СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(5–18.10)

2015 № 18

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(5–18.10)
№ 18

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

Исследовательская компания Factum Group по заказу ИнАУ составила актуальный рейтинг сайтов уанета по среднедневной доле и охвату по состоянию на сентябрь 2015 г. Список популярных среди украинских пользователей доменов определен по итогам медиа-панели численностью 5 тыс. человек. Тройка лидеров длительное время остается неизменной, пишет AIN.UA (http://ain.ua/2015/10/10/609026).

По сравнению с рейтингом за август первые три позиции остались за Google, «ВКонтакте» и Mail.ru, а на четвертом месте в сентябре оказался «Яндекс», потеснив YouTube на пятую позицию.

Домены	Среднедневная доля, %	Месячный охват, %
Google	58 %	67 %
Vkontakte (vk.com)	50 %	62 %
Mail.ru	33 %	57 %
Yandex	32 %	54 %
YouTube.com	31 %	59 %
Odnoklassniki (ok.ru)	30 %	40 %
Facebook.com	16 %	32 %
Olx.ua	14 %	42 %
Ukr.net	14 %	24 %
Sinoptik.ua	10 %	27 %
Privatbank.ua	9 %	36 %
Wikipedia.org	9 %	39 %
Aliexpress.com	9 %	35 %
Rozetka (.ua/.com.ua)	8 %	39 %
I.ua	7 %	20 %
Gismeteo.ua	6 %	19 %
Ex.ua	6 %	21 %
Prom.ua	5 %	31 %
Kinogo.co (.net)	5 %	18 %
Blogspot.com	5 %	27 %
Aukro.ua	5 %	20 %
Obozrevatel.com+uaportal.com+ uaclub.net	4 %	14 %
Fs.to	4 %	11 %
Twitter.com	4 %	16 %
Ask.fm	4 %	13 %

(Топ-25 сайтов уанета за сентябрь от ИнАУ: «Яндекс» обогнал YouTube // AIN.UA (http://ain.ua/2015/10/10/609026). – 2015. – 10.10).

***

Twitter представил новый формат работы с новостями и событиями – функцию Moments («Моменты»). Об этом сообщается в блоге компании.

Услуга представляет собой специальную кнопку в виде молнии, которая стала доступна 6 октября для американских пользователей Android, iPhone и десктопной версией сервиса. Нажав на нее, можно перейти к списку наиболее важных и популярных на текущий момент тем, о которых пишут пользователи. Например, важные мировые события или крупные культурные мероприятия.

Выбрав тему, читатель попадает на страницу, где собираются лучшие твиты, фото и видео. Новости располагаются по хронологии: от старых происшествий к самым последним. Каждую запись можно ретвитнуть, добавить в избранное, а также поделиться со своими подписчиками, приложив к ней свой комментарий.

На постоянно обновляющиеся «моменты» (например, церемонии вручения наград, спортивные соревнования) можно подписаться: события из выбранной темы будут в режиме реального времени отображаться прямо в ленте новостей пользователя. Как только событие закончится, подписка на эту ленту автоматически отключится.

Отбором интересного контента занимается внутренняя команда редакторов Twitter. Партнерами компании стали Bleacher Report, Buzzfeed, Entertainment Weekly, Fox News, Getty Images, Mashable, MLB, NASA, New York Times, Vogue и Washington Post. Ожидается, что этот список пополнится.

Пока пользователям по всему миру доступны «моменты», которыми поделились в своих лентах американские пользователи Twitter. В ближайшее время компания планирует запустить услугу в остальных странах.

Twitter не единственный среди интернет-площадок, кто заинтересован в новых форматах подачи информации ***(Twitter запустил новостной сервис // InternetUA (http://internetua.com/Twitter-zapustil-novostnoi-servis). – 2015. – 6.10).***

***

Несмотря на последние достижения Facebook на поприще цифрового видео, показатели социальной сети по-прежнему далеки от YouTube. Об этом говорят данные нового отчёта SimilarWeb, сообщает searchengines.ru.

С точки зрения совокупного времени просмотра, как внутри приложений, так и в веб-версии, здесь показатели YouTube в 11 раз или на 91 % выше, чем у Facebook. Ежедневно американцы тратят в общей сумме 8061 лет на YouTube и лишь 713 лет на просмотр видео в Facebook.

В мировом масштабе цифры YouTube выглядят ещё более впечатляюще: ежедневно на просмотр YouTube в мире тратится почти 46 тыс. лет. У Facebook этот показатель составляет 5625 лет.

Зрители YouTube тратят значительное время на просмотр видео в рамках сервиса – 20, 40 и даже 60 минут в день. При этом, чем они младше, тем более вероятен их выбор в пользу YouTube. Зрители цифрового видео в возрасте от

13 до 17 лет в 18,5 раз чаще выбирают видеохостинг вместо Facebook. Молодёжь в возрасте от 17 до 20 лет делает выбор в пользу видеохостинга в 16,5 раз чаще.

Люди в возрасте от 55 до 64 лет отдают предпочтение YouTube лишь в 1,8 раз чаще. Пожилые пользователи (старше 65 лет) – в 1,4 раза.

Тем не менее, представленная статистика не отрицает тех значительных результатов, которых Facebook достиг в направлении цифрового видео. За полгода количество просмотров видео в рамках платформы возросло с практически нуля до 4 млрд в день. Кроме того, социальная сеть обладает техническими возможностями ещё больше увеличить эти цифры. Поскольку то, что видят люди в новостной ленте, зависит от алгоритмов Facebook.

Хотя в настоящее время пользователи социальной сети не смотрят видео в течение длительных промежутков времени, эта ситуация может измениться с развитием и внедрением технологий виртуальной реальности. Также есть вероятность, что Facebook выпустит отдельное приложение для видео, что будет способствовать повышению видеопоказателей социальной сети ***(Общее время просмотра видео в YouTube на 91 % больше, чем в Facebook // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44880/118/lang,ru/). – 2015. – 5.10).***

***

В ответ на опасность и насилие, которым профессиональные репортеры подвергаются в процессе работы «в поле», Международный женский медиафонд (International Women's Media Foundation (IWMF)) выпустил мобильное приложение Reporta с функционалом социальной сети, с помощью которого журналисты могут общаться и запрашивать экстренную помощь. Об этом сообщает cossa.ru.

Reporta поддерживает отправку изображений, аудио и видео предустановленному списку личных и профессиональных контактов, чтобы журналисты могли всегда держать друг друга в курсе того, где они находятся и каков уровень безопасности их деятельности. Если репортер под реальной угрозой, он даже может отправить сигнал SOS с помощью приложения.

Мобильный продукт уже доступен для устройств на iOS и Android ***(Появилась мобильная соцсеть для журналистов // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44893/118/lang,ru/). – 2015. – 6.10).***

***

Facebook расширит возможности кнопки «Нравится». Новая версия «лайка» получит название «Реакции» (Reactions) и будет представлять из себя набор смайлов, выражающих целый спектр различных эмоций. Таким образом соцсеть планирует дать аудитории возможность более эмоционально реагировать на публикации в ленте новостей. Старый «лайк» при этом

останется, но дополнится смайликами, выражающими любовь, смех, улыбку, удивление и гнев.

В то же время соцсеть решила отказаться от популярной и широко обсуждаемой идеи внедрения «дислайка». По мнению основателя Facebook М. Цукерберга, кнопка «не нравится» сделает соцсеть похожей на систему форумов Reddit с их функцией голосования «за» и «против», а также негативно скажется на настроении пользователей ***(Facebook расширит возможности кнопки «Нравится» // NewsCloud (http://www.news-cloud.net/news/technologies/9649-facebook-rasshirit-vozmozhnosti-knopki-nravitsya.html). – 2015. – 8.10).***

***

Топ-менеджер Twitter К. Вайль сообщил, что в ближайшее время социальную сеть не станут снабжать опцией редактирования записей, передает портал Gizmodo.

По словам К. Вайля, дело не в технических сложностях вроде внесения необходимых изменений в программный код приложения. Он отметил, что компании требуется время, чтобы рассмотреть все возможные варианты злоупотреблений этой функцией и разработать меры для их пресечения.

Как пояснил К. Вайль, Twitter дает возможность дублировать (по терминологии сервиса – «ретвитить») чужие записи, а также размещать в виде вставок на других ресурсах. Если сообщения разрешат править, может получиться так, что пользователь поддержит своим ретвитом высказывание, которое не стал бы дублировать, если бы сразу увидел в отредактированном виде ***(Twitter повременит с функцией редактирования записей // InternetUA (http://internetua.com/Twitter-povremenit-s-funkciei-redaktirovaniya-zapisei). – 2015. – 8.10).***

***

Социальная сеть LinkedIn объявила о существенном обновлении функционала групп и запуске для них отдельного iOS-приложения, начиная с 14 октября 2015 г.

«Мы хотим, чтобы все участники получали максимальную пользу при каждом посещении групп в LinkedIn. С этой целью мы упростили некоторые возможности групп, чтобы группы по-прежнему оставались самым надежным местом встречи для профессионалов с общими интересами. Внесенные в группы изменения дадут возможность всем участникам легче ориентироваться и лучше понимать работу с LinkedIn», – сообщается в справочном центре LinkedIn.

Соцсеть запустит обновленную версию групп в веб-версии сервиса и отдельное iOS-приложение для этого функционала. Нововведения призваны повысить качество общения в группах, пространство которых переполнено спамом и саморекламой.

Самым крупным изменением станет перевод групп в закрытый режим. Исследование компании показало, что профессиональные обсуждения наиболее эффективны в конфиденциальном доверенном пространстве. Поэтому отныне просматривать обсуждения в группе смогут только участники. LinkedIn также закроет обсуждения от индексации поисковыми роботами, чтобы сделать общение более приватным ***(LinkedIn сделает все группы закрытыми // IGate (http://igate.com.ua/lenta/10601-linkedin-sdelaet-vse-gruppy-zakrytymi). – 2015. – 8.10).***

***

На конференции Code/Mobile старший вице-президент по продукту К. Вейл заявил, что в ближайшие 12 месяцев Twitter будет стараться сделать свой проект проще.

Это, по словам К. Вейла, пойдёт на пользу не только новичкам, но и всем зарегистрированным в Twitter пользователям. Когда К. Вейла спросили об увеличении лимита символом на одно сообщение (сейчас это 140 символов), то он сказал: «Мы не стыдимся менять что-то, что находится в самой основе Twitter».

В конце конференции К. Вейл сказал, что касательно прямых сообщений в Twitter у компании есть несколько отличных идей, а сам сервис всегда будет оставаться независимым – то есть вряд ли он когда-либо будет кому-нибудь продан ***(В ближайший год Twitter должен стать проще // InternetUA (http://internetua.com/v-blijaishii-god-Twitter-doljen-stat-prosxe). – 2015. – 10.10).***

***

Facebook расширила возможности своего фирменного чата. Теперь приложение Messenger можно использовать на «умных» часах Apple Watch под управлением watchOS 2. Созданное разработчиками социальной сети приложение дает возможность отправлять сообщения в любой момент одним нажатием кнопки.

Теперь Facebook Messenger дает возможность делиться с друзьями сообщениями, голосовыми записями и стикерами при помощи Apple Watch. Как показала практика, подобное общение отлично подходит для носимого на запястье изделия. То есть с часов удобно выполнять какие-либо простые действия, вроде быстрого ответа на сообщение. Когда требуется большая переписка, целесообразнее обратиться к более крупному устройству ***(Facebook выпустил Messenger для Apple Watch // InternetUA (http://internetua.com/Facebook-vipustil-Messenger-dlya-Apple-Watch). – 2015. – 9.10).***

***

Аудитория Facebook составляет порядка 1,5 млрд пользователей, что делает её самой массовой социальной сетью на нашей планете. Однако компания М. Цукерберга не собирается останавливаться на достигнутом. В

мире с лёгкостью можно насчитать еще 4–5 млрд человек, которые вообще не пользуются Интернетом, и все они являются потенциальными участниками сообщества сервиса.

Основной преградой для многих из них, по мнению компании, является низкоскоростной мобильный Интернет поколения 2G. Большинство онлайн-приложений работают при таком соединении крайне медленно, и Facebook не исключение. Чтобы повысить эффективность использования своего мобильного приложения в 2G-сетях, социальный гигант провел целый ряд усовершенствований и оптимизаций.

В первую очередь изменения коснулись новостной ленты, которая теперь стала работать гораздо быстрее, когда пользователь оказывается в зоне с медленным соединением. В зависимости от уровня сигнала система автоматически определяет, какой контент следует загружать и отображать на экране телефона в первую очередь. К примеру, в условиях медленной скорости передачи данных пользователь будет видеть в новостной ленте больше ссылок и обновлений статуса, а видео в целях экономии ресурсов загружаться не будет.

Когда пользователь просматривает новостную ленту, загрузка последующих постов и фотографий осуществляется в фоновом режиме, что обеспечивает более плавную прокрутку. Кроме того, разработчики отказались от использования формата изображений JPEG в пользу Progressive JPEG. На практике это означает, что отныне фотографии до окончания полной загрузки будут отображаться в низком разрешении – в Facebook посчитали что это в любом случае лучше, чем созерцать в течение продолжительного времени пустой экран. В начале года эта технология была реализована в iOS-версии Facebook, теперь же она поддерживается и приложением для Android ***(Приложение Facebook при медленном Интернете стало работать быстрее // InternetUA (http://internetua.com/prilojenie-Facebook-pri-medlennom-internete-stalo-rabotat-bistree). – 2015. – 9.10).***

***

Соцсеть Facebook выпустила новую версию приложения для iOS. Теперь обладатели iPhone 6s и iPhone 6s Plus получили возможность использовать преимущества дисплеев 3D Touch для более быстрого доступа к функциям сервиса.

Нажатие с усилием на значок Facebook с домашнего экрана приводит к выводу панели быстрого доступа. С ее помощью можно перейти в один из разделов приложения: «Сделать фото/видео», «Загрузить фото/видео», «Обновить статус».

Модуль 3D Touch стал главной инновацией новых iPhone 6s и 6s Plus. Помимо таких знакомых жестов, как касание, смахивание, сведение и разведение пальцев, технология дает возможность использовать функции Peek и Pop. Это новое измерение в работе с iPhone. Можно просматривать самый разный контент и работать с ним, даже не открывая. Например, если нажать на

письмо, функция Peek покажет превью. А если нажать посильнее – функция Pop откроет его.

Датчик, распознающий силу нажатия на экран, удобен в использовании. Особенно практично переходить в нужный раздел iOS-приложений. Изначально технология 3D Touch была доступна в ряде приложений, предустановленных в новых смартфонах, включая Почту, Музыку и Карты. Но вскоре после запуска iPhone 6s поддержка этого функционала стала появляться и в сторонних приложениях ***(В Facebook появилась поддержка 3D Touch для новых iPhone // IGate (http://igate.com.ua/lenta/10680-v-facebook-poyavilas-podderzhka-3d-touch-dlya-novyh-iphone). – 2015. – 13.10).***

***

Facebook создаст отдельную ленту для видео. Компания тестирует новые функции, включая отдельную видео ленту, где будут собраны расшаренные друзьями клипы, страницы, трендовые видео на Facebook и просмотренные видео. Сеть также тестирует функцию похожих видео. Кликнув на клип в ленте, пользователи увидят серию роликов, в том числе и рекламных. Еще одна новинка – «всплывающие» видео, которое дает возможность пользователю просмотреть видео, продолжая скроллить ленту, а также кнопка «сохранить», которая позволит просмотреть контент позже. Facebook рассматривает видео как естественное развитие формата от текста к фото и как плацдарм для виртуальной реальности ***(Facebook создаст отдельную ленту для видео // Marketing Media Review (http://mmr.ua/show/facebook_sozdast_otdelynuyu_lentu_dlya_video). – 2015. – 14.10).***

***

Социальная сеть профессионалов LinkedIn запускает новый сервис, призванный помочь компаниям нанимать людей, обладающих таким же набором талантов и профессиональных навыков, как у их лучших сотрудников, пишет Vector News (http://vnews.agency/news/world/18145-linkedin-predlozhila-novyy-instrument-dlya-poiska-sotrudnikov-zvezd.html).

