вимагається спостереження і синхронізації невербальних проявів емоцій.

Учені відібрали вибірку з 3800 користувачів Twitter, які зробили хоча б один твіт впродовж тижня у вересні 2014 р. Уся сукупність їх твітів за цей тиждень становила перший набір даних.

Потім учені сформували другу вибірку з користувачів, на яких був підписаний кожен учасник першої вибірки. З усієї сукупності твітів другої вибірки дослідники відібрали ті, які передували протягом години кожному з твітів представників першої вибірки. Таким чином, можна було відстежити – чи впливають твіти одних користувачів на утримання твітів їх фоловерів.

На другому етапі всі твіти (містять виключно текстову інформацію, тобто без URLs, фотографій і відео) вивчалися за допомогою методу аналізу тональності текстів (сентимент-аналіз). З його допомогою можна визначити думки авторів твітів щодо яких-небудь об’єктів або ситуацій, і відповідно, виявити три типи оцінок: позитивні, негативні і нейтральні. У даному випадку дослідники використовували алгоритм SentiStrength, який спеціально призначений для аналізу коротких повідомлень, які містять скорочення, абревіатури, сленг, емотикони (піктограма, що зображає емоцію. – Ред.) та ін.

Потім дослідники визначали – до якої з трьох пропорцій відноситься кожна конкретна сукупність твітів. Після чого відбирали ті, які були охарактеризовані як негативні і як позитивні. Фінальною процедурою стало виявлення залежності між емоційним забарвленням твітів першої групи користувачів від попередніх їм твітів.

З’ясувалося, що якщо впродовж години користувач міг бачити у своїй стрічці твіти, що на 4,34 % перевищують порогове значення негативних твітів (тобто можна сказати, що стрічка була більш негативною), то він з високою імовірністю також постив негативний твіт.

Для позитивних твітів пропорція повинна була зрушити на 4,5 %, тоді користувач слідом за іншими також постив позитивний твіт. При цьому

коефіцієнт кореляції між емоційним забарвленням попередніх твітів (позитивної або негативної) і твіти-реакції був дуже високий (R2 = 0,975) ***(Користувачі Twitter схильні емоційному зараженню – вчені // Корреспондент.net (http://ua.korrespondent.net/world/3588022-korystuvachi-Twitter-skhylni-emotsiinomu-zarazhennui-vcheni). – 2015. – 10.11).***

***

Чому в соціальних мережах так багато безпідставної самовпевненості і самомилування? Тому що нарциси використовують Facebook чи Twitter як інструмент генерування уваги до себе? Чи тому, що сам формат соціальних мереж підтримує культуру нарцисизму? Згідно з дослідженнями останніх років, відповідь на обидва запитання – так, пише Є. Кузнєцова для BBC Україна.

Нарцисизм – це розлад особистості, і його слід відрізняти від здорової любові до себе.

Любити себе – природно, тоді як нарциси часто втрачають здатність співчувати іншим людям, бажання допомагати, врешті, любити когось, крім себе. Слід розуміти, що це впливає не тільки на якість життя особистості, а й на здоров'я суспільства загалом.

Останнім часом і в медіа, і в академічному світі заговорили про епідемію нарцистичної поведінки у соціальних мережах.

Якщо раніше люди демонстрували нарцистичну поведінку у вузькому колі рідних і колег, то сьогодні у них набагато більша аудиторія. Тож дослідникам було цікаво дізнатися – що є першопричиною? Чи соціальні мережі роблять нас самозакоханими, чи просто люди, які і раніше проявляли ознаки нарцисизму, користуються ними як інструментом для генерування уваги до себе?

Ще кілька років тому журнал Personality and Social Psychology опублікував дослідження Л. Буфарді, яка спершу просила користувачів пройти психологічний тест, який визначав рівень їхньої схильності до нарцисизму, а потім аналізувала їхні профілі в соціальних мережах.

За результатами дослідження, ті люди, які мали найвищі показники нарцисизму, були найбільш активними і в соціальних мережах, публікували найбільшу кількість своїх фотографій, які автор охарактеризувала як self-promoting (Реклама себе. – Ред.), писали характерні тексти. Потім авторка дослідження попросила пересічних користувачів оцінити проаналізовані профайли і сказати, власники яких сторінок їм видаються самозакоханими.

Більшість учасників легко визначили саме тих користувачів, хто мав найбільше балів за шкалою нарцисизму за психологічним тестом.

Це дослідження підтвердило: все-таки нам не здається, що хтось поводиться в мережі надто нарцистично. Це справді характеризує особистість. І це можна визначити без складних психологічних тестів, неозброєним оком.

Підлітки і дорослі

Е. Панек, описуючи своє дослідження онлайн-нарцисизму в журналі Computers in Human Behavior, влучно порівняв Facebook із дзеркалом, а Twitter

з мегафоном. Підсумовуючи результати досліду, Е. Панек дійшов висновку, що соціальні мережі є одним з факторів продовження підліткового нарцисизму серед старших за віком користувачів.

Молодим людям властиво переоцінювати значення власної думки. Це абсолютно нормальний етап дорослішання – категоричність суджень. Проте люди, які вже перейшли підлітковий вік, продовжують виявляти ознаки нарцистичної поведінки в соціальних мережах (особливо до цього схиляє Twitter-формат). Наприклад, самовпевнено і категорично виражають свою думку щодо речей, на яких не розуміються, дозволяють собі різкі оціночні судження щодо інших людей тощо.

У психології така поведінка чітко асоціюється з етапом дорослішання, проте соціальні мережі роблять такий формат самовираження дедалі більш загальноприйнятним.

Крім того, існують побоювання, що вчорашні підлітки, які виросли онлайн, несуть такі моделі спілкування в доросле життя, вважаючи, що це нормально. Все ж у профайлах групи із середнім віком 35 нарцистичного контенту було значно менше. Тобто з часом, якщо користувач має достатнє коло спілкування поза соціальними мережами, реальність адаптує його до більш цивілізованих форм поведінки.

Ідеальна картинка

Іншим фактором того, чому онлайн спілкування затримує нарцистичні моделі поведінки у дорослих людей, є те, що сама система більшості соціальних мереж працює на «паливі» лайків. Сторінка на Facebook чи Instagram стає прообразом життя, яке хотілося б мати. Було вже декілька камінг-аутів про те, як люди «підсіли» на сердечки, лайки і репости, і зловили себе на тому, що дивляться на світ через свої онлайн-ідентичності. Один із недавніх випадків – відео австралійської моделі, яка в сльозах відмовилася від життя в Instagram, кажучи, що то не справжня людина, а лише штучний образ.

У соціальних мережах дуже легко намалювати ідеальну картинку свого життя. Зачесані, слухняні діти, фрагменти чистісінького помешкання, безкінечна любов без непорозумінь, квіти, сердечка, чашка какао на вікні.

Таке враження, що це заданий формат, і говорити про справжні речі, які не тільки радують, але й хвилюють – проти правил. Навіщо виставляти в мережу свої проблеми? Але чому ми тоді радо ділимося позитивним? Одна з відомих Instagram-блогерів, яка здобула популярність через фото своїх дітей, зізналася: я така втомлена, що не маю сил ні на що, але я все одно роблю фото дітей, стараючись, щоб не було помітно, як брудно у мене вдома, і пишу про те, яка я щаслива, хоча це останнє, що я справді відчуваю в той момент.

Такий тип поведінки поширюється, як вірус, змушуючи мільйони людей в усьому світі відчувати власну неповноцінність. Але ж ці самі люди своєю чергою слухняно підлаштовуються під задані правила гри.

А формат задаємо ми, користувачі. І правила гри може змінити кожен для себе. Тому іноді, пишучи таку цінну власну думку, варто задуматись про власну компетентність. Оцінюючи інших – подумати про загальноприйняті норми

спілкування, а малюючи картинку свого ідеального життя онлайн – подумати про те, що на дистанції «щастя» немає переможців ***(Як соцмережі сприяють нарцисизму // Рідна країна (http://ridna.ua/2015/11/yak-sotsmerezhi-spryyayut-nartsysyzmu/). – 2015. – 11.11).***

***

Інтравертам не варто зловживати відвіданням соціальних мереж, це може вкрай шкідливо впливати на психіку замкнутих людей, стверджують учені з Нової Зеландії.

У результаті кропітких досліджень виявилося, що замкнуті в собі люди надто болісно переживають різні публікації та висловлювання своїх знайомих у стрічці новин. І причиною депресивного настрою може бути не заздрість чи образа, а саме низька самооцінка людини. У такі миті інтраверти можуть дуже глибоко відчувати свою непотрібність у суспільстві.

Учені підкреслюють, що соціальні мережі були від початку орієнтовані на екстравертів, які не можуть прожити й хвилини без спілкування. Тому варто пам'ятати, що незалежно від типу характера варто проводити менше часу в Інтернеті і намагатися спілкуватися з людьми в реальному світі ***(Соціальні мережі шкідливі для інтравертів – вчені // NEW-S.COM.UA (http://new-s.com.ua/zdorovja/socialni_merezi_shkidluvi_dlja_intravertiv_03918.html). – 2015. – 10.11).***

***

Исследование, проведённое австралийскими учёными, показало, что больше половины австралийских подростков зависимы от социальных медиа. А в докладе Австралийского общества психологии также говорится о том, что около 60 % подростков не могут заснуть, пока не посетят свою страницу в социальных сетях. Каждый второй подросток сказал, что прибегает к социальным медиа, чтобы снять стресс, в 2011 г. таких было всего 37 %.

«Это можно сравнить с игровой зависимостью или любой другой, это затягивает, – сказал психолог А. Ферье. – Это работает как игровой аппарат. Никогда не знаешь, будешь ты радоваться или плакать. Так и с социальными сетями. Люди пытаются так доказать свою значимость, что их кто-то комментирует, поддерживает. Это глубокие психологические проблемы, которые особенно часто отмечаются у подростков».

Опрос также показал, что 72 % австралийцев чувствуют стресс и негатив, другие же отметили, что не обращаются к социальным медиа. Учёные отметили, что у этих 28 % более стабильное психическое состояние, здоровье и финансовое благополучие, сообщает uagazeta.net. Те же, кто сообщил о высоком уровне беспокойства, депрессии и стресса, часто прибегают к наркотикам, курению или алкоголю ***(Австралийские подростки зависимы от социальных медиа // Newsland (http://newsland.com/news/detail/id/1639863/). – 2015. – 13.11).***

Новый вид мошенничества атаковал одну из популярных соцсетей. Пользователям «ВКонтакте» со взломанных страниц друзей приходят сообщения с просьбой отправить немного денег им для помощи. Популярными причинами, которые указываются в таких письмах, являются: «с мамой что-то случилось, я не в городе. Отправь ей на телефон 15–20 гривен, я вернусь и отдам долг» или «маму положили в больницу из-за повышенного давления, все деньги ушли на лекарства, ей нужно пополнить счет, сам сейчас не могу, не выручишь ли? Я в понедельник верну».

Специалисты советуют не вестись на такие уловки и перезванивать «просящим» дабы удостовериться в правдивости информации ***(В ВКонтакте новый обман: «отправьте деньги моей маме» // Ура-Информ (http://ura-inform.com/ru/neformat/2015/11/10/v-vkontakte-novyj-obman-otpravte-dengi-moej-mame). – 2015. – 10.11).***

***

В Facebook стартовала черная PR-кампания либеральной налоговой реформы

После регистрации законопроекта № 3357 многие пользователи соцсети Facebook начали возмущаться появлению в своей ленте «странных» постов с пометкой «реклама». В рекламных сообщениях их информировали, что Украине грозит практически «апокалипсис» в случае принятия парламентского законопроекта: гривна упадет до 50 за доллар, банковскую систему настигнет коллапс, не будет денег на армию, образование, медицину, русские войска пойдут маршем по Украине. Причинно-следственные связи читателям не пояснялись.

Посты были размещены на страницах четырех групп соцсети – «Наша Варта», «Варта Майдану», «Баба і кіт» и «Міністерство Зради і Перемоги».

Все посты появились в Facebook 30 октября практически в одно и то же время. Группа «Баба і кіт» разместила сообщение в 12:16, «Міністерство Зради і Перемоги» – в 12:17, «Наша Варта» – в 12:18, «Варта Майдану» – в 12:19. Закон «О защите персональных данных» не позволяет официально выяснить, с одного ли IP-адреса размещались эти посты. Косвенно подтверждает это предположение анализ лент этих групп в соцсети: там присутствует немало идентичных сообщений, также опубликованных в одно и то же время.

По мнению пожелавшего остаться неназванным маркетинг-эксперта, в PR-кампании явно прослеживается использование одного из простейших приемов антикризисного пиара: «создаем внешнего врага – вешаем на него всех собак». «В данном случае один из предложенных проектов налоговой реформы категорически не приветствуется бизнесом. Вместо того чтобы довести его до ума, запускается критика конкурирующего законопроекта. За основу берутся мнимые факты (бюджетная дыра в 200 млрд грн, отказ МВФ финансировать

страну), исходя из них создаются логически и экономически необоснованные «страшилки» (глобальное падение гривны, прекращение финансирования соцсферы, марш российских войск по Украине). Месседжи рассчитаны на электорат, мягко говоря, не способный логически анализировать «вбросы». Подобную технологию регулярно используют российские политтехнологи, генерируя новости об Украине. К сожалению, и наши опустились до уровня «вата схавает». Или заказчики PR-кампании пригласили российских спецов».

Однако судя по суммарному количеству лайков (3019) и перепостов (658) только на страницах этих четырех групп, PR-кампания таки удалась. Многие читатели, не вдаваясь в анализ реформы, жестко раскритиковали парламентский законопроект. Далее разгорелись «баталии» между сторонниками либерального проекта и «поверившими рекламе». Некоторые комментаторы, которые пытались пояснить реальную суть реформы, жаловались на то, что их мнения почему-то были удалены.

Вскоре в соцсети появились посты с интересными вопросами.

Мнения экспертов:

І. Несходовський, експерт групи РПР «Податкова реформа»: «За нашою інформацією, за цим інформаційним вкидом стоїть О. Макеєва (заместитель министра финансов. – InternetUA), яка вже не перший раз використовує брудні технології, щоб дискредитувати опонентів. Вкид абсолютно безграмотний і будь-яка людина з економічною освітою може побачити необгрунтованість цих зауважень...».

