СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(16–29.11)

2015 № 21

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(16–29.11)
№ 21

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

© Національна бібліотека України
імені В. І. Вернадського, 2015

Київ 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Может показаться, что такой портал как социальная сеть уже по определению не может иметь слишком много общего с уединением или анонимностью. Вновь созданный сервис Minds.com другого мнения, и поддерживается он со стороны группы Anonymous, известной главным образом борьбой за свободный Интернет, что позволяет верить, что на самом деле так оно и есть.

На первый взгляд, данная социальная сеть, как и любая другая – позволяет пользователям делиться ссылками и мыслями. Однако в отличие от Facebook или Twitter код как настольной, так и мобильной версии является полностью открытым (open source), и все сообщения, передаваемые между пользователями, шифруются.

«По нашему мнению, пользователи заслуживают того, чтобы иметь возможность посещать медиа социальную сеть с любого доступного способа», – сказал основатель Minds, Б. Оттман.

Портал Minds должен быть тоже привлекательной платформой для всех тех, кто хочет поддерживать постоянный контакт со своей аудиторией. В отличие от знаменитого Facebook, здесь не будет алгоритмов, искусственно увеличивающих или ограничивающих доступ к отдельным постам.

Идея портала Minds понравилась, пожалуй, самой популярной группе интернет-активистов Anonymous. Они хвалят этот сервис и даже пригласили программистов, дизайнеров и разработчиков для совместной работы над развитием умов: «Мы нужны друг другу и проектируем топовую сторону, которая создана людьми с мыслью о людях и для людей» ***(Minds: портал, социальная сеть при поддержке Anonymous // Новости IT (http://interteam.com.ua/minds-portal-socialnaya-set-pri-podderzhke-anonymous/). – 2015. – 17.11).***

***

Google объявила о перезапуске своей социальной сети Google+, значительно изменив ее функциональность. Об этом сообщает Techcrunch.

В компании отмечают, что Google+ в основном используют для обсуждений, и нововведения должны сделать этот процесс проще и удобнее. Акцент теперь сделан всего на двух функциях – «коллекциях» и «сообществах», а остальные сведены к минимуму: например, пользователей лишили возможности организовывать встречи и оставлять геометки.

Функция «коллекции» была добавлена в Google+ в мае, она позволяет создавать страницы по определенной тематике в соответствии с конкретными увлечениями пользователей. Участники могут публиковать там фото и видео, размещать ссылки, а также подписываться на обновления конкретных «коллекций». «Сообщества» появились в соцсети еще три года назад, эта

функция позволяет людям объединяться в группы для обсуждения каких-либо общих тем ***(Google перезапустила соцсеть // InternetUA (http://internetua.com/Google-perezapustila-socset). – 2015. – 18.11).***

***

У соцмережі Google+ зареєстровано 2,5 млрд осіб, але при цьому нею майже ніхто не користується. Google в черговий раз робить спробу це виправити, пише видання «Новое время» (http://nv.ua/ukr/techno/gadgets/reanimatsija-trupa-navishcho-google-zapuskaje-svoju-sotsialnu-merezhu-80970.html).

Google відчайдушно хоче мати свій «власний Facebook»

Набагато ближча до реальності інша цифра – кількість активних користувачів. За цим показником Google+ гордо входить у десятку найбільш популярних соцмереж, приблизно на одному рівні з Twitter і Instagram.

Але і ця цифра багатьом здається завищеною. У силу своєї тісної інтеграції з іншими сервісами Google багато активних користувачів Google+ часто навіть не підозрюють, що користуються нею.

За даними аналітичного агентства Stone Temple Consulting, 90 % акаунтів Google ніколи не постили в Google+.

До аналогічних цифр дійшов у результаті своїх підрахунків незалежний аналітик Е. Морбіус. За його даними, за весь час існування Google+ сервісами соцмережі скористалися лише 9 % зареєстрованих акаунтів. Теоретично, це і є наведена вище цифра в 300 млн користувачів, яка ставить Google+ на один рівень із Twitter і Instagram.

Але Е. Морбіус йде далі і заявляє, що нині активно використовують Google+ не більше 4–6 млн осіб.

Іншими словами, намагаючись максимально зблизити всі свої сервіси, Google сама «підклала собі граблі». Google+ настільки міцно увійшла в життя користувачів компанії, що вони просто не помічають її.

І тепер Google хоче це виправити. У черговий раз.

Запущена у 2011 р. з неймовірним маркетинговим пафосом соціальна мережа Google+ була названа «вбивцею Facebook». На її розробку було витрачено близько 500 млн дол. Наплив реєстрацій повинен був забезпечити той факт, що, власне, реєструватися в мережі було необов'язково. Кожен, хто був власником облікового запису Gmail, автоматично ставав учасником Google+. Кнопка активації соцмережі була нав'язливо інтегрована в усі сервіси Google, а так звані Кола (спосіб організації спілкування з друзями в Google+) з'явилися в списку контактів Gmail.

Однак це не допомогло. Тепер Google хоче, щоб користувачі сприймали соцмережу – як засіб колективної взаємодії.

«Кінцевою метою є створення сервісу, який вирішував би реальні проблеми і полегшував життя людям», – говорить прес-реліз компанії. Це хороший слоган з вуст Google, коли мова йде про створення безпілотних автомобілів або ліків від раку, констатує технoблогер А. Естес. Але задається

питанням, чому Google наполегливо відмовляється від спроб створити власний клон Facebook?

На думку блогера, нові ініціативи не зроблять Google+ більше привабливим для користувачів. У світі, де є Reddit і Pinterest, – нові функції Google+ здаються дещо блідими.

Інший відомий техноблогер, колишній співробітник Google, М. Херн, упевнений, що інціативи Google не спрацюють, тому що не продумані до кінця. «Не уявляю, як спільноти Google+ можуть стати популярними, адже формат постів має великі тексти і великі фотографії, – пояснює він. – Мережа навіть не пропонує користувачам обрізати пости для попереднього перегляду».

За його словами, користувачі соцмереж хочуть, щоб їх розважали і інформували. Google+ не пропонує нічого особливого ні в тій, ні в іншій області, підкреслює М. Херн.

Google неодмінно скоро переконається в цьому і без всякого сумніву спробує направити свого соціального «зомбі» в якомусь черговому «новому» напрямі, підсумовує А. Естес.

Найпопулярніші соцмережі у світі за кількістю користувачів

Facebook – 1,49 млрд
QQ – 832 млн
WhatsApp – 800 млн
Qzone – 668 млн
WeChat – 549 млн
Twitter – 316 млн
Skype – 300 млн
Google+ – 300 млн
Instagram – 300 млн
Baidu Tieba – 300 млн ***(Реанімація трупа. Навіщо Google запускає свою соціальну мережу // Новое время (http://nv.ua/ukr/techno/gadgets/reanimatsija-trupa-navishcho-google-zapuskaje-svoju-sotsialnu-merezhu-80970.html). – 2015. – 19.11).***

***

Instagram запустил программу «большой зачистки» сторонних приложений, сообщает Techcrunch. Новая политика работы с API для неофициальных приложений позволит компании существенно сократить количество сторонних сервисов и сконцентрироваться на развитии собственного продукта, отмечает издание.

В первую очередь, Instagram планирует отключить доступ к своему API для приложений, которые позволяли просматривать ленту фотосервиса. Techcrunch объясняет, что такой шаг вызван низкой популярностью подобных приложений – так, количество пользователей даже самых известных сторонних сервисов для чтения ленты Instagram достигало только 2 млн пользователей при общей базе фотосервиса в 400 млн человек.

В частности, под удар Instagram попадут приложения Retro, Flow, Padgram, Pictacular для iPad, а также Webbygram, Webstagram, Instagreat, и Itsdagram для десктопов, считают в Techcrunch (у Instagram нет собственных приложений для iPad и настольных компьютеров). Также компания намерена отключить приложения, которые позволяют автоматически подписываться на пользователей, «лайкать» их фотографии и оставлять под ними комментарии. При этом сервисы типа Tinder, позволяющие загружать фотографии из Instagram, будут работать, как и раньше.

С 18 ноября Instagram прекращает подключение новых приложений к своему API. С 3 декабря 2015 г. компания начнет проверять все сервисы, которые заявляют о своем желании работать с сервисом, а также запустит сервис Sandbox, предлагающий тестовый API – с его помощью сторонние разработчики смогут проверить работу своих приложений. С 1 июня 2016 г. все приложения (новые и ныне подключенные) должны будут работать в соответствии с новыми правилами Instagram ***(Instagram будет бороться со сторонними клиентами // IGate (http://igate.com.ua/lenta/11454-instagram-budet-borotsya-so-storonnimi-klientami). – 2015. – 18.11).***

***

Отныне пользователи самой популярной в Украине социальной сети «ВКонтакте» смогут напрямую общаться с администраторами страничек. Для этого компания запустила в сообществах привычные для пользователей сообщения и диалоги, которые перед этим какое-то время тестировали, пишет AIN.UA (http://ain.ua/2015/11/19/616462).

Включить новый сервис в своей группе или публичной странице можно в управлении сообществом. Кнопка для отправки сообщения появится под аватаром сообщества. Отправить сообщение пользователи смогут не только в десктопной, но и мобильной версии сайта, а также во всех официальных клиентах соцсети для смартфонов. К слову, во время тестирования сервиса половина сообщений сообществам были отправлены именно с мобильных устройств, сообщили представители компании.

Сервис призван улучшить взаимодействие между компаниями и пользователями: например, вы можете забронировать столик в ресторане, проконсультироваться насчет покупки автомобиля, заказать еду на дом и узнать, есть ли понравившийся вам товар в наличии, написав сообщение в группу компании вместо того, чтобы звонить по горячей линии и ждать соединения с оператором под раздражающую мелодию. Развлекательные и информационные сообщества тоже могут придумать, как использовать новые возможности, например, связываться с победителями конкурсов, общаться с рекламодателями, собирать отзывы о контенте и просто ближе узнавать свою аудиторию.

Некоторые украинские сообщества уже протестировали сообщения. Например, компания «Алло» подключила сервис в тестовом режиме 3 ноября. «При формате “Написать сообщение сообществу” на 20 % увеличилось

количество сообщений относительно обращений к менеджеру в контактах группы. Сейчас через эту кнопку отправляется 75 % запросов (без учета записей на стене группы и специального приложения)», – рассказал Д. Мазур, маркетолог компании «Алло».

В десктопной версии сайта в окне написания сообщения пользователь увидит примерное время ожидания ответа, которое высчитывается автоматически на основе того, как быстро администраторы отвечали ранее. В первые дни после включения сообщений в сообществе этого показателя может не быть. Если же в вашем любимом сообществе нет кнопки для отправки сообщения, значит администраторы решили пока не подключать сервис.

Новая возможность пришла по вкусу и спортивному сообществу ФК «Шахтер» (Донецк). «Тестировать новый сервис “сообщения сообществу” мы начали 9 ноября. С того момента поступило больше 300 обращений от наших болельщиков. В первые дни тестирования нового сервиса нас засыпали расспросами о том, кто с ними общается, интересовались как у нас дела. Чаще всего интересовались покупкой билетов на предстоящий суперматч Лиги чемпионов против мадридского Реала. Немногим меньше интересовались покупками той или иной клубной атрибутики», – рассказал Н. Савченко, SMM-менеджер ФК «Шахтер» (Донецк).

По словам редактора сообщества «Вікіпедія про мову» С. Липко, «до сих пор диалог с подписчиками происходил косвенно с помощью комментариев на стене или в комментариях к записи. Подачи предложений, объявлений, жалоб осуществлялись с помощью инструмента “Предложить новость”, что затрудняло выбор хорошего материала для публикации постов, часто превращало их “ящик” в спам. Новый инструмент позволит отделить “мух от котлет”, сохранит историю записей в случае необходимости проверки другим администратором предложений и жалоб пользователей» ***(В сообществах и публичных страницах «ВКонтакте» появились сообщения и диалоги // AIN.UA (http://ain.ua/2015/11/19/616462). – 2015. – 19.11).***

***

Социальная сеть «ВКонтакте» ввела функцию автоматического воспроизведения видео. Анонс появился в официальном сообществе администрации «ВКонтакте».

Функцию применят для роликов, размещенных в закрепленных записях сообществ. Она будет включаться в полной версии «ВКонтакте». Будет ли возможность полностью ее отключить, не сообщается.

Согласно сообщению администрации, записи по умолчанию будут показывать в беззвучном режиме без рекламы. Показ сторонней рекламы также запрещен.

Похожую функцию 19 ноября ввели «Одноклассники». Автозапуск видео распространили на все видеозаписи, появляющиеся в новостных лентах пользователей. Сервис сообщил, что юзеры могут отключить функцию в

соответствующих настройках на странице профиля и уточнил, что пока автозапуск роликов включили только для части пользователей.