Сервис-рекрутер будет оказывать услуги организациям, которые не могут четко сформулировать, какими качествами должен обладать их «идеальный сотрудник», но в которых работает хотя бы один выдающийся профессионал – настоящая «звезда».

«Когда мы осуществляем поиск, используя профиль сотрудника-“звезды”, наш “Рекрутер” анализирует название должности, навыки, образование, опыт и строит поисковую цепочку, подбирая похожие на “звездный” профиль кандидатуры», – поясняет Э. Вивас, начальник отдела вербовки талантов – источника большинства доходов LinkedIn.

Но не приведет ли такой подход к однообразию в коллективах? Э. Вивас с этим категорически не согласен. Если компания желает улучшить качество своих кадров, она может использовать профили своих сотрудников, чтобы

подыскать кандидатов, совершенно иных в этнокультурном отношении, но схожих по уровню профессионализма.

«Например, рекрутеры могут искать кандидатов, учившихся в испаноязычных колледжах или принадлежащих к LinkedIn-группе программистов-афроамериканцев», – говорит Э. Вивас.

Для компаний, у которых пока нет сотрудников-«звезд», на которых можно было бы равняться, LinkedIn создала автоматический поиск профессиональных профилей, который может подсказать, в каких городах больше всего квалифицированных кандидатов, а также какие именно навыки и опыт ищут другие компании, нанимая себе тот или иной персонал.

LinkedIn также запустил продукт, помогающий активизировать обмен информацией между наемными работниками. LinkedIn Referrals указывает работодателю на потенциальных кандидатов, зарегистрированных на сайте, но находящихся вне круга знакомств его сотрудников, а потом рассылает последним письма с просьбой поделиться информацией о вакансиях с друзьями по социальной сети ***(LinkedIn предложила новый инструмент для поиска сотрудников-звезд // Vector News (http://vnews.agency/news/world/18145-linkedin-predlozhila-novyy-instrument-dlya-poiska-sotrudnikov-zvezd.html). – 2015. – 15.10).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Мерія м. Кузнецовськ у Рівненській області вже півтора роки ставить цікавий експеримент повного переходу міста на електронну демократію. Після Революції Гідності було створено ряд ініціатив залучення громадянського активу, а також сформовано команду ІТ-реформ, яку очолив розробник Є. Поремчук.

За півтора роки в цьому місті було запущено ряд електронних послуг для громадян, зокрема, SMS-інформування про готовність документів у мерії за запитом мешканців міста; повідомлення комунальних служб і мерії про проблеми в Facebook і Telegram – усі подібні звернення фіксуються як офіційні.

Поширеною стала практика повідомлень про проблеми через мобільний месенджер або онлайн-платформу OpenCity. Загальноміські проблеми при цьому вирішуються за допомогою механізму електронних петицій від спільноти Кузнецовська. Петиція, що набрала 100 голосів за три місяці, передається на розгляд до мерії. Механізм петицій дав змогу побудувати стадіон зі штучним покриттям, встановити на вулицях ліхтарі з LED-лампами та збудувати безкоштовний спортивно-тренувальний майданчик. Також у Кузнецовську працює система вуличних веб-камер, система надання державних

електронних послуг iGov і внутрішнього електронного документообігу «УкрДок».

Мерія цього Рівненського міста також відкрила для інтернет-підприємців безкоштовний коворкінг, запровадила мережу міського безкоштовного Wi-Fi і планує підключити систему держзакупівель ProZorro. У планах – запровадження електронних черг не лише до дитячих садків, але й до поліклінік; розширення переліку електронних державних послуг.

Раніше ми вже повідомляли, що платформа електронних тендерів ProZorro розпочала повноцінну роботу в дев'яти областях України ***(У Рівненській області місто перейшло на «Facebook-демократію» // Блог Imena.UA (http://www.imena.ua/blog/kuznetsovsk-case/). – 2015. – 7.10).***

***

7 жовтня в прес-центрі Департаменту інформаційної діяльності та комунікацій з громадськістю облдержадміністрації відбулася прес-конференція стосовно реалізації проекту «Українська мережа блогерів з питань інвалідності та ВІЛ/СНІД», розробленого Вінницькою міською організацією соціального розвитку та становлення окремих малозахищених категорій молоді «Паросток».

В обговоренні взяли участь заступник директора Департаменту соціальної політики Вінницької облдержадміністрації Л. Негода, директор Вінницького соціально-економічного інституту Університету «Україна» Г. Давиденко, заступник директора з науково-педагогічної роботи Вінницького соціально-економічного інституту Університету «Україна» С. Ілініч, керівник Вінницького обласного відділення ВБО «Всеукраїнська Мережа ЛЖВ» О. Шевчук і голова громадської організації «Рада Вінниччини» Л. Станіславенко.

«Метою проекту є сприяння розвитку громадянського суспільства в Україні онлайн. Так, шляхом переймання досвіду міжнародних блогерів, які висвітлюють проблеми людей з інвалідністю та людей, які живуть з ВІЛ-СНІДом формується мережа вітчизняних блогерів з цієї тематики у Вінницькій, Житомирській та Хмельницькій областях», – зауважила інформаційний менеджер інституції О. Смірнова презентуючи проект.

За її словами, до проекту залучаються представники громадських організацій медичного спрямування, засобів масової інформації та соціальні працівники. Реалізація проекту є можливою завдяки активній співпраці ГО «Паросток» із постійними партнерами, а саме: Департаментом інформаційної діяльності та комунікацій з громадськістю облдержадміністрації та Департаментом соціальної політики Вінницької облдержадміністрації, Вінницьким соціально-економічним інститутом Університету «Україна», Хмельницьким інститутом соціальних технологій Університету «Україна», ВОВ ВБО «Всеукраїнська мережа людей, які живуть з ВІЛ/СНІД», Житомирською обласною громадською організацією людей з інвалідністю «Молодь. Жінка. Сім'я».

У рамках прес-конференції учасниками заходу обговорювались наступні питання: методика роботи із формування відповідних знань і компетентностей учасників проекту стосовно проблем інвалідності, підвищення медіаграмотності через переймання досвіду американських блогерів, які опікуються питаннями інвалідності та ВІЛ/СНІДу, підвищення культури висвітлення проблем інвалідності та ВІЛ/СНІДу журналістами регіону.

Завершуючи засідання організатори наголосили, що на сьогодні блогери виконують важливу соціальну функцію, перетворивши інтернет-мережу на середовище комунікації, обміну досвідом і думками. У своїх публікаціях вони відображають настрої суспільства та стимулюють до обговорення суспільно важливих питань.

Завдання блогерів, у рамках проекту, полягає у поширені інформації (дотримуючись професійної етики та без упереджень) про ВІЛ/СНІД та проблеми людей з інвалідністю та людей, які живуть з ВІЛ/СНІДом.

Як зазначила О. Шевчук: «Висвітлюючи цю тематику, нам важливо впровадити ідею толерантного впливу на соціум. Оскільки інтернет-мережа є чи не головним засобом формування громадської думки, тобто ставлення різних груп людей до подій чи фактів соціальної дійсності, то варто розуміти всю силу кожного слова» ***(На Вінниччині обговорили роль блогерів у питаннях інвалідності та ВІЛ/СНІД // Вінницька ОДА (http://www.vin.gov.ua/web/vinoda.nsf/web_alldocs/DocДЕПІАЗЗLB2). – 2015. – 7.10).***

***

Кожна районна адміністрація Львова створила свою сторінку в соціальній мережі Facebook. Про це повідомляє кореспондент 032.ua.

Відтепер кожен львів'янин, який проживає у певному районі Львова може дізнаватись найновішу інформацію про події у своєму районі, коментувати їх, а також залишати скарги або ж пропозиції ***(Райадміністрації Львова мають власні сторінки у мережі Facebook // 032.ua (http://www.032.ua/news/990704). – 2015. – 11.10).***

***

Геологическая служба США (USGS) имеет 2 тыс. датчиков предупреждения землетрясений, но большинство из них находятся в США. Это ограничивает возможности службы в области контроля за землетрясениями в остальной части мира. Для покрытия своих белых пятен USGS наладила сотрудничество с Twitter.

Миллионы людей используют Twitter, чтобы сообщить о землетрясении, но чтобы эти данные могли принести пользу, их необходимо дорабатывать. USGS проанализировала такие твиты и обнаружила, что сообщения о землетрясениях, как правило, были короткими. Они также поняли, что эти твиты в основном не принадлежали пользователям, которые на самом деле пережили реальное землетрясение.

Поэтому специалисты службы решили фильтровать твиты, содержащие более семи слов и ссылки. Эти отфильтрованные твиты оказались полезными для мониторинга землетрясений в глобальном масштабе. Теперь, когда много людей начинают посылать твиты с сообщениями о землетрясении в определённом районе, Геологическая служба США получает предупреждение.

Предупреждение о подземных толчках в Чили было получено всего через одну минуту и 20 секунд – благодаря 14 твитам ***(Использование твитов позволяет учёным узнавать о землетрясении через 29 секунд // InternetUA (http://internetua.com/ispolzovanie-tvitov-pozvolyaet-ucs-nim-uznavat-o-zemletryasenii-cserez-29-sekund). – 2015. – 11.10).***

***

Представництво ЄС в Україні запускає новий проект UopenEU у соціальних мережах. UopenEU – це додатковий інформаційний ресурс про новації та можливості, що з'являться в українського бізнесу після вступу в дію DCFTA, на сторінках Facebook, «ВКонтакте» та Twitter.

Про це повідомляє прес-служба представництва ЄС.

Створення глибокої та всеохоплюючої зони вільної торгівлі (DCFTA) є частиною Угоди про асоціацію між Україною та Європейським Союзом, яка вступає в дію з 1 січня 2016 р.

«Відтак на Україну чекають зміни у всіх сферах торговельних відносин з Європейським Союзом: від переоснащення виробництва, підвищення вимог до якості та безпеки продукції, посилення захисту інтелектуальної власності, до змін у звітності та обліку. Результатом зазначених перетворень стане наближення українського бізнесу до єдиного європейського ринку, що становить більше півмільярда споживачів із однією з найвищих купівельних спроможностей у світі (близько 38 тис. євро середньорічного доходу на одну особу)», – ідеться в повідомленні.

На сторінках у соцмережах проекту планують подавати актуальну інформацію, яка допоможе в розвитку власного бізнесу на єдиному європейському ринку: коментарі вітчизняних і міжнародних експертів, урядовців, представників Європейського Союзу, бізнесменів та активістів. Історії успішних українських компаній, які вже торгують з європейськими країнами.

«Стартапи, розроблені та захищені за міжнародними стандартами. Нові правила справжньої конкуренції. Доступ до держзакупівель у країнах-членах ЄС. Вільні від конкуренції торговельні квоти та боротьба за збільшення наявних. Про всі складні проблеми будемо говорити простою та зрозумілою мовою у соціальних мережах, відповідати на запитання та коментарі читачів», – зазначили у представництві ***(ЄС запускає інформаційну кампанію у соцмережах щодо зони вільної торгівлі // Європейська правда (http://www.eurointegration.com.ua/news/2015/10/15/7039522/). – 2015. – 15.10).***

Lobster, платформа для лицензирования user generated контента в социальных сетях, анонсировала заключение партнерства с крупнейшим видеохостингом YouTube. Теперь пользователи сервиса смогут запрашивать разрешение на использование и загрузку видеороликов на YouTube у их авторов за единовременную плату. Об этом пишет cossa.ru.

В настоящее врямя ситуация такова, что медиа-, креативным и рекламным агентствам приходится использовать контент на условиях creative commons либо создавать собственный, уникальный, и это стоит немалых денег. Lobster даст возможность профессионалам наряду с обычными пользователями находить качественные и релевантные их целям видео, а затем отправлять запрос на их использование.

Правообладатели YouTube-роликов, в свою очередь, получат возможность активно продвигать свой контент на платформе Lobster для лицензирования креативными агентствами. В то же время если пользователь найдет на YouTube нужное видео, которого нет в списке Lobster, он сможет просто отправить его ID для установления контакта с автором и запроса лицензионного соглашения.

Лицензия на использование YouTube-видео будет стоить около 7 дол. ***(YouTube позволит покупать лицензию на использование видео за 7 дол. // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44871/118/lang,ru/). – 2015. – 5.10).***

***

«ВКонтакте» запустила партнерскую программу, которая дает возможность владельцам сообществ в соцсети зарабатывать на выручке от показов рекламы в роликах, размещаемых на страницах групп. Об этом сообщает VC.

Издание отмечает, что партнерской программой могут воспользоваться «владельцы крупных сообществ, в которых размещается пользовательское и полупрофессиональное видео». Они смогут получать долю выручки от показов рекламы, которую увидят подписчики сообщества и пользователи, среди которых будет распространена эта видеозапись.

Согласно условиям программы, в ней могут участвовать только сообщества, в которых состоит не менее 500 тыс. подписчиков, у которых нет неурегулированных споров с правообладателями и шокирующего контента (порнографии, насилия, жестокости, экстремизма, призывов к совершению противоправных действий).

После подключения программы «ВКонтакте» начнет модерировать все видеозаписи, которые загружаются от имени сообщества. Если они подходят

под правила программы, то администратор увидит значок включенной монетизации около названия ролика.

В настоящее время неизвестно, какую долю выручки от показов рекламы будут получать руководители сообществ ***(«ВКонтакте» позволит популярным группам зарабатывать с рекламы в видеороликах // IGate (http://igate.com.ua/lenta/10578-vkontakte-pozvolit-populyarnym-gruppam-zarabatyvat-s-reklamy-v-videorolikah). – 2015. – 7.10).***

***

В начале октября популярный фотосервис Instagram открыл возможность размещать рекламу для 30 стран мира, в их число вошла и Украина. В настоящее время агентства готовят к запуску первые рекламные кампании. Прелесть в том, что управлять такими кампаниями можно из кабинета в Facebook. Редакция обратилась к экспертам из компании Admixer (они являются официальным реселлером Facebook), и они подготовили пошаговую инструкцию о том, какие рекламные форматы доступны для украинских рекламодателей, а также – как оформить и запустить кампанию, пишет AIN.UA (http://ain.ua/2015/10/08/608664?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed %3A+ainua+ %28AIN.UA %29).

В настоящее время в Украине судя по цифрам рекламного кабинета аудитория этой соцсети составляет 460 тыс. пользователей. Ее ядро – молодые люди 15–24 лет, причем 63 % пользователей – девушки.

Доступные на сейчас рекламные форматы – это изображение (обычный пост с пометкой «реклама») и видео до 30 секунд.

Как отмечают в компании, реклама в Instagram может быть нацелена на сбор переходов на сайт, продажи из каталога, конверсию на сайт, повышение вовлеченности для публикации, установки приложения, сбор «лайков», генерацию лидов. Это может быть интересно интернет-магазинам, ритейлу, ресторанам, FMCG и т. д. Всем, у кого может быть качественный визуальный контент.

Далее приводим пошаговую инструкцию от Admixer о том, как украинскому пользователю запустить рекламную кампанию в Instagram.

1. Заходим в Power Editor в рекламном кабинете Facebook и создаем кампанию.

2. Вводим название кампании, выбираем тип модели закупки и цель.

Стоимость размещения может устанавливаться по аукционному принципу или быть фиксированной. В этом пункте рекомендуется выбирать «аукцион».

Цели кампании аналогичны Facebook, выбираем необходимую именно вам. К примеру, клики на веб-сайт.

3. Затем вводим название группы объявлений, название нового объявления и нажимаем «Создать». После этого мы попадаем в Power Editor и переходим непосредственно к настройке кампании.

4. Выбираем нашу группу объявлений. Первое, что мы вводим – бюджет. Допустим, 5 дол.

5. После этого – период проведения кампании. Кампания также может быть без даты окончания, или показываться по графику.

Перед тем, как ввести настройки аудитории, в разделе «Плейсмент» необходимо выбрать Instagram.

6. Здесь же можно выбрать, на каких мобильных устройствах будет показана реклама.

7. Переходим к аудитории. Тут вы можете выбрать сохраненную аудиторию или создать новую. Таргетинги аудитории аналогичны Facebook: гео, демография, интересы и поведение.

8. Оптимизация и ценообразование. Доступные варианты оптимизации: оплата за показы, оплата за клик, показ рекламы как можно чаще, или не чаще одного раза в день.