В. Дубровский, старший экономист CASE Украина, эксперт группы «Податкова реформа» РПР: «Думаю, распространяемая информация заказного характера. Весьма симптоматично, что появились люди, готовые заплатить за не проведение либеральной реформы. Значит она “наступила” на серьезные интересы. И это не интересы малого и среднего бизнеса…».

Т. Козак, координатор «Нова Країна», засновник, президент «Инвестиционная Группа УНИВЕР»: «Проти ліберальної реформи хтось спланував і координує дії по дискредитації. Хто може бути замовником? Точно не бізнес, бо ця реформа несе податкові послаблення для бізнесу. Точно не громадянське суспільство, бо реформа адміністрування податків зменшить корупцію. Значить, залишається система, чи Гідра – як ми її називаємо» ***(В FB стартовала черная pr-кампания либеральной налоговой реформы // InternetUA (http://internetua.com/v-FB-startovala-csernaya-pr-kampaniya-liberalnoi-nalogovoi-reformi). – 2015. – 5.11).***

***

Мошенник ограбил инвесторов при помощи Twitter

Комиссия по ценным бумагам и биржам США подала иск против торговца ценными бумагами, который обрушил акции двух компаний при помощи ложных твитов.

Трейдер А. Крейг создал в социальной сети поддельные аккаунты крупных аналитических агентств Muddy Waters Research и Citron Research и

разместил от их имени ложные сообщения о публичных компаниях Audience и Sarepta Therapeutics, в том числе о том, что против них начаты расследования. В результате, стоимости акций этих компаний упали, и инвесторы на рынке понесли значительные финансовые потери, при этом мошеннику не удалось заработать за счет покупки и продажи этих ценных бумаг ***(Мошенник ограбил инвесторов при помощи Twitter // InternetUA (http://internetua.com/moshennik-ograbil-investorov-pri-pomosxi-Twitter). – 2015. – 7.11).***

***

В социальных сетях группы сепаратиского направления агитируют во втором туре выборов мэра Николаева голосовать за И. Дятлова, пишет «Эгалите» (http://egalite.com.ua/news/13771).

В частности, такие объявления были опубликованы в открытых группах «На оккупированной территории» и «Группа поддержки Александра Захарченко». Как первая, так и вторая группа открыто поддерживают идеи террористических организаций ЛНР и ДНР.

В тексте объявления И. Дятлова называют «лидером оппозиции», который «во время силовых захватов власти зимой 2014 г. не побоялся и призвал жителей города стереть с лица земли этих бандеровцев» ***(В социальных сетях сепаратисты призывают николаевцев голосовать за «лидера оппозиции, который призвал стереть с лица земли бандеровцев» // Эгалите (http://egalite.com.ua/news/13771). – 2015. – 12.11).***

***

Пользователи российской социальной сети «Одноклассники» пустили фейк о том, что «бандеровцы» якобы обезглавили памятник Родине-матери неподалеку от моста Патона в Киеве, пишет «Обозреватель» (http://kiyany.obozrevatel.com/life/42165-sotsseti-v-shoke-rossiyane-obezglavili-rodinu-mat-v-kieve.htm).

На это обратило внимание сообщество «Український наступ» в Facebook.

«Доблестная 1-я низкомобильная диванная бригада Наступа совершила рейд вражескими тылами “Одноклассников”. Предметом вброса послужила фотография 1980 г., на которой запечатлён процесс постройки известного памятника Киева – Родины-Матери. Был добавлен необходимый текст, и пикча разошлась по ОК-пабликам», – сказано в сообщении.

На картинке, которую распространяли россияне, был памятник без головы и подпись: «Доскакались? Обезумевшие в своей руссофобии укронацисты продолжают бороться с памятниками. На этот раз был варварски снесен монумент “Родина-мать” в столице бандеровской хунты – в Киеве» ***(Соцсети в шоке: россияне «обезглавили» Родину-мать в Киеве // Обозреватель (http://kiyany.obozrevatel.com/life/42165-sotsseti-v-shoke-rossiyane-obezglavili-rodinu-mat-v-kieve.htm). – 2015. – 13.11).***

Зарубіжні спецслужби і технології «соціального контролю»

Кремль следит за пользователями социальных сетей в России

Путин мечтает о собственном контролируемом Интернете, но это убьет российскую экономику.

Когда продавец-консультант из Екатеринбурга Е. Вологженинова распространила на своей странице в «ВКонтакте» несколько десятков ссылок о войне в Украине, она ждала лишь несколько злых комментариев.

Но комментариями ее 52 друзей в социальной сети дело не кончилось. Как оказалось, за ее сообщениями в Интернете следят и работники Следственного комитета России.

Об этом сегодня пишет Newsweek. В феврале 2014 г. агенты Следственного комитета и ФСБ ворвались домой к Е. Вологжениновой. У нее отобрали компьютер и цифровую камеру, а также планшетный компьютер ее 12-летней дочери. Ей также объявили обвинения в «разжигании ненависти» против «российских добровольцев», которые воюют в Украине, и против правительства России.

Обвиняемую женщину, которая никогда не была за границей и имеет только около тысячи долларов сбережений, также занесли в список «террористов и экстремистов» наряду с «Исламским государством» и «Аль-Каидой». А ее банковские и кредитные карточки были заморожены. В прокуратуре также пояснили, что, оказывается, Е. Вологженинова размещала в Интернете «материалы экстремистского характера», хотя это были только новости о войне в Донбассе из украинских СМИ. За это женщину приговорили к четырем годам тюрьмы.

«Я лишь искала альтернативную точку зрения к российским государственным СМИ, которые очень однобоко описывают конфликт в Украине. Ничто из того, что я распространила, не было предварительно признано экстремистским в России. И моя страница была частной, только мои друзья могли видеть сообщения», – рассказала Е. Вологженинова.

Оппозиционный блогер А. Малгин говорит, что дело против нее лишь одно из тысяч. Такие преследования власть России использует для того, чтобы запугивать других. Когда В. Путин только стал президентом, около одного миллиона россиян пользовались Интернетом.

За 10 лет количество пользователей возросло в 50 раз. Сам российский президент говорит, что не пользуется всемирной сетью и уверяет, что «50 % информации там – это порнография». При этом с первых дней своего правления он сильно ограничил свободу прессы, но до недавнего времени Кремль мало уделял внимания именно СМИ в Интернете. И, казалось, в этом не было необходимости, поскольку главным источником информации было телевидение, которое полностью контролирует власть.

Однако с развитием скоростного Интернета, оппозиционные активисты начали использовать его как инструмент для освещения коррумпированности

власти в России. Один из них – А. Навальный, который в декабре 2011 г. опубликовал в сети видео с фактами фальсификаций на выборах в пользу В. Путина.

«Путин увидел, что Интернет стал способен мобилизовать людей за очень короткий срок. Он понял, что контролировать крупные СМИ недостаточно, надо еще и взять власть над сетью», – говорит А. Малгин.

С 2012 г. Кремль закрыл сайты оппозиционных политиков, блогеров и активистов, а также прибрал к рукам социальную сеть «ВКонтакте», основатель которой П. Дуров эмигрировал из России. В 2015 г. организация Freedom House опустила рейтинг российского Интернета к статусу «несвободный». Хотя еще годом ранее он считался «частично свободным».

Но на этом подавление сети не закончилось. В этом месяце Госдума должна рассмотреть законопроект, который позволит ФСБ допрашивать комментаторов, которые «подозрительно себя ведут» в сети и «могут планировать террористический акт».

Для Е. Вологжениновой, которую в России осудили за несколько сообщений в социальной сети, такие законы кажутся абсурдными. «Российское государственное телевидение сами занимаются экстремизмом. Они спровоцировали волну ненависти к украинцам», – говорит она.

Кремль также пытается контролировать иностранные сайты. С 1 января 2016 г. Москва обязывает все иностранные компании, такие как Google и Facebook, держать свои серверы на территории России. В. Путин также хочет установить право «выключать» Интернет в России, если начнутся массовые протесты из-за усиления экономического кризиса.

«Путин мечтает о своем собственном Интернете. Но как только Россия отключится от глобальной сети, все: промышленность, наука, транспорт перестанет работать. Пытаясь подавить распространение нежелательных точек зрения, он убью российскую экономику», – говорит А. Малгин.

Ранее издание «Коммерсантъ» писало, что РФ будет бороться с «предвзятой информацией» и «подрывом патриотических традиций» в Интернете. В 2016 г. должна быть принята новая «Доктрина информационной безопасности РФ» на смену действующему документу от 2000 г. Согласно доктрине, национальным интересам в информационной сфере России может помешать ряд угроз, поскольку «информационное пространство все чаще используется «для решения военно-политических задач, а также в террористических и иных противоправных целях».

В свою очередь интернет-омбудсмен РФ предложил экспортировать технологии с помощью военной силы. «Мы сможем давать технологии другим странам, только когда у нас будет военное присутствие. Когда у других стран не будет альтернативной возможности не брать это в нас», – сказал Д. Мариничев в ходе слушаний в Общественной палате РФ на тему импортозамещения технологий, доступ к которым оказался закрыт через западные санкции.

В сентябре директор Национальной разведки США Д. Клеппер выразил серьезную обеспокоенность в связи с киберактивностью России, которая угрожает национальной безопасности Соединенных Штатов Америки. «Российское Минобороны создает собственно киберкомандование, которое, по высказываниям российских официальных должностных лиц, будет отвечать за реализацию наступательных мероприятий в киберпространстве», – заметил глава американской национальной разведки.

Издание Newsweek писало, что хакеры стали мощнейшим оружием России. В жаргоне хакеров существует понятие эффекта «от кибернетического к физическому». Это означает способность хакера влиять на реальный мир с помощью инструментов в виртуальном. И часто это влияние носит деструктивный характер ***(Кремль следит за пользователями социальных сетей в России // InternetUA (http://internetua.com/kreml-sledit-za-polzovatelyami-socialnih-setei-v-rossii). – 2015. – 3.11).***

***

Суд оштрафовал карельского журналиста В. Штепу за размещенную на странице в соцсети «ВКонтакте» фотографию визитки украинского политика Д. Яроша, передает ТАСС.

«Признать Штепу Вадима виновным в совершении правонарушения, предусмотренного ст.20.3 КоАП РФ и назначить наказание в виде штрафа в размере одна тысяча рублей», – огласила решение судья В. Полякова.

По словам самого В. Штепы, визитка с символикой запрещенного в России движения была размещена им «не с целью пропаганды, а с информационными целями», а позже удалена ***(В России журналиста оштрафовали за фотографию визитки Яроша в соцсети // InternetUA (http://internetua.com/v-rossii-jurnalista-oshtrafovali-za-fotografiua-vizitki-yarosha-v-socseti). – 2015. – 4.11).***

***

В Таджикистане интернет-провайдеры частично заблокировали доступ к популярным социальным сетям – Facebook, «ВКонтакте», «Одноклассники» и видеохостингу YouTube. Также с вечера 2 ноября недоступны сайты таджикской службы радио «Свобода» и оппозиционного интернет-ресурса «Озодагон», сообщает bbc.com

Как рассказали Русской службе Би-би-си представители крупных интернет-провайдеров страны, блокировка произведена по устному распоряжению Службы связи при правительстве республики.

Официально ситуацию объяснили техническими проблемами и профилактическими работами. В Службе связи отказались от комментариев.

Между тем Ассоциация интернет-сервис провайдеров Таджикистана выступила против блокировок интернет-ресурсов, призывая власти отказаться от ставшей уже обычной практики закрытия доступа в Интернет для жителей страны.

«Такие меры угрожают информационной безопасности страны. Ослабевает отечественное информационное пространство. К сожалению, последние годы ограничения доступа происходят без официальных, письменных распоряжений Службы связи, и без объяснения конкретных причин блокировки сайтов», – заявил Русской службе Би-би-си А. Атоев, глава Ассоциации интернет-провайдеров.

Ограничение доступа к социальным сетям началось во время визита в Таджикистан госсекретаря США Д. Керри, который 3 ноября встретился с президентом Э. Рахмоном. Как сообщалось, одной из главных тем переговоров стало соблюдение прав человека и недопущение нарушений религиозных прав.

Это уже не первая попытка таджикских властей блокировать популярные социальные сети и независимые интернет-издания, которые публикуют критические статьи в адрес властей. В июне этого года провайдеры уже блокировали доступ к соцсетям. При этом тогда они предполагали, что блокировка связана с проведением в Душанбе конференции «Вода для жизни», на которую прибыли более 1,5 тыс. представителей из 99 стран мира, в том числе Генсек ООН Пан Ги Мун ***(В Таджикистане накануне визита Керри заблокировали соцсети // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45179/118/lang,ru/). – 2015. – 3.11).***

***

Instagram может стать полем по сбору информации об употреблении несовершеннолетними алкогольных напитков.

С такой идеей выступили американские ученые Рочестерского университета предложили, они предложили при помощи соцсети создать статистику, о чем сообщили на сайте вуза.

По мнению исследователей, подростки не так искренне могут делиться информацией об употреблении алкоголя во время теста, нежели в социальных сетях. Поэтому, при мониторинге Instagram можно создать базу данных о возрасте несовершеннолетнего и месте его проживания.

Однако существенную проблему вызывает тот факт, что отсортировать пользователей по возрасту в соцсети нельзя. Однако ученые не растерялись, они считают, что можно применить технологию, которая по лицу на фото будет вычислять примерный возраст человека, пол и расу.

Кроме того, чтобы увеличить эффективность противоалкогольной кампании, направленной на подростков, ученые еще составили словарь сленговых выражений, в котором приводятся примеры названий алкоголя в других выражениях. Таким образом исследователи намереваются помочь активнее бороться с зависимостью от алкоголя среди несовершеннолетних ***(Instagram поможет выявить выпивающих подростков // UKR-TODAY.com (http://ukr-today.com/high-tech/75178-instagram-pomozhet-vyyavit-vypivayuschih-podrostkov.html). – 2015. – 3.11).***

***

В Запорожье Служба безопасности Украины прекратила деятельность местного жителя, который вел активную антиукраинскую пропаганду в социальных сетях.

По данным пресс-службы СБУ, представитель террористической организации «ДНР» вышел на запорожца через Интернет и за денежное вознаграждение предложил ему размещать в социальных группах антиукраинские материалы.