Социальная сеть Facebook ввела автопроигрывание видеороликов в 2013 г., по умолчанию записи запускаются в беззвучном режиме ***(«ВКонтакте» появился автозапуск видео // Ultramir.NET (http://ultramir.net/techno/30227-vkontakte-poyavilsya-avtozapusk-video.html). – 2015. – 20.11).***

***

Facebook продолжает свою экспансию на рынок мессенджеров и недавно выпустила приложение для рабочих переписок под названием Work Chat. Программа является дополнением к платформе Facebook for Work, которая создана для обеспечения удобной и простой коммуникации между сотрудниками компаний.

Work Chat позволяет участвовать в личных переписках и групповых чатах, совершать голосовые вызовы, обмениваться документами, фотографиями и роликами, а также использовать в своих сообщениях стикеры. Таким образом, сотрудники могут максимально быстро связываться друг с другом и оперативно распространять информацию или же какие-либо материалы среди коллег.

В Facebook утверждают, что Work Chat составит конкуренцию таким приложениям, как Yammer, HipChat, Salesforce Chatter и Slack. Так ли это, станет понятным позже, но уже сейчас сервис обладает весьма широким набором функций.

В настоящее время новый мессенджер доступен лишь для Android-устройств, однако разработчики сообщают, что совсем скоро появится и версия программы для iOS. Отметим, что использовать приложение могут лишь компании, которые на сегодняшний день пользуются бета-версией Facebook at Work ***(Facebook выпустила приложение Work Chat // InternetUA (http://internetua.com/Facebook-vipustila-prilojenie-Work-Chat). – 2015. – 22.11).***

***

Социальная сеть Facebook тестирует программу, которая поможет пережить боль от расставаний, сообщает The Wall Street Journal.

«Мы начинаем тестировать инструменты, которые помогут людям управлять своим взаимодействием с бывшим партнером на Facebook после того, как отношения закончились. Когда люди меняют статус своего семейного положения и пишут, что больше не находятся в отношениях, им предлагается попробовать новые инструменты», – говорит представитель социальной сети К. Уинтерс.

Пользователи, которые решили попробовать новую разработку, не будут видеть в ленте посты бывшего партнера. В поиске не будет его/ее имя, а также можно ограничить доступ к своей странице либо к записям и фотографиям, на которых отмечен бывший партнер ***(Facebook поможет при расставании //***

InternetUA (http://internetua.com/Facebook-pomojet-pri-rasstavanii). – 2015. – 21.11).

***

YouTube представил новые инструменты перевода, разработанные специально для создателей каналов. Новый функционал поможет им сделать свой контент более доступным и понятным для международной аудитории. Об этом пишет searchengines.ru

По статистике компании, 60 % просмотров видео приходится на пользователей, которые находятся за пределами родной страны владельца канала. Соответственно, двое из трёх его зрителей могут говорить на другом языке.

Добиться того, чтобы контент могли легко найти и понять пользователи по всему миру, помогут следующие инструменты:

- Субтитры, добавленные сообществом. У владельцев канала теперь есть возможность привлечь к переводу субтитров добровольцев из числа своих подписчиков.
- Перевод названий и описаний. К видео можно добавить переведенные заголовки и описания. Это поможет поклонникам найти их через поиск на родном языке. Информация о ролике будет отображаться на языке зрителя.
- Рынок переводов (бета-версия). Создатель канала также может заказать профессиональный перевод контента непосредственно в Менеджере видео. Для этого нужно выбрать один или несколько языков перевода, а затем оформить и оплатить заказ. Когда перевод будет готов, контент будет опубликован автоматически, а владелец канала получит уведомление по электронной почте.

Некоторые из партнёров YouTube уже протестировали новый функционал. В их числе компания TED. «В течение более чем пяти лет мы работали над устранением языкового барьера, препятствующего главной миссии TED – распространению прогрессивных идей по всему миру. Компания YouTube, один из наших ключевых партнеров, открыла для нас новые горизонты – теперь наши видео не только доступны, но и понятны зрителям во всем мире», – отметил К. Виндбиглер, директор проекта открытого перевода компании TED.

Более подробная информация о новых инструментах перевода доступна в справочном центре YouTube ***(YouTube представил новые инструменты перевода для создателей каналов // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45363/118/lang,ru/). – 2015. – 20.11).***

***

Социальная сеть Facebook намерена запустить собственную краудфандинговую платформу, по аналогии с Kickstarter и Indiegogo.

Компания осваивает все новые направления и теперь намерена создать дочернюю площадку для краудфандинга. Сервис получил название Fundraiser. Площадка дает возможность формировать кампании, размещать видео, а пользователи получают возможность вносить любую сумму без переходов на иные ресурсы.

В соответствии с объявленным функционалом сервис будет достаточно легко конкурировать с площадкой Crowdrise. На сегодня сервис от Facebook используется исключительно с целью сбора средств на благотворительность, но при этом он может стать конкурентом краудфандинговой площадки Kickstarter.

Как правило, до того как перейти на Kickstarter либо Indiegogo, авторы проекта проводят продвижение в соцсетях. При этом получить возможность сбора средств прямо через внутренний функционал Facebook позволит, по оценкам аналитиков, в несколько раз увеличить приход средств ***(Facebook создала собственный аналог Kickstarter // iLenta.com (http://ilenta.com/news/internet/news_9200.html). – 2015. – 21.11).***

***

Мобильное приложение Free Basics, запущенное в рамках проекта Internet.org Facebook, теперь доступно всем жителям Индии. Об этом объявил глава компании М. Цукерберг на своей странице в социальной сети.

На сегодня Free Basics предлагает более 60 сервисов, включая информационные и образовательные ресурсы. Все они – бесплатны для пользователей. Изначально, приложение работало лишь на территории 6 из 29 штатов в Индии.

Теперь все индийцы смогут оставаться в курсе последних новостей, взаимодействовать с местными властями, искать вакансии, информацию о местных мероприятиях, повышать свой уровень образования и находить ответы на вопросы о проблемах, связанных со здоровьем, рождением детей и т. д.

Проект Internet.org, запущенный Facebook, призван объединить лидеров в области технологий, некоммерческие организации, местные сообщества и экспертов для обеспечения доступа к Интернету двум третям населения мира, у которых его нет. В мае компания открыла доступ к платформе Internet.org для сторонних разработчиков.

После шквала критики в адрес проекта, в сентябре этого года Facebook объявила, что теперь использовать защищённые сервисы можно без платы за передачу данных. В том же месяце мобильное приложение и веб-сайт Internet.org были переименованы во FreeBasics.

В настоящее время Internet.org предлагает доступ к Интернету 1 млрд людей в Азии, Африке и Латинской Америке ***(Facebook расширяет Internet.org на всю территорию Индии // IGate (http://igate.com.ua/lenta/11599-facebook-rasshiryaet-internetorg-na-vsyu-territoriyu-indii). – 2015. – 25.11).***

***

Согласно данным нового отчёта аналитической компании Parse.ly, по пяти из семи основных событий 2015 г. социальные сети обошли поиск по числу переходов на сайты новостных изданий. Об этом пишет searchengines.ru

В рамках исследования аналитики Parse.ly определили семь основных событий года. Эта выборка основана на наиболее читаемых новостных материалах в сети компании, в которую входят свыше 400 издателей, включая Fox News, Telegraph Media Group, Mashable, Business Insider, The Atlantic и Reuters.

Сотрудники Parse.ly выбирали новости, центрированные вокруг одного события. Затем эти данные были нормализованы, исходя из размера сайта.

Анализ полученных данных показал, что число переходов из поиска превысило аналогичный показатель для социальных сетей лишь по двум событиям – бой боксёров Ф. Мэйвезера и М. Пакьяо и взлом сайта знакомств Ashley Madison.

Боксёрский бой был особенно популярным в поиске за несколько дней до битвы. В этот период 66,4 % читателей пришли на сайты изданий из поисковых систем. Что касается взлома сайта знакомств, доли переходов распределилось следующим образом: 28 % – поиск; 15 % – социальные медиа. Ввиду интимного характера попавших в сеть материалов, пользователи больше искали информацию о взломе в поисковых системах, чем делились ею в социальных сетях.

По данным компании за октябрь этого года, реферальный трафик из Facebook превысил трафик из Google. Распределение их долей выглядело так: 39,2 % и 34 % соответственно.

Редакция Marketing Land обратилась к ещё одной аналитической компании, которая сотрудничает со СМИ – Define Media Group – с просьбой дать свою оценку распределению реферального трафика. По данным этой компании, большая часть переходов на сайты изданий приходится на поиск. В сеть Define Media Group входят такие издания, как the New York Times, Hearst, Bloomberg, NBCUniversal и Time.

За период с августа по октябрь в сети Define Media Group доля переходов на сайты изданий из поиска составляла 26,7 %, из социальных сетей – 22,7 %.

Что касается крупных событий, социальные медиа зачастую демонстрируют лучший результат на начальной стадии – в первые 24–48 часов, отмечают в компании. В то время как поиск остаётся стабильным источником трафика на протяжении всего периода события.

Напомним, что по данным SimpleReach, с января по октябрь 2015 г. количество переходов на сайты 30 издателей-партнёров социальной сети Facebook – как с мобильных, так и с десктоп-устройств – сократилось на 32 % ***(Социальные медиа опередили поиск по числу переходов на сайты СМИ // МедиаБизнес***

(http://www.mediabusiness.com.ua/content/view/45433/118/lang,ru/). – 2015. – 27.11).

***

Instagram тестирует поддержку многопрофильных аккаунтов на Android

Функция окажется особенно полезной для smm-менеджеров. Instagram добавил для пользователей приложения на Android возможность создания многопрофильного аккаунта. В настоящее время функция тестируется. В ближайшее время ее сделают доступной в обновленной версии приложения.

Ожидается, что функция окажется полезной для предпринимателей и smm-специалистов, ведь теперь им будет гораздо проще совмещать персональное использование Instagram и бизнес ***(Instagram тестирует поддержку многопрофильных аккаунтов на Android // InternetUA (http://internetua.com/Instagram-testiruet-podderjku-mnogoprofilnih-akkauntov-na-Android). – 2015. – 28.11).***

***

Разработчики «Одноклассников» объявили о скором начале прямых видеотрансляций игровых матчей в социальной сети.

Проект запущен в сотрудничестве с порталом GoodGame. В группе портала (ok.ru/gg) в ближайшее время появятся 10 круглосуточных игровых каналов.

Напомним, GoodGame представляет собой стриминговый игровой сервис. По своим собственным данным, портал является самым популярным в своем классе по России и СНГ. На GoodGame проходят трансляции Hearthstone, StarCraft II, Dota 2, League of Legends, Fallout 4, Counter Strike, World of Tanks, War Thunder, World of Warcraft, Battlefield, Call of Duty: Black Ops и др. ***(Одноклассники запустили игровые трансляции // Ultramir.NET (http://ultramir.net/techno/30867-odnoklassniki-zapustili-igrovye-translyacii.html). – 2015. – 27.11).***

***

Социальные сети – это пространство для обмена мыслями, идеями и взглядами. Кроме общеизвестных «ВКонтакте», Facebook, Twitter есть ещё и специализированные сети для любителей книг, в которых они могут узнать, что читают их друзья, написать собственную рецензию, составить список книг для прочтения в год и быть в курсе новинок в литературе, пишет Hyser (http://hyser.com.ua/tehnology/socseti-dlya-knigolyubov-43288).

Книжные соцсети

Goodreads

Одна из самых популярных англоязычных соцсетей читателей с аудиторией более 20 млн. Наиболее полезная функция ресурса – наличие обширной базы рекомендаций, отзывов и рецензий. Вы можете просматривать литературу ваших друзей и выбирать книги, которые планируете прочитать,

создавая свою библиотеку. Кроме этого, там можно обнародовать книги, которые читаете сейчас, и ежедневно обновлять прогресс.

В зависимости от предпочтений пользователей, Goodreads создает для каждого персональные рекомендации. Для этого надо отметить минимум 20 книг, которые вам понравились.

В соцсети также найдется много интересных сообществ молодых авторов, где можно обнародовать собственные произведения. Они доступны также на украинском.

Rubuki

Социальная сеть и одновременно дискуссионный клуб для читателей и издательств. Ресурс является русскоязычным и выполняет роль онлайн-площадки для поиска книг и создание собственной книжной библиотеки. Дополнительная функция, отличающая эти ресурсы – возможность добавить на Rubuki книгу, которая отсутствует в библиотеке, и читать ее с любого компьютера. Вы также можете делать заметки, вести дискуссию в специальном разделе и отмечать любимые цитаты.

Практическая польза Rubuki – возможность связаться с авторами и издательствами.

Wattpad

Масшабный онлайн-сервис для книгоманов, где в свободном доступе собрано более 10 млн книг. Wattpad – это также стартовая платформа для писателей. Ежедневно здесь появляются произведения новых авторов, а те, которые набирают больше всего «лайков», переходят к рубрике «популярное». Кроме общих функций и рекомендаций, команда Wattpad ежегодно проводит конкурсы для пользователей и молодых писателей.

Соцсеть имеет удобный мобильное приложение.