9. Далее можем выбрать автоматическую или ручную ставку и скорость откртки рекламы: обычный или ускоренный. Все, группа объявлений настроена. Возвращаемся наверх страницы и сохраняем изменения.

10. Переходим к настройке объявления. Здесь сначала выбираем Facebook-страницу и связанный с ней Instagram-аккаунт, с которого и будет показана реклама.

11. Вводим URL рекламируемого сайта, текст поста и загружаем изображение (или видео). Требования к изображению: размер 1080*1080 пикселей, формат 1:1. И не забываем про допустимые 20 % текста на изображении. Видео – .mp4 или .mov, не больше 30 МБ и не дольше 30 секунд.

12. Если необходимо, добавляем кнопку призыва к действию.

13. Чтобы отслеживать эффективность кампании, добавляем URL-метки.

14. Все, объявление готово.

Следить за его статусом и, в случае необходимости, редактировать, можно в том же Power Editor ***(Украинцы теперь могут размещать рекламу в Instagram: как это сделать // AIN.UA (http://ain.ua/2015/10/08/608664?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed %3A+ainua+ %28AIN.UA %29). – 2015. – 8.10).***

***

Twitter внедрил видеорекламу в виде прероллов. Компания добавит прероллы к видеозаписям студий и издателей, которые загружают видеоконтент на сервис и разделит с ними доход от рекламы. «Издатели и создатели смогут монетизировать свой видеоконтент на Twitter, помогая рекламодателям достичь широкую аудиторию и спонсировать отличный контент», – сообщает компания в официальном блоге.

Для использования новой функции издатели загружают видео на video.twitter.com, после чего доходы от рекламы будут поступать им автоматически. Рекламодатели могут выбрать категории видеоконтента, в которых они хотят размещать объявления, и настроить таргетинг на

определенную группу пользователей. Максимальная длительность ролика – шесть секунд. Издатели получат 70 % выручки с рекламы, в отличие от 55 % при размещении в YouTube и Facebook. К программе уже присоединились Mashable, Inc, BuzzFeed, TechCrunch, USA Today, MTV, FOX и другие медиакомпании ***(Twitter внедрил видеорекламу в виде прероллов // Marketing Media Review (http://mmr.ua/show/twitter_vnedril_videoreklamu_v_vide_prerollov). – 2015. – 10.10).***

***

Facebook углубляется в e-commerce, запуская отдельный раздел для шопинга. Социальная сеть хочет поощрить пользователей активней совершать покупки через Facebook, не покидая приложения. Так как только 2 % совершают покупки с мобильных девайсов из-за скорости мобильного трафика, Facebook тестирует размещение каталога ритейлера в рамках рекламных предложений Canvas. Эти посты могут открываться во весь экран, позволяя пользователям пролистывать страницу с видео, фото и текстовыми сообщениями. Цель – дать возможность ритейлерам представить всю коллекцию, чтобы пользователи могли выбрать подходящий для них товар. Совершить саму покупку они смогут на сайте бренда.

Facebook также запускает новый раздел в приложении, который появится в раскрывающемся меню рядом с «группами», «ивентами» и «друзьями». Кроме того, бренды смогут разместить фото с товарами на своих страницах, приобрести которые можно благодаря кнопке «купить». Сеть надеется, что новые функции помогут пользователям больше узнать о новых продуктах, кроме тех, которые появляются в их лентах. А это в свою очередь, должно привести к росту рекламных доходов от брендов ***(Facebook углубляется в e-commerce, запуская отдельный раздел для шопинга // Marketing Media Review (http://mmr.ua/show/facebook_uglublyaetsya_v_e-commerce__zapuskaya_otdelynyy_razdel_dlya_shopinga_). – 2015. – 13.10).***

***

Twitter запустил новую функцию для лучшего таргетирования. Компания представила аналитическую функцию для рекламодателей под названием Conversion Lift. Она измерит конверсию продвигаемых твитов и, проанализировав данные кампании, предложит рекламодателям способы для лучшего таргетирования их аудитории.

Conversional Lift определит успешность рекламных твитов, анализируя клики, установки приложений и подписки на сервисы. Функция разделит целевую аудиторию на две части: людей, которые видели и не видели рекламу, стилизированную под ленту пользователя. Используя эти данные, будет создан отчет, сравнивающий показатели по обеим группам, включая параметр просмотра: на мобильном или на ПК. Twitter сообщил о позитивных результатах тестирования: пользователи, увидевшие рекламный твит,

взаимодействовали с брендом в 1,4 раза чаще и в 3,2 раза вероятней проходила точку конверсии на сайте ***(Twitter запустил новую функцию для лучшего таргетирования // Marketing Media Review (http://mmr.ua/show/twitter_zapustil_novuyu_funktsiyu_dlya_luchshego_targetirovaniya). – 2015. – 18.10).***

***

Symphony, в сентябре запустившая социальную сеть для финансовых компаний Уолл-стрит, привлекла более 100 млн дол. от ряда инвесторов, в число которых входят Google и швейцарский банк UBS, пишет interfax.ru.

Полученные денежные средства будут использованы на «ускорение адаптации глобальных потребителей», отмечается в сообщении компании.

Новая соцсеть позиционируется как более дешевая и удобная альтернатива терминалам Thomson Reuters и Bloomberg, которые в настоящее время доминируют на рабочих местах трейдеров по всему миру. Стоимость услуги составляет 15 дол. в месяц против 1850 дол. в месяц у Bloomberg.

Тестовая версия Symphony насчитывала около 30 тыс. пользователей в банках и управляющих компаниях, в середине сентября был осуществлен официальный запуск соцсети.

В проекте принимают участие McGraw Hill Financial, Dow Jones и Selerity. McGraw-Hill предоставляет соцсети финансовый инструмент S&P Capital IQ, в то время как Dow Jones обеспечивает новостную составляющую. Selerity специализируется на поиске в социальных медиа информации, которая может вызвать изменение котировок.

Директор по данным S&P Capital IQ Д. Рив ранее заявлял, что группа McGraw Hill может увеличить объем контента, предоставляемого через Symphony, в том числе за счет информации энергетического агентства Platts и рейтингового агентства Standard & Poor's.

Symphony была создана при финансовой поддержке крупнейших банков и финкомпаний мира: Goldman Sachs, Bank of America Merril Lynch, Deutsche Bank, Credit Suisse, Citigroup, Bank of New York Mellon, BlackRock, Citadel, HSBC, Jefferies, JPMorgan, Maverick Capital, Morgan Stanley и Wells Fargo. В прошлом году они вложили в этот проект 66 млн дол.

Главным исполнительным директором Symphony является Д. Гюрле, который основал разрабатывающий мессенджеры стартап Perzo в 2012 г. Он не является новичком в сфере мгновенных сообщений, технологий и финансов, поскольку за свою карьеру успел поработать в Skype, Thomson Reuters и Microsoft ***(Соцсеть для финансистов Symphony привлекла 100 млн дол. // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44977/118/lang,ru/). – 2015. – 13.10).***

***

«ВКонтакте» запустила рекламные записи на Android. Теперь, благодаря новой функции, при создании рекламной записи или ее редактировании пользователь может выбирать место ее размещения – на всех платформах, на мобильных устройствах или только на стационарных ПК. Создание объявления доступно в личном кабинете, сообщает softnex.ru.

При помощи опции «Продвижения записей» рекламодатель получает возможность размещать в новостной ленте пользователя рекламу от имени сообщества компании, причем это не зависит от того, подписан пользователь сети на него или нет.

Рекламные записи по внешнему виду абсолютно не отличаются от обычных, но они имеют отметку «Рекламная запись» ***(«ВКонтакте» запустил рекламные записи на Android // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45012/118/lang,ru/). – 2015. – 16.10).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Соцсети не так влияют на успеваемость детей, как видеоигры, следует из результатов проведенного в Великобритании исследования.

Авторы исследования, проводившегося в школах Северной Ирландии, не установили прямой связи между временем, которое тратится детьми на сосцети, и их оценками, передает BBC.

Почти 81 % исследуемых подростков по несколько часов в день проводят в социальных сетях.

Видеоигры же, как утверждают исследователи, напротив, могут ухудшить результаты выпускных экзаменов в средней школе.

77 % подростков, игравших в видеоигры меньше одного раза в неделю, получили на пяти экзаменах GCSE (экзамены, завершающие первую ступень среднего образования в Британии), оценку A (высший балл), B или C ***(Исследование: соцсети не вредят учебе так, как видеоигры // ЗапорожьеИнфо (http://zpinfo.cinfoo.com/news-50266.html). – 2015. – 12.10).***

***

Двойная жизнь: темная реальность за «идеальным» профилем в соцсетях.

4 октября успешный американский дерматолог К. Рикенбах была найдена мёртвой в вестибюле жилого дома. Её кончина по предварительным данным, наступила от передозировки наркотиками, рассказывает издание TJournal. Большой резонанс вызвал характер её смерти: К. Рикенбах годами создавала в соцсетях образ «блондинки-отличницы», далёкой от подобных опасных увлечений.

История женщины сподвигла западные СМИ обратить внимание на набирающую всё больший вес проблему – идеальные профили в соцсетях могут ввести в заблуждение даже самых близких друзей человека, тогда как за ними может скрываться стресс или психическое расстройство.

Профили погибшей в Instagram и Facebook заполнены позитивными фотографиями из путешествий.

По словам друзей семьи, К. Рикенбах была «лучом солнца», и никто не мог ожидать от неё подобного поведения. Несмотря на то, что кончина женщины могла быть просто неудачным стечением обстоятельств, она вызвала бурное обсуждение в американских СМИ.

Однако за последнее время это уже не первый подобный случай в США. В начале 2014 г. в местных СМИ вызвала широкий резонанс история 19-летней студентки М. Холлеран. Привлекательная девушка, занимавшаяся атлетикой, имела успех среди сверстников: её Instagram – это хроника встреч с друзьями, вечеринок и посиделок с родственниками. 14 января М. Холлеран опубликовала снимок украшенных лампочками деревьев в парке, а затем спрыгнула с девятого этажа автомобильной парковки.

Родители М. Холлеран приняли решение не закрывать профиль девушки в Instagram, оставив его как напоминание о том, что реальная жизнь человека, излучающего благополучие в соцсетях, чаще всего катастрофически отличается от виртуальной.

В 2013 г. учёные из двух немецких университетов занимались мониторингом 584 пользователей Facebook. Исследователи выяснили, что один из трёх людей чувствует себя хуже, смотря на снимки друзей – особенно, если они из отпуска. Кроме того, одиноких пользователей соцсетей расстраивают многочисленные поздравления с днём рождения в чужих профилях, а у тех, кто недавно пережил расставание, может вызвать сильный стресс информация о том, что кто-то из их знакомых вступил в новые отношения.

Этот феномен был описан ещё в 1954 г. социальным психологом Л. Фестингером: по его мнению, большинству людей свойственно оценивать самих себя, основываясь на успехах и неудачах других людей. Поэтому соцсети, пользователи которых показывают только свои лучшие стороны, вызывают у многих сильный стресс.

Однако напряжение возникает не только со стороны наблюдателей, но и со стороны самих обладателей «безупречных профилей». Полностью вовлекаясь в создание иллюзии счастья, выбор лучшей еды, лучшей одежды и лучших мест для посещения, они испытывают на себе огромное давление, которое перечёркивает все плюсы такой жизни.

Американка Ч. Фэган даже запустила специальный сайт The Financial Diet, который помогает девушкам справляться с такими зависимостями. На нём она рассказала, что её реальная жизнь в последние годы была достаточно скучной, но она тратила огромные деньги на поддержание иллюзии успеха в соцсетях. В определённый момент она осознала, что залезла в долги на 3400 дол.

В 2014 г. норвежские режиссёры сняли короткометражный фильм, посвящённый этому явлению, который набрал более 13 млн просмотров на YouTube. Короткое видео демонстрирует, как отличается реальная жизнь людей и их статусы на Facebook.

Тогда же художник З. Борн продемонстрировала пользователям сети бессмысленность красивых фотографий из отпусков, «путешествуя» по миру, не выходя из дома – все её снимки были сделаны в фотошопе. Таким образом она хотела напомнить людям, что их друзья в соцсетях каждый день создают «ложную реальность» в своих профилях.

Среди американок в начале 2015 г. начал набирать популярность тренд под названием Finstagram. Чтобы снизить психологическое давление, девушки создают второй профиль в Instagram только для самых близких друзей, в котором рассказывают о своей жизни без прикрас.

Аналогичную концепцию предложила и создательница сайта The Financial Diet. Чтобы снижать накал страстей в социальных сетях она придумала «вторник полной честности». В этот день девушки используют тег #TotalHonestyTuesday, чтобы показывать своим подписчикам свою настоящую жизнь – от целлюлита до выписок по кредитной карте.

Как отмечает The New York Post, такие меры могут помочь справиться со стрессом и не повторить участь К. Рикенбах или М. Холлеран, которые отчаянно нуждались в помощи, но создавали для окружающих иллюзию полного благополучия ***(Двойная жизнь: темная реальность за «идеальным» профилем в соцсетях // UAinfo (http://uainfo.org/blognews/1444733159--.html). – 2015. – 13.10).***

***

Якщо підліток любить проводити ніч безперервно з гаджетами, то він ризикує заробити ожиріння протягом найближчих п’яти років.

Дослідники з Університету Каліфорнії проаналізували дані понад 3300 юнаків і дорослих, передає Business Standard. Виявилося, через кожну втрачену годину нічного сну добровольці набирали зайві 2,1 одиниці Індексу Маси Тіла (ІМТ). Фахівці з’ясували: на вагу підлітків впливав саме час засинання, а не загальна кількість нічного сну. Також дослідження показало, що підлітки рідко спали дев’ять годин і потім страждали від сонливості на уроках у школі. За словами вчених, у підлітковому віці циркадний ритм, що відповідає за фізіологічні та метаболічні функції, зсувається на більш пізній цикл сну. Таким чином, звичка рано лягати спати є запорукою нормальної ваги ***(Нічне сидіння в соцмережах призводить до ожиріння // Експрес онлайн***

(http://expres.ua/news/2015/10/09/155096-nichne-sydinnya-socmerezhah-pryzvodyt-ozhyrinnya). – 2015. – 9.10).

Маніпулятивні технології

В Украине идет тайная война в соцсетях

Штаб информационных войск, созданный Министерством информации, практически перестал присылать задания. Как выяснилось, теперь вместо штаба работают целые спецбатальоны, которые ведут тайную войну в социальных сетях. Сотрудники министерства уверяют, что и сами в лицо не знают своих «агентов», только раз в месяц получают от них отчеты, пишут vesti-ukr.com.

Нефть и вертолеты

Примерно с середины августа штаб информационных войск практически перестал делать рассылку с заданиями – распространять в сети такие-то статьи. Если раньше на почту приходило каждый день по два сообщения с просьбой опубликовать у себя на страничке ту или иную информацию, то теперь штабисты ограничиваются одной-двумя рассылками в неделю.

Самое свежее письмо пришло 2 октября. Нас просят распространять информацию об участии российских войск в операции в Сирии. Еще одно письмо от штаба пришло на почту 21 сентября. Там предлагалось распространить статью о том, что российский канал НТВ назвал британского врача политологом. Этот «политолог» упрекал Президента Украины П. Порошенко в том, что он внес в черный список иностранных журналистов. Также штаб просит распространить информацию, что санкции Украины в отношении авиакомпаний РФ нанесут ей непоправимый удар в части авиатранзита. По словам одного эксперта, РФ понесет потери в десятки миллионов долларов.

Также бойцу информвойск нужно активно размещать в сети информацию о том, что цены на нефть будут продолжать падать и могут достигнуть уровня 20 дол. Причем тема цены на нефть присутствует и в других письмах-инструкциях. Там нам предлагали распространить статью с прогнозом цены на нефть в октябре в 43–46 дол.

Но есть и позитивные новости, касающиеся Украины. Например, в одном из заданий нужно было расширить статью о том, что наш министр финансов Н. Яресько похвалилась перевыполнением бюджета по итогам января – августа. Также в статье сообщается, что доходы бюджета за семь месяцев в целом возросли на 44 %, якобы это связано с увеличением налоговых поступлений.