В задачи интернет-пропагандиста входило размещение в российских соцсетях специально подготовленных сепаратистами сообщений в поддержку т. н. «ДНР/ЛНР». Он распространял антиукраинские материалы с призывами к насильственному изменению конституционного строя Украины, гражданского неповиновения действующей власти, инструкции по предотвращению мобилизации и тому подобное.

Во время обысков правоохранители обнаружили компьютерное оборудование с доказательствами антиукраинской деятельности.

Продолжаются оперативно-следственные действия ***(В Запорожье СБУ задержала пропагандиста боевиков // InternetUA (http://internetua.com/v-zaporoje-sbu-zaderjala-propagandista-boevikov). – 2015. – 5.11).***

***

Социальные сети помогут Украине в борьбе с терроризмом

Самое важное, по словам специалиста, в работе подразделения Информационно-психологических и специальных операций Сил спецопераций (ИПСО ССО) – четко выделить и узнать про какую-то ситуацию, на которую можно реально повлиять.

Офицер подразделения ИПСО ССО, который попросил не раскрывать свое имя, рассказал в интервью изданию «Тыждень», что основная задача ИПСО ССО – деморализация личного состава противника, незаконных вооруженных формирований сепаратистов на Донбассе.

По его словам, главный канал налаживания связей и установления контактов с информаторами – социальные сети. Находясь по эту сторону фронта, это вполне логично. В свою очередь, основным каналом связи в соцсетях для нас был и является Twitter.

Офицер отмечает, что основным методом и был, и до сих пор остаётся распространение выгодных нам слухов среди врагов. «Итак, приезжаешь и сначала первые две-три недели изучаешь местность и реакцию людей на тебя. А местное население сразу узнает новеньких, приезжих. Не верьте, что нам легко работать, потому что, мол, нет языкового барьера. Все нюансы, как говор, диалект, произношение, внешний вид, сразу заметные и очень важные в нашей работе. Поэтому просто устанавливаешь контакты, например, через центры для переселенцев.

И дальше мы должны сделать, чтобы через наши контакты, вольно или невольно, люди перенесли нужную нам информацию на ту сторону. Чтобы

посеять там или панику, или деморализацию личного состава, заставить их к дезертирству и бегству, вызвать недоверие к собственному руководству, чтобы не выполнялись приказы их командования», – рассказал он.

По его словам, это то, что противник так хорошо делал в свое время с нашими бойцами. «Надо отдать им должное: наши враги-коллеги работают достаточно неплохо, у них больше финансовых и организационных ресурсов, их постоянно поддерживает Россия», – отметил он.

Вместе с тем офицер подчеркнул, что с украинской стороны, наоборот, поиск ресурсов для работы занимает львиную долю времени. Например, напечатать что-то для распространения на оккупированной территории, создания качественных роликов и видеоматериалов и тому подобное.

Самое важное, по его словам, в работе ИПСО ССО – четко выделить и узнать про какую-то ситуацию, на которую можно реально повлиять. «Мы воздействуем через своих агентов, распространяем слухи, статьи за журналистов и лидеров общественного мнения, которых читают и на нашей, и на их стороне», – пояснил офицер. При этом он посетовал, что достаточно тяжело работать с нашими, украинскими журналистами. Ведь все они, прежде всего, хотят сенсацию, а не послужить своей стране, распространив нужную информацию в нужной форме.

Ранее сообщалось, что Силы специального назначения могут освободить оккупированные территории ***(Социальные сети помогут Украине в борьбе с терроризмом // Донецкие вести (http://www.donetskie.com/news/incident/sotsialnye-seti-pomogut-ukraine-v-borbe-s-terrorizmom/58053/). – 2015. – 5.11).***

***

У Казахстані розблокували закриту з 2011 р. блог-платформу LiveJournal.

Про це заявили в комітеті зв'язку, інформатизації та інформації Міністерства з інвестицій та розвитку республіки, повідомляє ТАСС.

«Доступ був відновлений після виконання адміністрацією блог-платформи LiveJournal рішень судових органів про видалення протиправних матеріалів, розміщених на ресурсі. Представники LiveJournal повідомили про видалення з блог-платформи матеріалів, що містять ознаки пропаганди тероризму і релігійного екстремізму, публічних закликів до вчинення актів тероризму і виготовлення вибухових пристроїв», – зазначила прес-служба комітету.

Доступ до LiveJournal був заблокований згідно з постановою Сариаркінського суду Астани з 20 серпня 2011 р. через поширення протиправних матеріалів.

У комітеті також повідомили, що LiveJournal планує відкрити представництво в Казахстані і розвивати казахстанський сегмент блог-платформи ***(У Казахстані розблокували закритий з 2011 року LiveJournal // MediaSapiens***

(http://osvita.mediasapiens.ua/media_law/government/u_kazakhstani_rozblokuvali_zakritiy_z_2011_roku_livejournal/). – 2015. – 11.11).

***

Русская православная церковь (РПЦ) приняла решение не оставаться в стороне от такого глобального феномена, как Интернет, поэтому в ближайшее время будет запущена православная версия «чистого» Wi-Fi. Об этом сообщил руководитель секретариата Межрелигиозного совета России, заместитель председателя Синодального отдела по взаимодействию Церкви и общества РПЦ священник Р. Багдасаров.

По его словам, «религиозный» Wi-Fi не пропустит сообщения от сектантов или экстремистов, информацию об искаженных фактах истории и будет блокировать любые развратные запросы.

Сообщается, что бесплатные точки доступа к «чистому» Интернету разместят около храмов, а также на городских площадках, которые популярны среди горожан, особенно среди молодежи.

По словам священника, группа специалистов будет вручную отбирать данные, которые безопасны, и блокировать ненужную информацию. «Мы не говорим, что в православном Интернете будут только проповеди патриарха и православные сайты. Там будет много всего, в том числе нормальное кино – например, фильмы «Александр Невский», «Утомлённые солнцем» и многие другие отечественные и зарубежные картины, которые прививают людям правильные ценности, такие как традиционная нравственность, патриотизм, защита семьи и детей. И чтобы не кормить троллей, которые сразу же начнут кричать, что мы ограничиваем людей в правах, я отмечу: мы никого не ограничиваем. Не хочешь пользоваться православным Интернетом – пользуйся обычным», – рассказал Р. Багдасаров.

Стоит отметить, что подобную инициативу РПЦ по очистке Интернета от непотребщины уже поддержали департамент национальной политики города Москвы, Совет муфтиев России и Федерация еврейских общин России ***(РПЦ запустит православную версию «чистого» Wi-Fi // Mignews.com.ua (http://mignews.com.ua/world/7886277.html). – 2015. – 9.11).***

***

Власти венгерского города Тата подали в суд на женщину, поделившуюся в Facebook постом с критикой расходов городских чиновников.

По данным новостного сайта 444.hu, в записи утверждалось, что местные власти сначала продали объект недвижимости, а затем оплачивали аренду того же самого здания по высокой ставке. Также в публикации поднималась тема возможной связи чиновников с новыми владельцами недвижимости. Изначально суд приговорил М. Шомоди к штрафу в 175 дол. за клевету, но по итогам рассмотрения апелляции сумма штрафа была снижена до 35 дол. По решению суда М. Шомоди также должна возместить судебные издержки, которые, согласно информации Index.hu, составили порядка 260 дол.

В 2013 г. сайт журналистских расследований Atlatszo.hu призвал к декриминализации клеветы. Тем не менее, соответствующая уголовная норма действует до сих пор и часто используется для борьбы с критикой в адрес власти. Венгерский союз гражданских свобод запустил краудсорсинговую кампанию в поддержку М. Шомоди.

Активисты ВСГС также разработали приложение по созданию саркастичных «мемов». Изображения венгерских политиков, сопровождающиеся высказываниями известных медиаперсон и журналистов, распространяются сторонниками свободы слова в соцсетях. Желающие смогли выразить свое мнение и оффлайн: 9 ноября в Будапеште активисты ВСГС в рамках своего проекта PolitiKuss собирали письменные отзывы граждан ***(В Венгрии оштрафовали женщину за «расшаривание» поста в Facebook // UAINFO (http://uainfo.org/blognews/1447405295-v-vengrii-oshtrafovali-zhenshchinu-za-rassharivanie-posta.html). – 2015. – 13.11).***

***

Facebook відзвітувала про звернення урядів різних країн щодо видалення інформації із соцмережі або розкриття інформації про користувачів. У першому півріччі 2015 р. кількість запитів на видалення контенту зросла на 112 % у порівнянні з другим півріччям 2014 р. і досягла 20 568. А запити про дані користувачів зросли на 18 % – до 41 214.

З боку українського уряду було здійснено шість запитів щодо семи акаунтів. Лише один із запитів був задоволений з боку Facebook. Соцмережа не розкриває інформацію про те, кого саме стосувалися запити, і в чому суть запиту.

За попередній період – з липня по грудень 2014 р. з боку української влади був усього один запит, і він не був задоволений соцмережею.

Компанія підкреслює у своєму повідомленні, що не дає урядам прямого доступу до акаунтів своїх користувачів. Facebook ретельно вивчає, наскільки обґрунтованим є кожен запит від влади: «Якщо запит здається нам неоднозначним або може бути занадто загальним, ми його не виконуємо і готові відстоювати свою позицію в суді, якщо це необхідно» ***(Facebook вперше розкрив дані користувача соцмережі на вимогу української влади // UkrainianWatcher (http://watcher.com.ua/2015/11/13/facebook-vpershe-rozkryv-dani-ukrayinskoho-korystuvacha-na-vymohu-ukrayinskoyi-vlady/). – 2015. – 13.11).***

***

Прокуратура Санкт-Петербурга має намір перевірити на предмет розміщення екстремістських матеріалів сторінку українського добровольчого батальйону «Азов» у соціальній мережі «ВКонтакте». Про це повідомляє прес-служба Справедливої Росії з посиланням на відповідь з генпрокуратури РФ, пише «Корреспондент.net» (http://ua.korrespondent.net/ukraine/3588455-storinku-azova-mozhut-vydalyty-z-vkontakte).

Раніше заступник голови комітету Держдуми з безпеки та протидії корупції Д. Горовцев (Справедлива Росія) направив листа на ім'я генпрокурора РФ Ю. Чайки з проханням перевірити сторінку, присвячену «Азову». Депутат посилався на повідомлення користувачів про те, що на сторінці «публікуються матеріали екстремістського характеру, в яких містяться заклики до насильства і порушення територіальної цілісності РФ», а також демонструється нацистська символіка ***(Сторінку «Азова» можуть видалити з ВКонтакте // Корреспондент.net (http://ua.korrespondent.net/ukraine/3588455-storinku-azova-mozhut-vydalyty-z-vkontakte). – 2015. – 11.11).***

***

Личная страница так называемого «уполномоченного ДНР» по правам человека Д. Морозовой в Facebook заблокирована администрацией социальной сети. Об этом сообщает сайт сепаратистов «ДАН».

«Руководство Facebook заблокировало сегодня личную страницу омбудсмена ДНР Д. Морозовой без каких-либо причин», – говорится в сообщении.

Члены группировки связывают блокировку страницы «с многочисленными необоснованными жалобами "украинских оппонентов"» ***(Facebook заблокировала страницу «омбудсмена ДНР» // Новости Донбасса (http://novosti.dn.ua/details/263381/). – 2015. – 11.11).***

Проблема захисту даних. DDOS та вірусні атаки

Snapchat будет использовать распространяемые через приложение изображения

В последние годы всё большей популярностью пользуется приложение Snapchat, обещающее безопасную передачу изображений между двумя пользователями. Основной возможностью является установка времени жизни передаваемого контента, по истечении которого он уничтожается.

В недавнем обновлении приложения были внесены изменения в политику конфиденциальности и условия пользования сервисом. Отныне разработчики оставляют за собой право «сохранять, использовать, отображать, изменять, редактировать, публиковать, транслировать, распространять передаваемый контент в любой форме, в любых средствах информации и любыми методами распространения, существующими и созданными в будущем».

Теперь разработчики могут использовать пользовательский контент для продвижения сервиса; говоря по-простому, работая с приложением, пользователи дают разработчикам разрешение делать со своими файлами всё что им угодно, включая отображение на сайте Snapchat и в социальных сетях.

Snapchat ранее обвинялся Федеральной торговой комиссией США в обмане пользователей, которых убеждали в том, что передаваемые через

приложение изображения удаляются с устройств получателей безвозвратно. На самом деле было установлено, что файлы могут быть восстановлены и сохранены, вне зависимости от установленного срока их годности. После разработчики представили возможность платного повторного просмотра контента ***(Snapchat будет использовать распространяемые через приложение изображения // InternetUA (http://internetua.com/Snapchat-budet-ispolzovat-rasprostranyaemie-cserez-prilojenie-izobrajeniya). – 2015. – 2.11).***

***

Иранские хакеры демонстрируют повышенный интерес к мобильным троянам удаленного доступа, в частности, к вредоносам, разработанным для инфицирования Android-устройств. Такой вывод сделали специалисты аналитической компании RecordedFuture по итогам проведенного ими исследования.

По словам экспертов, наибольший интерес у злоумышленников вызывают трояны AndroRAT и DroidJack, которые могут скрываться в замаскированных под легитимные приложения. Эксперты подчеркивают, что такие угрозы, как njRAT, широко используются в кампаниях по шпионажу и в различных видах криминальной деятельности, тогда как XtremeRAT применяется в атаках, нацеленных на предприятия в Израиле, Египте и Саудовской Аравии.

Согласно статистике компании IDC, Android является наиболее популярной мобильной операционной системой на Ближнем Востоке и в Африке – порядка 80 % устройств работают под управлением этой платформы.

Все варианты Android-троянов обладают широким рядом функций, позволяющих осуществлять шпионскую деятельность и получить контроль над устройством. RAT способны перехватывать SMS-сообщения, просматривать журналы звонков, историю браузера, контакты и другие важные данные, в том числе учетные.