Readrate

Еще одна соцсеть для читателей от команды PocketBook, которая еженедельно предлагает читателям новые рейтинги. Это могут быть лучшие исторические книги, популярные в мире. Здесь также есть список рекомендаций от знаменитостей. Кроме этого, на ресурсе вы можете создавать свою библиотеку, делиться впечатлениями от прочитанного, а также записывать любимые цитаты и распространять их в других соцсетях.

Ресурс доступен на двух языках: русском и английском.

Riffle Books

Узнайте друзей через их книги и книги из своих друзей – лозунг книжной соцсети Riffle Books. Сервис хорошо визуализированный, что делает поиск литературы еще интереснее. После регистрации вам предложат пройти небольшой опрос, из-за которого определят ваши вкусы и предложат свой список книг.

На ресурсе вы сможете подписаться на интересных пользователей и следить за их рекомендациями.

Shelfari

В соцсети Shelfari читатели могут самостоятельно обновлять и редактировать описания к книгам в каталоге. Это главное отличие ресурса от других книжных онлайн-клубов. Каждому пользователю выделяется личная «книжная полка». Книги для чтения можно искать в удобном поисковике. Выбираете жанр, отмечаете другие предпочтения и добавляете книгу из предложенного списка в опции «планирую прочитать». Кроме этой функции, здесь также можно отметить, что вы уже прочитали, а читаете именно сейчас. Доступна также возможность вступать в тематические сообщества.

Librarything

Книжная соцсеть для поиска и обмена книгами, доступна на многих языках. В каталоге ресурса собрано почти 100 млн различных книг из магазинов Amazon. Здесь, как и в других соцсетях, вы найдете рекомендации и отзывы на книги, а также списки не только интересной литературы, но и авторов.

LiveLib

LiveLib – это живая библиотека в сети, которая объединяет читателей и авторов. Вы можете создать свою подборку книг и поделиться ею с друзьями. Кроме списков литературы и отзывов, здесь можно играть в литературные игры и получать за это призы. В соцсети существует опция заметок и записей любимых цитат ***(Гринь Ю. Соцсети для книголюбов // Hyser (http://hyser.com.ua/tehnology/socseti-dlya-knigolyubov-43288). – 2015. – 28.11).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Журнал «Новое Время» опублікував рейтинг найпопулярніших українців у соціальних мережах (http://nv.ua/ukr/ukraine/politics/nv-sklalo-rejting-najpopuljarnishih-ukrajintsiv-v-sotsialnih-merezhah-82828.html).

Першу десятку очолив лідер української рок-групи «Океан Ельзи» С. Вакарчук. На другому місці розташувався Президент України П. Порошенко, а слідом за ним – Прем'єр-міністр А. Яценюк.

Далі розташувалися: губернатор Одеської області М. Саакашвілі (має українське громадянство, 4 місце), народний депутат, журналіст М. Найєм (5), міністр внутрішніх справ А. Аваков (6), народний депутат, військовий експерт Д. Тимчук (7), мер Києва В. Кличко (8) і руфер, громадський активіст Г. Mustang Wanted (9). Замикає десятку лідерів народний депутат, лідер Радикальної партії О. Ляшко.

Бум соціальних мереж, що стався на тлі зростання соціальної активності українців, призвів і до зміни структури споживання новин. За даними дослідження міжнародної компанії Nielsen, проведеного серед 30 тис. онлайн-респондентів у 60 країнах світу (в тому числі в Україні), у соціальних мережах

свіжу інформацію про останні події черпає 47 % співвітчизників. Для порівняння: майже стільки ж – 48 % українців отримують новини з інтернет-видань, а 51 % – з телепрограм.

Фахівці називають активність українців у Facebook прикметою часу: якщо тебе немає в соцмережах, тебе немає ніде. Тому соціальні мережі й облюбували політики, які часто використовують ці майданчики не стільки для спілкування з народом, скільки для піару. Утім, у Facebook панує демократія: схвальні лайки тут отримують не за портфелі, а за точно сформульовані та актуальні пости.

Більше того: колективний розум соціальних мереж перетворився на своєрідний орієнтир для влади. Наприклад, після того як лідери думок Facebook назвали прийняття закону від 2 липня 2015 р. про повернення кредитів фізичними особами за курсом на момент взяття їх згубним для банківської системи, це не на жарт налякало багатьох депутатів. Багато хто став публічно виправдовуватися, намагатися відкликати голос, і в результаті одіозний закон скасували.

Однак наявність сотень тисяч передплатників у блогера аж ніяк не гарантує, що всі вони читають кожен його пост. Facebook, залежно від налаштувань, показує в стрічці не всі пости, і алгоритми формування стрічки постійно змінюються. Також фахівці вважають, що для впливовості блогеру вистачить 10 тис. передплатників, а іноді і 5 тис. передплатників достатньо, щоб бути почутим.

Впливовість у соціальних мережах тримається на трьох китах – лайку, шерах і коментарях ***(НВ склало рейтинг найпопулярніших українців у соціальних мережах // Новое Время (http://nv.ua/ukr/ukraine/politics/nv-sklalo-rejting-najpopuljarnishih-ukrajintsiv-v-sotsialnih-merezhah-82828.html). – 2015. – 29.11).***

***

Основатель Facebook М. Цукерберг объяснил, почему функция «проверки безопасности» появилась в соцсети только после терактов в Париже 13 ноября, но не после взрывов в пригороде Бейрута 12 ноября. Сообщение он опубликовал на своей странице в сервисе.

По словам М. Цукерберга, до событий во Франции правила Facebook предусматривали, что функцию необходимо включать только для регионов, затронутых стихийными бедствиями. «Мы поменяли эти правила и теперь планируем включать проверку безопасности также в случаях других катастроф, происходящих с людьми», – говорится в сообщении.

В расширенном пресс-релизе соцсети уточняется, что функцию решили активировать в ответ на резко возросшее количество записей в Facebook, в которых пользователи делились информацией о происходящем и пытались узнать, как обстоят дела у их близких и знакомых в Париже.

Суть «проверки безопасности» в том, что в Facebook появляется особая страница, с помощью которой пользователи, оказавшиеся в пострадавшем

районе, могут сообщить, что находятся в безопасности. Остальные пользователи могут проверить, попал ли в опасную зону кто-то из их друзей.

«Спасибо всем, кто обращается с вопросами по этому поводу. Вы правы, что в мире происходит много других важных событий. Мы заботимся обо всех людях одинаково и мы будем стараться помочь всем попавшим в беду», – сообщил М. Цукерберг.

Вечером 12 ноября двое террористов-смертников, передвигавшихся на мотоциклах, атаковали южную окраину Бейрута. Мощные взрывы произошли с интервалом в семь минут. Один из нападавших подорвался у блокпоста рядом с шиитской мечетью, другой – через 150 м возле торгового центра. В результате терактов погиб 41 человек, более 200 получили ранения ***(Основатель Facebook ответил на обвинения в игнорировании трагедии в Бейруте // InternetUA (http://internetua.com/osnovatel-Facebook-otvetil-na-obvineniya-v-ignorirovanii-tragedii-v-beirute). – 2015. – 16.11).***

***

В соцсети Facebook активирована функция «Проверка безопасности» в Нигерии после взрывов, передает Reuters.

Соцсеть включила данную функцию в Нигерии после критики со стороны пользователей, недовольных тем, что соцсеть выборочно выбирает страны для запуска функции ***(На Facebook активирована функция «Проверка безопасности» после взрывов в Нигерии // InternetUA (http://internetua.com/na-Facebook-aktivirovana-funkciya--proverka-bezopasnosti--posle-vzrivov-v-nigerii). – 2015. – 18.11).***

***

В Николаеве на выборах Facebook победила пропаганду

В Николаеве в день выборов, 15 ноября, хотя и не получилось установить рекорд для «Книги Рекордов Гиннеса» по явке избирателей на избирательные участки, зато показатель был наибольший по Украине.

Об этом в социальной сети Facebook написал волонтер Д. Арахамия, отметив, что общался с представителем «Книги Рекордов Гиннеса». По его словам, эти выборы в Николаеве должны войти в историю, «так как впервые Facebook и интернет-СМИ победили оффлайн пропаганду» ***(Давид Арахамия: В Николаеве на выборах Facebook победил пропаганду // НикВести (http://nikvesti.com/news/politics/78579). – 2015. – 16.11).***

***

Работу чиновников г. Шостки будут оценивать по работе в соцсетях. Об этом мэр Шостки Н. Нога заявил на аппаратном совещании в горисполкоме.

«Це нова форма роботи, без якої неможливо державному службовцю місцевого самоврядування…працювати», – отметил городской голова.

Н. Нога поблагодарил заведующих сектором молодежи О. Сокульскую и зав. сектором по физкультуре и спорту А. Доценко за активность в соцсетях

(Работу чиновников будут оценивать по работе в соцсетях // Шостка.ИНФО (http://www.shostka.info/news_shostka/rabotu_chinovnikov_budut_ocenivat_po_rabote_v_socsetyah). – 2015. – 23.11).

***

Контрреволюція соцмереж

У популізмі звикли звинувачувати політиків.

Вони дійсно дають усі підстави для цього: обіцяють зниження тарифів, контрактну армію, мільйони робочих місць та інші, навряд реальні, блага для українців.

…Українці вносять свій внесок у загальний популістичний фон. Зокрема, зараз на цю тенденцію працюють соціальні мережі.

Красномовним прикладом служить Facebook-шторм навколо скандальної антидискримінаційної поправки. Особливо дісталося «Самопомочі», яка позиціонувала себе як нова, проєвропейська демократична сила. Спроби раціонального діалогу з виборцем через платформу соцмереж переросли в гротеск на кшталт шоу «за склом» із показовим відлученням нардепа Є. Соболєва від будинку дружиною.

Ця історія зібрала набагато більше новин і відгуків, аніж коментар одного з представників політсили з докладним мотивованим виправданням. Юзери, що критикують телевізійні ток-шоу за показушність, з радістю повелися на такий же – дещо вульгарний – «Дом-2», але тільки в соцмережах.

Основним бачиться коментар одного з користувачів під постом «Самопомочі»:

– Нам не важливо, чому і як ви голосуєте. Ми хочемо їздити до ЄС без віз.

Варто визнати – популізм зіпсував не тільки партії, але й виборців. Побіжний щоденний перегляд соцмереж показує відносний зріз політичного попиту «Facebook-виборця», на якого поступово починає орієнтуватися частина політиків. За шумом «зрад» і «перемог» він хоче того ж, що і «гречаний» електорат, нехай і в складніше сформульованих пропозиціях.

Виборець хоче негайного поліпшення свого життя, приховуючи це через переживання за країну.

Політик, прагнучи до популярності, розривається між «лайкабельними» постами і раціональними, врешті схиляючись у бік популізму.

А між тим, як показало свіже дослідження Nielsen, соцмережі стали третім за значущістю джерелом інформації для українців з 47 %, після ТБ (51 %) і новинних сайтів (48 %).

У австрійського економіста і політолога Й. Шумпетера є економічна ідея «креативного руйнування» – демонтажу старих структур і виробництв заради інновацій і створення нових. Українська ж політика поки намагається надбудувати над убогим заводом епохи пізніх Рад високотехнологічне виробництво, замість того, щоб зруйнувати звичні правила роботи вітчизняних

партій. Серед них – залежність від капіталу, внутрішній авторитаризм і диктатура партійної еліти, відсутність реальної роботи з виборцем і його політпросвіти, ніяка кадрова політика і слабкий рекрутинг молоді, дефіцит стрижневих цінностей.

Україні потрібні політики-новатори, за якими вже будуть здатні прийти реформи. До тих пір система приречена на самовідновлення і не менш стабільне гниття ***(Шевченко Л. Контрреволюція соцмереж // INSIDER (http://www.theinsider.ua/politics/5652d33020ffe/). – 2015. – 23.11).***

***

Украинцам предлагают рассказать о том, что их волнует больше всего, какие проблемы конкретного города, села или поселка требуют решения. Такую возможность дает новый социальный проект #хто_вирішить общественной организации «Успішна країна», который стартовал 23 ноября.

«Уже всем очевидно, что местные выборы не решили и сотой доли проблем обычных украинцев. Может власти всех уровней просто не знают о том, что в стране разбитые дороги, сумасшедшие цены в магазинах, дикая коррупция, запущенная медицина, да и много еще чего неприемлемого для цивилизованной страны? Мы обращаемся ко всем украинцам, кто не утратил надежду, и кто верит, что только сообща, можно решить самые больные проблемы страны. Пришло время во всеуслышание заявить о своих проблемах и вместе искать того, #хто_вирішить!» – заявляют активисты.