Еще нам предстояло порадоваться тому, что незаконное правительство ЛНР и ДНР кинуло жителей Донбасса с курсом рубля и гривни. На неподконтрольных территориях, по мнению политолога, установили грабительский курс гривни и рубля – 1:2, так переводят пенсии. В результате люди, конечно, теряют деньги.

Неизвестные волонтеры

В самом Штабе информационных войск говорят, что перешли на новый формат работы. «Да, действительно, раньше мы высылали по два задания в день. В настоящее время перешли на другой режим – одно-два письма в неделю. Дело в том, что у нас сейчас появились информационные спецбатальоны, которые работают в социальных сетях. Они делятся на два лагеря – одни борются с кремлевскими ботами и тролями. Вторые направили свои силы на Восток – борются с местными ботами. Собственно, ведут такую же войну, как и Россия», – рассказал замглавы Министерства информации А. Биденко.

По словам А. Биденко, это волонтеры, которые организовались сами по себе, и он даже сам не знает в лицо этих людей. «Они работают абсолютно бесплатно, сами познакомились и так решили действовать. Теперь каждый день в соцсетях они дают по пять-шесть публикаций. В конце месяца мы только получаем отчеты о проделанной работе», – говорит А. Биденко ***(В Украине идет тайная война в соцсетях // Индустриалка (http://iz.com.ua/ukraina/81453-v-ukraine-idet-taynaya-voyna-v-socsetyah.html). – 2015. – 5.10).***

***

Группа лиц, назвавших себя «Безымянный Союз», собирается бороться с политикой социальной сети, предписывающей использование только реальных имен для собственной странички, сообщает The Verge. Открытое письмо в адрес Facebook было опубликовано на портале Electronic Frontier Foundation.

Facebook имеет строгие правила касательно имени в социальной сети. Так, аккаунт в соцсети может быть заблокирован, если возникнут сомнения в том, что указанное имя – настоящее. Подобная политика, по словам представителя Facebook, дает возможность выявлять аккаунты, созданные для рекламных или мошеннических целей. Кроме того, борьба с анонимностью позволит бороться и с террористами, и с онлайн-преследователями.

«Безымянный Союз» выступает против таких правил. По их словам, Facebook нарушает права трансгендеров, не находящих свое имя соответствующим, людей, скрывающихся от интернет-преследователей, а также тех, чье имя не подпадает под стандартное определение «настоящего имени». Союз требует от Facebook отказаться от такой политики в срок до 31 октября, в противном случае энтузиасты обещали не останавливаться в своей борьбе, пока не будут введены радикальные изменения ***(«Безымянный Союз» будет бороться с политикой Facebook // InternetUA (http://internetua.com/bezimyannii-souaz--budet-borotsya-s-politikoi-Facebook). – 2015. – 13.10).***

***

Time: США програють війну в соцмережах

«Наші вороги використовують проти нас наші технології, а нам для свого захисту використовувати їх заборонено», – Р. Уолцман, колишній керівник програми Агентства передових оборонних дослідницьких проектів.

У новинах часто говорять про кібербезпеки, проте наша увага зосереджена в основному на таких питаннях, як незаконне запозичення інтелектуальної власності, мережеві атаки та порушення закону про недоторканність особистого життя.

Набагато менше уваги приділяється тому, як соціальні мережі сприяють поширенню пропаганди та брехні в масштабах значно небезпечніших, ніж раніше. Безперервний наступ на об'єктивну, правдиву інформацію створює загрозу ослаблення демократичних інститутів, у тому числі й негативного впливу на вільну пресу.

Р. Уолцман: «Як колишній керівник програми Агентства передових оборонних дослідницьких проектів (DARPA), я недавно завершив проект вартістю 50 млн дол. під назвою "Соціальні мережі в системі стратегічних комунікацій", у результаті чого було опубліковано 200 статей, і була створена наука про соціальні мережі.

Під час роботи ми дізналися, що ця "нісенітниця" є тим засобом, який у всьому світі використовується по суті справи для атаки на пресу, а також те, що питання свободи преси – це насправді відволікаючий маневр.

Наприклад, великим фахівцем такого маніпулювання свідомістю є президент Росії В. Путін.

Генеральний директор російського міжнародного інформаційного агентства Д. Кисельов проник у саму суть цієї стратегії, заявивши: "Об'єктивність – це міф, який нам пропонують і нав'язують". Рекламний слоган цієї стратегії – "атакуй пресу, атакуй сенс".

Як відомо, протягом багатьох сторіч пропаганда відігравала важливу роль у роботі уряду та міжнародних відносин. Як правило, слово "пропаганда" використовується в негативному або зневажливому сенсі. Але так було не завжди. У 1622 р. Папа Григорій XV заснував Конгрегацію пропаганди віри з тим, щоб здійснювати нагляд за діяльністю місіонерів у Новому Світі та в інших місцях. Частково це було реакцією на поширення протестантизму і повинно було допомогти людям слідувати "вірним" шляхом.

Е. Бернейз, якого багато хто вважає батьком сучасної PR-індустрії, пропонував кілька більш гнучких визначень. Він говорив: "Пропаганда – це послідовна, доволі тривала діяльність, спрямована на створення або інформаційне оформлення різних подій з метою впливу на ставлення мас до підприємства, ідеї або групи". Він також відзначав силу її впливу, заявляючи, що "свідоме та вміле маніпулювання впорядкованими звичками і смаками мас є важливою складовою демократичного суспільства. Приводить у рух цей невидимий суспільний механізм невидимий уряд, який є істинною правлячою силою в нашій країні".

На жаль, США не здатні ефективно скористатися перевагами соціальних мереж та Інтернету через непродуману американську політику та застарілі

закони. Наприклад, згідно з главою 3093 (f) розділу 50 Кодексу США, нашим розвідувальним органам і службам фактично забороняється здійснювати діяльність “з метою здійснення впливу на політичні процеси в США, громадську думку, політичний курс і засоби масової інформації”.

Відносно соціальних мереж та Інтернету не існує ніяких заходів, що дають змогу гарантувати, що жоден американець не буде піддаватися ненавмисному впливу інформаційних операцій, об’єктом яких він не є, і це положення широко застосовується як підстава для заборони будь-якого виду протидії цим операціям. Хоча цей принцип був доцільний у ті часи, коли інформаційному впливу піддавалися лише друковані ЗМІ, радіо і телебачення, у сучасному світі глобального миттєвого обміну інформацією він не має ніякого сенсу.

У міністерстві оборони через нестачу розуміння та через страх юристам доводиться тлумачити в буквальному сенсі та педантично застосовувати закони, ухвалені стосовно розвідувальних операцій, цілі яких – зовсім інші. У Держдепартаменті аналітикам у більшості випадків фактично забороняється активно користуватися відкритими соціальними мережами – в основному через те, як юристи Держдепу трактують Закон про недоторканність приватного життя 1974 р. та інші законодавчі акти. Це означає, що, по суті, будь-яка доцільна дія, яку можуть виконувати їхні аналітики, наприклад, запис результатів виявлення та профілювання становлять небезпеку груп або окремих осіб на основі наявної у відкритому доступі інформації, відразу ж підпадає під категорію “збір розвідувальних даних” з усіма відповідними наслідками у вигляді бюрократичних і заборонних заходів.

Спроби юристів усіх урядових органів застосувати ці та багато інших застарілих законів і положень призвели до впровадження надто суворих порядків, зайвої перестраховки та нестандартних методів роботи, через що виникла плутанина та повна бездіяльність. Сенс проблеми полягає в тому, що уряд США не в змозі захистити нас від маніпулювання, яке здійснюють не визнаючи ніяких кордонів діячі та політичні сили – державні та інші – у неймовірних масштабах.

Ось вам приклад маніпулювання свідомістю. У березні 2006 р. батальйон спецназу США вступив у бій з угрупованням “Джаїш аль-Махді”, що використовував тактику “ескадрону смерті” і більше відому як “Армія Махді”. Американські солдати вбили 16–17 бойовиків, ще 17 узяли в полон, знищили схрон із зброєю та врятували сильно побитого заручника. Усе це виглядає як успішна операція, якщо не враховувати того, що за той час, поки солдати поверталися на базу (тобто, менш ніж за годину) бойовики повернулися на поле бою, розчистили його і поклали тіла своїх загиблих товаришів таким чином, щоб усе виглядало так, ніби американські солдати їх убили, коли ті були беззбройні та здійснювали наказ. Бойовики виклали фотографії та прес-релізи арабською та англійською мовами, представивши все як нібито скоєний кривавий злочин.

Американські солдати зняли всі свої дії на плівку і могли довести, що все відбувалося зовсім не так. Однак минуло майже три дні перш ніж американські військові спробували викласти свою версію події в ЗМІ. Але було вже пізно – передбачуваної шкоди було завдано. І що ще гірше, військових змусили провести розслідування, яке тривало 30 днів, протягом яких батальйон діяв.

Це прекрасний приклад того, як можна використовувати соціальні мережі та Інтернет, щоб завдати поразки противнику, якого перемогти за допомогою фізичної сили не виходить.

Цей випадок став першим наочним прикладом того, як наші супротивники можуть відслідковувати реакцію американської аудиторії на свої послання в режимі реального часу, перебуваючи на відстані тисяч кілометрів. Соціальні мережі та Інтернет відкривають нашим супротивникам необмежений доступ до потрібної їм аудиторії в будь-якій точці планети, поки американський уряд не діє з причин правового та політичного характеру.

Використання соціальних мереж та Інтернету стрімко стає потужним засобом ведення інформаційної війни та змінює характер конфлікту всюди в світі. Через невідповідність політики та законодавства США ми як і раніше можемо розраховувати виключно на звичайні способи ведення війни, що ставить нас у вкрай невигідне становище. Ми втрачаємо свою військову та політичну перевагу та конкурентоспроможність.

У рамках нашого проекту "Соціальні мережі в системі стратегічних комунікацій" ми займалися створенням фундаментальної науки про соціальні мережі. Ми показали, що існує можливість протидіяти маніпулюванню свідомістю і захистити вільну пресу. Наприклад, вчені розробили технології, що дають змогу виявляти ботів – автоматичні програми, що діють у соціальних мережах, у тому числі облікові записи-автомати, що діють у Twitter і створені для спілкування з цільовою аудиторією і впливу на неї шляхом переконання. Ми також створили новий та ефективний спосіб визначення мема (теми, ідеї чи поняття в соціальних мережах) і метод раннього виявлення потенційно значущих мемів.

Проте наш разовий внесок у проект у сумі 50 млн дол. необхідно оцінювати порівняно з річним бюджетом інформаційного агентства Russia Today, що становить більше 300 млн дол., не кажучи вже про ті суми, які витрачають Китай, ІГІЛ та інші держави, число яких постійно зростає. Але що ще гірше, наші вороги без обмежень використовують проти нас наші технології, а от нам для свого захисту використовувати їх заборонено» ***(Time: США програють війну в соцмережах // INFORMAL (http://informal.com.ua/western-view/time-ssha-prohrayut-vijnu-v-sotsmerezhah/). – 2015. – 14.10).***

Зарубіжні спецслужби і технології «соціального контролю»

В настоящее время Херсонская область является территорией Украины, где не проходят активные боевые действия. Но это не значит, что российские сепаратисты оставили этот регион в покое. Сотрудники правоохранительных органов и Службы безопасности Украины активно мониторят и пресекают антиукраинскую деятельность на Херсонщине.

По словам одного из сотрудников СБУ Херсона: «Из-за того, что на Востоке Украины стали стрелять меньше, сепаратисты начали активно проявлять себя в Интернете. Они участвуют во всевозможных обсуждениях, часто захотят на проукраинские сайты и “тролят” патриотическую информацию».

Чаще всего обсуждению со стороны сепаратистов подвергаются материалы про мобилизацию, отвагу украинских воинов, ситуацию в зоне АТО. Люди, которым хорошенько заплатили, готовы приводить разнообразные доводы против подобной информации.

Кроме активного общения интернет-сепаратисты занимаются вербовкой новых приспешников. Чаще всего это происходит после того, как человек регистрируется на пророссийских группах в социальных сетях. После визуального изучения «кандидата» на связь с ним выходит «куратор». Если в результате общения человек соглашается на условия «работы», он получает обещания о вознаграждении и конкретные указания. Когда вербовка не получатся, «гости» из России приезжают в Украину с «рабочим визитом».

Распространение неправдивой информации в Интернете, призывы к свержению власти и установление «Русского мира» – всё это активно «продвигают» наёмники соседней страны в виртуальном пространстве. За 2015 г. за подобную деятельность к ответственности всё чаще и чаще привлекались иностранцы из России. К примеру, за январь – июль этого года сотрудниками Управления СБУ Херсонской области было установлено трое граждан РФ, которые причастны к подрывной деятельности в информационной сфере. Правоохранители провели относительно задержанных лиц тщательную проверку и по её итогу приняли правомерные решения. На основании наработанных материалов гражданам страны-агрессора было запрещено въезжать на территорию Украины в течении пяти лет.

Антиукраинская деятельность в Интернете в настоящее время переживает не лучшее время из-за постоянного контроля со стороны СБУ. Для обеспечения безопасности в «интернет-паутине» в правоохранительных органах есть специальные отделы. Они занимаются тем, что отслеживают деятельность «подозрительных личностей». Благодаря новейшим системам слежения, работники СБУ могут получить доступ практически к любой информации в Интернете. Именно из-за этого и опыта работы, правоохранителям удаётся пресекать действия, которые направлены на раскол Украины ***(СБУ отлавливает на Херсонщине кремлевских интернет-***

троллей // Типичный Херсон (http://www.t.ks.ua/sbu-otlavlivaet-na-hersonshchine-kremlevskih-internet-trolley). – 2015. – 5.10).

***

Користувачі смартфонів майже нічого не можуть зробити для того, аби не дозволити спецслужбам отримати «повний контроль» над своїм телефоном, сказав викривач американських спецслужб Е. Сноуден.

Колишній співробітник американських спецслужб розповів, що Управління урядового зв'язку Великобританії (GCHQ) має можливість зламувати телефони без відома користувача, повідомляє ВВС Україна.

За словами Е. Сноудена, GCHQ може отримати доступ до телефону, відправивши на нього зашифроване текстове повідомлення, після чого спецслужби зможуть слухати все, що відбувається навколо, а також робити фотографії.

Уряд Великобританії відмовився прокоментувати цю заяву.

Э. Сноуден дав інтерв'ю телепрограмі ВВС «Панорама» з Москви, куди він втік 2013 р., передавши до цього пресі деталі широкомасштабної програми стеження за Інтернетом і мобільними телефонами, яку здійснювало Агентство національної безпеки США, на яку він працював.

Він не сказав, що GCHQ або АНБ зацікавлені в масовому моніторингу повідомлень простих громадян, але при цьому заявив, що обидва агентства доклали чимало зусиль для того, щоб розробити технологію, що дає можливість їм зламувати смартфони. «Вони хочуть не вас, а ваш телефон», – сказав він ***(Спецслужби дистанційно управляють смартфонами, – Сноуден // Західна інформаційна корпорація (http://zik.com.ua/ua/news/2015/10/06/spetssluzhby_dystantsiyno_upravlyayut_smartfonamy__snouden_630638). – 2015. – 6.10).***

***

Служба безпеки України затримала мешканку м. Кривій Ріг, яка за вказівкою кураторів з Російської Федерації вела активну антиукраїнську пропаганду в соціальних мережах.

Як повідомляє прес-центр АТО, 32-річна зловмисниця поширювала матеріали, направлені на зрив процесу мобілізації, дискредитацію діяльності чинної влади, відкрито закликала до підтримки злочинних дій терористів так званих ДНР/ЛНР та створення подібних «республік» в інших областях України.

За словами затриманої, після її спроби припинити незаконну діяльність куратори зі спецслужб РФ, погрожуючи розправою, примусили жінку продовжити антиукраїнську пропаганду.

Під час обшуку за місцем проживання правоохоронці вилучили комп'ютерну техніку, за допомогою якої поширювали спеціальні інформаційні матеріали сепаратистського характеру.