Как пояснил аналитик RecordedFuture Р. Бижу, DroidJack и AndroRAT представляют меньшинство в рамках общей активности троянов удаленного доступа, однако доступность и необязательность наличия особых технических навыков для работы с ними способствуют популярности данных вредоносов. Скорее всего, отмечает исследователь, трояны так и будут оставаться наиболее очевидным выбор ***(Иранские хакеры проявляют интерес к мобильным RAT // InternetUA (http://internetua.com/iranskie-hakeri-proyavlyauat-interes-k-mobilnim-RAT). – 2015. – 2.11).***

***

Как сообщается в отчете Фонда электронных рубежей (Electronic Frontiers Foundation), автоматизированные системы распознавания номерных знаков автомобилей (Automatic license plates recognition, ALPR), широко используемые правоохранительными органами для выявления нарушителей правил дорожного движения, крайне незащищены. Утверждается, что любой

желающий может подключиться к камерам ALPR через браузер и наблюдать за водителями.

Эксперты изучили работу ALPR-систем, в автоматическом режиме фотографирующих и фиксирующих данные о номерных знаках автомобилей. Отметим, что такие устройства часто устанавливаются на полицейских машинах. Специалисты сообщают, что в нынешнем году ими было обнаружено более 100 незащищенных камер, позволяющих любому желающему подключиться к трансляции в режиме реального времени. «Некоторые из этих камер подключены к Интернету. Если знать, где искать, то любой желающий сможет подключиться к трансляции и видеть все, что фиксируют ALPR-системы», – говорится в отчете.

В рамках исследования специалисты EFF проверяли, удается ли подключиться к камере через Интернет и требует ли веб-интерфейс ввода логина или пароля. Если веб-интерфейс и Telnet-соединение были защищены надежным паролем, эксперты признавали камеру безопасной. В противном случае исследователи получали доступ к устройствам – чаще всего в них использовались пароли по умолчанию.

Специалисты EFF связались с владельцами некоторых камер и сообщили им об уязвимости. Большинство уведомленных пользователей исправили ошибку – например, правоохранительные органы штата Луизиана и Университет Южной Калифорнии, США, незамедлительно устранили брешь ***(Системы распознавания номерных знаков недостаточно защищены // InternetUA (http://internetua.com/sistemi-raspoznavaniya-nomernih-znakov-nedostatocsno-zasxisxeni). – 2015. – 2.11).***

***

Исследователи компании Context Information Security разработали и опубликовали утилиту WSUSpect, позволяющую пен-тестерам внедрять вредоносные обновления Windows в корпоративные сети, использующие для обновления ОС сервер WSUS. WSUSpect представляет собой PoC-скрипт, основанный на представленных разработчиками данных во время конференции Black Hat USA 2015.

Утилита работает на Python 2.7 и может поражать ПК под управлением Windows 7 или 8, получающие обновления с сервера WSUS по незашифрованному каналу. Для того чтобы передать вредоносный файл на компьютеры жертв, необходимо, чтобы система с запущенным WSUSpect выступала в качестве прокси-сервера, к которому должны быть подключены все ПК, на которые злоумышленник планирует установить вредоносные обновления.

Для того чтобы распространять вредоносные обновления, WSUSpect использует уязвимость в Windows Update, связанную с установкой драйверов для сторонних USB-устройств. Проблема существует из-за того, что такие драйверы могут быть размещены в Windows Update без цифровой подписи Microsoft и могут быть установлены даже пользователями без соответствующих

привилегий. Злоумышленник может создать специально сформированный файл обновления и с помощью WSUSpect распространить его по всей корпоративной сети.

Единственным способом защититься от подобных атак является включение SSL-трафика для распространения обновлений по WSUS. Несмотря на то, что Microsoft рекомендует использовать SSL во всех случаях, эта опция отключена по умолчанию ***(В трафик Windows Update можно внедрять вредоносный код // InternetUA (http://internetua.com/v-trafik-Windows-Update-mojno-vnedryat-vredonosnii-kod). – 2015. – 2.11).***

***

Новые технологии могут значительно облегчить жизнь людей, но вместе с ними часто появляются новые угрозы кибербезопасности. Исследователь Р. Паап уверен, что в ближайшее время киберпреступники смогут создать DDoS-ботнеты невиданной раньше мощности, которые будут состоять из уязвимых устройств «Интернета вещей».

Эксперт сослался на отчет Verizon Data Breach Investigation Report, в котором указывалось, что в нынешнем году количество DDoS-атак увеличилось как минимум вдвое. Злоумышленники используют неверно настроенные службы наподобие NTP, DNS и SSDP, что позволяет им подменять исходные IP-адреса и отправлять огромное количество запросов на целевые серверы.

Большинство DDoS-атак в настоящее время осуществляются по устаревшему протоколу IPv4, но хакеры все чаще и чаще прибегают к IPv6. По данным CNET, относительная новизна IPv6 не позволяет провайдерам и администраторам должным образом контролировать сетевой трафик и отсеивать вредоносные пакеты. Помимо этого, гейтвеи, связывающие IPv4- и IPv6-сети, вынуждены хранить информацию об обрабатываемом ими сетевом трафике, из-за чего злоумышленникам становится проще их взломать.

«Интернет вещей» также стал привлекательным вектором осуществления DDoS-атак. Согласно отчету компании InfoSec Institute, большинство «умных» устройств для дома и малого бизнеса почти не защищены от хакерских атак. Во многих девайсах «Интернета вещей» содержатся серьезные уязвимости, а настройки безопасности по умолчанию не выдерживают никакой критики. К примеру, в некоторых устройствах используются жестко запрограммированные логины и пароли.

Р. Паап уверен, что сложившуюся ситуацию можно назвать «сценарием судного дня». Используя отсутствие полноценных средств мониторинга IPv6-трафика, слабый уровень защиты IPv4/IPv6-гейтвеев и огромное количество незащищенных устройств «Интернета вещей», злоумышленники смогут создавать DDoS-ботнеты огромных масштабов ***(Хакеры используют новые технологии для создания DDoS-ботнетов // InternetUA (http://internetua.com/hakeri-ispolzuuat-novie-tehnologii-dlya-sozdaniya-DDoS-botnetov). – 2015. – 3.11).***

***

Специалисты компании Zscaler нашли новый Android-троян, который распространяется под видом документа Microsoft Word.

Специалисты ИБ зафиксировали несколько сотен заражений, в основном, на территории Китая. Android троян с ярлыком Word Вирус маскируется под файл данных с ярлыком, похожий на тот, который используется Microsoft Word. После активации троян получает повышенные привилегии, поэтому удалит его не так просто.

Вирус проводит сканирование на наличие SMS-сообщений и другой личной информации, такой как номер IMEI, номер SIM-карты, ID устройства, контактных данных жертвы и пр. Затем вся собранная информация отправляется по e-mail или в виде текстовых сообщений на C&C-сервер злоумышленников.

После того как жертва запустит приложение, на экране появится сообщение об ошибке с предупреждением о том, что данное ПО не совместимо со смартфоном, а затем ярлык исчезает с дисплея. В то время как показывается сообщение, приложение выполняет ряд действий, в том числе отправляет SMS-сообщения на жестко закодированный номер, запускает службу MyService и два потока (SMSTask и MailTask), которые работают в фоновом режиме, а также звонит на номера, обозначенные атакующими.

Как заявил эксперт ИБ Zscaler Ш. Десаи, создатели вредоносного ПО реализовали функции, позволяющие посылать ему номера телефонов в виде SMS. Вирус перехватывает такие сообщения и звонит на указанный номер. Скорее всего, в данном случае речь идет о премиум-сервисе, причем оператор трояна получает вознаграждение за звонки. Специалист также подчеркнул угрозу конфиденциальности, поскольку SMS могут содержать не только частную переписку жертвы, но и банковские коды и коды подтверждения для других online-сервисов.

Текущая кампания была выявлена 10 октября этого года. Экспертам Zscaler удалось получить доступ к панели управления, содержащей списки похищенных данных. Стоит заметить, что за неполный месяц в результате действий злоумышленников пострадало более 300 пользователей ***(Android – троян прячется под ярлыком Microsoft Word // IT новости (http://itnovosti.org.ua/2015/11/internet/bezopastnost/android-malware-disguises-itself-as-ms-word-doc-spies-on-your-phone.html). – 2015. – 4.11).***

***

Протягом жовтня 2015 р. кількість спроб зламу ТСН.ua перевищила 33 тис., у вересні – понад 36 тис. Про це свідчить щомісячний внутрішній звіт технічного департаменту 1+1 медіа.

«Кількість атак традиційно пов’язана із ситуацією в країні. Ми вже не раз мали справу із спробами зламати наші ресурси: сайт активно атакували під час Майдану, ще один пік був, коли Росія розпочала своє вторгнення в Україну. Зараз ми пильно стежимо за місцевими виборами в Україні. Природно, що

багатьом така підвищена увага з нашої сторони не подобається. Це, на нашу думку, і є головною причиною активізації хакерів», – коментує цю ситуацію головний редактор ТСН.ua К. Войтенко.

За словами технічного директора 1+1 медіа П. Петренка, відбивати атаки вдається як завдяки найсучаснішому софту, так і за допомогою комплексу заходів безпеки, розроблених ІТ департаментом компанії: «Ми щоденно працюємо над удосконаленням системи безпеки веб-ресурсів 1+1 медіа. Для нас це питання є пріоритетним, адже увага до наших ресурсів з боку хакерів є дуже значною»

Нагадаємо, що у квітні 2015 р. ТСН.ua посів перше місце серед українських новинних сайтів за кількістю відвідувань.

Наразі, усі інтернет-ресурси 1+1 медіа продовжують безперебійну роботу та, як завжди, доступні для відвідування користувачами ***(Протягом останніх двох місяців сайт ТСН.ua намагалися зламати близько 70 тисяч разів // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/protyagom_ostannikh_dvokh_misyatsiv_sayt_tsnua_namagalisya_zlamati_blizko_70_tisyach_raziv/). – 2015. – 4.11).***

***

Появилась новая «дырка» в безопасности ОС Android. Более 100 млн устройств включает в себя приложения, которые открывают лазейку для хакеров, обеспечивая им доступ ко всем данным пользователя.

Moplus – это набор инструментов для разработчиков (SDK), подготовленный китайской компанией Baidu, которая используется в тысячах приложений на Android. К сожалению, как сообщает Trend Micro, она включает в себя восприимчивость, под названием Червоточина, которая может быть использована хакерами.

Когда приложение с упомянутой SDK устанавливается на смартфоне, автоматически открывается HTTP-сервер, который не требует проверки подлинности, принимает любой запрос и устанавливает без ведома пользователя подключение в фоновом режиме. Злоумышленник, который очень легко может найти указанный сервер, может также использовать предопределенные в SDK команды, которые позволяют выполнять несколько операций, имеющих доступ к конфиденциальной информации. Кроме того, хакеры имеют возможность установить свои приложения.

SDK Moplus можно найти в более чем 14 тыс. приложений (в том числе 4 тыс. Baidu). Они были загружены на более чем 100 млн устройств с Android. Специалисты Trend Micro утверждают, что уже существует вредоносный код ANDROIDOS_WORMHOLE.HRXA, который использует описанную уязвимость. Кроме того, отмечают, что во многих отношениях она хуже, если от уязвимость Stagefright, которая несколько месяцев назад была названа самой опасной в истории Android.

Baidu и Google были проинформированы об обнаруженной уязвимости. Китайская компания подготовила новую, безопасную версию SDK. Будем

надеяться, что разработчики будут обновлять свои приложения ***(100 миллионов пользователей Android под угрозой взлома // Новости IT (http://interteam.com.ua/100-millionov-polzovatelej-android-pod-ugrozoj-vzloma/). – 2015. – 4.11).***

***

В сентябре нынешнего года в App Store были обнаружены вредоносные программы, зараженные трояном XcodeGhost. Самая масштабная атака в истории магазина приложений Apple затронула преимущественно пользователей в Китае. Тем не менее, по данным исследователей из FireEye, новый, еще более сложный, вариант трояна инфицирует устройства пользователей в Европе и США.

Как сообщили эксперты, XCodeGhost S поражает приложения для iOS 9 и способен намного лучше обходить обнаружение инструментами статического анализа. В течение четырех недель исследователи из FireEye определили 210 предприятий на территории США, где использовались инфицированные приложения, которые в общей сложности предприняли 28 тыс. попыток связаться с C&C-серверами. Большинство зараженных систем (62 %), пытавшихся связаться с серверами, находятся в Германии. Вторую позицию занимают США (33 %).

По словам экспертов, XCodeGhost S использовался параллельно с оригинальным XcodeGhost, и за их созданием стоит один и тот же автор. Однако не исключено, что за теперешнюю активность трояна ответственны другие. Как сообщает издание Dark Reading, 19 сентября, через два дня после того как стало известно о XCodeGhost, неизвестный опубликовал в Twitter извинение за распространение вредоноса. Он заявил, что это был всего лишь эксперимент в ходе исследования потенциальных брешей в инструменте XCode, которые можно было бы использовать для доставки рекламы.

ИБ-эксперт из ThreatBook Labs X. Цзя сообщила Dark Reading, что не верит в правдивость этого извинения, поскольку возможности трояна обходить инструменты обнаружения намного шире, чем об этом говорил неизвестный.

В отличие от оригинального XCodeGhost, XCodeGhost S способен обходить обнаружение инструментами статического анализа с помощью конкатенации символов, что существенно усложняет процесс поиска инфицированных приложений. До настоящего времени исследователи обнаружили только две зараженные программы, но в действительности их может быть гораздо больше ***(Обнаружен новый вариант трояна XcodeGhost // InternetUA (http://internetua.com/obnarujen-novii-variant-troyana-XcodeGhost). – 2015. – 6.11).***

***

Группа хакеров Anonymous распространила в социальных сетях список из тысячи имен предполагаемых членов Ку-клукс-клана (ККК) или сочувствующих этой организации. Об этом 6 ноября сообщает BBC.

В список включены владельцы аккаунтов в соцсетях Facebook и Google+, которые присоединялись или лайкали связанные с ККК группы в соцсетях. В сопроводительной информации отмечается, что перечень фамилий получен не путем взлома, а путем аналитической работы.

«Люди в этом списке проверены через открытые (интервью экспертов) и негласные (цифровой шпионаж) методы», – утверждают хакеры.

Публикация списка является ответным ходом Anonymous на угрозы со стороны ККК участникам акций протеста в городе Фергюсон, которые прошли после убийства чернокожего подростка белым полицейским. «Мы никогда не забудем ваши угрозы жителям Фергюсона, и мы никогда не простим вас», – говорится в заявлении группы хакеров Anonymous.