Первыми к новой акции присоединились жители Чернигова, которые в рамках проекта #хто_вирішить рассказали о проблемах, которые их волнуют: дефицит мест в детсадах, грязные, разбитые и темные по вечерам улицы, безработица, отсутствие социальных лифтов для молодежи

Принять участие в акции может любой желающий – для этого необходимо сформулировать свою проблему и выложить фотографию с хэштегом #хто_вирішить на своей страничке в одной из социальных сетей или через сайт http://uspishna.org/ и социальные сети организации «Успішна країна» https://www.facebook.com/uspishna.kraina/?fref=ts ***(В соцсетях стартовал новый социальный проект «#хто_вирішить» // Час Пик (http://vchaspik.ua/politika/356176v-socsetyah-startoval-novyy-socialnyy-proekt-htovirishit). – 2015. – 24.11).***

***

В Украине появится «социальная сеть» для переселенцев

В Украине будет разработан специальный сайт для внутренне перемещенных лиц. Об этом на своей странице в Facebook сообщает общественная организация «Донбасс SOS».

Разработкой ресурса занимается Министерство социальной политики. У каждого ВПЛ будет свой аккаунт, с помощью которого можно будет разместить информацию о своих потребностях и отслеживать актуальные программы и предложения помощи в регионе, где переселенец проживает.

«Другими словами, каждый, кто посетил УТСЗН и официально зарегистрировался, как внутренне перемещенное лицо, получит персональный аккаунт», – поясняет «Донбасс SOS».

По данным организации, в настоящее время готовятся программы для освоения целевых средств на оказание помощи ВПЛ местными органами самоуправления. «И местные органы осваивают их так, как считают нужным, не всегда исходя из актуальных потребностей внутренне перемещенных лиц. Возможно, в отдельно взятом городе/селе/районе переселенцы не нуждаются во временном жилье, зато в местной больнице не хватает мест, персонала, оборудования. Можно было бы перераспределить денежные средства и построить новый корпус с современным оборудованием, чтобы людям не приходилось ездить по 50 км в центр и обратно», – подчеркивает «Донбасс SOS».

Организация приводит пример: в Одессе проживает большое количество переселенцев-инвалидов, которым необходима специфическая помощь, «и там уж точно переселенцы лучше знают, что им больше нужно». «А вот если дать аккаунту на сайте МинСоц право голоса, этот голос можно будет отдать за принятие решений о том, как осваивать и контролировать затраты на нужды переселенцев в регионе. Другими словами, на основе того, что за каждым аккаунтом – мнение гражданина, можно запустить первый в Украине национальный проект по электронному самоуправлению. А вы готовы управлять и принимать решение?» – отметили в организации ***(В Украине появится «социальная сеть» для переселенцев // NewsCloud (http://www.news-cloud.net/news/ukraine/society/13026-v-ukraine-poyavitsya-socialnaya-set-dlya-pereselencev.html). – 2015. – 21.11).***

***

Паблики в социальных сетях призывают харьковчан выразить свое мнение по вопросу переименования районов города.

К примеру, в группе «Типичный Харьков» пользователям предлагается несколько вариантов переименования районов, из которых люди выбирают понравившийся. Так, в группе предложено три варианта для названия Фрунзенского района. Первый – оставить нынешнее название, второй – Новодомовский, третий – Машиностроительный. На сегодняшний день в голосовании приняли участие 3,5 тыс. человек. Более 80 % проголосовали за то, чтобы район остался Фрунзенским, 7,9 % хотят, чтобы район назывался Новодомовским, 10,8 % – Машиностроительным.

Также большинство проголосовавших в паблике хочет оставить нынешнее название Орджоникидзевскому району (72,5 %), Баварским район хотят назвать 17,6 %, Юго-Западным – 9,9 %. Всего в этом голосовании приняли участие более 3,5 тыс. человек.

Большинство проголосовавших пользователей также выступают против переименования Октябрьского района (71,2 %), поменять название на

Холодногорский хотят 16,2 %, на Баварский – 12,6 %. Всего проголосовало в этом опроснике почти 4 тыс. человек.

Также был проведен опрос относительно изменения названия Дзержинского района. 72,5 % не хотят его переименования, 15,2 % выступают за название Шевченковский, а 12,3 % – за Университетский. Всего проголосовали 3,5 тыс. человек.

Что касается Ленинского района, то 33,3 % проголосовавших хотят, чтобы он назывался Холодногорским, 12,9 % хотят назвать его Благовещенским, 8,1 % – Слободским, 6,2 % – Железнодорожным. Остальные предлагают либо свой вариант, либо не определились с названием. Всего в голосовании приняли участие 3,8 тыс. людей.

Похожие результаты и в других пабликах – «Харьков (Kharkov)», «Харьков – 1-я столица» и прочих, где размещены такие голосования ***(В социальных сетях проводят соцопросы по переименованию районов Харькова // Сайт Харьковского городского совета (http://www.city.kharkov.ua/ru/news/u-sotsialnikh-merezhakh-provodyat-sotsopituvannya-z-pereymenuvannya-rayoniv-kharkova-30000.html). – 2015. – 19.11).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Социальная сеть «Одноклассники» официально объявила о запуске нового рекламного инструмента – промопостов с видео с автоматическим запуском. Заметки с видео будут отображаться в тех же слотах, что и привычные рекламные публикации в ленте, поэтому рекламная нагрузка на пользователя «Одноклассников» нисколько не увеличится. Об этом пишет searchengines.ru

С. Боярский, менеджер по развитию проекта «Одноклассники», рассказывает: «Для многих брендов продвижение owned media и собственных видеоканалов является приоритетом в стратегии. Теперь у рекламодателей есть возможность делать “посевы” с детальным таргетингом на свою целевую аудиторию. Особенность формата заключается в том, что рекламодатель платит только за показы видео в ленте, а весь виральный эффект достается бесплатно. Таким образом, чем интереснее контент для пользователя, тем дешевле просмотр. А благодаря возможностям узкого таргетирования инструмент может быть полезен не только крупным рекламодателям, но и локальным. Видеоблогеры и группы могут использовать его для того, чтобы привлечь внимание к собственному контенту».

Рекламные кампании для постов с видео управляются с помощью платформы myTarget. Кроме стандартных настроек по полу и возрасту доступен таргетинг по интересам, доходу и телесмотрению.

Продажа нового формата осуществляется по количеству показов с аукционным ценообразованием. Минимальная ставка в системе myTarget будет начинаться со 150 р. за 1 тыс. показов. Отчетность по рекламным видеопостам построена по стандарту VAST: данные о процентах просмотра видео, включении и выключении звука, открытии видео в полноэкранном режиме и др. ***(Нативная видеореклама в Одноклассниках – новый инструмент для продвижения брендов // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45403/118/lang,ru/). – 2015. – 24.11).***

***

Популярная американская соцсеть Facebook экспериментирует с несколькими видами кнопок call to action в спонсируемых видеороликах. Об этом сообщают пользователи ресурса.

Некоторые владельцы аккаунтов Facebook заметили нечто непривычное в рекламных видео, появляющихся в их лентах, а именно призыв перейти на сайт рекламодателя, расположенный в нижнем левом углу ролика.

При этом сама кнопка разработана таким образом, что она показывается поверх видео на протяжении всего времени его проигрывания ***(Facebook тестирует навязчивую кнопку // Reklamaster (http://reklamaster.com/marketing-and-advertising/facebook-testiruet-navjazchivuju-knopku). – 2015. – 27.11).***

***

«ВКонтакте» добавила несколько нововведений в работу Биржи рекламы.

Теперь пользователи смогут получать уведомления о новых заявках в виде личных сообщений. Ранее они рассылались только по SMS и email.

Чтобы быстрее разослать несколько заявок в разные сообщества, рекламодатели теперь останутся на странице со списком доступных рекламных площадок после подачи рекламной заявки. Во всех видах уведомлений о новых заявках теперь будет указываться желаемое время публикации записи.

При отзыве заявки ее время публикации продолжит показываться на вкладке «Невыполненные». Таким образом можно будет легко выяснить, какой рекламный слот свободен, и заполнить его при необходимости.

Проверочный код («капча»), возникавший ранее в некоторых случаях во время приема заявок с Биржи, больше не будет показываться. А для того, чтобы пользователям было более удобно просматривать список писем, в уведомлении на email название сообщества было вынесено ближе к началу письма ***(ВКонтакте обновил функционал Биржи рекламы // Sostav.ua (http://sostav.ua/publication/vkontakte-obnovil-funktsional-birzhi-reklamy-69295.html). – 2015. – 25.11).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Большое количество друзей в соцсетях приводит к стрессу

Избыток друзей на Facebook повышает в организме молодых людей уровень кортизола – гормона стресса. Специалисты из Университета Монреаля предполагают: это может рано или поздно привести к депрессии. В новом исследовании приняли участие 88 добровольцев в возрасте от 12 до 17 лет, пишет UBR (http://ubr.ua/ukraine-and-world/society/bolshoe-kolichestvo-druzei-v-socsetiah-privodit-k-stressu-366677).

Участников спрашивали о частоте использования Facebook, количестве друзей в соцсети и саморекламе. Еще добровольцы рассказали о поддержке, оказываемой ими друзьям в социальной сети. Кроме того, ученые измерили уровни кортизола в организме подростков. Образцы у участников брали по четыре раза в день в течение трех дней.

Специалисты выяснили: уровень гормона стресса оказался повышен у добровольцев, имевших больше 300 друзей на Facebook. Из-за избытка друзей уровень гормона возрастал примерно на 8 %. Вероятно, у подростков, имеющих больше 1000 или 2000 друзей в соцсети, уровень кортизола еще выше. Также исследователи обнаружили, что у участников, поддерживавших своих друзей на Facebook, например, оценивавших их сообщения или писавших им слова поддержки, уровень гормона стресса был снижен ***(Большое количество друзей в соцсетях приводит к стрессу // UBR (http://ubr.ua/ukraine-and-world/society/bolshoe-kolichestvo-druzei-v-socsetiah-privodit-k-stressu-366677). – 2015. – 22.11).***

***

Зачем люди ругаются в соцсетях?

Защищать свою точку зрения в Интернете стало делом чести, а у некоторых людей превратилось в своеобразное хобби. Прививочники спорят с антипрививочниками, чайлдфри – с детными, сторонники власти с оппозицией. Зачем нам споры в сети, которые нередко портят настроение, а подчас способны рассорить нас с настоящими друзьями и близкими?

Отсутствие реального контакта с собеседником создает иллюзию безопасного общения. Можно отойти от компьютера, продумать аргументацию, сочинить более точный и остроумный ответ. К сожалению, это чувство безопасности порой выявляет наши худшие качества. Феномен безнаказанности в Интернете стал заметен с появлением первых форумов и чатов, когда под масками ников и аватаров люди писали то, что никогда не решились бы озвучить на публике. Но прошло 10–15 лет, и наступила эпоха социальных

сетей. Сетевая анонимность практически сошла на нет, однако градус дискуссий в Интернете по-прежнему высок.

Идеальный «Я»

Как ни странно, одной из причин популярности «сетевых войн» является наше стремление к совершенству. Споры и противопоставление себя группе помогают поддержать свое «идеальное Я»: «они – такие, а я не такой, они – плохие, а я – хороший». Для этой цели человек выбирает «виртуальных врагов» – людей, взгляды которых кажутся жестокими, неуместными или несовременными. А затем последовательно и методично пытается развенчать их заблуждения, параллельно делясь наболевшим в закрытых постах для друзей.

Виртуальные битвы за истину притягательны еще и тем, что в них кипят настоящие страсти. Изящные уколы, парирование реплик оппонента и бан как крайняя мера… Люди, чья жизнь бедна событиями, идут на поля сетевых сражений за яркими эмоциями. Беда в том, что споры в переписке, увы, не способны заменить реальные впечатления. Жизнь остается бедной красками и эмоциями, а вместе с неудовлетворенностью растет и уровень агрессии.

Когда нечем заняться

Для некоторых отстаивание истины в виртуальном мире становится привычным заполнителем времени. Не нужно рисковать, пытаясь завести друзей или отправляясь на свидание с новым поклонником. Нет ожиданий – нет и разочарований. Кроме уходящего впустую времени и жизни, которая застыла на месте.

Вовремя остановиться

Как понять, что вы тратите на «ломание копий» в Интернете слишком много времени и душевных сил?

Вы слишком остро реагируете на критику от других пользователей или сами провоцируете споры.

Выйдя в офлайн, вы продолжаете думать о том, «что написал вам этот грубиян».

Виртуальные диалоги все чаще становятся предметом беседы с вашими реальными друзьями.

После чтения комментариев или переписки вы чувствуете злость, бессилие или эмоциональную опустошенность.

Если вы отметили у себя хотя бы один-два признака – можно предположить, что общение в Интернете заполняет какие-то лишние ниши в вашей жизни, пора вернуть его на законное место. Постарайтесь понять: какую потребность восполняют бурные споры и выплеск негатива в сети? Может, вам стоит записаться в турклуб или секцию боевых искусств? А возможно, уже пора завести новых друзей или сходить наконец на свидание ***(Зачем люди ругаются в соцсетях? // Medinfo (http://medinfo.ua/analitic/00015f9e2547564901e288c7bcba7a5d). – 2015. – 24.11).***

***

Социальные сети – неотъемлемая часть жизни многих людей. Здесь можно не только узнавать новости о знакомых людях и смотреть их фото, но и выражать своё позитивное отношение с помощью нажатия кнопки «лайк» («нравится»). Оказывается, это простое действие влияет на память и нейронные связи как одобряющего, так и получателя. Нередко человек ставит «нравится» даже когда и не испытывает восторга от прочитанного (увиденного). Почему же? Стоит проанализировать психологию «лайков»…

Признание

Человек заходит со своей странички в Facebook и ставит «нравится» возле опубликованной фотографии виртуального друга. И что же получается? Ответ прост: акт признания. Поставить «лайк» означает выразить свою симпатию или солидарность.