У рамках кримінального провадження за ч. 2 ст. 110 (посягання на територіальну цілісність і недоторканність України) Кримінального кодексу

України тривають слідчі дії ***(Мешканку Кривого Рогу затримали за антиукраїнську пропаганду в соцмережах // Інформаційна агенція «Вголос» (http://vgolos.com.ua/news/meshkanku_kryvogo_rogu_zatrymaly_za_antyukrainsku_propagandu_u_sotsmerezhah_194268.html). – 2015. – 6.10).***

***

За останні два роки відеосервіс YouTube, що належить Google, видалив до 14 млн відеозаписів, які містили пропаганду чи заклики до вербування бойовиків у різні терористичні організації.

З такою заявою виступив глава виконавчого директора Контртерористичного комітету Радбезу ООН Ж. Лаборде.

Про це пише видання «Дождь» з посиланням на Jordan Times.

Він зазначив, що такі угруповання, як заборонена «Ісламська держава», активно займаються набором бойовиків у соціальних мережах. За його словами, приватні компанії роблять свій внесок у боротьбу з таким вербуванням: YouTube видалив 14 млн відеозаписів за два роки, Facebook реагує на мільйон порушень на тиждень.

У контртерористичному комітеті СБ ООН підрахували, що за чотири місяці в кінці минулого року прихильники «Ісламської держави» завели до 46 тис. облікових записів у Twitter, що надало вербувальникам великі можливості по веденню пропаганди серед молодих людей.

За даними ООН, нині у світі налічується близько 30 тис. бойовиків, які вступили до лав збройних угруповань за кордоном. Це вихідці з більш ніж сотні країн світу. «Це не проблема певного регіону, це проблема всього світу», – підкреслив Ж. Лаборде ***(14 млн екстремістських відео було видалено на «YouTube» – СБ ООН // Інформаційна агенція «Вголос» (http://vgolos.com.ua/news/14_mln_ekstremistskyh_video_bulo_vydaleno_na_youtube__sb_oon_194374.html). – 2015. – 7.10).***

***

В Германии планируют создать службу по цензурированию сети, в частности, немецкого сегмента социальной сети Facebook. Контроль за комментариями и сообщениями вероятнее всего будет курировать экс-агент немецкого Министерства государственной безопасности А. Кахене. Такое решение было объяснено необходимостью соблюдения норм политкорректности.

По словам министра юстиции Х. Мааса, нельзя быть терпимыми к тем пользователям, которые призывают к ксенофобии и расизму. Известно, что простым удалением комментариев дело не ограничится. Х. Маас считает, что нужно создать специальную комиссию, которая будет заниматься потенциально опасными экстремистами. С этой целью ведомство обратилось в спецслужбы за помощью.

В самой соцсети Facebook такой подход был оценен положительно. Пресс-секретарь немецкого сегмента социальной сети отметил, что вопрос был

рассмотрен и воспринят очень серьезно. Пользователям желательно соблюдать законы и не использовать сеть для возбуждения ненависти ***(В Германии создают службу по цензуре в сети // InternetUA (http://internetua.com/v-germanii-sozdauat-slujbu-po-cenzure-v-seti). – 2015. – 7.10).***

***

Социальную сеть Facebook и несколько других крупных игроков американского коммуникационного рынка обвинили в массовой правительственной слежке.

По мнению европейского суда, Facebook не обеспечивает достаточного уровня защиты персональных данных жителей ЕС. Такой вывод был сделан из обращения одного из пользователей, потребовавшего не передавать его личные данные на серверы в США из-за сотрудничества сервиса с американским АНБ. Как доказательства пользователь привел документы, рассекреченные Э. Сноуденом.

В 2000 г. Еврокомиссия разрешила обмен данными коммерческого характера между США и ЕС. Решение получило название Safe Harbour и дало возможность тысячам компаний обмениваться электронными данными и информацией в упрощенном порядке, то есть без дорогостоящих мер защиты. Однако Facebook, по мнению Европейского суда, должной защиты не обеспечивает. В итоге, передача информации о пользователях из Европы на американские сервера компании Facebook может быть прервана до получения результатов расследования ***(Facebook обвинили в работе на спецслужбы // InternetUA (http://internetua.com/Facebook-obvinili-v-rabote-na-specslujbi). – 2015. – 8.10).***

***

СБУ разоблачили противоправную деятельность двух жителей Черкасс, которые пропагандировали сепаратизм через российские социальные сети.

Как сообщили в пресс-группе УСБУ в Черкасской области, они распространяли материалы антиукраинского содержания с призывами к насильственному изменению или свержению конституционного строя и захвату государственной власти. А также размещали сообщения, фото- и видеоматериалы, перепечатки сепаратистского характера, содержащие призывы, направленные на насильственное изменение границ территории или государственной границы Украины.

По этому факту начаты уголовные производства по ч. 1 ст. 110 (посягательство на территориальную целостность и неприкосновенность Украины) и ч. 2 ст. 109 (распространение материалов к насильственному изменению или свержению конституционного строя или захвату государственной власти) Уголовного кодекса Украины. Продолжается следствие ***(СБУ разоблачила двух пропагандистов сепаратизма в Черкассах / InternetUA (http://internetua.com/sbu-razoblacsila-dvuh-propagandistov-separatizma-v-cerkassah). – 2015. – 11.10).***

***

В Анкаре стали недоступны Twitter и Facebook. Об этом сообщает BGN News.

Официальными комментариями по поводу блокировки издание не располагает, но отмечает, что власти ранее прибегали к ограничению доступа к социальным платформам при угрозе безопасности.

Соцсети стали недоступны сразу после серии взрывов, которые прогремели в центре Анкары. Теракт произошел перед началом мирной демонстрации за прекращение боевых действий между турецкими властями и курдами ***(Жителям Анкары заблокировали доступ к Twitter и Facebook // InternetUA (http://internetua.com/jitelyam-ankari-zablokirovali-dostup-k-Twitter-i-Facebook). – 2015. – 10.10).***

***

У Луганській області Служба безпеки України припинила протиправну діяльність редактора групи антиукраїнської спрямованості в одній із соціальних мереж російського походження.

Про це повідомляє прес-служба СБУ у Facebook.

«На сторінці групи, що існувала з кінця травня цього року, публікувалася інформація антидержавного характеру, у тому числі й про вербування найманців до терористичного угруповання ЛНР, організацію фінансової допомоги бойовикам. Також розміщувалися матеріали, що дискредитували Збройні сили та правоохоронні органи України, українську мову та державну символіку», – ідеться у повідомленні.

Як зазначають у відомстві, місцевим редактором спільноти був студент із Сєвєродонецька, а його діями керував адміністратор, який користувався анонімним акаунтом із зареєстрованою в Санкт-Петербурзі IP-адресою. Саме від нього студент отримав інструкції щодо реєстрації фейкового акаунта, прав редактора групи та контенту, який регулярно мав розміщувати на сторінці.

Крім того, за завданням «координатора», правопорушник повідомляв про пересування військової техніки та особового складу українських підрозділів.

Прес-служба зазначає, що редактора групи затримано, він визнав свою провину. Розпочато кримінальне провадження за ч. 2 ч. 110 (посягання на територіальну цілісність і недоторканість України) Кримінального кодексу України. Триває досудове розслідування ***(СБУ викрила вербувальника терористів ЛНР у соцмережах // InternetUA (http://internetua.com/sbu-vikrila-verbuvalnika-terorist-v--lnr--u-socmerejah). – 2015. – 10.10).***

***

В Украине в рамках реформы в системе правоохранительных органов появится киберполиция. Ведомство будет заниматься защитой в виртуальном пространстве, в том числе, борьбой с пиратством, а также полицейской

помощью онлайн. Об этом сообщил глава МВД А. Аваков на своей странице в Facebook.

«С 26 октября начнется конкурс для будущих киберполицейских. До 5 ноября штат киберполиции будет сформирован и начнется заключительный переходный этап выстраивания нового функционала киберполиции и переподготовки персонала», – написал А. Аваков.

Как отметил министр, в задачи киберполиции входит:

1. Реализация государственной политики в сфере противодействия киберпреступности.

2. Противодействие киберпреступности:

В сфере использования платежных систем:

– Скимминг (шиминг) – незаконное копирование содержимого треков магнитной полосы (чипов) банковских карт;

– Кэш-треппинг – похищение наличности из банкомата путем установки на шатер банкомата специальной удерживающей накладки;

– Кардинг – незаконные финансовые операции с использованием платежной карточки или ее реквизитов, не инициированные или не подтвержденные ее держателем;

– Несанкционированное списание средств с банковских счетов с помощью систем дистанционного банковского обслуживания.

В сфере электронной коммерции и хозяйственной деятельности:

– Фишинг – выманивание у пользователей Интернета их логинов и паролей к электронным кошелькам, сервисам онлайн-аукционов, перевода или обмена валюты;

– Онлайн-мошенничество – завладение средствами граждан через интернет-аукционы, интернет-магазины, сайты и телекоммуникационные средства связи.

В сфере интеллектуальной собственности:

– Пиратство – незаконное распространение интеллектуальной собственности в Интернете;

– Кардшаринг – предоставление незаконного доступа к просмотру спутникового и кабельного TV;

В сфере информационной безопасности:

– Социальная инженерия – технология управления людьми в интернет-пространстве;

– Создание и распространение вирусов и вредоносного программного обеспечения;

– Противоправный контент – контент, который пропагандирует экстремизм, терроризм, наркоманию, порнографию, культ жестокости и насилия;

– Рефайлинг – незаконная подмена телефонного трафика.

3. Заблаговременное информирование населения о появлении новых киберпреступлений.

4. Внедрение программных средств для систематизации и анализа информации о киберинциденты, киберугрозы и киберпреступления.

5. Реагирование на запросы зарубежных партнеров, которые будут поступать по каналам Национальной круглосуточной сети контактных пунктов.

6. Участие в повышении квалификации работников полиции по применению компьютерных технологий в противодействии преступности.

7. Участие в международных операциях и сотрудничество в режиме реального времени. Обеспечение деятельности сети контактных пунктов между 90 странами мира ***(В Украине появится киберполиция: чем займутся правоохранители в сети // InternetUA (http://internetua.com/v-ukraine-poyavitsya-kiberpoliciya--csem-zaimutsya-pravoohraniteli-v-seti). – 2015. – 13.10).***

***

Все больше онлайн-СМИ закрывают для читателей доступ к комментированию своих материалов, утверждает Wired. По мнению издания, такой тренд появился из-за роста интернет-пользователей и, как следствие, больших затрат на модерацию их комментариев, а также появления роста трафика из социальных сетей Facebook и Twitter. Об этом пишет sostav.ru.

Тренд на отказ от комментирования новостей на сайте наметился в 2013 г., утверждает Wired. Тогда журнал Popular Science стал первым изданием, демонстративно отказавшимся от комментариев. На такой шаг издание пошло после публикации исследования, согласно которому мнения читателей под статьей сильно меняли восприятие от текста.

В 2014 г. своим читателям закрыли доступ к комментированию Chicago Sun-Times, CNN, Reuters и Re/code. «Годами онлайн-медиа использовали пользовательские комментарии – от The New York Times до Fox News. Тем не менее, в этом году от отзывов читателей онлайн отказались и такие порталы как Bloomberg, The Verget и The Daily Beast», – отмечают авторы публикации.

В течение прошлой недели доступ к комментариям также закрыл сайт Motherboard, предложив читателям направлять свои замечания и мнения напрямую в письме к редактору. Портал Reddit запустил новый сайт Upvoted, где также не стал вводить функцию пользовательского комментирования.

Российские СМИ также следуют мировым тенденциям. На фоне политической ситуации в стране и ужесточения ответственности за то, что на сайтах пишут читатели, от возможности комментирования материалов уже отказалась газета «Ведомости» и Lenta.ru. Частично доступ закрыл также портал Slon.ru ***(СМИ закрывают комментарии пользователей // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44962/118/lang,ru/). – 2015. – 12.10).***

***

Российские власти проводят эксперименты по отключению Интернета в стране.

Министерство связи и массовых коммуникаций России и Роскомнадзор весной 2015 г. попытались отключить Россию от Интернета. Об этом сообщает CNews со ссылкой на вице-президента Медиакоммуникационного союза (МКС) и генерального директора провайдера «Эр-Телеком» А. Семерикова.

Роскомнадзор посылал на диспетчерские пункты крупных операторов связи указания блокировать трафик с различных зарубежных магистральных каналов. Крупные провайдеры смогли заблокировать его через соответствующую настройку в системах управления трафиком.

Однако эксперимент оказался неудачным: трафик продолжал уходить за рубеж, и его маршруты остались для правительства неизвестными. По мнению А. Семерикова, причиной неудачи является большое количество небольших, «серых», провайдеров, работу которых государство контролирует слабо. У этих компаний нет систем DPI, что не дает возможности правительству управлять их трафиком. Кроме того, они часто используют спутниковые каналы, из-за чего появляются неконтролируемые властями стыки между российским и зарубежным Интернетом.

Лицензии на провайдерскую деятельность выдаются практически в уведомительном порядке, посетовал А. Семерюк. Из-за этого в России насчитывается около 11 тыс. обладателей таких лицензий. В МКС считают, что госконтроль за деятельностью небольших операторов кабельного ТВ и интернет-провайдеров надо усилить.

В пресс-службе Минкомсвязи отказались комментировать слова главы «Эр-Телекома» ***(Российские власти проводят эксперименты по отключению Интернета в стране // IGate (http://igate.com.ua/lenta/10715-rossijskie-vlasti-provodyat-ehksperimenty-po-otklyucheniyu-interneta-v-strane). – 2015. – 15.10).***

Проблема захисту даних. DDOS та вірусні атаки

Данные многочисленных пользователей соцсети «ВКонтакте» были украдены с помощью музыкального приложения для смартфонов на базе ОС Android, сообщили специалисты «Лаборатории Касперского».

Жертвами преступников могли стать сотни тысяч человек, проживающие в основном в России.

Приложение «Музыка ВКонтакте», которое содержало вредоносный код и предлагало пользователям ввести свой логин и пароль от соцсети, можно было скачать в официальном магазине Google Play. При этом злоумышленники проверяли подлинность введенных данных через легитимный сервер аутентификации «ВКонтакте».

На сайте «Касперского» отмечается, что в основном преступники, занимавшиеся также продвижением групп в соцсетях, использовали украденные данные для добавления аккаунтов пользователей в эти группы,

однако встречаются и случаи, когда законный владелец терял доступ к своей странице, поскольку злоумышленники меняли его пароль.

«Лаборатория Касперского» уже уведомила Google Play о вредоносной проблеме, однако злоумышленники добавляют новые версии программы взамен удаленных. В настоящее время, сообщают специалисты, работает уже седьмая такая версия.

Антивирусная лаборатория советует пользователям устанавливать только официальные приложения «ВКонтакте» и использовать двухфакторную авторизацию с получением необходимого для входа кода по СМС.

Если же владельцы смартфонов уже установили сомнительное приложение, им рекомендуется как можно скорее его удалить и сменить логин и пароль в соцсети ***(Данные сотен тысяч пользователей «ВКонтакте» оказались в руках злоумышленников // InternetUA (http://internetua.com/dannie-soten-tisyacs-polzovatelei--vkontakte--okazalis-v-rukah-zloumishlennikov). – 2015. – 10.10).***

***

В компании «ВКонтакте» прокомментировали сообщение о краже учетных данных пользователей соцсети через приложение для проигрывания музыки, пишет РБК.

По словам пресс-секретаря социальной сети Г. Лобушкина, пользователи «добровольно» отдали данные мошенникам.

«Речь не идет о взломе. Люди фактически сами добровольно отдали мошенникам свои данные. Мы не раз предупреждали, что посторонние программы могут быть опасны», – отметил он.

Г. Лобушкин добавил, что сотрудники «ВКонтакте» периодически находят такие приложения и жалуются на них в Google, но появляются новые ***(«ВКонтакте» прокомментировала кражу данных сотен тысяч пользователей соцсети // InternetUA (http://internetua.com/vkontakte--prokommentirovala-kraju-dannih-soten-tisyacs-polzovatelei-socseti). – 2015. – 10.10).***

***

ИБ-исследователи из Cisco Talos обнаружили новую разновидность вредоносного ПО Fareit. По словам специалистов, вредонос изначально предназначался для взлома компьютеров и загрузки другого вредоносного ПО, которое инфицировало систему. Однако Fareit «эволюционировал», и его начали использовать для эксфильтрации данных, в частности для хищения пользовательских паролей из браузеров.