В 2012 г. Anonymous распространили имена и личные данные людей, которые, по мнению хакеров, были причастны к сокрытию изнасилования 16-летней девушки в Огайо. В начале лета 2015 г. группа заблокировала сайт Королевской канадской полиции после того, как один из офицеров застрелил демонстранта в маске.

Группа хакеров стала известной, когда пообещала отомстить за теракт в редакции Charlie Hebdo, а после этого объявила войну «Исламскому государству» ***(Хакеры распространили в интернете список тысячи сторонников Ку-клукс-клана // InternetUA (http://internetua.com/hakeri-rasprostranili-v-internete-spisok-tisyacsi-storonnikov-ku-kluks-klana). – 2015. – 6.11).***

***

За последний год количество вредоносных программ под Mac OS X в пять раз превысило их число за предыдущие пять лет. Такая ситуация вызвана ростом популярности мобильных гаджетов и компьютеров Apple и увеличением использования в офисах персональных устройств, принесенных из дома. Это может привести к росту количества атак на средние и крупные компании и возрастанию ущерба, наносимого хакерами.

В период с 2010 по 2014 г. количество разновидностей вредоносного программного обеспечения, выявленного специалистами по кибербезопасности, составило 180 единиц. При этом только с начала 2015 г. уже выявлено 948 типов вирусов и троянов для Mac OS X, говорится в исследовании Bit9 + Carbon Black.

Исследователи проанализировали 1,4 тыс. образцов вредоносного программного обеспечения для Mac OS X и выяснили, что разработчики вирусов все реже используют общие методы проникновения в систему, характерные для UNIX-систем, и все больше фокусируются на изучении индивидуальных особенностей и механизмов операционной системы Apple. Это упрощает разработку вирусов и требует от хакеров меньшей «изощренности». Несмотря на большое разнообразие вредоносных программ для Mac OS X, их механизмы сводятся всего лишь к семи методам, позволяющим вирусу остаться активным в системе. В большинстве случаев это

модификация настроек учетной записи пользователя для включения вируса в список программ, загружаемых при входе в профиль.

«“Маки”, по большому счету, до недавнего времени игнорировались киберпреступниками, – говорит ведущий исследователь киберугроз Bit9 + Carbon Black Майк Сконзо. – Однако признаки формирования преступного рынка в сегменте OS X налицо, и количество вредоносных программ для этой платформы будет стремительно возрастать уже в ближайшие месяцы».

При этом распространение платформы Apple Mac будет возрастать в том числе благодаря популярности смартфонов и других гаджетов Apple и тому, что компания уже создала единую экосистему, объединяющую все устройства и сервисы пользователя в единый продукт, а конкуренты в лице Microsoft и Google только работают в этом направлении. Этому способствует также традиционно высокое внимание Apple к пользовательскому опыту.

С учетом повсеместного распространения концепции BYOD (Bring Your Own Device), когда сотрудник приносит на работу и использует свой персональный ноутбук, к обеспечению компьютерной безопасности в компаниях будут предъявлены новые требования, а сотрудники соответствующих подразделений столкнутся с новыми угрозами со стороны платформы Apple Mac.

Во многом это будет связано с тем, что сами пользователи «маков» все еще считают их безопасными. «В силу того, что пользователи считают Mac защищенным от вирусов и кибератак, компании и частные владельцы окажутся не в состоянии своевременно внедрить на OS X те средства защиты, которые применяют на платформе Windows, – считает Сконзо. – И так как количество угроз растет, а разрыв в обеспечении безопасности сохраняется, многие организации и потребители не смогут выявить и остановить заражения».

Руководитель аналитического центра компании Zecurion В. Ульянов считает, что тенденции с безопасностью Mac OS X во многом напоминают аналогичную ситуацию с антивирусной защитой смартфонов в 2010 г.

Тогда антивирус для мобильных платформ был не нужен – заражение смартфонов было редкостью. Сейчас же iOS и Android – очень распространены, и риски пользователей стали выше, так как каждый второй пользователь сейчас привязывает к гаджету онлайн-банк и автоплатежи, и к нему надо относиться как к пластиковой банковской карте. Этот рынок очень легко монетизировать преступным путем, чем и вызвана плачевная ситуация с вирусами для Android.

«Mac все больше распространяется в корпоративной среде, – говорит В. Ульянов. – Поэтому риски растут, но я не вижу проблем с тем, чтобы отделы кибербезопасности быстро перестроились и начали ставить антивирусы сотрудникам на OS X – соответствующие продукты на рынке есть».

Эксперт уверен, что на пользователя возлагать задачу по обеспечению безопасности своего рабочего места нельзя. «Да, надо проводить разъяснительную работу, но сам переход с платформы на платформу – это тяжелая задача для неподготовленного потребителя, – говорит В. Ульянов. – Поэтому обеспечение киберзащиты должны взять на себя офицеры службы

информационной безопасности. По крайней мере, такая служба должна быть в каждой компании, особенно в крупных».

Также эксперт говорит о росте использования социальной инженерии для заражения Mac-платформы. За последние два года наблюдается существенный рост подобных атак, которые будут весьма эффективны в свете низкой защиты OS X.

Растет количество векторов кибератак, и Mac, как и любое приносимое устройство, добавляет еще один вектор в их список. Платформа Apple может стать даже не целью сама по себе, а плацдармом для заражения корпоративных сетей, что может привести к гораздо более значительной выгоде для киберпреступников и куда более существенному вреду для бизнеса ***(Вирусы на Apple угрожают офисам // InternetUA (http://internetua.com/virusi-na-Apple-ugrojauat-ofisam). – 2015. – 6.11).***

***

Хакеры «Исламского государства» из группы «КиберХалифат» взломали 54 тыс. аккаунтов в Twitter и разместили телефоны глав ЦРУ и ФБР, пишет The Daily Mail.

В сообщении говорится, что таким образом хакеры мстят за убийство своего лидера британского подданного Д. Хуссейна.

Как отмечается, большинство подвергшихся взлому аккаунтов зарегистрированы в Саудовской Аравии, но среди них также есть и британские ***(Хакеры ИГ взломали 54 тысячи аккаунтов в Twitter и разместили телефоны глав ЦРУ и ФБР // InternetUA (http://internetua.com/hakeri-ig-vzlomali-54-tisyacsi-akkauntov-v-Twitter-i-razmestili-telefoni-glav-cru-i-fbr). – 2015. – 8.11).***

***

Что делать, если вы стали жертвой кибермошенников?

На тот случай, если вы стали жертвой утечки информации, но пока не готовы явить миру все ваши секреты – ряд советов, подготовленных аналитическим центром SearchInform.

Электронный почтовый ящик. Один из самых излюбленных хакерами объектов для взлома – почтовые ящики. Пользователями, к сожалению, зачастую недооценивается взлом электронной почты. Однако именно к электронному почтовому ящику, как правило, привязаны многие службы: онлайн-банки, учетная запись в социальной сети, аккаунт в онлайн-игре и прочее.

Если вы стали жертвой утечки информации и вашу электронную почту «хакнули», первым делом просканируйте компьютер антивирусной программой: очень часто взламывают почту именно вирусы или вредоносные программы, попавшие на компьютер. Затем зайдите в свой аккаунт, постарайтесь изменить пароль. Если не получается сделать это самостоятельно, попробуйте обратиться в службу поддержки.

Что делать, если взломали электронный ящик иностранных почтовых служб (Яндекс, Google, Bing, Baidu, Rambler, Mail.Ru и др.)? Если у вас нет возможности зайти в почту по старому паролю, нажмите на опцию «забыл пароль». Вы попадете на страницу авторизации, где вам придется указать все данные о своем почтовом ящике, правильно вписать в поле указанный текст и перейти дальше. Затем необходимо будет указать резервный почтовый ящик или мобильный номер, который вы указывали при регистрации. Можно сделать попытку обращения в службу поддержки. Сервис Google заранее предупреждает своих пользователей о попытке взлома ящика – не пренебрегайте такими сообщениями. Если возможности электронной почты позволяют, установите опцию «показывать последний вход». Если Вы увидите, что вход был выполнен под другим IP-адресом, лучше смените пароль входа.

Аккаунт смартфона Apple/Google/Windows. На смартфонах, вне зависимости от производителя и рабочей операционной системы, как правило, хранится самая нужная информация: контакты, фотографии, пароли, открытые учетные записи в социальных сетях, рабочая и личная почта, привязка к банкам и прочее. Взлом аккаунта чреват не только обнародованием всей этой информации и потерей денежных средств – вы рискуете потерять контроль над всем, что происходит с вашим смартфоном, и стать дистанционно управляемой игрушкой в чужих хакерских руках.

iOS. Техника Apple, в силу своей популярности, давно стала интересна хакерам и мошенникам. Он легко управляется дистанционно при условии, что хакеру известны ваши логин и пароль, а их, как описывалось ранее, не так уж и сложно заполучить. Если вы вдруг поняли, что с вашим iPhone творятся «странные вещи» и антивирусная чистка не помогает, придётся стереть все данные. Благо, такая функция присутствует. Она полностью удалит все ваши данные на устройстве, чтобы они никоим образом не смогли попасть к злоумышленникам. Есть минус: этими данными впредь не воспользуетесь и вы. Но поверьте, это намного лучше, чем потерять средства и управление над мобильным устройством. Если вы не уверены в том, что аккаунт беспощадно взломан, а данные терять очень не хочется – обратитесь в сервисный центр.

Android. В операционной системе этого смартфона есть встроенный инструмент под названием Android Device Manager (Диспетчер устройства), как правило, привязанный к учетной записи Google. Дистанционно управлять устройством можно с любого компьютера с доступом в Интернет – это не очень хорошо, если вас хакнули. Хакер может даже заблокировать дисплей вашего смартфона или изменить графический пароль. В этом случае вы так же дистанционно можете стереть все данные с устройства – эта функция сбрасывает все настройки на заводские. При этом внутренняя память телефона будет стерта. Правда, информация, находящаяся на отдельной карте SD (в последних версиях Android) останется в целости и сохранности.

Windows Phone. Чтобы помочь смартфону справиться с несанкционированным проникновением, придётся зайти на сайт сервиса

Windows Phone, где можно воспользоваться функцией «Очистить». Настройки будут сброшены на заводские, и всё придётся начинать и создавать с нуля.

Подобные взломы аккаунтов смартфонов становятся популярными не только благодаря целенаправленным хакерским атакам. Часто пользователи невнимательны, и по собственной воле попадаются на уловки хакеров из-за особенностей мобильных устройств. Те же фишинговые сайты в смартфоне кажутся «не такими уж кривыми», а скачиваемые в сети программы для смартфонов – вполне безобидными. Работая в сети посредством мобильного устройства, будьте внимательны. Не скачивайте непроверенные программы, особенно осторожно относитесь к файлам-архивам и файлам с расширением .exe. При малейшем подозрении удаляйте скачанный файл, не открывая его, и запускайте антивирус.

Социальные сети. Два года назад одна из самых известных российских социальных сетей «ВКонтакте» была взломана. Тогда хакерам удалось завладеть списками пользователей и паролями более 100 тыс. человек. Данные были опубликованы и долгое время находились в открытом доступе на одном из хакерских сайтов. А это значит, что абсолютно любой человек мог заходить в чужие аккаунты и делать с ними все, что его душе угодно: менять пароли, рассылать спам от имени пользователя и много других гадостей. Столь серьезная утечка информации стала результатом создания хакерами приложения, содержащего в себе достаточно примитивную троянскую программу. Они распространили его с помощью спам-рассылки среди пользователей и те, кто устанавливал у себя это приложение, получал вместе с ним и вирус, считывавший пароль и логин. И подобные ситуации время от времени случаются с абсолютно различными социальными платформами, включая «Одноклассники», Facebook или Pinterest.

Что же делать, если ваш аккаунт в социальной сети взломан? Необходимо почистить файлы hosts. Если в них обнаружены ссылки на вашу социальную сеть – удалите их. Кроме того, необходимо устроить полную антивирусную проверку компьютера. Ну и, конечно, смените пароль и впредь будьте внимательны. Не реагируйте на спам-рассылки, даже если они приходят от друзей. Нельзя открывать подозрительные приложения (не только предлагающие просмотр каких-то эротических фотографий, но и, к примеру, выдающие себя за бесплатный сервис). Как можно быстрее примите все меры, чтобы обезопасить вашу учетную запись. Там, где это возможно, включите смс-уведомление об изменениях вашего профиля. Привязка к телефону надежнее секретного вопроса. Она позволит вам получать смс-сообщения обо всех глобальных манипуляциях на вашей странице, таких, например, как смена пароля. Кроме того, вы сможете легко восстановить доступ к ней в случае потери пароля или повторного взлома.

Данные банковских карт и паспорта. В этом году, как пример, более 10 тыс. белорусов получили фальшивые уведомления о блокировке кредиток. Мошенники просили прислать свой номер карты якобы для ее разблокировки. Банально и просто, но, к сожалению, многие «повелись» – и стали жертвами

своей собственной доверчивости. Мы наслышаны о киберпреступлениях, но никогда не предполагаем, что это может случиться с нами. Напрасно. Тем более, если, став жертвой утечки информации, вы рискуете потерять ваши сбережения, а не только фотографии вашего класса из 90-х на фоне школьной доски.

В настоящее время на просторах глобальной сети широко распространён фишинг. Как это работает? Система чуть сложнее, чем описанная выше: хакерами создаются в сети Интернет копии сайтов, например, банковского учреждения. Рассылаются рекламные сообщения с завлекающим текстом (оформить заявку на кредит онлайн, получить карту рассрочки), пользователи заходят на сайты-ловушки и беспечно оставляют там свои реквизиты (пин-код, номер счета), данные паспорта, адрес. Понятное дело, в скором времени их банковские счета пустеют. Явление, на самом деле, не такое уж новое. Самой первой попыткой подобного кибермошенничества стала хакерская атака на платёжную систему e-gold в июне 2001 г. Но тогда это был лишь эксперимент. Сейчас фишинг представляет большую угрозу, как для пользователей, так и для компаний.