Однако есть одно «но» – пользователь нередко ставит положительную оценку посту, который ему и не нравится. Вероятно, в этом случае своим «лайком» человек хочет заявить (напомнить) о своём существовании другому.

Социальный капитал

Это понятие означает сеть социальных связей между людьми, а также их общие ценности и взгляды на нормы поведения.

Социальные сети идеально подходят для формирования такого капитала, и «лайк» играет в этом процессе особую роль.

Способ заявить о себе

Когда человек нажимает кнопку «нравится» под статусом или цитатой известной личности, таким образом он заявляет о своём мнении. С помощью поставленного «лайка» пользователь, по сути, самовыражается.

Уверенность в себе

К сожалению, с популяризацией социальных сетей, самооценка многих людей стала зависеть от количества полученных «нравится». Часто человек выражает своё одобрение фотографии или заметке своего виртуального друга не потому, что они действительно вызывают у него позитивные эмоции. Ставя «лайк», пользователь надеется получить одобрение в ответ, тем самым пополняя личную коллекцию положительных оценок под фотографиями или статусами.

Замена отношений

Многие считают, что один щелчёк мышью заменяет полноценное общение (разговор, комплименты, дискуссию). Последнее требует значительного количества времени и душевных сил. С помощью «лайков» человек пытается оставаться на связи с теми, кому лень позвонить или написать письмо. Получается эффект присутствия в чьей-то жизни.

Пользуясь социальными сетями, важно не сосредотачиваться на количестве одобрительных кликов виртуальных друзей. Ведь ни один «лайк» не сможет заменить искренней улыбки или комплимента, полученного в реальной жизни ***(Что на самом деле означают «лайки» в соцсетях // Час***

Пик (http://vchaspik.ua/zhizn/355351chto-na-samom-dele-oznachayut-layki-v-socsetyah). – 2015. – 20.11).

Маніпулятивні технології

Американец по имени Р. Бредбери в фейковом аккаунте в Twitter написал, что Эйфелева башня погасила огни в память о погибших в Париже 14 ноября. Неправдивый твит быстро набрал 30 тыс. репостов, а несколько СМИ даже написали по его мотивам вполне серьезные заметки, хотя многие пользователи сообразили, что информация абсурдна. Своим экспериментом Р. Бредбери хотел продемонстрировать, как легко подменить факты домыслами с помощью социальных сетей, пишет AIN.UA (http://ain.ua/2015/11/16/615760).

В день теракта Р. Бредбери, управляющий одной из американских компаний по разработке ПО, заметил, что по некоторым аккаунтам пользователей и СМИ пронеслась информация, якобы Эйфелева башня погасила подсветку в память о жертвах терактов во Франци.

Американец решил провести эксперимент и опубликовать эту историю со своего дополнительного аккаунта @ProfJeffJarvis. В информации профиля указана сатирическая информация, до этого в нем несколько раз публиковались фейковые твиты, так что было несложно сразу заподозрить подвох. Впрочем, как выяснилось, очень немногие пользователи Twitter критически оценивают информацию.

Бредбери написал: «Вау. Огни Эйфелевой башни погасли впервые с 1889 г.», и снабдил его соответствующей фотографией.

Твит мигом разлетелся по соцсети. Помимо тысяч пользователей, информацию подхватили СМИ разного размера и охвата. Несмотря на то что в ответах к твиту многие обратили внимание на абсурдность заявления, почти 30 тыс. человек это не смутило.

Огни не могли гореть с 1889 г., потому что были установлены только в 1915 г. К тому же, с тех пор прошло две войны, в ходе которых подсветка периодически отключалась (держать ее все время было, как минимум, не экономно). Совсем недавно Эйфелевую башню выключали в память о жертвах Charlie Hebdo. Не говоря уже о том, что каждый день огни гасят в 01:00, как и произошло в тот день. Так что твит никак не мог быть правдивым.

Фейк успешно разошелся и в русскоязычном сегменте соцсетей. Многие российские и украинские СМИ подхватили «утку» и начали ее тиражировать.

«Большинство информации в соцсетях в такие моменты – это просто мусор. Да, были удачные решения, например, хештег #porteouverte или функция Facebook Search – однако и тут остается вопрос касательно их реальной эффективности», – прокомментировал Р. Бредбери.

Урок, который хотел преподнести миру американец, заключался в том, что в современном мире настоящая история очень легко подменяется ложной при помощи соцсетей. Для этого используются так называемые

«псевдоавторитеты» (thinkfluencers) – люди, которые умеют очень убедительно и уверенно подавать заведомо фейковую информацию.

Отметим, что разгон фейков дошел до многих уголков Интернета. К примеру, недавно фейковая бритва с лазерным лезвием собрала на KickStarter 4 млн дол. ***(Доверчивые соцсети: Фейковый твит про «траурную» Эйфелеву Башню ретвитнули 30 000 раз и растиражировали в СМИ // AIN.UA (http://ain.ua/2015/11/16/615760). – 2015. – 16.11).***

***

У соціальній мережі Twitter була розпочата кампанія зі збору коштів на придбання зброї «для вбивства євреїв». Повідомляють «Акценти» з посиланням на 9 канал (http://accents.today/news/u-tvitteri-rozpochato-rozprodazh-zbroji-dlya-vbyvstva-jevrejiv/).

Як повідомляє Інститут дослідження ЗМІ Близького Сходу, декларована мета ініціаторів – «підготувати моджахедів до виконання джихадистських акцій проти євреїв» і «звільнити Аль-Аксу від єврейської нечисті».

Бажаючим пожертвувати гроші на зброю пропонуються кілька опцій на вибір: ракету RPG можна купити за 3 тис. дол., снайперську гвинтівку за 6 тис. дол., ракету для «Катюші» за 9 тис. дол., ракету «Град» з 20-кілометровою дальністю польоту за 4 тис. і ракету «Град» з 40-кілометровою дальністю польоту за 10 тис. дол. ***(У «Твіттері» розпочато розпродаж зброї для вбивства євреїв // Акценти (http://accents.today/news/u-tvitteri-rozpochato-rozprodazh-zbroji-dlya-vbyvstva-jevrejiv/). – 2015. – 17.11).***

***

Боевики «Исламского государства» отреагировали на блокировку администрацией Telegram своих ботов и каналов, начав создавать закрытые групповые чаты, попасть в которые можно исключительно по приглашению. Приглашения в групповой чат пересылались в еще не закрытые каналы ИГ, которые после этого удалялись самими создателями.

Кроме того, джихадисты написали инструкцию по взаимодействию в Telegram, согласно которой писать в чат сообщения имеют право только его создатели, то есть администрация. При этом написание в чат сообщения будет приравнено к нарушению правил, и пользователь будет удален. Кроме того, присоединяться к чату по приглашению могут все желающие. Также предлагается жаловаться администрации на подозрительных пользователей.

Джихадисты сразу нарушили выбранные ими правила и начали общаться в чате. Нарушители были заблокированы администраторами группового чата.

За первый час после появления чата и рассылки приглашений в него вступили все 200 пользователей, после чего джихадисты начали заводить дублирующие группы, удаляя из них тех, кто вступал в предыдущие. После этого каждому участнику написал администратор соответствующей группы с просьбой удалить фотографию с аватара, мотивируя это опасностью быть вычисленным спецслужбами.

Ранее 18 ноября Telegram заблокировал более 78 каналов на 12 языках, которые могли быть связаны с террористической группировкой «Исламское государство», а руководство мессенджера заявило об обеспокоенности тем, что их сервис используется для вербовки и координации действий боевиков.

В середине марта 2015 г. администрация Telegram добавила в групповые чаты поддержку хештегов, возможность упоминать конкретных пользователей и отвечать на отдельные сообщения, а также пересылать их с добавлением собственных комментариев. Возможность приглашать новых пользователей в групповые чаты стала доступна в Telegram с 30 апреля 2015 г. В одном групповом чате могут участвовать до 200 человек. Ссылка с приглашением в группу присылается отдельным сообщением, после чего пользователь должен дать согласие на присоединение к чату ***(Джихадисты научились обходить блокировку в Telegram // InternetUA (http://internetua.com/djihadisti-naucsilis-obhodit-blokirovku-v-Telegram). – 2015. – 20.11).***

***

Міфи та фейки поширюються мережею після терактів у Парижі.

Таку підбірку фейків зробив BuzzFeedNews.

Напади не були передбачені у пості на французькому сайті JeuxVideo. Скріншот – фейк.

Скріншот, який поширювався в мережі після нападів терористів у Парижі, імовірно, показує пост за 5 листопада, передбачаючи напади, які вбили б більше 100 чоловік у Парижі через «декілька днів», але насправді скріншот був відредагований. Фактично допис не каже нічого про ймовірні атаки.

Ейфелеву вежу не вимикали в пам'ять про загиблих.

Відео The Sky News, на якому вогні Ейфелевої вежі вимикаються, активно поширили мережею. Однак воно було зняте у січні, після нападу терористів на редакцію французького сатиричного журналу Charlie Hebdo.

Більше того, так чи інакше вогні Ейфелевої вежі вимикаються щоночі о 1:00.

Полум'я дійсно спалахувало у таборі мігрантів «Джунглів» у Калі, але не зрозуміло, чи це був напад з метою помсти.

Причини вогню в таборі мігрантів у Калі на даний час не визначені. «Усіх деталей на даний момент невідомо», – розповів один із співробітників гуманітарної місії. На даний час немає жодних доказів, які би підтвердили чутки про те, що це був підпал з метою помсти за події у Парижі; це був не перший випадок за останні місяці, коли у таборі спалахував вогонь.

У мережі поширюються фото зі зверненням ідентифікувати акаунти деяких терористів у соціальних мережах, але влада ще не встановила цих осіб.

«Влада Франції повинна все ж таки розпізнати котрогось з нападаючих, доти неможливо перевірити, чи є точними зображення», – ідеться в матеріалі. Після попередніх атак невинні люди регулярно були ідентифіковані як терористи як у соціальних мережах, так і в пресі.

Твіт Д. Трампа щодо французьких законів про контроль над зброєю був опублікований у січні, а не у відповідь на поточні події.

Потенційний республіканський кандидат у президенти піддався критиці людей за це повідомлення у Twitter, оскільки, на думку користувачів, це була не зовсім тактовна відповідь на напади терористів у п'ятницю. Однак це була відповідь Д. Трампа на напад на Charlie Hebdo у січні (тоді це також піддалося критиці з тієї ж причини).

Посол Франції у США був одним з тих, хто розкритикував Д. Трампа в нині видаленому твіті.

The Empire State Building не змінювала свої кольори.

Велика кількість користувачів у своїх твітах стверджувала, що The Empire State Building у Нью-Йорку була висвітлена кольорами французького прапору в п'ятницю вночі. Насправді фото були зроблені ще в січні, коли кольори були змінені на знак солідарності з постраждалими внаслідок нападу на офіс Charlie Hebdo.

Нагадуємо, що раніше російські ЗМІ поширювали фейкові новини про те, що українці тішаться падінню російського літака ***(Фейки про паризькі теракти у соціальних мережах, яким ви не повинні вірити // MediaSapiens (http://osvita.mediasapiens.ua/web/social/chutki_pro_parizki_terakti_u_sotsialnikh_merezhakh_yakim_vi_ne_povinni_viriti/undefined/). – 2015. – 19.11).***

***

Нідерланди хочуть боротися з російською пропагандою, виділивши 1,3 млн на євро на підтримку незалежних російськомовних ЗМІ в різних країнах. Про це повідомив міністр закордонних справ Нідерландів Б. Кундерс.

«Стимулюючи незалежну пресу, ми хочемо поліпшити доступність незалежних новин, щоб російськомовному населенню було з чого вибирати», – ідеться в заяві. Як зазначається, дослідження, проведене в рамках проекту European Endowment for Democracy, показало, що Кремль здійснює прямий та непрямий контроль над медіа не лише в Росії, а й у інших країнах з російськомовними медіа.

За словами Б. Кундерса, це тривожний сигнал і мета цього проекту – підтримати медіа, які б надавали незалежні новини, що не були б під контролем з боку російської влади.