В мае 2013 г. Fareit распространялся в масштабной хакерской кампании, во время которой использовался набор эксплоитов Blackhole. В 2014 г. ИБ-эксперты из Fidelis Cybersecurity обнаружили новый вариант спам-ботнета Pushdo, который атаковал компьютерные системы в 50 странах мира. Ботнет был способен рассылать 7,7 млрд спам-сообщений в день. Больше всего от

хакерской кампании пострадали пользователи в Индии, Индонезии, Турции и Вьетнаме. Последняя версия ботнета Pushdo использовалась злоумышленниками для распространения таких вредоносов, как Fareit, Cutwail, Dyre и Zeus. В начале текущего года хакеры использовали тактику перенаправления жертв на содержащие Fareit интернет-ресурсы.

Новая версия Fareit способна изменять хэш файла для каждой «инфекции», даже если имя файла остается таким же. Эта возможность позволяет вредоносу оставаться незамеченным для антивирусных программ. ИБ-эксперты из Cisco Talos обнаружили подозрительные исполняемые файлы, которые загружались с последующих адресов – 89.144.2.119/cclub02.exe и 89.144.2.115/cclub02.exe в одной из сети своих клиентов.

ИБ-эксперты обнаружили 2455 образцов Fareit, из которых только 23 имели одинаковый хэш. Все обнаруженные экспертами варианты вредоноса были связаны с двумя C&C-серверами. Специалисты отмечают, что несмотря на попытки злоумышленников создать вредонос с различными хэшами, они используют аналогичные или крайне схожие имена файлов.

Проверка IP-адресов, связанных с вредоносной кампанией Fareit, показала, что практически все они находятся в США, Украине и Китае. Предполагается, что за хакерской кампанией может стоять одна группа злоумышленников ***(Вредонос Fareit обходит антивирусы благодаря использованию разных хэшей файла в каждой атаке // InternetUA (http://internetua.com/vredonos-Fareit-obhodit-antivirusi-blagodarya-ispolzovaniua-raznih-heshei-faila-v-kajdoi-atake). – 2015. – 6.10).***

***

Мы все привыкли к тому, что персональные компьютеры то и дело атакуют вирусы. Однако реалии таковы, что от вредоносного кода страдают даже смартфоны и другие девайсы. Например, вы когда-нибудь могли себе представить, что вирус способен поселиться в фотоаппарате?

Пользователь Twitter @arvidOS поведал о случае заражения фотоаппарата вирусом. Речь идет о фотоаппарате Nikon Coolpix S800c, и это первая фотокамера, работающая на платформе Android, выпущенная еще в далеком 2012 г. Девайс имеет модуль Wi-Fi, а потому он способен выходить в Интернет, чем и пользовался ее владелец. По всей видимости, мужчина часто посещал ресурсы порнографического характера. Там он и подхватил вирус.

Вредоносное ПО получило полный контроль над девайсом, заблокировав его. Чтобы вернуть себе фотоаппарат, пользователь должен в течение 24 часов «оплатить штраф» в размере 500 р. ***(Страшный вирус атакует фотоаппараты // InternetUA (http://internetua.com/strashnii-virus-atakuet-fotoapparati). – 2015. – 5.10).***

***

5 октября MacDigger написал о новом вредоносном приложении YiSpecter, которое, по заявлению экспертов, успешно инфицирует iOS-

устройства без джейлбрейка с ноября 2014 г. Спустя несколько часов после публикации Apple официально прокомментировала эту информацию.

«Проблема касается только пользователей старых версий iOS, которые при этом скачивали вредоносное ПО из недоверенных источников, – заявил представитель Apple. – Мы закрыли эту проблему еще в iOS 8.4 и уже также заблокировали приложения, распространявшие этот вредонос.

Мы призываем пользователей устанавливать свежие версии iOS для того, чтобы быть защищенными от любого вредоносного ПО. Мы также призываем их скачивать контент только из проверенных источников, вроде App Store и обращать внимание на любые предупреждения, которое появляются перед началом загрузки приложений».

Троян YiSpecter, который выдавал себя за медиаплеер для просмотра порно-контента QVOD, был обнаружен 10 месяцев назад. Векторами атак являлись перехват интернет-трафика, червь для Windows, атаковавший мессенджер Tencent QQ, а также онлайн-сообщества, участники которых устанавливали сторонние приложения за вознаграждение от их разработчиков.

Точное количество пострадавших устройств пока неизвестно, однако, по данным исследователей, YiSpecter инфицирует iPhone и iPad без джейлбрейка с ноября 2014 г. Инфицировав устройство, вредонос может устанавливать нежелательные приложения, загружать ПО и заменять им легитимные программы, отображать на весь экран нежелательную рекламу, изменять закладки и поисковую систему по умолчанию в Safari, отсылать информацию пользователей на свой сервер и автоматически восстанавливаться после того, как пользователь вручную удалил его ***(Apple прокомментировала сообщения о трояне, который атакует iOS-устройства без джейлбрейка // InternetUA (http://internetua.com/Apple-prokommentirovala-soobsxeniya-o-troyane--kotorii-atakuet-iOS-ustroistva-bez-djeilbreika). – 2015. – 6.10).***

***

У патріотичній мережі «Друзі» заявляють про рейдерське захоплення українського соціального ресурсу невідомими. Про це Львівському порталу повідомляє адміністрація сайту.

Згідно з інформацією, у ніч з 1 на 2 жовтня 2015 р. близько першої години ночі сайт зазнав хакерської атаки, після якої адміністрація мережі «Друзі» втратила остаточний контроль і доступ до соціального ресурсу.

За словами одного із власників мережі «Друзі» Ю. Ковальчука, «протягом останніх шести місяців адміністрація мережі отримувала численні погрози у свій бік, однак за відмову співпрацювати з політичною силою “Опозиційний блок” сайт зазнав потужного рейдерського захоплення».

Адміністратори наголошують, що на сьогодні сайт «Друзі» перенесено та попереджають про можливі провокації. Також адміністрація припускає, що атака невідомих рейдерів – це помста за патріотичне спрямування мережі.

«Ми переконані, що захоплення мережі – це робота проросійських сил, адже “Друзі” виключно українська, патріотична мережа. Також ми звертаємось

до губернатора Одеської області М. Саакашвілі із проханням взяти під особистий контроль хід цього розслідування правоохоронними органами. Ми переконані, що захоплення мережі “Друзі” повинно бути розслідуване якнайшвидше», – наголосив Ю. Ковальчук.

Варто додати, що ще одна українська соціальна мережа Weua після серйозних збоїв у роботі перебуває на оновленні та є тимчасово недоступною для користувачів ***(Хакери захопили українську патріотичну мережу «Друзі» // Львівський портал (http://portal.lviv.ua/news/2015/10/06/hakeri-zahopili-ukrayinsku-patriotichnu-merezhu-druzi). – 2015. – 6.10).***

***

Пользователи «ВКонтакте» массово пожаловались на блокировки их страниц в социальной сети, сообщает TJournal.

Как причина блокировки, по словам пользователей, указывалась «подозрительная активность страницы» – одинаковые сообщения об этом получили все «замороженные» участники. Для решения проблемы пользователям предлагалось обратиться в службу технической поддержки.

Как утверждает один из пострадавших, сначала на его смартфоне отказала авторизация «ВКонтакте», а после этого, зайдя на сайт «ВКонтакте» с компьютера, он получил сообщение о том, что его аккаунт заблокирован.

Блокировка, как выяснил TJournal, стала результатом программного сбоя, который затронул около семи тысяч человек.

В настоящее время всем заблокированным пользователям вернули доступ к страницам. Объем подверженных сбою пользователей составил около 0,01 % суточной аудитории сайта ***(«ВКонтакте» массово заблокировал своих пользователей // InternetUA (http://internetua.com/vkontakte--massovo-zablokiroval-svoih-polzovatelei). – 2015. – 8.10).***

***

Вредоносная реклама – это один из самых популярных методов, который киберпреступники используют для инфицирования компьютеров. Прежде всего, для этой цели не обязательно взламывать ресурсы. К тому же рекламные серверы часто доставляют контент большому количеству различных пользователей, поэтому список жертв может быть достаточно обширным. Кроме того, рекламные объявления отображаются в произвольном порядке, а значит, вредоносная реклама появляется не всегда, поэтому обнаружить ее гораздо сложнее.

ИБ-компания SophosLabs опубликовала статистику инфицирования вредоносным ПО в сентябре 2015 г. Особый интерес представляет информация о вредоносной кампании, направленной на серверы под управлением Revive Adserver. В настоящее время под управлением этой системы работает 7,5 тыс. рекламных серверов по всему миру. По словам специалистов, порядка 15 тыс. клиентов Sophos столкнулись с вредоносной рекламой, которую злоумышленники распространяли во время кампании. Отмечается, что

преступники практически не добавляли новый контент в базу данных рекламного сервера. К примеру, скомпрометированный рекламный баннер мог включать всего одну дополнительную строку с кодом JavaScript. Большинство внедренных скриптов содержали экземпляры набора эксплоитов Angler.

Исследователи сообщили об угрозе администрациям сайтов и, как выяснилось, многие из них используют устаревшую версию Revive Adserver (3.0.1 и ранее). Эти версии до сих пор остаются уязвимыми к внедрению SQL-кода. Эксперты рекомендуют всем пользователям Revive Adserver обновиться до версии 3.2.2 и установить на серверы антивирусные решения ***(Уязвимые рекламные серверы – отличная возможность для распространения вредоносной рекламы // InternetUA (http://internetua.com/uyazvimie-reklamnie-serveri---otlicsnaya-vozmojnost-dlya-rasprostraneniya-vredonosnoi-reklami). – 2015. – 11.10).***

***

Как сообщает издание Threatpost со ссылкой на технического директора швейцарской ИБ-компании Compass Security Schweiz A. Херцога, неназванная организация стала жертвой атаки с эксплуатацией уязвимости в маршрутизаторах Netgear.

Бреши в сетевых устройствах были обнаружены Compass Security Schweiz в июле нынешнего года, а в сентябре исследователи Shellshock Labs публично раскрыли подробности о них. Несмотря на то, что Netgear было известно об уязвимости с момента ее обнаружения, исправление пока еще не выпущено. Тем не менее, компания уже разработала обновление, которое, по словам экспертов, эффективно устраняет брешь.

Во время расследования атаки исследователи Compass Security Schweiz обнаружили, что все запросы DNS перенаправлялись на подконтрольный злоумышленникам сервер. Ставшая жертвой инцидента компания предоставила экспертам IP-адрес одного из используемых во время атаки C&C-серверов. Благодаря этому им удалось загрузить с него данные, и в результате оказалось, что уязвимость эксплуатировалась еще в 10 тыс. маршрутизаторов.

Брешь в версиях прошивки маршрутизаторов N300_1.1.0.31_1.0.1.img и N300-1.1.0.28_1.0.1.img дает возможность обойти аутентификацию и получить доступ к интерфейсу администратора без ввода пароля. Единственным условием для осуществления атаки является вход в веб-интерфейс управления, который доступен по умолчанию во внутренней сети. С активированной возможностью удаленного администрирования все, что нужно для эксплуатации бреши – это наличие подключения к Интернету ***(Уязвимость в маршрутизаторах Netgear эксплуатируется злоумышленниками // InternetUA (http://internetua.com/uyazvimost-v-marshrutizatorah-Netgear-ekspluatiruetsya-zloumishlennikami). – 2015. – 11.10).***

***

По данным исследователей AVAST Software, киберпреступники все чаще используют как вектор атак поддельные приложения, загружаемые жертвами из сторонних магазинов. Чаще всего подделываются такие популярные программы, как Facebook Messenger, CNN, BBC, WhatsApp и др.

Как сообщают исследователи, за многими подделками стоят Н. Уолтер и Ч. Деннис – им принадлежат 58 липовых приложений, доступных в Windows Phone Store. Большинство из них имеют схожие черты. К примеру, приложения собирают базовые данные пользователя и отображают рекламу в зависимости от его местонахождения. Некоторые программы также перенаправляют жертву на страницы с требованием оформить покупку чего-либо.

Эксперты AVAST Software подробнее рассмотрели некоторые из этих приложений.

World News CNN (a.k.a. Abundant Life). Приложение, которое на первый взгляд кажется легитимным CNN World News, на самом деле представляет собой уведомление религиозного характера, озаглавленное «Жизнь с избытком» (Abundant Life).

Поддельный антивирусный продукт Avast. Помимо поддельных приложений соцсетей и новостных изданий, исследователи обнаружили несколько фальшивых антивирусов Avast. Правда, все они являются сравнительно безобидными и только перенаправляют пользователей на сайт Avast и отображают рекламу.

Главной причиной, по которой злоумышленники подделывают приложения, является нажива. Исследователи обнаружили два способа монетизации фальшивок. Первый заключается в так называемой «накрутке» кликов пользователей – чем больше рекламируемых приложений в магазине, тем больше кликов можно получить. Именно поэтому злоумышленники зачастую предлагают сразу несколько подделок.

Второй способ монетизации заключается в отображении ложной рекламы. Некоторые серверы таких приложений удаленно контролируются, что дает возможность включать и выключать рекламные объявления. В некоторых случаях они ведут на мошеннические страницы, на которых отображаются фальшивые уведомления о том, что устройство жертвы якобы имеет проблемы с безопасностью, и, чтобы исправить их, нужно установить платный продукт ***(Злоумышленники все чаще подделывают популярные приложения // InternetUA (http://internetua.com/zloumishlenniki-vse-csasxe-poddelivauat-populyarnie-prilojeniya). – 2015. – 11.10).***

***

По данным специалистов ИБ-компании Volexity, злоумышленники используют решение Cisco Clientless SSL VPN (WebVPN) для хищения важных учетных данных и компрометации корпоративных систем различных организаций. Cisco WebVPN дает возможность организовать удаленный доступ к сетям. Для наладки безопасного соединения, WebVPN использует Secure

Socket Layer Protocol и Transport Layer Security (SSL/TLS1). Через корпоративный веб-портал пользователи могут получить доступ к внутренним документам и ресурсам компании.

Как сообщают специалисты, атаки злоумышленников направлены на страницу авторизации клиентов WebVPN с целью компрометации важных учетных данных пользователей. Атаки осуществляются несколькими методами. Один из них предполагает эксплуатацию уязвимости (CVE-2014-3393), позволяющей обойти механизм аутентификации. Брешь существует из-за ошибки в механизме авторизации фреймворка Clientless SSL VPN.

В атаках, зафиксированных экспертами Volexity, злоумышленники внедряли вредоносный код JavaScript в страницу авторизации целевой компании. В свою очередь, код вызывал удаленный скрипт, предназначенный для хищения данных из формы регистрации. В рамках одной из кампаний атакующие размещали скрипт на взломанном сайте одной из неправительственных организаций. Список жертв включает медицинские компании, специализированные научно-исследовательские институты, неправительственные организации, университеты и академии, а также производителей электроники.

Согласно пояснению эксперта Volexity С. Эдэра, злоумышленники получали «законный» доступ в корпоративные системы путем использования кейлоггеров, хищения учетных данных, эксфильтрации документов, содержащих списки паролей, а также идентифицируя наиболее популярные пароли. Получив доступ к сети, атакующий обычно мог производить те же действия, что и администратор или высоко привелигированный пользователь. В основном вредоносная кампания носила разведывательный характер, отмечает специалист ***(Злоумышленники атакуют компании через Cisco WebVPN // InternetUA (http://internetua.com/zloumishlenniki-atakuuat-kompanii-cserez-Cisco-WebVPN). – 2015. – 11.10).***

***

Согласно статистике Kaspersky Lab, Украина заняла пятое место в мире по рискам столкновения с веб-угрозами в III квартале 2015 г. Как свидетельствуют данные, полученные при помощи облачной инфраструктуры Kaspersky Security Network (KSN) за июль – сентябрь 2015 г., треть (33,7 %) украинских пользователей KSN столкнулись с угрозами, распространяемыми через Интернет.