Основной метод фишинга – поддельный сайт или ссылка на сайт, который замаскирован под настоящий. Для этого, чаще всего, используются субдомены (в адресной строке сайта вы увидите опечатку). Например, twiter.com очень похож на адрес социальной платформы Twitter, но в действительности, это – фишинговый сайт. Ещё одна популярная уловка – использование внешне правильных ссылок, которые в реальности привязаны не к оригинальным, а к фишинговым сайтам. Например, ссылка http://www.google.com@members.tripod.com/ приведёт не на www.google.com, а на members.tripod.com от имени пользователя www.google.com.

Казалось бы, следует быть внимательным и периодически смотреть на адресную строку? Безусловно, но в последние годы хакеры научились обходить и эту маленькую подсказку для пользователей: с помощью JavaScript можно изменить адресную строку. Например, разместить картинку с фальшивым URL поверх адресной строки. Существует масса методов фишинга, в том числе и межсайтовый (в 2006 г. по этой причине рухнула система PayPal), с более совершенными маскировками, голосовыми инструкциями и даже поддержкой телефонных операторов. Чтобы не стать жертвой утечки информации и не попасться на уловки хакеров, никому и никогда не сообщайте полный номер банковской карты, паспортные данные и пин-код.

Итак, если вы всё-таки попались на удочку мошенников и данные вашей карты стали известны не только вам, немедленно обратитесь в банк-эмитент карты (банк, выпустивший карточку) и заблокируйте её, а ещё лучше – перевыпустите. Для интернет-покупок заведите отдельную карту (с ограниченной суммой денежных средств), предназначенную для покупок в сети. В банке подключите услугу «смс-информирование». По любой операции из банка будет приходить смс-сообщение на ваш мобильный телефон, что

позволит контролировать операции в онлайне. Такую услугу предоставляют фактически все крупные банки.

К счастью или к сожалению, в современном мире невозможно отказаться от высоких технологий. Желая идти в ногу со временем, мы внедряем новейшие разработки в свою жизнь. В наших силах сделать безопасной эту интеграцию, защитить себя от мошенничества и киберпреступлений ***(Что делать, если вы стали жертвой кибермошенников? // InternetUA (http://internetua.com/cto-delat--esli-vi-stali-jertvoi-kibermoshennikov). – 2015. – 8.11).***

***

ИБ-компания «Лаборатория Касперского» опубликовала отчет за III квартал 2015 г., иллюстрирующий основные направления развития в сфере DDoS-атак и инструментов для их осуществления. По данным экспертов, доля DDoS-атак с ботнетов на базе ОС Linux в III квартале 2015 г. составила 45,6 %.

В своей публикации эксперты ЛК ссылаются на отчет компании Akamai Technologies, согласно которому в III квартале был зафиксирован рост мощностей ботнета XOR DDoS, состоящего из Linux-компьютеров, жертвами которого стали преимущественно азиатские сайты образовательных учреждений и игровых сообществ. Особенностью этого ботнета является применение XOR-шифрования как в самой вредоносной программе, так и для взаимодействия с C&C-серверами.

ОС Linux чаще всего используется в качестве серверной операционной системы. Это означает, что у сервера также имеются канальные и вычислительные ресурсы, которые злоумышленники могут применять для осуществления DDoS-атак.

В III квартале более половины атак пришлось на SYN-DDoS (51,7 % всех атак), доля TCP-DDoS составила 16,4 %, HTTP-DDoS – 14,9 %. На четвертое место поднялся метод ICMP-DDoS, чей показатель за два последних квартала увеличился в более чем два раза и составил 5,1 %.

Специалисты ЛК привели статистические данные, согласно которым в III квартале нынешнего года DDoS-атакам подвергались мишени, расположенные в 79 странах мира. При этом 91,6 % атакованных ресурсов были размещены на территориях всего 10 стран. В рейтинге стран по количеству атакованных уникальных ресурсов по-прежнему лидирует Китай, где в III квартале были расположены 34,5 % мишеней DDoS-атак, что на 4,6 % больше, чем в предыдущем квартале. Второе место удерживают США с показателем в 20,8 %. На третьем месте осталась Республика Корея с результатом 17,7 %. Россия разместилась на четвертом месте (5,3 %).

Отмечается, что в десятке появился новичок в лице Японии, на которую пришлось 1,3 % всех атакованных ресурсов, а также вернулись Нидерланды (1,1 %). В этот раз в топ 10 не фигурируют Германия (1 %) и Гонконг (0,9 %).

Что интересно, Китай, США и Южная Корея являются лидерами как по количеству атак, так и по числу их жертв. Предполагается, что такое

бессменное лидерство обусловлено дешевизной веб-хостинга в этих странах ***(В 3 квартале в 45,6 % DDoS-атак использовались Linux-боты // InternetUA (http://internetua.com/v-3-kvartale-v-45-6--DDoS-atak-ispolzovalis-Linux-boti). – 2015. – 8.11).***

***

Новый Android-троян поселяется настолько глубоко в системе, что его становится практически невозможно удалить. В некоторых случаях пользователи вынуждены менять устройство на новое.

Новый вид

Аналитики антивирусной компании Lookout обнаружили новый вид вредоносного программного обеспечения для Android, которое поселяется глубоко в устройстве так, что в некоторых случаях, чтобы избавиться от него, единственным выходом является замена смартфона.

Принцип действия

Новый вредоносный софт объединяет в себе функции трояна и рекламного приложения (adware). После того он попадает на мобильное устройство, он самостоятельно выполняет рутинг (получает права на полный доступ к системе), используя любую из известных уязвимостей в платформе, и затем выполняет установку вредоносного кода как системного приложения.

«После таких действий удалить вредоносный софт практически невозможно. Как правило, желание избавиться от него, ведет жертву к покупке нового устройства, если он не знает, как его вылечить или не обращается к специалисту для решения этой задачи», – сообщили представители Lookout в блоге компании. Аналитики добавили, что сброс к заводским настройкам не позволяет удалить троян.

Что делает вредоносный софт

Вредоносный софт нового типа, так как содержит в себе функции трояна, позволяет злоумышленникам получать доступ к персональным данным, а рекламная функциональность – отображать рекламные объявления по мере того, как жертва пользуется устройством, и зарабатывать на этом деньги.

Как он попадает на устройство

Авторы нового софта распространяют его через сторонние магазины приложений для Android. Они берут из Google Play популярные программы, например, Facebook, Snapchat и Twitter, и перепаковывают их, внедряя вредоносный код. Таким образом, приложение продолжает обладать функциональностью, которую пользователь от нее ожидает.

Владелец мобильного устройства загружает с неофициального каталога Android-приложений, например, клиент Facebook и начинает им пользоваться, ни о чем не подозревая. Приложение с внедренным в него вредоносным кодом, выполняет рутинг системы и надежно поселяется в ней в виде системного приложения.

Разновидности вредоносного софта

За последний год аналитики изучили три семейства комбинированных вредоносных приложений. Первое из них называется Shuanet. Приложения этого семейства самостоятельно выполняют рутинг и скрываются в системной папке. Второе семейство – Kemoge (или ShiftyBug). Его представители также выполняют рутинг, после чего устанавливают в систему дополнительные компоненты. И, наконец, третье семейство – Shedun (также известное как GhostPush). Многие классифицируют эти приложения как рекламные, однако они также являются троянами. Эксперты не считают, что указанные семейства вредоносных программ были разработаны одной командой хакеров.

Масштаб заражения

Аналитики Lookout обнаружили на просторах Интернета свыше 20 тыс. образцов поддельных приложений с внедренных в них вредоносным кодом описанного действия. Были найдены поддельные модификации следующих популярных приложений, помимо упомянутых выше: Candy Crush, Google Now, New York Times, Okta и WhatsApp.

Наибольшее количество случаев заражения было зафиксировано в США, Германии, Иране, России, Индии, Ямайке, Судане, Бразилии, Мексике и Индонезии.

В официальном каталоге Google Play эксперты не нашли аналогичных подделок ***(Новый троян заставляет владельцев менять Android-устройства // InternetUA (http://internetua.com/novii-troyan-zastavlyaet-vladelcev-menyat-Android-ustroistva). – 2015. – 7.11).***

***

Специалисты компании Duo Security обнаружили способ обхода специализированного ПО Microsoft EMET, предназначенного для предотвращения атак на оперативную память. Обойти EMET возможно путем эксплуатации ошибки в подсистеме WoW64 – компоненте ОС Windows, позволяющем запускать 32-битные приложения на 64-битных версиях операционной системы.

Для того чтобы выполнить обход ограничений безопасности, исследователи использовали модифицированную версию эксплоита для уязвимости использования после высвобождения в Adobe Flash. В своем блоге эксперты отметили, что под управлением WoW64 32-битные приложения работают иначе, чем на нативных 32-битных системах. Эксплуатация уязвимости возможна во время переключения процессора между разными режимами в ходе исполнения программы.

Подсистема WoW64 значительно затрудняет вызов низкоуровневых функций для защитного ПО из пространства пользователя, что является одним из самых важных ограничений подсистемы. В Windows отсутствует «официальный» механизм для интеграции 64-битных модулей в 32-битные процессы, и значительная часть функционала API, контролируемого EMET, реализована в отдельной 64-битной копии ntdll.dll.

По версии исследователей, злоумышленник может перевести процессор в длительный режим, после чего определить размещение 64-битных модулей и их функций и обойти ограничения 64-битных API. Это позволит ему миновать используемые защитным ПО хуки. EMET привязан к ntdll.dll – библиотеке, обеспечивающей используемые приложениями низкоуровневые функции. По свидетельству Duo Security, в 64-битной версии библиотеки отсутствуют хуки в необходимых местах.

Эксперты отметили, что исправить ситуацию возможно лишь в случае внесения значительных архитектурных правок в часть Windows, отвечающую за поддержку устаревшего ПО. Поскольку это может привести к значительным проблемам с совместимостью, Microsoft вряд ли решится на столь радикальные шаги. Тем не менее, специалисты передали компании все материалы исследования и функциональный эксплоит ***(Обнаружен способ обхода EMET на 64-битных системах // InternetUA (http://internetua.com/obnarujen-sposob-obhoda-EMET-na-64-bitnih-sistemah). – 2015. – 7.11).***

***

«Доктор Веб» предупреждает о появлении новой вредоносной программы, способной инфицировать компьютеры под управлением операционных систем Linux.

Зловред Linux.Encoder.1 предназначен для шифрования файлом с целью последующего получения выкупа за восстановление доступа к ним. Причём выбор каталогов кодирования данных позволяет предположить, что главная мишень вирусописателей – администраторы сайтов, на машине которых развёрнут собственный веб-сервер.

После запуска с правами администратора троян загружает файлы с требованиями злоумышленников и файл, содержащий путь до публичного RSA-ключа, после чего запускает себя как демон и удаляет исходные файлы. Данный RSA-ключ в дальнейшем используется для хранения AES-ключей, с помощью которых троян шифрует файлы на заражённом компьютере.

Зловред прежде всего кодирует все файлы в домашних каталогах пользователей и каталогах, относящихся к администрированию веб-сайтов. После этого вредоносная программа рекурсивно обходит всю файловую систему. При этом шифруются файлы с расширениями из заданного списка и только при условии, что имя каталога начинается с одной из заданных вирусописателями строк.

Для восстановления доступа к закодированным данным жертве предлагается оплатить расшифровку с помощью криптовалюты Bitcoin. Стоимость процедуры составляет несколько сотен долларов США ***(Новый троян-шифровальщик атакует Linux-пользователей // InternetUA (http://internetua.com/novii-troyan-shifrovalsxik-atakuet-Linux-polzovatelei). – 2015. – 9.11).***

***

Люди стали больше обеспокоены хакерскими атаками, нежели реальными. К такому выводу пришла компания Citrix, которая опросила 2 тыс. британцев касательно виртуальных и реальных угроз.

Согласно результатам опроса, 48 % молодых людей в возрасте от 16 до 24 лет хранят свои секреты на персональных компьютерах, а 45 % респондентов испытывают перед хакерами больший страх, нежели перед реальными взломщиками. Среди лиц в возрасте от 55 лет доля обеспокоенных виртуальными угрозами составляет только 16 %.

Оказалось также, что четверть молодых людей хранят все свои пароли в одном файле на компьютере или мобильном устройстве, что существенно упрощает работу хакерам ***(Хакеры сравнялись с домушниками по уровню угрозы // InternetUA (http://internetua.com/hakeri-sravnyalis-s-domushnikami-po-urovnua-ugrozi). – 2015. – 9.11).***

***

Злоумышленники похитили базу данных пользователей приложения Touchnote. Программа разработана для того, чтобы создавать открытки из снятых на камеру мобильного устройства фото. Приложение предустановлено на миллионах смартфонов и является весьма популярным среди пользователей. Более 4 млн открыток было отправлено через Touchnote, начиная с 2008 г.

Представители Touchnote уже отправили пользователям электронные письма с сообщением о случившемся инциденте. В числе скомпрометированных данных – имена, адреса электронной почты и домашние адреса. Также в руках злоумышленников оказались последние четыре цифры банковских карт пользователей. Точное количество пострадавших пока неизвестно.

Несмотря на то что Touchnote хранит пароли пользователей в зашифрованном виде, представители компании рекомендуют поменять их ***(Хакеры похитили данные пользователей Touchnote // InternetUA (http://internetua.com/hakeri-pohitili-dannie-polzovatelei-Touchnote). – 2015. – 10.11).***

***

Исследователи немецкой компании Botfrei обнаружили новый образец мошеннического ПО, который они назвали Chimera. Chimera распространяется через письма электронной почты, которые содержат ссылки на веб-страницу Dropbox.

Об этом ИА «МОСТ-ДНЕПР» сообщили в пресс-службе Департамента киберполиции Национальной полиции Украины.

«После того как жертва перешла по ссылке и загрузила Chimera, файлы на компьютере и сетевых дисках шифруются и требуется выкуп за расшифровку в размере 2,45 биткоинов (около 694 дол.). В отличие от других видов грабительских ПО, пользователь предупреждается о том, что в случае

неуплаты его данные будут опубликованы в Интернете. Тем не менее, эксперты уверены, что эти угрозы – не более чем блеф, целью которых является устрашение жертв», – передает пресс-служба киберполиции.

«Не существует никаких доказательств или информации о том, что преступники похитили данные, хранящиеся на системах жертв, или эта информация была опубликована в Интернете», – сообщают исследователи.