Як повідомляється, реалізацією проекту займатиметься громадська організація Free Press Unlimited ***(Нідерланди фінансуватимуть незалежні російські ЗМІ для боротьби з пропагандою // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45352/118/lang,ru/). – 2015. – 19.11).***

***

Як у Чехії почали боротися з російською пропагандою

Гібридна війна в Україні привернула увагу не лише європейців, але й світу до політичного, медійного і соціального феномену, яким є інформаційна

війна Росії проти України і ширше – сучасна російська пропаганда, яка нині вже кинула виклик всьому демократичному світові, дієво впливаючи на формування громадської думки, на погляди людей, особливо молоді. Як виявити джерела пропаганди, як навчитись їй протистояти? Таку програму розробила і запроваджує в школах найбільша чеська гуманітарна організація «Людина у скруті». Про це пише radiosvoboda.org.

В Україні триває «громадянська війна», авторитетно заявляє президент Чехії М. Земан. Комуністи в чеському парламенті три чверті року закликали не ратифікувати угоду ЄС з Україною, бо в Україні «нелегітимна влада», а сама Україна є зоною інтересів Росії. Розгубленість панує і в суспільстві, яке не знає точно, чи в Києві до влади прийшли «бандерівці», чи проєвропейський уряд. Причину цієї розгубленості, на думку фахівців, слід шукати в інформаційній війні, що її проводить Росія на всіх фронтах, передусім по телебаченню, радіо і в пресі. За оцінками аналітиків, до 15 % чехів розглядають події у світі, у тому числі й агресію Росії в Україні, крізь російську інформаційну мережу.

Протягом останнього року особливо зросла кількість російських інформаційних джерел в Інтернеті, які чеською мовою поширюють російську інформаційну пропаганду. Це, на думку фахівців, – Aeronet чи Sputnik, які нав'язують російський погляд на ключові події у світі, насамперед ті, що стосуються війни в Україні.

Аналітик О. Кундра, який займається пошуком і вивченням першоджерел – інтернет-порталів, зокрема російських, розповідає, що у 10-мільйонній Чехії, далеко не найбільшій і не найвпливовішій країні ЄС, діють десятки проросійських ЗМІ.

«Залежить від того, як ви це розглядаєте. Я б сказав, що порталів є кілька десятків, але чи є їх 30, 35 чи 40 – ці цифри різняться, але, безумовно, що цих проросійських серверів є десятки. Серед них я б назвав сервер Parlamentní listy як одне з найбільш впливових джерел, де працюють дуже обдумано. Обдумано тому, що в них частина новин є правдивою і серйозною, але між ними виринає і російська пропаганда. Це становить ризик, тому що сервер Parlamentní listy має велику кількість читачів, а відтак ця інформація дістається до великої кількості людей і на них впливає. Саме в цьому бачу проблемний фактор», – зазначив О. Кундра.

Чеський користувач інформації, який за роки демократії звик до відповідальної журналістики, виявися не готовим до того, щоб йому під виглядом інформації подавали відверту брехню, каже чеський політолог, оглядач ділової газети «Господаржске новіни» О. Соукуп. На його думку, те, що колеги з відомої чеської гуманітарної організації «Людина у скруті» розпочали навчання інформаційної грамотності, є важливим кроком, щоб навчити чехів, передусім молодь, відрізняти дезу від об'єктивної інформації.

«Це цікава програма, тому що вона стосується не тільки російської пропаганди. Мета – навчити дітей сприймати і працювати із засобами масової інформації, з їх джерелами. Щодо російської пропаганди, то зараз її всі

згадують, на неї вказують і говорять про ці різні техніки маніпуляції», – каже О. Соукуп.

Чеська гуманітарна організація «Людина у скруті» підготувала 14 різноманітних освітніх програм, якими буде охоплено 600 чеських шкіл. На лекціях, які підготували чеські фахівці із засобів масової інформації, учнів учитимуть зіставляти правду з перекрученою чи недоговореною до кінця інформацією, планується також проведення зустрічей та бесід із журналістами – свідками подій.

Наприклад, цикл освітніх програм «Один світ у школах» включає демонстрацію російського пропагандистського фільму про окупацію Криму «Крим. Повернення на батьківщину». Після показу стрічки відбувається розмова про побачене, порівнюється реальний факт – захоплення Криму агресором із запереченням факту агресії Росією.

Керівник програми «Один світ у школах» К. Страхота вважає, що сьогодні найважливіше звернутися до шкіл, до молоді, на яку спрямована нинішня потужна хвиля російської інформаційної пропаганди. «Чеська Республіка, її громадяни, молоді люди опинились під інформаційним пропагандистським тиском. Ми хочемо навчити молодь підходити критично до цієї інформації, щоб вони знали, що повинні перевіряти джерела. Так, це є наша реакція на сьогодення. Ми сподіваємось на значний інтерес чеських шкіл до нашої програми», – пояснює К. Страхота.

Відомий чеський журналіст і дисидент Я. Урбан говорить, що сьогодні російська інформаційна пропаганда зовсім інша, вона набагато небезпечніша, ніж стара, радянська. «Нинішня пропаганда є більш осмисленою завдяки розвитку електронних засобів масової інформації, соціальних мереж. Адже тоді існувало тільки телебачення і радіо, не були потрібні тролі чи дезінформаційні хвилі, які сьогодні становлять базу для звернень Росії до світу. Це – нові явища, а тому ми всі зараз вчимося», – зауважує Я. Урбан.

І ще один крок, реалізований чеськими журналістами. Вони створюють портали, які збирають, аналізують та інформують чехів про російську інформаційну пропаганду в країні. Наприклад, вебсайт Hlídací pes – дослівно «Сторожовий пес» подає інформацію про російський вплив у різних сферах життя Чехії: від економіки до культури. Велика частина цього впливу є закулісною, тому найбільш дієвим шляхом його викриття є просто говорити правду, наголосила в розмові з Радіо Свобода чеська дисидентка П. Шустрова. «Єдине, що можемо робити з пропагандою, – будемо говорити правду про те, що діється, якою є реальна ситуація», – наголошує вона.

Проте зробити це через потужність цих впливів, які сягають вищих політичних ешелонів країни, буде нелегко. Саме тому чеські журналісти, громадські діячі та працівники недержавних організацій, сподіваються передусім на чеське громадянське суспільство та на суспільні ЗМІ ***(Як в Чехії почали боротися з російською пропагандою // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45329/118/lang,ru/). – 2015. – 18.11).***

***

СМИ: ИГИЛ уходит из Facebook и Twitter

После Арабской весны 2011 г. хлынул поток статей и научных исследований, посвященных новой роли социальных сетей, в частности Facebook и Twitter, в организации сопротивления авторитарным режимам.

Об этом пишет издание «Новое время», информирует «Обозреватель» (http://obozrevatel.com/abroad/69314-smi-igil-uhodit-iz-facebook-i-twitter.htm).

Террористы могут использовать те же платформы для общения и планирования, обходя американские сети, жестко цензурируемые и находящие под тщательным наблюдением.

ИГИЛ и подобные террористические группировки по-прежнему используют американские сети для пропаганды и вербовки, но более серьезную информацию перенесли на другие платформы – разработанный в России зашифрованный мессенджер Telegram и консоль Sony PlayStation 4.

После терактов в Париже соцсети принялись удалять восторженные твиты и угрозы от сторонников ИГИЛ, использовавших хэштег ?????_?????# (в переводе – «Париж в огне»). Теперь за про-игиловскими аккаунтами следят.

Это означает, что теперь сторонники экстремистов не смогут использовать американские соцсети полнофункционально. Один из них предложил создавать анонимные аккаунты, которые сложнее идентифицировать, как поддерживающие ИГИЛ, но свои могли бы распознать их по оговоренным хэштегам. Для масштабной работы, вероятно, потребуется серьезная координация, поэтому ИГИЛ, скорее всего, продолжит вещать свою пропаганду через Twitter, Facebook и YouTube, несмотря на их ненадежность.

А вот Telegram – надежный канал. Мессенджер, появившийся в 2013 г., так кодирует данные, что даже сотрудники не имеют доступа к частным сообщениям и групповым чатам, в которых могут участвовать до 200 человек. Кроме того, мессенджер может отправлять сообщения с функцией самоуничтожения.

Но парижские террористы при планировании операции могли пользоваться чатом PlayStation 4. За несколько дней до кровопролития в Бельгии заявили, что этот метод становится все популярнее, а отслеживать переговоры очень сложно. В отчетах указывалось, что при обыске дома в Бельгии, связанного с террористами, следователи нашли PlayStation 4. Ее использование для планирования атаки – гипотеза, но весьма правдоподобная.

У каждой из соцсетей есть собственная идеология – Facebook, например, нетерпим к нецензурной лексике, а Telegram ставит конфиденциальность превыше всего. Каждая из них связана с своей страной, хоть на первый взгляд они и кажется глобальной ***(СМИ: ИГИЛ уходит из Facebook и Twitter // Обозреватель (http://obozrevatel.com/abroad/69314-smi-igil-uhodit-iz-facebook-i-twitter.htm). – 2015. – 21.11).***

***

Священники Кіровоградської єпархії УПЦ Московського патріархату в соцмережах не приховують своїх антиукраїнських позицій

Дослідження постів попів у соцмережах зробила блогер В. Добронравова. Усе, що накопала, виклала у блозі «РК», передає Depo.Кіровоград.

Сторінки священників, які на публіці є аполітичними, просто кишать проросійськими постами.

Екс-священик Кафедрального собору Кіровограда В. Кашлюк (нині він перебрався на окупований півострів) вітає користувачів соцмережі з Днем народної єдності Росії і постить відео з В. Жириновським, де той захисників України називає катами.

Священникам УПЦ МП подобається, як «ластівка Путіна» обзиває бійців АТО катами.

Ще один священик з Високих Байраків О. Федотов у мережі «Одноклассники» має одного друга з Росії, Р. Коннова, який систематично розміщує антиукраїнську пропаганду і закликає допомагати «Новоросії». Також односельчани Федотова підтверджують, що їм вже давно відомо про його проросійські пристрасті. До прикладу, півтора року тому батюшка, виступаючи перед людьми, всіляко виправдовував російську агресію щодо України, за що люди його освистали.

Свою неоднозначну громадську позицію висловив і єпископ Олександрійський Боголеп на останніх громадських слуханнях з приводу перейменування Кіровограда, пропагуючи імперське назву «Єлисаветград» ***(Священникам УПЦ МП подобається, як «ластівка Путіна» обзиває бійців АТО катами // Depo.Кіровоград (http://kr.depo.ua/ukr/kr/kirovogradski-popi-v-sotsmerezhah-laykayut-prorosiyski-25112015132500). – 2015. – 25.11).***

***

Як розпізнати роботу ботів у соцмережах

Ви заходите в якийсь важливий пост – і ось що там бачите: всі між собою гризуться. І думаєте: та вони всі хворі. «В Раде же все на одно лицо!» Вуа-ля! Робота ботів виконана на відмінно, пише видання ТЕКСТИ.org.ua (http://texty.org.ua/pg/news/textynewseditor/read/63438/Kutepov_Jak_rozpiznaty_robotu_botiv_u_socmerezhah).

Огляд від журналіста Б. Кутєпова.

…За ними, фейковими акаунтами, стоїть лише пара десятків реальних людей, які отримують за свої послуги реальні гроші. Якщо ви підозрюєте, що «щось тут не так», не треба бути супер-розслідувальником, аби визначити: це бот чи реальна людина. Елементарно:

1. Ідентифікуйте потенційного бота по штампованих фразах, загальновживаних «мемах».

Боти часто не читають самого поста, вони лише отримують від своїх «старших» лінк на пост, який треба коментити, і набір меседжів, які треба переказати своїми словами.

2. Дослідіть сторінку бота.

Бот він чи ні – видно з кількох факторів. Коли він завів акаунт? Відтоді що він постив? Якщо хоч щось постив, крім власної обкладинки й аватарки, це успіх.

Але досліджуйте далі. Якщо це лише лінки, без коментарів від себе, якщо це не пости, а просто лінки на картинки і статті з підозрілих сайтів про криваву хунту, розбавлені демотиваторами, якщо ці всі лінки жодна людина не лайкнула, якщо в нього до 50 друзів – все це вкупі означає, що це точно бот. Кожна з цих.

3. Поговоріть з ботом.

Очевидно, що кілька акаунтів, якщо не кілька десятків, веде одна людина. Їй важко буде комунікувати.

4. Прогугліть аватарку бота.

Часто боти не обтяжують себе редагуванням і видозміною картинки. Вони просто крадуть її в Інтернеті, і знайти джерело легко, використовуючи в Google «Пошук за зображенням».

Водночас, майте на увазі, що не всі «зомбі», які повторюють політичні меседжі, ніби мантри, є ботами. Ідеології та організації з ознаками деструктивної секти, не потребує проплачених фейків. Їхні адепти готові зі скляними очима й піною на губах за власні ідеали задушити голими руками.

Це наслідок багаторічної ідеологічної роботи, підкріплений також значними фінансовими й іншими ресурсами.

Пильнуйте. Часто важливі для суспільства теми скочуються в соцмережах до масштабних дискусій, тільки тому, що нас із вами стравлюють між собою.