По данным Kaspersky Lab, украинские пользователи в высокой степени подвержены заражениям через необновлённое программное обеспечение и пиратские копии программ. Показательно также, что 17 % всех заражений приходится на пользователей, работающих с устаревшей операционной системой Windows XP. В Украине также было отмечено большое количество срабатываний антивируса на программы-вымогатели и шифровальщики – вредоносные программы, цель которых – заблокировать устройство или

браузер или зашифровать файлы пользователя, сделав их недоступными без специального ключа, за который требуется заплатить выкуп.

Чтобы привлечь внимание пользователей, злоумышленники применяют методы социальной инженерии, спекулируют на актуальных темах, в том числе связанных с обостренной политический ситуацией в стране. Для распространения вредоносного программного обеспечения (ПО) они рассылают спам и фишинговые сообщения в социальных сетях, создают вредоносные сайты и используют другие более изощренные способы.

«Злоумышленники постоянно ищут новые способы извлечь выгоду из неосторожных действий интернет-пользователей. Ситуацию ухудшает то, что часто украинцы используют пиратские версии программ, не устанавливают обновления для ПО и не делают резервные копии своих файлов, – комментирует Д. Эмм, старший антивирусный эксперт Kaspersky Lab. – Чтобы исключить возможность потери денег, времени и файлов, как своих личных, так и работодателя, пользователям следует со всей серьезностью относиться к защите компьютеров и мобильных устройств. Компании и домашние пользователи должны быть осведомлены о рисках и следовать правилам информационной безопасности» ***(Главные киберугрозы для украинских пользователей // InternetUA (http://internetua.com/glavnie-kiberugrozi-dlya-ukrainskih-polzovatelei). – 2015. – 11.10).***

***

В июле этого года стало известно о разработке системы, которая может атаковать беспроводные сети с использованием дрона. Демонстрация такой возможности была впервые показана командой Hacking Team на конференции Defence Exposition and Conference (IDEX) в Абу-Даби. Свою версию системы для взлома Wi-Fi с помощью дрона предложили также исследователи Сингапурского университета технологий и дизайна.

Как известно, принтер с модулем Wi-Fi, который является частью беспроводной сети, часто становится объектом атаки, так как это самое слабое звено. Исследователи разработали метод для получения доступа к сети через такой незащищённый принтер. Чтобы физически «достать» атакуемую сеть, им пришлось использовать дрон с прикреплённым к нему смартфоном. Изначально подобные системы проектируются для того, чтобы дать возможность компаниям с небольшими затратами тестировать безопасность своих Wi-Fi-сетей. Но, как показали исследователи, это может использоваться и злоумышленниками. Дрон транспортирует смартфон к месту, где находится беспроводной принтер. В отличие от традиционных систем на базе ноутбуков, которые требуют непосредственного доступа к помещению, дрон удобен тем, что может свободно перемещаться и преодолевать различные препятствия. Система фокусируется именно на принтерах, потому что эти устройства по умолчанию слабо защищены и являются прекрасным объектом для атаки. Многие предприятия забывают закрыть эту «дыру», что чревато доступом злоумышленника к важной конфиденциальной информации.

Система использует дрон DJI и смартфон Samsung. Приложение Cybersecurity Patrol сканирует наличие принтеров с Wi-Fi и уведомляет пользователя, если найдено уязвимое устройство. Второе приложение уже пытается провести атаку. Оно создаёт подложную точку доступа, которая имитирует легальный принтер. В случае успеха такой «фейковый» принтер может перехватывать все документы, подаваемые на печать, и направлять их, например, на сервис Dropbox.

Впрочем, пути к взлому системы могут быть самыми разнообразными. Вместо дрона можно использовать роботизированный пылесос, который также может свободно перемещаться в помещении с прикреплённым смартфоном злоумышленника и сканировать сеть на наличие «дыр» ***(Предложен метод атаки сети Wi-Fi с помощью дрона и смартфона // InternetUA (http://internetua.com/predlojen-metod-ataki-seti-Wi-Fi-s-pomosxua-drona-i-smartfona). – 2015. – 11.10).***

***

Согласно статистическому отчету, опубликованному компанией Corero Network Security, во II квартале 2015 г. число DDoS-атак увеличилось почти на треть (32 %) по сравнению с предыдущей четвертью. В среднем в указанный период злоумышленники ежедневно осуществляли 4,5 DDoS-атак. При этом скорость большинства атак (свыше 95 %) составляла не более 10 Гбит/с, а их продолжительность не превышала 30 минут.

По мнению специалистов, рост числа инцидентов связан с возрастающей доступностью дешевых DDoS-инструментов, в том числе ботнетов, которые легко можно арендовать для совершения анонимных атак. Как правило, отмечают эксперты, менее масштабные атаки осуществлялись в попытках обхода средств защиты и в некоторых случаях для маскировки попыток хищения важных данных.

Как пояснил изданию Infosecurity технический директор Corero Д. Ларсон, изначально DDoS-атаки осуществлялись с целью вызова отказа в обслуживании системы, однако сейчас они зачастую служат прикрытием для другой вредоносной активности, к примеру, эксфильтрации важной информации или персональных данных.

По мнению Д. Ларсона, компаниям, которые еще не сталкивались с масштабными DDoS-атаками, следует не терять бдительность и обращать внимание на любую, даже незначительную активность в корпоративных сетях и системах ***(Во II квартале 2015 г. количество DDoS-атак увеличилось на 32 % // InternetUA (http://internetua.com/vo-vtorom-kvartale-2015-goda-kolicsestvo-DDoS-atak-uvelicsilos-na-32). – 2015. – 11.10).***

***

Аналист информационных систем и этический хакер компании CliftonLarsonAllen А. Хейден предупреждает, что большинство компьютерных сетей практически не защищены от фишинга и социальной инженерии (СИ).

Специалист утверждает, что использование методов СИ обеспечивает почти 100 -процентную гарантию взлома той или иной компании. Об этом А. Хейден сообщил во время конференции 2015 AHIMA Convention.

Хакер рассказал, что недавно во время аудита одной из медицинских компаний смог взломать внутреннюю сеть организации, отправив ее гендиректору фишинговое письмо якобы от имени финансового директора. Пентестеру удалось получить доступ к логину и паролю руководителя.

Имея на руках учетные данные сотрудника, хакер может от его имени осуществлять в сети произвольные действия. Если злоумышленнику удалось получить доступ к аккаунту администратора, он может установить вредоносное ПО для перехвата других данных. Более того, киберпреступник сможет разослать фишинговые письма от имени пострадавшего пользователя, вследствие чего еще большее количество жертв пострадает от его действий.

Как сообщает директор по развитию бизнеса High-Tech Bridge Е. Хрусталева в своей статье в журнале IT Manager, противостоять социальной инженерии можно, применив три шага по обеспечению безопасности компании. При этом организация должна позаботиться не только об их интеграции, но и о своевременном их использовании.

Первый шаг заключается в четком обрисовывании и донесении до персонала протоколов безопасности. Все сотрудники должны знать, кто и в какое время и место может работать с коммерчески ценной информацией, а также какие шаги необходимо предпринять в случае инцидента информационной безопасности, возникшего вследствие применения способов СИ. Второй шаг заключается в аудите системы безопасности компании и проведении пентестов. Е. Хрусталева рекомендует прибегнуть к независимым сторонним «этическим хакерам», которые смогут подобрать и внедрить наиболее эффективные средства противодействия таким атакам. Заключительный шаг предусматривает проведение тренингов по безопасности для всех сотрудников без исключения ***(С помощью фишинга и социальной инженерии хакеры добиваются 100-процентной эффективности атак // InternetUA (http://internetua.com/s-pomosxua-fishinga-i-socialnoi-injenerii-hakeri-dobivauatsya-100--noi-effektivnosti-atak). – 2015. – 9.10).***

***

Имеются основания полагать, что платежная система Samsung Pay, запущенная южнокорейским производителем в августе, подверглась взлому. По сообщениям газеты New York Times, хакеры смогли получить доступ к сервису, воспользовавшись брешью в корпоративной сети американского стартапа LoopPay, который Samsung приобрела в начале этого года для улучшения технологии бесконтактных платежей.

Samsung Pay выступает аналогом платежной системы Apple Pay, однако на фоне конкурирующего решения его выделяет одна важная особенность – это фирменная технология под названием Magnetic Secure Transmission (MST). В отличие от NFC, которая пока не получила повсеместного распространения,

MST дает возможность работать со старыми платежными аппаратами, передавая со смартфона бесконтактным путем данные магнитной полосы банковской карты.

Эксперты по безопасности допускают, что целью китайской хакерской группировки Codoso, которая подозревается во взломе, как раз могла стать эта технология. Представители Samsung говорят, что атака на серверы LoopPay не нанесла ощутимого ущерба компании. Специалисты по безопасности своевременно отреагировали на угрозу и быстро устранили уязвимость в системе. При этом следов проникновения во внутренние системы Samsung, а также кражи личных данных клиентов не замечено ***(Платежная система Samsung Pay могла быть тайно взломана // IGate (http://igate.com.ua/lenta/10659-platezhnaya-sistema-samsung-pay-mogla-byt-tajno-vzlomana). – 2015. – 12.10).***

***

В социальной сети «ВКонтакте» обнаружена новая уязвимость, которая дает возможность перехватывать данные с мобильных устройств.

Обнаружение бреши похвастался эксперт компании HeadLight Security М. Фирстов. Он сообщил, что уязвимость в безопасности дает возможность перехватывать личные сообщения пользователей при атаке известной как Man-in-The-Middle (человек посередине).

Для чтения чужой персональной переписки в соцсети достаточно находиться в одной беспроводной или локальной сети с компьютером или мобильным устройством жертвы, авторизованным во «ВКонтакте». Для демонстрации возможности эксплуатации этой уязвимости можно воспользоваться соответствующей утилитой – vkmitm, которая дает возможность обрабатывать сообщения из трафика в режиме реального времени или офлайн из PCAP-файла.

«ВКонтакте» пока не прокомментировала сообщения об обнаруженной уязвимости ***(Уязвимость «ВКонтакте» позволяет перехватить данные с гаджетов // InternetUA (http://internetua.com/uyazvimost--vkontakte--pozvolyaet-perehvatit-dannie-s-gadjetov). – 2015. – 17.10).***

***

Специалисты британского национального агентства по борьбе с преступностью (National Crime Agency) сообщают о новом компьютерном вирусе, с помощью которого мошенникам уже удалось украсть с банковских счетов британцев более 20 млн фунтов стерлингов.

Известно несколько названий нового вируса: Dridex, Bugat и Cridex. Он был разработан хакерами из Восточной Европы для перехвата конфиденциальных данных клиентов банков. В связи с этим сотрудники ведомства призывают пользователей онлайн-банкинга регулярно обновлять антивирусные программы на своих компьютерах.

Чаще всего вирус проникает в устройства посредством зараженных электронных писем, замаскированных под официальные письма от банка, и содержится в документах, прикрепленных к этим письмам. По предварительным оценкам, только в Великобритании тысячи компьютеров могут быть заражены этим вирусом.

Специалисты агентства в сотрудничестве со спецслужбами других стран работают над задержанием хакеров, запустивших вирус в сеть, в связи с чем уже произведено несколько арестов ***(Клиенты банков теряют миллионы из-за нового вируса // InternetUA (http://internetua.com/klienti-bankov-teryauat-millioni-iz-za-novogo-virusa). – 2015. – 16.10).***

***

Состоялся выход обновленной версии браузера Google Chrome 46.0.2490.71. В нем разработчики исправили как минимум девять уязвимостей. Пять брешей давали возможность удаленному пользователю скомпрометировать систему.

Уязвимости CVE-2015-6755 и CVE-2015-6756 существовали из-за ошибки использования после высвобождения в компонентах PDFium и Service Worker. Проэксплуатировав их, удаленный пользователь мог выполнить произвольный код на целевой системе. В компоненте PDFium также была обнаружена неразглашенная ошибка (CVE-2015-6758), позволявшая раскрыть важные данные.

Две из девяти обнаруженных уязвимостей давали возможность обойти ограничения политики общего происхождения (CVE-2015-6761) и совместного использования ресурсов между разными источниками (CVE-2015-6762). Отметим, что для эксплуатации второй бреши злоумышленнику требовались специально сформированные шрифты CSS.

Разработчики Chrome также исправили множественные неуточненные ошибки в браузере, которые позволяли злоумышленнику выполнить неаутентифицированные действия на целевой системе. Этим исправлениям был присвоен единый идентификатор CVE-2015-6763.

Вдобавок ко всему в браузере были исправлены четыре уязвимости в различных компонентах, позволяющие удаленному пользователю скомпрометировать систему ***(Google исправила множественные уязвимости в браузере Chrome // InternetUA (http://internetua.com/Google-ispravila-mnojestvennie-uyazvimosti-v-brauzere-Chrome). – 2015. – 15.10).***

***

Apple атакуют вирусы

Времена отсутствия вирусов на устройствах Apple остались в прошлом – число вредоносных программ на iOS и OS X растет, а ложное чувство безопасности ставит многих пользователей под угрозу. С дальнейшей популяризацией iPhone и iPad количество вирусов будет лишь увеличиваться, предупреждают эксперты.

Одним из основных аргументов владельцев ПК и гаджетов от Apple всегда было отсутствие вирусов на десктопной и мобильной операционных системах OS X и iOS. Сама Apple также неоднократно отмечала, что ее устройства в разы безопаснее, чем у конкурентов. Так, в 2013 г. вице-президент корпорации по маркетингу и продуктам Ф. Шиллер на различных мероприятиях постоянно ссылался на данные исследовательской компании F-secure, согласно которым более 90 % всех мобильных вирусов приходится на ОС Android.

Однако за последние годы число вирусов, поражающих устройства Apple, серьезно возросло, так что сегодня слова Ф. Шиллера смело можно поставить под сомнение.

Тем не менее, один из первых вирусов для OS X появился еще в 2011 г. Он проникал в компьютеры Mac через вредоносные сайты и предлагал очистить устройство через программу Mac Defender.

Доверчивый пользователь соглашался и совершал платеж за услугу с кредитной карты, доступ к которой в итоге получали злоумышленники. В том же году тысячи пользователей Mac стали жертвой трояна Flashback, маскировавшегося под программу установки Adobe Flash.

Эксперты по безопасности компании Intego и вовсе отмечали, что 2011 г. стал рекордным по числу вирусов для компьютеров Apple, от которых пострадало более 300 тыс. пользователей по всему миру.

Проблема усугублялась и тем, что владельцы устройств Apple верили в полное отсутствие вредоносных программ для OS X, а потому 57,5 % пользователей не считали нужным устанавливать на свои компьютеры антивирусы. Это привело к тому, что злоумышленники массово использовали Mac для хранения и рассылки вирусов, поражающих устройства на базе Windows.

Так, компания Sophos в 2012 г. установила, что хранилищем для вирусов является каждый пятый Mac, а сотрудники Dr.Web обнаружили ботнет-сеть из 550 тыс. компьютеров Apple.

В отличие от десктопной версии, мобильная iOS сравнительно долго оставалась одной из немногих безопасных операционных систем. Вплоть до недавнего времени основную опасность для пользователей iPhone и iPad представляли иногда пропускаемые модераторами вредоносные приложения в AppStore и похищавшие данные поддельные подарочные карты iTunes.

Все изменилось в 2014 г., когда владельцы гаджетов Apple с разницей всего в пару недель стали жертвами двух мощных троянов. Сначала китайские пользователи стали жертвами распространяемого через сторонние магазины приложений вируса WireLurker. Программа шпионила за пользователями и похищала их личные и финансовые данные. Спустя некоторое время китайские власти закрыли сайт, через который распространялся троян, а также арестовали создавших его программистов.

Однако куда более опасной эксперты признали уязвимость Masque Attack, позволявшую злоумышленникам подменять приложения iPhone и iPad своими версиями и получать доступ ко всем данным смартфона.

В то же время опасность вновь угрожала лишь любителям качать приложения из сторонних источников. А вот массовый взлом профилей iCloud в сентябре 2014 г. уже всерьез поставил под вопрос безопасность личных данных, хранящихся на устройствах Apple. Тогда в сети оказались интимные фото ряда голливудских звезд, а на след организовавших взлом хакеров ФБР вышло лишь в октябре 2015 г.