Теоретически, авторы Chimera могли бы найти способ похитить данные, а затем выложить их в сеть. Тем не менее, это было бы непрактично, поскольку, таким образом, они оставили бы слишком много зацепок, которые позволили бы выследить их. Кроме того, им придется создать большое хранилище данных, что также не оправдывает себя ***(В Украине появилось мошенническое ПО, которое вымогает деньги у пользователей // InternetUA (http://internetua.com/v-ukraine-poyavilos-moshennicseskoe-po--kotoroe-vimogaet-dengi-u-polzovatelei). – 2015. – 10.11).***

***

Специалисты компаний Heimdal Security и BitDefender обнаружили новую, более скрытную версию программы-вымогателя CryptoWall. На просторах Интернета предыдущая версия CryptoWall 3.0 появилась в январе этого года и, по данным организации Cyber Threat Alliance, ее жертвами стали десятки тысяч пользователей по всему миру. По предварительным оценкам, ущерб от активности вредоноса составил 325 млн дол. Предполагается, что CryptoWall 4.0 превзойдет результат своего предшественника.

Как утверждают эксперты Heimdal Security, в последней версии CryptoWall реализованы модификации, позволяющие ей избегать обнаружения антивирусами, включая межсетевые экраны нового поколения. CryptoWall 4.0 зашифровывает не только сами файлы, но также их имена. Новая техника увеличивает замешательство пользователей, тем самым повышая шансы на быструю выплату выкупа.

Новый вариант CryptoWall выводит на экран сообщение, отличающееся от уведомлений, отображающихся предыдущими версиями вымогателя, призванных обеспокоить и взволновать жертву. Как поясняют аналитики BitDefender, новое сообщение с требованием выкупа «более длинное, менее тревожное и даже содержит долю иронии».

Так же как и предыдущие версии, CryptoWall 4.0 использует анонимную сеть TOR для отправки жертвам инструкций по выплате выкупа, а также по аналогии с CryptoWall 3.0 подключается к ряду скомпрометированных веб-сайтов для загрузки полезной нагрузки на целевую систему. Распространяется вредонос посредством атак drive-by и спам-рассылки, которые по-прежнему остаются самыми распространенными векторами атак.

Авторы CryptoWall действуют, как владельцы компаний-производителей ПО – постоянно совершенствуют код, модифицируют механизмы для обхода средств защиты, а также используют все доступные методы социальной инженерии для обеспечения выплаты требуемого выкупа, отмечают

исследователи Heimdal Security ***(Обнаружен новый вариант вымогателя CryptoWall // InternetUA (http://internetua.com/obnarujen-novii-variant-vimogatelya-CryptoWall). – 2015. – 9.11).***

***

Украинские хакеры заблокировали сепаратистские сайты dnrpress.ru и novorossia.tv. Об этом на своей странице в Facebook сообщил программист Е. Докукин.

«Украинские кибервойска заблокировали сайты террористов dnrpress.ru и novorossia.tv. Операция “Возмездие” продолжается. Также работаем над другими сайтами. Всего заблокировали 130 сайтов террористов», – написал он ***(Возмездие по-украински: хакеры взломали 2 сайта террористов // Обозреватель (http://obozrevatel.com/society/10659-vozmezdie-po-ukrainski-hakeryi-vzlomali-2-sajta-terroristov.htm). – 2015. – 9.11).***

***

Будь-яка людина може дізнатися, що за незнайомець дзвонив йому по телефону, ввівши його номер у поле пошуку на Facebook

Про це пише Еспресо.TV із посиланням на tjournal.

Хоча ця можливість не нова, 9 листопада на неї звернули увагу відразу кілька користувачів соцмережі.

«Познайомтеся тепер з новим способом перевірки дзвінка з будь-якого невідомого телефону. Просто вбийте номер у верхньому вікні пошуку», – написала письменник і ресторатор І. Тундра. Судячи з коментарів її друзів і передплатників, багато не знали про таку функцію.

За словами доцента факультету гуманітарних НДУ ВШЕ О. Глухова, він прив’язав свій номер після того, як про це його попросила сама соціальна мережа. З’явилися й інші скарги. «Я додав телефон заради якихось опцій аутентифікації, але передбачливо закрив його в профілі. Насолоджувався приватним життям, поки одна добра людина не ввела мій номер в пошуковий рядок зверху. Facebook видав мене з усіма потрохами» – сказав О. Глухов, доцент факультету гуманітарних НДУ ВШЕ.

Судячи по форуму підтримки Facebook, користувачі вже спантеличувалися питанням видалення свого номера із соцмережі і прив’язкою електронної пошти на випадок втрати доступу. Однак деякі з них скаржилися, що одного разу «засвічений» номер неможливо використати в іншому обліковому записі.

Перевірка TJ показала, що насправді знайти людину на Facebook за номером телефону можна, якщо він пов’язаний із профілем. Уникнути цього неможливо: єдине, що може зробити користувач, це поміняти рівень приватності – замість доступного для всіх переключитися на «Тільки для друзів і друзів друзів» або «Тільки для друзів». При цьому за умовчанням включений саме перший варіант, при якому знайти людину за номером може будь-яка людина.

Повністю уникнути «пробивання» за номером телефону можна тільки тоді, коли він буде відв'язаний від акаунта через налаштування. Однак у цьому випадку людина не зможе ні ввійти за цим номером, ні отримати на нього повідомлення про скиданні пароля і коди доступу – хоча Facebook поступово переводить користувачів на використання мобільних додатків для цих цілей.

Головну проблему тут становить спеціалізоване меню приватності, яке у Facebook винесено на верхню панель. У списку з трьох пунктів користувачеві пропонується перевірити, з ким він хоче ділитися своїми телефонами – там можна вибрати опцію «Тільки з самим собою», проте мова йде про відображення номера в профілі, а не про функції пошуку.

Схожа функціональність є у Twitter: у налаштуваннях конфіденційності сервісу мікроблога можна вказати «Мене можна знайти за адресою електронної пошти», проте прямий запит у вікні пошуку не видає відповідний акаунт користувача ***(Користувачі Facebook звернули увагу на можливість «пробивати» номери незнайомих людей // Espreso.tv (http://espreso.tv/news/2015/11/10/korystuvachi_facebook_zvernuly_uvagu_na_mozhlyvist_quotprobyvatyquot_nomery_neznayomykh_lyudey). – 2015. – 10.11).***

***

Исследователь Н. Скотт обнаружил вариант программы-вымогателя Power Worm, который случайно уничтожает файлы жертвы в процессе шифрования из-за ошибки в программировании. Впервые Power Worm был обнаружен специалистами ИБ-компании Trend Micro в марте 2014 г. в ходе анализа вредоносной кампании, нацеленной на документы в форматах Microsoft Word и Excel.

Данный вариант вымогательского ПО атакует широкий спектр типов файлов, однако это не единственная «особенность», которая выделяет его среди подобного рода вредоносов. Как поясняет Скотт, отличие заключается в некорректно реализованном процессе шифрования, с помощью которого автор вредоноса попытался упростить шифрование и сократить эксплуатационные расходы. По словам исследователя, разработчик внедрил криптографический модуль с поддержкой алгоритма AES, однако вместо сгенерированных случайным образом ключей намеревался использовать статический AES-ключ, одинаковый для каждого пользователя.

Проблема заключается в том, пишет интернет-портал Bleeping Computer, что в результате программной ошибки вымогатель начал генерировать случайные ключи для дешифровки вместо статических. Поскольку автор не предусмотрел специальный сценарий для обработки и хранения сгенерированных случайным образом ключей, программа шифровала файлы, а затем удаляла ключ для дешифрования. Таким образом, жертвы вредоноса могли восстановить свои файлы, только воспользовавшись их резервными копиями ***(Вымогатель Power Worm случайно уничтожает файлы в процессе шифрования // InternetUA (http://internetua.com/vimogatel-Power-Worm-slucsaino-unicstojaet-faili-v-processe-shifrovaniya). – 2015. – 10.11).***

***

Мобильные приложения для Android и iOS передают большие объемы пользовательских данных третьим сторонам. К такому выводу пришли исследователи из Массачусетского технологического института, Гарвардского университета и Университета Карнеги – Меллон, проанализировав 110 приложений из Google Play и Apple App Store.

По данным экспертов, 73 % Android-приложений передают третьим сторонам электронные адреса пользователей, и 47 % iOS-приложений передают данные о местоположении. Исследователи записывали трафик при использовании приложений с целью обнаружить передачу персональной идентификационной информации, сведения о местонахождении и поисковые запросы. Обнаружилось, что в среднем каждое Android-приложение передает данные на 3,1 стороннего домена, iOS-приложение – на 2,6.

Android-приложения чаще передают такую информацию, как имя пользователя (49 %) и адрес (25 %), чем программы для iPhone. Для iOS-приложений этот показатель равняется 18 % и 16 % соответственно.

Три из тридцати изученных экспертами программ для занятий спортом и слежения за показателями здоровья передавали третьим сторонам данные о поисковых запросах и вводимую пользователями информацию. Android-приложение Drugs.com пересылает медицинские сведения (в том числе такие поисковые запросы, как «герпес») на пять сторонних доменов, среди которых doubleclick.net и googlesyndication.com.

Программы для Android чаще передают данные Google и Facebook. Больше всего информации пересылает Text Free, на счету у которой 11 сторонних доменов. Что касается iOS, то здесь лидером по «утечкам» является браузер Localscope, предающий информацию на 17 доменов.

93 % всех исследованных приложений для платформы от Google подключаются к домену safemovedm.com ***(Приложения раскрывают данные пользователей третьим сторонам // InternetUA (http://internetua.com/prilojeniya-raskrivauat-dannie-polzovatelei-tretim-storonam). – 2015. – 10.11).***

***

Среди множества видов вредоносных программ существует отдельная категория приложений, которые сами по себе не являются опасными, однако злоумышленники могут использовать их в противозаконных целях.

Речь идет о так называемых программах удаленного администрирования, которые могут использоваться как совершенно легально – для управления компьютером по сети, так и незаконно: с той же целью, но без ведома пользователя. Специалисты антивирусной компании «Доктор Веб» изучили одну из используемых злоумышленниками схем атаки, в ходе которой использовалось легально распространяемое приложение для организации удаленного доступа.

Целый пакет вредоносных программ, получивших общее наименование BackDoor.RatPack, киберпреступники распространяли при помощи эксплойта Exploit.CVE2012-0158.121 в виде документа в формате RTF, при попытке открыть который на компьютере жертвы расшифровывался и сохранялся вредоносный файл. Примечательно, что этот файл, представляющий собой программу-установщик, имеет действительную цифровую подпись (как, впрочем, почти все файлы из комплекта BackDoor.RatPack).

При запуске инсталлятор пытается выявить присутствие на атакуемом компьютере виртуальных машин, программ-мониторов и отладчиков, после чего проверяет наличие в системе программ «банк-клиент» нескольких российских кредитных организаций. Если все проверки прошли успешно, установщик скачивает с сервера злоумышленников и запускает на атакуемом компьютере другой установщик в формате NSIS (Nullsoft Scriptable Install System), содержащий еще один набор исполняемых файлов и несколько защищенных паролями архивов. Этот установщик распаковывает архивы и запускает исполняемые файлы.

Полезной нагрузкой установщика является несколько вариантов вполне легальной условно-бесплатной утилиты Remote Office Manager – специалисты компании «Доктор Веб» зафиксировали как минимум три таких варианта с разными конфигурационными настройками. С помощью перехвата ряда системных функций вредоносная программа скрывает значки этой утилиты в области уведомлений и панели задач Windows, чтобы пользователь не мог вовремя ее обнаружить. Можно предположить, что с применением BackDoor.RatPack злоумышленники пытаются получить доступ к банковским счетам и хранящейся на атакованной машине конфиденциальной информации методом удаленного управления зараженным компьютером.

Сигнатуры всех входящих в состав BackDoor.RatPack вредоносных файлов добавлены в вирусные базы Dr.Web, и потому они не представляют опасности для пользователей наших антивирусных продуктов ***(Набор троянцев открывает доступ к зараженному компьютеру // ITnews (http://itnews.com.ua/news/78921-nabor-troyantsev-otkryvaet-dostup-k-zarazhennomu-kompyuteru). – 2015. – 12.11).***

***

Социальные сети так плотно интегрировались в жизнь людей, что стали ее неотъемлемой частью. Но кроме своей очевидной пользы, несут в себе массу угроз.

Издание «Вести» разобралось, как соцсети используют данные пользователей и чем это грозит.

«Facebook, как и любая отдельная транснациональная корпорация, существует обособленно, на нее влияние могут иметь лишь большие государства – например, США, но не Украина», – пояснил глава украинского подразделения международной компании Dune HD А. Глущенко.

По его словам, номер телефона можно удалить, но важно помнить: в сети ничего не исчезает бесследно.

«Люди сами добровольно позволяют за собой следить. Например, чиновник постит фотографии с дорогих курортов, а это совершенно не совпадает с тем, что в декларации», – говорит А. Глущенко.

Маркетологи также используют личные данные в сети. После того как человек «погуляет» по сайту, выйдя на него через Facebook, все его действия запоминаются. И уже на следующий день пользователю будут приходить рекламные объявления, спам и разные приглашения.

«Идет глобальная слежка за местоположением человека. Информация о том, где вы бываете, сохраняется в истории местоположений со всех устройств, на которых вы вошли в аккаунт Google. Соответственно, с Facebook тоже зачастую переходят по ссылкам. Ваши геоданные могут использовать любые сервисы и приложения», – рассказал эксперт в сфере IT В. Токарь.

Также если вы ходите со смартфоном и пользуетесь им, входя через Google, то система отмечает точки, где вы именно были. Потом их можно посмотреть в своих данных. Но это не факт, что они доступны только вам.

Кстати, отмечание местоположения на фотографиях в Facebook может привести к серьезным последствиям.

«Моя подруга общается со многими известными людьми, часто с ними фотографируется. И судьба сыграла злую шутку с ней. Как оказалось, позже, грабители отслеживали, как она чекинилась, и в один из вечеров обчистили квартиру. Там было много техники и шубка», – поделилась киевлянка Олеся.

В настоящее время в Украине отслеживанием и контролем безопасности в сети занимается новая структура – киберполиция. Правда, о методах ее работы не говорят.