Часом інші дуже важливі теми армії ботів відволікають своїми коментарями. І думаєте: та вони всі хворі. «В Раде же все на одно лицо!» Вуаля! Робота ботів виконана на відмінно.

Не лінуйтесь копнути хоч трішечки глибше. Вами маніпулюють. Не будьте бездумною ватою ***(Кутєпов: Як розпізнати роботу ботів у соцмережах // ТЕКСТИ.org.ua (http://texty.org.ua/pg/news/textynewseditor/read/63438/Kutepov_Jak_rozpiznaty_robotu_botiv_u_socmerezhah). – 2015. – 27.11).***

***

Российские социальные сети заполнили мемы (картинки) с угрозами в адрес стран, которые Россия теперь считает своими врагами.

Картинки, которые изображают фашистами США, Украину и Турцию, практически вытеснили привычные для сетей изображения с котиками и смеющимися детьми. При этом за последнее время список «врагов» России увеличился. В списке уже давно были США, страны Евросоюза, Великобритания и Украина, теперь добавились сирийские повстанцы (умеренная оппозиция), ИГИЛ и Турция. Для каждого из государств подобраны свои уникальные оскорбления, хотя некоторые из них перекликаются. Так, например, американцы – обязательно тупые, все европейцы – геи и лесбиянки,

Украина и Турция – марионетки США, а вся сирийская оппозиция – террористы, как и ИГИЛ.

Но не так страшны эти гневные картинки, как количество людей, которые делятся ими с другими пользователями уже на своих страницах. Эти люди распространяют вирус ненависти сначала по сети, а позже переносят его на улицы. В жизни у таких россиян всё просто и понятно: В. Путин – национальный лидер, Россия – самая великая страна в мире и поэтому весь мир стремится её разрушить. Так же понятно для них то, что выступать против политики Путина может только агент гос.депа или национал-предатель. Исходя из этих фактов можно сделать вывод, что рейтинг власти будет оставаться таким же высоким до тех пор, пока большинство россиян будет думать, что весь мир – это враги России ***(Третья Мировая война уже идет в российских социальных сетях // Час Пик (http://vchaspik.ua/v-mire/356636tretya-mirovaya-voyna-uzhe-idet-v-rossiyskih-socialnyh-setyah). – 2015. – 27.11).***

Зарубіжні спецслужби і технології «соціального контролю»

Служба безопасности Украины (СБУ) поймала администратора пабликов в социальных сетях, которые агитировали за создание «Харьковской народной республики» и присоединение к России.

Аудитория этих страниц достигала 25 тыс. человек, утверждают в пресс-службе СБУ.

Во время обыска правоохранители нашли доказательства его причастности к распространению материалов с призывами к изменению границ территории Украины с нарушением порядка, установленного Конституцией Украины. На компьютере злоумышленника было установлено программное обеспечение, что позволяло осуществлять администрирование электронных страниц: размещать сообщения, создавать новые «ветки», блокировать отдельных пользователей.

Начато уголовное производство по ч. 2 ст. 110 (посягательство на территориальную целостность и неприкосновенность Украины) Уголовного кодекса Украины ***(СБУ поймала администратора ХНР-пабликов // InternetUA (http://internetua.com/sbu-poimala-administratora-hnr-pablikov). – 2015. – 18.11).***

***

Первый заместитель главы конституционного комитета Госдумы России А. Агеев попросил главу ФСБ А. Бортникова рассмотреть возможность ограничения доступа российских пользователей к мессенджеру Telegram.

По мнению депутата, боевики «Исламского государства», совершившие террористические атаки в Париже, для координаций действий пользовались именно приложением П. Дурова.

«По сообщениям, неоднократно появляющимся в российских СМИ, мессенджер Telegram активно используется в целях пропаганды террористами из “Исламского государства”. Можно предположить, что там же происходит процесс вербовки граждан России в ряды ИГ», – говорится в тексте обращения чиновника.

По мнению А. Агеева, бан Telegram не сможет ударить по свободе слова или нарушить иные права и свободы граждан.

«Предлагаю запретить слова. Есть информация, что с помощью них общаются террористы», – отреагировал П. Дуров на предложение чиновника.

Министр связи Н. Никифоров полагает, что предлагаемая депутатом мера не поможет в борьбе с терроризмом. По его словам, если запретить Telegram, то террористы просто воспользуются другими мессенджерами, поддерживающими аналогичную технологию шифрования. «Блокировать в России Telegram или другой мессенджер за то, что им пользуются террористы из ИГИЛ – это было бы так же разумно, как, например, запретить в России эксплуатацию автомобилей Toyota, так как они тоже оказались популярными у ИГИЛовцев», – сказал Н. Никифоров.

Предложение депутата Госдумы также раскритиковал и интернет-омбудсмен Д. Мариничев. «С таким же успехом можно определить, какими телефонами пользовались террористы, и запретить использовать такую модель телефона на конкретной территории», – сказал спикер ***(Российские спецслужбы хотят запретить Telegram // GoGetNews.info (http://www.gogetnews.info/news/techno/108521-rossiyskie-specsluzhby-hotyat-zapretit-telegram.html). – 2015. – 17.11).***

***

Из-за угрозы массовых протестов в Бангладеш заблокированы социальная сеть Facebook, а также мессенджеры WhatsApp и Viber, сообщил пакистанский телеканал Geo TV.

Население страны протестует из-за смертного приговора двум лидерам оппозиции, Али Мохаммаду Муджахиду и Салахуддину Кайдеру, которых обвиняют в зверствах во время войны 1971 г.

«Мы заблокировали работу соцсети Facebook, а также мессенджеров WhatsApp и Viber после того как получили распоряжение правительства», – сообщили в комиссии по телерадиовещанию ***(Протесты в Бангладеш: власти заблокировали Facebook, Viber и WhatsApp // InternetUA (http://internetua.com/protesti-v-bangladesh--vlasti-zablokirovali-Facebook--Viber-i-WhatsApp). – 2015. – 19.11).***

***

Профілі із соцмереж претендентів на посади в Національній поліції перевірятимуть. Про це радник міністра МВС А. Геращенко написав на своїй сторінці в соціальній мережі Facebook.

«У майбутньому при прийомі в Національну поліцію перевірятимуться сторінки претендентів у соціальних мережах на предмет їх громадянської позиції. Прохання до активних громадян допомагати Національній поліції в цьому питанні», – заявив А. Геращенко.

Раніше в мережі з'явилися фото записів у Twitter київського поліцейського О. Савкіна, де він негативно відгукувався про Євромайдан і писав, що потрібно «розігнати цих бомжів». У зв'язку з цими висловлюваннями його звільнили ***(МВС перевірить, що пишуть у соцмережах кандидати до поліції // InternetUA (http://internetua.com/mvs-perev-rit--sxo-pishut-u-socmerejah-kandidati-do-pol-c). – 2015. – 22.11).***

***

Украинским полицейским запретили иметь аккаунты в российских соцсетях. Об этом сообщил спикер МВД А. Шевченко в комментарии корреспонденту ЛІГА.net.

Распоряжение пока касается страниц в «Одноклассниках» и «ВКонтакте». Запрет не коснулся соцсетей Facebook и Twitter.

А. Шевченко добавил, что полицейским также запретили обсуждать в своих профилях информацию, связанную со служебной деятельностью.

Такие ограничения связаны с недавним скандалом вокруг полицейских и их оскорбительных публикаций против активистов Евромайдана.

Несколько дней назад губернатор Одесской области М. Саакашвили потребовал отстранить от работы нескольких одесских полицейских, которых уличили в размещении антиукраинских постов в соцсетях ***(Для полицейских ввели ограничения на общение в соцсетях // InternetUA (http://internetua.com/dlya-policeiskih-vveli-ogranicseniya-na-obsxenie-v-socsetyah). – 2015. – 25.11).***

***

Власти США заявили о намерении потребовать у компаний Apple, Google и Microsoft доступ к зашифрованной переписке пользователей их программ. Об этом сообщает The Wall Street Journal со ссылкой на информированные источники. Отмечается, что причиной такого решения стали террористические атаки в Париже.

Белый дом и члены Конгресса США в ходе переговоров с представителями компаний обсудят использование технологии сверхзащиты переписки и доступа к частной информации пользователей.

До сих пор компании не готовы были идти навстречу властям. В заявлении, в частности Google и Microsoft, отмечается, что «ослабление безопасности с целью достижения надежной защиты не имеет смысла». В Apple

отметили, что не готовы отказываться от кодирования, которое защищает триллионы онлайн-транзакций в день, поскольку этим могут воспользоваться злоумышленники. «Я не знаю, как защитить людей без шифрования», – заявил глава Apple Т. Кук.

Отмечается, что согласно французским СМИ, парижские террористы использовали обыкновенные текстовые сообщения, которые могут контролироваться полицейскими, если их отправитель или получатель – подозреваемый.

16 ноября, выступая во время онлайн-конференции Wall Street Journal, глава Пентагона Э. Картер заявил о необходимости мониторинга социальных сетей для борьбы с активностью террористической группировки «Исламское государство» (ИГ) в Интернете.

12 ноября, со ссылкой на информированные источники, СМИ сообщили, что ФБР заплатило миллион долларов за поиски технологии деанонимизации пользователей в зашифрованной сети Tor.

Премьер-министр Великобритании Д. Кэмерон в январе высказывался против мессенджеров, шифрующих переписку, однако эта инициатива не реализована на данный момент.

Технологии американских спецслужб по сбору и отслеживанию данных интернет-пользователей подверглись серьезной критике после массовых разоблачений бывшего сотрудника АНБ и ЦРУ Э. Сноудена.

В настоящее время АНБ имеет свободный доступ лишь к телефонным звонкам на территории США, после анализа которых вычисляются подозреваемые в терроризме американцы. Но с конца ноября, согласно ранее принятому Конгрессом закону, данные о телефонных переговорах можно будет получить у сотовых операторов только по решению суда ***(Власти США намерены получить доступ к перепискам пользователей Apple и Google // InternetUA (http://internetua.com/vlasti-ssha-namereni-polucsit-dostup-k-perepiskam-polzovatelei-Apple-i-Google). – 2015. – 21.11).***

***

За антиукраїнську пропаганду в соціальних мережах черкащанина притягнули до відповідальності. Про це УНН-Центр повідомили в прес-службі Черкаської ОДА.

Зловмисник розповсюджував в Інтернеті матеріали з публічними закликами до насильницької зміни конституційного ладу, громадської непокори, а також розміщував повідомлення, фото-, відеоматеріали, «репости» сепаратистського характеру, які містять заклики спрямовані на зміну державного кордону України. Суд призначив пропагандисту покарання у вигляді позбавлення волі на строк до чотирьох років з іспитовим терміном один рік.

Також набрав чинності вирок стосовно депутата Ватутінської міської ради, якого суд визнав винним у посяганні на територіальну цілісність і недоторканість України. Посадовець був активним учасником груп у

російських соціальних мережах, де поширював ідеї сепаратизму та пропагував насильницькі методи політичної боротьби. На сьогодні зловмисника засуджено до одного року позбавлення волі з іспитовим строком в один рік.

Упродовж року на Черкащині припинено функціонування більш ніж 140 інтернет-сайтів антиукраїнського спрямування, які адмініструвалися з тимчасово окупованих територій Донецької та Луганської областей ***(Пропагандистів сепаратизму засудили на Черкащині // УНН-Центр (http://region.unn.ua/uk/news/12689-propagandistiv-separatizmu-zasudili-na-cherkaschini). – 2015. – 20.11).***

***

В России проходят массовые забастовки дальнобойщиков, однако власти страны игнорируют протест людей и запрещают СМИ сообщать об этом.

Об этом пишет журнал «Їжачок» со ссылкой на сообщения пользователей в соцсетях. Новость передает «Пресса Украины».

«Из-за забастовки дальнобойщиков Первый канал РФ на своей странице банит за любую фотку грузовика. Доходит до абсурда: подписчиков банили за размещение картинок с изображением игрушечного грузовика или за скриншот из сериала “Дальнобойщики”...», – говорится в сообщении.

По словам россиян, темпы бана просто мгновенные – за 15 минут в «черный список» сбрасывают более 200 человек.

Такое демонстративное игнорирование прокремлевского канала к требованию людей быть услышанными еще раз показывает, насколько власти России интересуются улучшением жизни соотечественников ***(Россиян банят в соцсетях за картинки с грузовиками // NewsCloud (http://www.news-cloud.net/news/world/politics-world/12999-rossiyan-banyat-v-socsetyah-za-kartinki-s-gruzovikami-foto.html). – 2015. – 21.11).***

***

В «Одноклассниках» заблокировали аккаунт ТСН.ua. По мнению администрации российской соцсети, аккаунт ТСН.ua «распространяет идеи национализма», а его публикации «содержат публичные оскорбления представителей власти» и рекламу запрещенной в РФ экстремистской организации «Правый сектор».

Никаких объяснений относительно того, будет ли восстановлен аккаунт ТСН.ua и как долго продлится его блокировка, администрация не предоставила.