В 2015 г. число уязвимостей iOS лишь увеличилось. В августе 2015 г. маскирующиеся под Skype, Twitter и Facebook вредоносные приложения попали в AppStore и дали злоумышленникам доступ к личной информации пользователей. В сентябре новый вирус дал возможность хакерам украсть 225 тыс. аккаунтов Apple ID, а заражение инструментов для разработчиков привело к появлению 340 вредоносных приложений в AppStore.

Даже выход новой версии мобильной ОС iOS 9 не добавил пользователям оптимизма.

Несмотря на заявления Apple про обновленные протоколы безопасности, занимающаяся скупкой уязвимостей компания Zerodium уже пообещала награду в 1 млн дол. за взлом новой версии операционной системы.

Наконец, 14 октября, исследователи из французского Национального агентства информационных систем (ANSSI) продемонстрировали метод взлома iPhone и iPad через голосовой помощник Siri.

Хакер может беззвучно отдавать команды устройству с расстояния чуть менее пяти метров, если в смартфон подключены наушники. Их провод выполняет функцию антенны, на которую может быть передан радиосигнал, который будет воспринят iOS как голосовая команда владельца устройства. Таким образом злоумышленник может добиться выполнения ряда команд, отправки сообщений и набора номера на смартфоне жертвы.

Антивирусные продукты для iOS существуют так же, как и для других систем, рассказал «Газете.Ru» руководитель аналитического центра компании Zecurion В. Ульянов.

Даже несмотря на то, что архитектура этих систем разная, но принципиально антивирусные программы похожи. Просто на Mac OS X и iOS антивирусами пользуются реже в силу сложившегося стереотипного ощущения безопасности, отмечает эксперт.

Кроме того, менее популярные системы менее интересны для злоумышленников, добавляет он. А операционные системы Apple, на самом деле, все еще мало распространены. Так, по состоянию на середину 2015 г. Mac OS занимает долю в 4,5 %, что в два раза меньше, чем у морально устаревшей Windows XP. При этом Windows 7 имеет более 60 %. Доля iOS увеличилась с 12 до 14 %, при этом Android занимает 82 % рынка.

«Да, аудитория пользователей iPhone более премиальная, но значительное число пользователей Android дает возможность злоумышленникам

разрабатывать более надежные и стабильные схемы нелегального заработка, – считает В. Ульянов. – На iOS также есть большое количество уязвимостей, но она менее популярна у киберпреступников. Когда разница между долями рынка этих систем сократится, тогда и вредоносного кода под iOS будет писаться значительно больше» ***(Apple атакуют вирусы // InternetUA (http://internetua.com/Apple-atakuuat-virusi). – 2015. – 18.10).***

***

Компания Trend Micro обнаружила в составе Flash Player версий от 19.0.0.185 (возможно, и в более ранних) до выпущенной на этой недели 19.0.0.207 уязвимость нулевого дня. Она используется хакерской группой Pawn Storm для незаметной установки вредоносного ПО на компьютеры жертв.

Согласно сообщению разработчиков, ряд министерств иностранных дел получили фишинговые письма. Они содержат ссылки на сайты, якобы с новостями о текущих событиях в мире, с заголовками вроде «Подконтрольная правительственными войсками Сирии территория расширяется», «Россия обещает ответные меры на размещение американских ядерных ракет в Сирии» и «Путин выступил в поддержку авиаударов по Сирии». На самом деле на этих сайтах располагается использующий эту уязвимость эксплоит.

Группа Pawn Storm ранее отмечалась проведением атак в России и инфицированием мобильных устройств Apple в западных правительствах и новостных агентствах. Компания Adobe подтвердила наличие уязвимости и в своём каталоге присвоила ей номер CVE-2015-7645.

Пользователям рекомендуется ограничить использование Flash Player на веб-сайтах, поскольку инфицирование популярных сервисов и атака их посетителей является распространённой практикой. Наиболее же безопасным вариантом станет полное удаление Flash Player с компьютера.

Недавно выпущенные бюллетени безопасности для Flash Player, содержащие исправления для 13 уязвимостей, не исправляют эту брешь. В Adobe подтвердили наличие уязвимости и обещают выпустить патч в ближайшее время ***(В составе Flash найдена критическая уязвимость, Adobe обещает выпустить патч на следующей неделе // InternetUA (http://internetua.com/v-sostave-Flash-naidena-kriticseskaya-uyazvimost--Adobe-obesxaet-vipustit-patcs-na-sleduuasxei-nedele). – 2015. – 18.10).***

***

Группу российских хакеров заподозрили во взломе системы Dow Jones и краже информации еще до того, как она стала общедоступной, и использовании ее для инсайдерской торговли.

В настоящее время расследованием этого инцидента занимаются американские власти, ФБР и Секретная служба и комиссия по ценным бумагам и биржам. О вероятной причастности к атаке российских хакеров сообщает агентство Bloomberg.

По информации издания, атака на компанию Dow Jones, которая владеет газетой The Wall Street Journal, началась еще год назад. После того, как стало известно о намерении хакеров похитить платежную информацию около 3500 клиентов, агентство Dow Jones заявило о начале работы по обеспечению фирмы кибербезопасностью.

Два источника агентства сообщили, что хакеры искали также готовящуюся к публикации информацию, отмечает NEWSru.com. По данным Bloomberg, эта информация необходима для получения преимущества над другими участниками рынка. Стоит отметить, что издание не уточняет, есть ли конкретные доказательства в причастности российских хакеров к атаке на Dow Jones у американских властей ***(Российские хакеры взломали систему Dow Jones, украв информацию для инсайдерской торговли // InternetUA (http://internetua.com/rossiiskie-hakeri-vzlomali-sistemu-Dow-Jones--ukrav-informaciua-dlya-insaiderskoi-torgovli). – 2015. – 17.10).***

***

Компания Cheetah Mobile обнаружила новый троян Ghost Push, заражающий мобильные устройства на платформе Android. Сразу после появления на устройстве троян сохраняется в корневом каталоге системы, что значительно усложняет процесс удаления. По словам представителей Cheetah Mobile, количество заражённых устройств превышает 900 тыс. Сегодня Ghost Push можно найти в самых разных приложениях. В большинстве случаев заражённые программы и утилиты размещаются на различных форумах и сторонних ресурсах. Однако эксперты отмечают, что некоторые программы с Ghost Push были замечены и в Google Play. В основном это калькуляторы и другие подобные вспомогательные утилиты.

Основная задача этого трояна заключается не в нанесении вреда устройству или хищении данных пользователя – он позволяет зарабатывать своим авторам. Ghost Push «поселяется» в корневом каталоге и начинает показывать рекламу. По примерным подсчетам Cheetah Mobile Ghost Push приносил своим создателям до 4 млн дол. в день. Компания Google уже отреагировала на это заявление и изъяла из своего магазина все приложения с вредоносным кодом. Пользователи, устройства которых уже были заражены, могут скачать специальную утилиту для удаления вируса из системного каталога ***(Новый троян атакует устройства на Android // InternetUA (http://internetua.com/novii-troyan-atakuet-ustroistva-na-Android). – 2015. – 17.10).***

***

Троян маскируется под антивирусную утилиту известного разработчика

Специалисты антивирусной компании «Доктор Веб» обнаружили трояна, угрожающего в том числе и любителям одного из российских сериалов, причем эта вредоносная программа маскируется под антивирусную утилиту известного разработчика. Об этом CNews сообщили в «Доктор Веб».

Троян, получивший наименование Trojan.BPLug.1041, был обнаружен при переходе из результатов поиска Google на взломанную злоумышленниками веб-страницу российского телеканала, посвященную одному из российских телесериалов. Позже выяснилось, что компрометации подверглось еще несколько посещаемых интернет-ресурсов, в том числе связанных с телевизионными шоу. Если пользователь переходит на зараженный сайт с другого домена, а также при соблюдении ряда условий (использование 32-битной ОС семейства Windows или ОС семейства Mac OS X с архитектурой Intel и браузера, отличного от Opera), вредоносный скрипт открывает на вкладке, откуда был осуществлен переход, страницу злоумышленников. Встроенный в код этой веб-страницы специальный обработчик не позволяет закрыть эту вкладку, при нажатии клавиш или щелчке мышью демонстрируя на экране назойливое окно, предлагающее пользователю установить некое расширение для браузера. При этом злоумышленники выдают это расширение за утилиту, якобы созданную широко известной компанией-производителем антивирусного ПО, рассказали в «Доктор Веб».

В процессе установки этот плагин требует у пользователя предоставить ему ряд специальных разрешений и после инсталляции отображается в списке установленных расширений Chrome под именем «Щит безопасности KIS».

Плагин, детектируемый «Антивирусом Dr.Web» как Trojan.BPLug.1041, включает в себя два обфусцированных файла на языке JavaScript. Основное предназначение трояна заключается в выполнении веб-инжектов, то есть встраивании постороннего содержимого в просматриваемые пользователем веб-страницы. При этом на всех сайтах вредоносная программа блокирует демонстрацию сторонней рекламы с любых доменов, кроме тех, список которых предусмотрен в ее конфигурации.

За отображение рекламы отвечает отдельная функция, с помощью которой троян анализирует содержимое открытой пользователем веб-страницы. Если ее контекст включает порнографическое содержимое, Trojan.BPLug.1041 загружает рекламу соответствующей тематики из двух отдельных сетей. Кроме того, это расширение содержит список сайтов, на которых троян не показывает рекламу, среди них – fsb.ru, gov.ru, government.ru, mos.ru, gosuslugi.ru и некоторые другие. На сервер злоумышленников Trojan.BPLug.1041 отправляет сведения о других расширениях Chrome, установленных на инфицированном компьютере. При этом сервер может указать трояну, какие расширения следует отключить.

Если пользователь авторизовался в «Одноклассниках», Trojan.BPLug.1041 пытается предоставить определенному приложению доступ к API этой социальной сети от имени жертвы путем авторизации по протоколу OAuth. При этом в процессе авторизации запрашиваются привилегии на изменение статуса, просмотр, редактирование, загрузку фотографий, просмотр и отправку сообщений от имени пользователя, а также некоторые другие. В «Доктор Веб» полагают, что этот функционал может использоваться злоумышленниками в

различных рекламных целях – например, для продвижения групп, рассылки спама или каких-либо голосований.

Примечательно, что в интернет-магазине Chrome имеются целых три расширения с именем «Щит безопасности KIS», созданных одним и тем же автором, однако два из них по различным причинам нефункциональны. Общее число установок всех трех плагинов на сегодняшний день превышает 30 тыс., отметили в компании.

Специалисты «Доктор Веб» предостерегают пользователей от загрузки и инсталляции подозрительных расширений, полученных из недоверенных источников. Если в окне браузера появилась подобная вкладка, не позволяющая себя закрыть, можно воспользоваться диспетчером задач, доступным в меню Google Chrome, и остановить соответствующий процесс браузера. Сигнатура Trojan.BPLug.1041 добавлена в вирусные базы Dr.Web, а веб-сайт, с которого распространялся этот троян – в списки нерекомендуемых для посещения интернет-ресурсов. Администрация взломанных злоумышленниками сайтов была своевременно проинформирована об инциденте ***(Троян маскируется под антивирусную утилиту известного разработчика // InternetUA (http://internetua.com/troyan-maskiruetsya-pod-antivirusnuua-utilitu-izvestnogo-razrabotcsika). – 2015. – 18.10).***

***

Специалисты Кембриджского университета (Великобритания) проанализировали информацию, полученную примерно от 20 тыс. устройств на базе Android, и пришли к неутешительному выводу: почти девять из каждых десяти таких гаджетов уязвимы для кибератак.

Данные были получены при помощи специализированного приложения Data Analyzer, которое желающие могут загрузить через сайт магазина Google Play. Программа в фоновом режиме накапливает сведения об устройстве (персональные данные не собираются) и отправляет их на сервер Кембриджского университета.

Итак, как показало исследование, приблизительно 87,7 % устройств под управлением операционных систем Android содержат как минимум одну из 11 наиболее опасных известных уязвимостей в этой платформе. Подобная ситуация, как полагают эксперты, объясняется в том числе нерасторопностью производителей гаджетов, не спешащих с выпуском новых версий прошивок для своих смартфонов и планшетов. Более того, некоторые компании и вовсе забывают про обновление ОС после снятия конкретной модели устройства с производства.

В результате, как сообщается, наибольшую степень защиты демонстрируют аппараты Google Nexus. Далее следуют мобильные устройства, выпускающиеся под марками LG, Motorola, Samsung, Sony и HTC ***(Почти 90 % android-устройств остаются уязвимыми // IGate (http://igate.com.ua/lenta/10716-pochti-90-android-ustrojstv-ostayutsya-uyazvimymi). – 2015. – 15.10).***

***

Глава Европейского агентства авиационной безопасности (EASA) П. Ки заявил, что технический консультант, нанятый агентством и сам являющийся пилотом гражданской авиации, обнаружил уязвимости в адресно-отчетной системе авиационной связи (ACARS, Aircraft Communications Addressing and Reporting System), использующейся для передачи текстовых сообщений между самолетами и наземными радиостанциями.

Во время пресс-конференции П. Ки отметил, что эксперт смог взломать ACARS за пять минут и еще за пару дней смог найти способ получения доступа к системам управления самолетом.

«В целях безопасности я не расскажу вам, как именно эксперт смог взломать систему, однако решать, опасна подобная уязвимость или нет, позволю вам», – цитирует П. Ки французское издание Les Echos.

О некоторых из этих проблем рассказывал ИБ-исследователь Х. Тесо во время своего выступления на конференции Hack in the Box в 2013 г. Изучив ACARS, он обнародовал ряд присущих ей уязвимостей. По убеждению эксперта, линия связи между самолетом и наземной радиостанцией имеет очень слабую защиту.

«Уязвимым местом системы является отсутствие верификации пакетов во время передачи сообщения на борт самолета, – заявил А. Никишин, директор по спецпроектам департамента перспективных разработок “Лаборатории Касперского”. – Подобная брешь дает возможность обмануть систему, внедрив новый пакет во время передачи».

По словам А. Никишина, атакующий получает возможность посылать пилотам ложные сообщения, способные повлиять на принятие ими тех или иных решений.

«В теории атакующий может послать пилоту поддельное сообщение о приближающемся шторме и тем самым вынудить того сменить курс, – заявил эксперт. – Таким же образом можно обмануть и механизм GPS – система будет уверена, что самолет находится не там, где он есть на самом деле».

В публикации Les Echos упоминаются также результаты исследования, проведенного Международной организацией гражданской авиации. Исследователи заключили, что, поскольку системы навигации и управления должны быть по идее изолированы от других некритических систем, к примеру развлекательных, риск взлома критических систем крайне низок.

«ACARS использует собственную схему шифрования/дешифрования, созданную еще в 1978 г.; в те времена авиационное оборудование разрабатывали, не думая о кибербезопасности, – заявил А. Никишин. – Эта система сильно устарела, и производителям самолетов уже давно пора бы заняться разработкой новой системы, используя более современный подход».

Сообщение П. Ки об уязвимости лишь на день опередило анонс новой европейской системы управления полетами, названной Sesar.

«Завтра состоится ввод в строй системы Sesar, которая позволит передавать инструкции от авиационно-диспетчерских служб напрямую системам управления самолетами, и риски, связанные с этой уязвимостью, возрастут в разы, – заявил П. Ки. – Нужно в первую очередь создать структуру, которая будет предупреждать экипажи самолетов об угрозе кибератак».

Вопрос о безопасности самолетов и ранее поднимался в текущем году. В минувшем мае исследователь К. Робертс был снят с рейса после того, как он похвалился в Twitter, что смог взломать системы самолета, на борту которого находился. Исследователь был задержан и допрошен агентами ФБР. В отчете агенты указали, что К. Робертс смог через развлекательный центр получить доступ к критическим системам самолета, что дало возможность ему отдавать команды на набор или сброс высоты.

В правдивости содеянного К. Робертсом усомнились многие производители самолетов – к примеру, представители Boeing в комментарии CNN заявили, что подобное в принципе невозможно, ведь развлекательные и навигационные системы изолированы друг от друга ***(Уязвимость в ACARS позволяет взламывать самолеты // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/10/15/european-aviation-agency-warns-of-aircraft-hacking.html). – 2015. – 15.10).***