«Хакерские атаки на личную переписку украинцев растут. Киберполиция уже занимается частными обращениями граждан, конфиденциальную информацию которых хотят украсть. Используются свои оперативные методы, которые раскрывать нельзя», – рассказал пресс-секретарь МВД А. Шевченко ***(Как соцсети следят за пользователями и помогают ворам // InternetUA (http://internetua.com/kak-socseti-sledyat-za-polzovatelyami-i-pomogauat-voram). – 2015. – 12.11).***

***

В последнее время Adobe Flash пользуется плохой репутацией у ИБ-экспертов. Новое исследование компании Recorded Future в очередной раз подтверждает, что плагин является излюбленным вектором атак у киберпреступников и несет угрозу безопасности.

В ходе исследования было проанализировано 100 наборов эксплоитов, представляющих собой внедренные в веб-страницы фреймворки, которые начинают искать уязвимости в ПО, как только пользователь заходит на эти страницы. Эксперты обнаружили, что 8 из 10 наиболее часто эксплуатируемых

брешей затрагивают Adobe Flash, используемый на миллионах компьютеров для воспроизведения медиа-контента.

Эксперты исследовали уязвимости, добавленные в популярные наборы эксплоитов Angler, Neutrino и Nuclear Pack и предлагаемые на подпольных форумах в период с января по сентябрь 2015 г. В результате они пришли к выводу, который подтверждает мнение ИБ-экспертов о небезопасности Adobe Flash и «ставит под вопрос целесообразность использования плагина в безопасной операционной среде».

«Регулярная эксплуатация злоумышленниками брешей в Adobe Flash не является для экспертов безопасности чем-то неожиданным, однако масштабы использования просто невероятные», – говорится в отчете Recorded Future.

В течение многих лет Adobe работает над усилением безопасности плагина, регулярно просматривая код, однако это непростая задача, учитывая, что приложению уже почти два десятка лет ***(Новые доказательства небезопасности Adobe Flash // InternetUA (http://internetua.com/novie-dokazatelstva-nebezopasnosti-Adobe-Flash). – 2015. – 12.11).***

***

Киберпреступники научились распространять вирусы через рекламное видео. Сама зараженная интернет-реклама, или малвертайзинг – явление не новое. Но распространение вредоносного программного обеспечения через видеоролики можно считать относительно новым инструментом злоумышленников. Эксперты утверждают, что код, применяемый преступниками, чрезвычайно сложно обнаружить. Он активирует на странице всплывающее окно, которое уведомляет пользователя о необходимости обновить какой-либо важный компонент браузера. Если человек поверит сообщению и начнет следовать инструкциям, на его компьютер будет загружен вирус или троян. Учитывая сложившуюся ситуацию, эксперты снова предупреждают всех пользователей о необходимости крайне осторожно обращаться с интернет-рекламой и разнообразными всплывающими окнами ***(Вредоносное рекламное видео и еще 5 новостей из мира IT, которые нужно знать сегодня // IGate (http://igate.com.ua/news/11335-vredonosnoe-reklamnoe-video-i-eshhe-5-novostej-iz-mira-it-kotorye-nuzhno-znat-segodnya). – 2015. – 13.11).***

***

Компании Apple и Google удалили из своих магазинов приложений один из самых популярных клиентов Instagram, после того как выяснилось, что оно похитило множество паролей пользователей и публиковало фотографии без разрешения пользователя. Речь идет о приложении InstaAgent, которое сохраняло данные пользователей Instagram в зашифрованном виде, а затем отправляло их на неизвестные серверы.

Google очень быстро отреагировала на эту ситуацию, удалив приложение из Play Store, Apple сделала то же самое лишь спустя несколько часов.

Несмотря на то что официальное приложение Instagram рекомендует не использовать сторонние программы для пользования сервисом, многие пользователи все равно решили загрузить InstaAgent, поскольку оно дает ряд дополнительных возможностей. В частности, многие купились на то, что приложение позволяет видеть, кто просматривал ваш профиль в Instagram.

Следы вредоносного приложения были стерты, но сотни тысяч аккаунтов все равно уже похищены. Приложению удалось стать одним из самых популярных в британском и канадском App Store, а вот в США InstaAgent почему-то не снискало популярности. Если вы пользовались данным приложением, то вам строго рекомендуется сменить свой пароль в Instagram ***(Популярный альтернативный клиент Instagram воровал пароли пользователей // IGate (http://igate.com.ua/lenta/11324-populyarnyj-alternativnyj-klient-instagram-voroval-paroli-polzovatelej). – 2015. – 12.11).***

***

Согласно отчету ИБ-компании CyberArk, подавляющее большинство корпоративных сетей уязвимы к атакам на привилегированные учетные записи. По данным экспертов, большинство сетей на базе Windows сконфигурированы некорректно и предоставляют злоумышленникам возможность получить учетные данные привилегированных пользователей.

В ходе исследования специалисты CyberArk получили доступ к 51 корпоративной сети на базе Windows и обнаружили в 88 % случаев «машины, предоставляющие большую угрозу». Исследователи также выяснили, что взлом 40 % Windows-хостов может привести к полной компрометации.

«Каждая Windows-сеть, независимо от размеров, потенциально может быть скомпрометирована атакующими с помощью хищения привилегированных учетных данных», – говорится в отчете.

В каждой корпоративной сети эксперты выявили все связи привилегированных пользователей. В результате оказалось, что в некоторых из них компрометация лишь одного узла Windows предоставляет злоумышленникам возможность получить доступ к большому объему данных.

Проникнув в корпоративную сеть, хакеры могут добраться до серверных ресурсов, что, в свою очередь, грозит хищением учетных данных с других компьютеров в этой же сети. По данным экспертов, риски в таких случаях в 10 раз превышают риски, возникающие при взломе рабочей станции ***(Корпоративные сети уязвимы к атакам на привилегированные аккаунты // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/11/13/corporate-networks-vulnerable.html). – 2015. – 13.11).***

***

Гражданский суд Брюсселя запретил социальной сети Facebook отслеживать поведение пользователей из Бельгии без получения их

предварительного согласия. В случае несоблюдения решения суда компанию ждет штраф 250 тыс. евро в день.

В июне нынешнего года представители Бельгийской комиссии по защите неприкосновенности частной жизни инициировали судебное разбирательство в отношении Facebook, поскольку «отслеживание социальной сетью поведения ее членов, и незарегистрированных в ней граждан, нарушает нормы бельгийского и европейского законодательства». Это первый случай в европейской практике, когда национальный орган по защите личной информации подал в суд на Facebook из-за нарушения Закона «О персональных данных».

Основанием для иска стало проведенное комиссией исследование, которое показало, что Facebook по умолчанию собирает информацию о поведении пользователей на сторонних сайтах. По существующим правилам соцсети пользователь может постфактум запретить сбор такой информации, хотя, по мнению специалистов, социальной сети следовало бы заранее получать соответствующее разрешение. Также исследование показало, что Facebook отслеживает поведение граждан, которые не зарегистрированы в нем, что является нарушением действующих в ЕС правил. В связи с этим председатель указанной комиссии В. Дебекеларе посчитал неприемлемым такой аспект деятельности Facebook. Тогда же представители компании назвали этот иск лишенным всякого смысла «недоразумением», поскольку не признают «бельгийское законодательство и компетенцию бельгийской комиссии».

И вот Гражданский суд Брюсселя рассмотрел дело и вынес решение, что Facebook в течение двух дней должен прекратить указанные действия в отношении пользователей или придется ежедневно выплачивать Комиссии по защите неприкосновенности частной жизни четверть миллиона евро. Американский гигант уже объявил о намерении подать апелляцию на решение суда: «Мы использовали cookies «Datr» в течение более чем пяти лет, чтобы обеспечить удобство использования Facebook 1,5 млрд человек во всем мире. Поэтому менеджеры обжалуют данное решение».

Госсекретарь по защите неприкосновенности частной жизни Б. Томмелан отметил, что это решение суда свидетельствует, что даже в такой маленькой стране, как Бельгия, граждане могут рассчитывать на справедливость в противостоянии с интернет-гигантом. По мнению министра, итог судебного разбирательства доказывает, что «закон о защите частной жизни – не просто бумажка». Третьим положительным моментом, с точки зрения Б. Томмелана, является возможность рассмотрения таких дел в суде. «Facebook утверждал ранее, что бельгийские суды не имели никакой юрисдикции в этом вопросе, но этот аргумент не был принят. Компания настаивала, что регулировать такие вопросы может только надзорный орган государства, где расположен субъект, который осуществляет обработку данных, а именно Ирландский комитет защиты частной жизни» ***(Facebook запретили следить за жителями ЕС // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/facebook-zapretili-sledit-za-zhitelyami-es.html). – 2015. – 11.11).***

***

Антивирусам будущего не понадобятся обновления. Сегодня они ищут вредоносное ПО, сверяя код файлов на компьютере со своими базами данных. Таким образом, если антивирус не имеет соответствующего «маркера», то он не сможет обнаружить вредоносную программу. Для защиты от вирусов требуется постоянное обновление программ безопасности.

Решение проблемы кроется во внедрении самообучающихся алгоритмов, которые позволят определять вредоносный код без постоянного обновления баз данных. Разработчики исходят из того, что если нейронные сети уже научили идентифицировать людей по лицам, то и также они смогут отличать вредоносное ПО от нормального.

Данную технологию разрабатывает израильский стартап. Разработчики обещают, что их антивирус будет выявлять новые вредоносные программы на 20 % точнее, чем лучший сегодняшний ***(Антивирусам будущего не понадобятся обновления // InternetUA (http://internetua.com/antivirusam-budusxego-ne-ponadobyatsya-obnovleniya). – 2015. – 14.11).***

***

В популярной библиотеке Java свыше девяти месяцев назад была обнаружена уязвимость, которая в настоящее время подвергает риску удалённых атак тысячи приложений и серверов. Библиотека Apache Commons содержит набор широко используемых компонентов, поддерживаемых организацией Apache Software Foundation. Эта библиотека используется по умолчанию в многочисленных продуктах, таких как Oracle WebLogic, IBM WebSphere, JBoss, Jenkins OpenNMS.

Уязвимость находится в компоненте Apache Commons под названием Collections и происходит от небезопасной десериализации объектов Java. Сериализацией в языках программирования называется процесс перевода данных в двоичный формат для их хранения в файле, памяти или отправки в сеть. Процесс обратного преобразования данных называется десериализацией.

В январе на конференции по сетевой безопасности об уязвимости рассказали исследователи К. Фрохофф и Г. Лоуренс. Должного внимания этой новости уделено не было; возможно, считается, что за предотвращение таких атак отвечают разработчики приложений, а не библиотек. Внимание к уязвимости в очередной раз было привлечено 7 ноября, когда компания FoxGlove Security выпустила эксплоит для приложений WebLogic, WebSphere, JBoss, Jenkins и OpenNMS.

Компания Oracle в ответ на это 10 ноября выпустила временные инструкции для WebLogic Server, работая над закрывающим уязвимость патчем. Разработчики Apache Commons Collections также готовят своё обновление. Предположительно, проблема может затрагивать и другие компоненты Java. Уязвимость относится к классу InvokerTransformer и ещё три класса находятся сейчас под подозрением ***(В тысячах Java-приложений***

существует уязвимость // InternetUA (http://internetua.com/v-tisyacsah-Java-prilojenii-susxestvuet-uyazvimost). – 2015. – 14.11).

***

Независимый исследователь безопасности из Лондона П. Амар разработал ПО, предназначенное для эксплуатации расширенной функции обмена сообщениями в Twitter. Инструмент, получивший название Twittor, позволяет создать ботнет из скомпрометированных компьютеров, которые могут взаимодействовать меду собой, а также получать инструкции и обновления через социальную сеть.

В августе этого года Twitter сняла ограничения на количество символов в сообщениях, позволив тем самым оправлять уведомления с неограниченным количеством знаков. Отметим, изменения коснулись только основных сообщений.

По словам разработчика, ботов довольно сложно вычислить и уничтожить, поскольку C&C-трафик Twittor выглядит аналогично легитимному. Ежедневно ботнет оправляет ограниченное количество (100) личных сообщений. Как пояснил П. Амар, Twittor представляет собой созданный на базе Python бэкдор, который использует Twitter в качестве C&C-сервера. Таким образом автор ПО пытался продемонстрировать недостаточную защищенность соцсети и необходимость реализации дополнительных функций безопасности, таких как шифрование и пр.

Инструмент доступен для скачивания на портале для разработчиков GitHub ***(Новый инструмент позволяет создать ботнет в Twitter // InternetUA (http://internetua.com/novii-instrument-pozvolyaet-sozdat-botnet-v-Twitter). – 2015. – 15.11).***

***

Как выяснили эксперты ИБ-компаний Checkmarx и AppSec Labs, специализирующихся на мобильной безопасности, iOS-приложения более подвержены уязвимостям, чем программы, разработанные для Android. Согласно отчету, одно приложение в среднем содержит порядка девяти брешей.

Что касается уязвимостей в iOS, 40 % из них имеют критическую или высокую степень опасности, в то время как для Android этот показатель составляет 36 %. Исследователи проанализировали сотни типов ПО, включая банковские приложения, игры, программы для online-шопинга и обеспечения безопасности. Оказалось, что даже защищенные банковские приложения подвержены уязвимостям, позволяющим утечку данных или связанных с некорректным процессом аутентификации.

Наиболее распространенные уязвимости (27 % от общего количества найденных брешей) связаны с утечкой персональных данных или важной информации. На втором месте оказались проблемы аутентификации и авторизации (23 %). Последние представляют наиболее высокий риск для

пользователей, поскольку львиная доля из них (60 %) классифицируется как критические или высококритические.

Бытует мнение, что iOS более безопасна по сравнению с ОС Android в связи с ограничениями, которые накладывает Apple. Тем не менее, строгий контроль над сторонними разработчиками, усиленные механизмы обеспечения безопасности и налаженная доставка обновлений и патчей заставляют разработчиков прилагать меньше усилий при создании кодов приложений. В будущем, учитывая тенденции в мире угроз, это может стать серьезной проблемой, считают специалисты ***(iOS-устройства более уязвимы, чем гаджеты на базе Android // InternetUA (http://internetua.com/iOS-ustroistva-bolee-uyazvimi--csem-gadjeti-na-baze-Android). – 2015. – 14.11).***

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Касаткіна** Тетяна Петрівна

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. Голосіївський, 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz@pochta.ru
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.