«К сожалению, все новости, которые не совпадают с кремлевской идеологией, считаются “Одноклассниками” “экстремистскими” и подлежат блокировке, – говорит главный редактор ТСН.ua К. Войтенко. – В случае с аккаунтом ТСН.ua, его просто удалили, не предоставив четких объяснений. Понятно, что эта сеть нацелена на российскую аудиторию, и в то же время она пользуется популярностью среди определенного процента украинцев. Подобные действия со стороны администрации сайта считаем

противоправными» ***(Аккаунт ТСН заблокировали в «Одноклассниках» // Медианяня (http://mediananny.com/novosti/2313447/). – 2015. – 24.11).***

***

Федеральная служба безопасности Российской Федерации блокирует украинский интернет-трафик в Донецке и Луганске, но на оккупированной части Донбасса есть трансляции некоторых каналов украинского телевидения и радио.

Об этом заявил министр информационной политики Украины Ю. Стець на заседании правительства.

Премьер-министр А. Яценюк обратился к министру с просьбой разработать план восстановления на территории Донецка и Луганска украинских интернет-ресурсов ***(ФСБ блокирует украинский интернет-трафик в Донецке и Луганске, – Стець // InternetUA (http://internetua.com/fsb-blokiruet-ukrainskii-internet-trafik-v-donecke-i-luganske----stec). – 2015. – 25.11).***

***

Жителям КНР, що використовують зарубіжні програми, слід готуватись до візиту в поліцейську дільницю.

Жителі Сіньцзяну в повній мірі відчули, що значить «жорстка цензура». Деяким з них почали відключати мобільний зв'язок за спроби скористатися «західними» мессенджерами й іншими програмами.

Про це повідомляє New York Times, посилаючись на кількох людей, які безпосередньо зіткнулися з проблемою. При відключенні зв'язку місцеві оператори направляли таке повідомлення: «У зв'язку з поліцейським повідомленням, ми відключимо ваш номер протягом двох годин, у відповідності з законодавством. Якщо у вас є які-небудь питання, прохання якомога швидше звернутися до відділу кіберзлочинів найближчого поліцейського відділку».

За словами мешканки Сіньцзяну (північно-західний регіон Китаю), у поліції їй сказали, що відключення зв'язку націлене на людей, що використовують VPN-сервіси, щоб обійти «Великий китайський фаєрвол» – фільтр інтернет-контенту, покликаний «захищати» громадян КНР від небажаної інформації. Ті, хто намагався завантажити іноземні месенджери, наприклад, WhatsApp, теж опинилися під прицілом.

За словами іншого учасника подій, він опинився у ділянці за те, що використовував VPN-сервіси для доступу в Instagram. Поліція вилучила у нього телефон, але повернула його за декілька хвилин. Від мобільного зв'язку його відключили на три дні. У підсумку він сказав NYT, що відмовляється від Instagram, тому що користуватися цією соціальною мережею надто проблематично.

Іншим пощастило менше, оскільки їм навіть не повідомили, на який термін відключили зв'язок. Скільки людей у Сіньцзяні зіткнулися з цією проблемою, невідомо. Один зі співрозмовників видання сказав, що після

прибуття до відділку міста Урумчі побачив чергу з 20 осіб, які потребували відновлення зв'язку.

Пекін витратив значну суму на створення системи інтернет-цензури, але лазівки в ній все ж залишилися. Заморожування мобільних номерів у спробі прикрити ці лазівки свідчить про те, що китайська влада вийшла на новий рівень пильності ***(Китайцям почали відключати телефони за користування WhatsApp і Instagram // Новое время (http://nv.ua/ukr/techno/gadgets/kitajtsjam-pochali-vidkljuchati-telefoni-za-koristuvannja-whatsapp-i-instagram-82357.html). – 2015. – 26.11).***

***

В этом году по Украине прокатилась волна обысков в IT-компаниях. Но сейчас под угрозой оказался сам головной офис Facebook. Еще 18 ноября Печерский суд Киева обязал администрацию социальной сети предоставить доступ к штаб-квартирам в Менло-Парке и Лондоне. Соответствующее решение опубликовано в реестре, пишет AIN.UA (http://ain.ua/2015/11/27/618239).

В документе речь идет об уголовном расследовании дела по ч. 2 ст. 115 (умышленное убийство, совершенное группой лиц). Следователям в ходе расследования нужно получить доступ к данным некоего Facebook-аккаунта, уже удаленного из сети. В самом этом факте, конечно, нет вообще ничего смешного, обычная работа следственных органов. Но дальше в решении суда начинается очевидное и невероятное.

Администрацию Facebook обязывают предоставить доступ к вещам и документам, которые находятся у администрации сети по адресам Facebook Inc. 10 Brock Street, NW1 3FG London, United Kindom и 1601 Willow Road Menlo Park, CA 94025 United States. А в случае, если администрация сети откажется предоставить физический доступ к документам, которые требуют следователи, суд может решить провести обыск в Facebook, чтобы эти документы и вещи изъять.

Если под вещами понимать, к примеру, серверы с пользовательскими данными, то давний фейк о том, что Facebook закрывается, может стать ужасной явью. Очень надеемся, что Facebook успеет сделать резервную копию до того, как к нему придут с обыском ***(Украинский суд обязал Facebook предоставить следователям доступ к офису с правом изъятия документов // AIN.UA (http://ain.ua/2015/11/27/618239). – 2015. – 27.11).***

***

Агентство национальной безопасности (АНБ) США прекратит программу по сбору данных о телефонных коммуникациях американцев 29 ноября. Об этом сообщил 27 ноября официальный представитель Совета национальной безопасности (СНБ) при Белом доме Н. Прайс, передает ТАСС.

Он отметил, что «согласно законодательству, АНБ закончит свою масштабную программу наблюдения в 23:59 28 ноября, в субботу».

В Белом доме указали, что собранные за последние пять лет данные будут храниться до 29 февраля 2016 г.

Все записи уничтожат, как только будет вынесено соответствующее решение специального американского суда по надзору за деятельностью иностранных разведок ***(АНБ прекратит электронную слежку за американцами 29 ноября // InternetUA (http://internetua.com/anb-prekratit-elektronnuua-slejku-za-amerikancami-29-noyabrya). – 2015. – 28.11).***

Проблема захисту даних. DDOS та вірусні атаки

Міжнародна хакерська група Anonymous оголосила війну «Ісламській державі» після масштабних терористичних атак у Парижі

Про це повідомляє Еспресо.TV із посиланням на Newsweek.

«Війну оголошено. Готуйтеся», – говорить фігура в масці у відеопосланні французькою мовою. Авторами двохвилинного ролику на YouTube є хакерська група Anonymous.

«Французький народ сильнійший за вас і вийде із цього звірства навіть сильнішим. Anonymous із усього світу будуть за вами полювати. Вам слід знати, що ми вас знайдемо і не відпустимо. Ми запустимо найбільшу операцію проти вас», – зазначається в погрозі.

Хакери заявляють, що використовуватимуть свої кібернетичні навички для «об'єднання людства» і що терористи мають готуватися до «масштабних кібератак».

У Twitter хакери також заявили: «Anonymous оголошує війну Daesh (інша назва для «Ісламської держави». – Ред.). Ми не перестанемо протистояти «Ісламській державі». А ще ми кращі хакери» ***(Хакери оголосили «найбільшу операцію» проти «ІД» після теракту в Парижі // Espreso.tv (http://espreso.tv/news/2015/11/16/khakery_ogolosyly_quotnaybilshu_operaciyuquot_proty_id_pislya_teraktu_v_paryzhi). – 2015. – 16.11).***

***

В рамках операции против террористической группировки «Исламское государство Ирана и Леванта», хакерская группа Anonymous рассекретила более 5500 тыс. Twitter-аккаунтов боевиков, сообщается на странице группы в Twitter.

В сообщении хакеров говориться, что с их помощью администрация соцсети заблокировала уже более 5500 тыс. аккаунтов, поддерживающих ИГ и занимающихся вербовкой в сети ***(Anonymous раскрыла более 5,5 тысяч аккаунтов боевиков иг в Twitter // IGate (http://igate.com.ua/lenta/11418-anonymous-raskryla-bolee-55-tysyach-akkauntov-boevikov-ig-v-twitter). – 2015. – 17.11).***

***

В Интернете появились менее крупные группы хакеров, избравшие для борьбы с ИГ другую стратегию, которая, по их утверждению, уже позволила предотвратить по меньшей мере один теракт.

Группа, о которой идёт речь, говорит, что сыта по горло «бесхитростной», по её мнению, тактикой Anonymous. После террористического акта в редакции Charlie Hebdo в январе основатели хакерской группы Ghost Security Group решили порвать с Anonymous.

«Они [Anonymous] вообще не имеют никакого опыта борьбы с терроризмом, – сообщил в телефонном интервью каналу BBC Trending руководитель антитеррористической хакерской группы Ghost Security Group (прежнее название – Ghost Security). – Мы чувствовали, что делалось недостаточно, и после нападения Charlie Hebdo стало ясно, что ИГ не ограничится Ближним Востоком».

В группу Ghost Security Group входят добровольцы из США, Европы и Ближнего Востока, включая лингвистов и «людей, знакомых с методами сбора разведданных». Вместо попыток закрыть аккаунты сторонников террористов и обрушить их сайты с помощью DDoS-атак, участники Ghost Security Group действуют больше как шпионы, чем хакеры. Они отслеживают подозрительные аккаунты в Twitter, проверяют доски объявлений сторонников ИГ в поисках информации о планах боевиков, чтобы передать её органам правопорядка. Очень часто твиты удаляются спустя короткое время после публикации, поэтому нужно быть начеку.

«Мы бы предпочли предотвращать атаки, чем закрывать сайты, – сказал координатор хакерской группы. – Не думаю, что DDoS-атаки наносят большой урон ИГ» ***(Хакеры: «Лучше шпионить за террористами, чем атаковать сайты» // InternetUA (http://internetua.com/hakeri---lucsshe-shpionit-za-terroristami--csem-atakovat-saiti). – 2015. – 24.11).***

***

Хакеры нашли новый способ взлома мобильных Android-устройств и получения удаленного контроля над ними. Этот метод действует даже в том случае, если на гаджете установлена самая свежая версия ОС.

Китайский исследователь Г. Гун обнаружил критическую уязвимость в последней версии браузера Chrome для Android, которая позволяет атакующему получить доступ с правами администратора на смартфоне жертвы. Созданный хакером эксплоит работает для всех версий мобильной платформы Google.

В рамках конкурса MobilePwn2Own на конференции PacSec 2015 в Токио эксперт продемонстрировал пример атаки на основе созданного им эксплоита. Программа эксплуатирует уязвимость в движке JavaScript V8, который предустановлен практически на всех современных Android-смартфонах. Для того чтобы взломать устройство, злоумышленнику необходимо всего лишь заманить жертву на веб-ресурс, который содержит вредоносный код.

В то время как ничего не подозревающий пользователь просматривает сайт, атакующие могут проэксплуатировать брешь в Chrome, загрузить вредоносное приложение и удаленно получить контроль над гаджетом.

Эксперт сообщил об уязвимости команде безопасности Google, но не стал публично раскрывать все детали атаки, пишет Securitylab. На создание эксплоита исследователь потратил три месяца ***(В Chrome найдена уязвимость, позволяющая взломать любое устройство на Android // IGate (http://igate.com.ua/lenta/11397-v-chrome-najdena-uyazvimost-pozvolyayushhaya-vzlomat-lyuboe-ustrojstvo-na-android). – 2015. – 16.11).***

***

Вирусные угрозы в III квартале 2015 года

В III квартале 2015 г. украинских пользователей ПК чаще всего атаковали трояны и программы, демонстрирующие рекламу – adware. Но лидером рейтинга в Украине стал adware, пишет UBR.UA (http://ubr.ua/ukraine-and-world/technology/virusnye-ugrozy-v-iii-kvartal-2015-goda-ukraincev-atakuut-adware-i-troiany-366301).

Эпидемия adware

В Украине набирает обороты эпидемия adware. Более половины всех атак – 51% – вредоносного ПО в III квартале 2015 г. в Украине, осуществлено вредоносными программами, которые показывали пользователям рекламные баннера, подменяли поисковую выдачу, мешали комфортно просматривать сайты.

Активность этого вида вредоносного ПО, в сравнении с аналогичным периодом 2014 г., возросла на 17 % от общего числа выявленных угроз.

При этом в среднем на каждом атакованном ПК заражалось 20 файлов, которые распознавались антивирусными программами, как источники вредоносных данных. Специалисты антивирусной лаборатории Zillya! отмечают, что этот факт еще раз подтверждает, что борьба с adware должна базироваться на комплексном подходе лечения ПК. Удалив один найденный зараженный файл, как правило, проблему не решить.

Троянцы: шифруют и воруют

Второе место по активности за III квартал 2015 г. заняли троянские программы разнообразных модификаций. Наиболее активными оказались банковские троянцы, созданные для кражи личной информации доступа до банковских счетов.

Отметился данный период и резким ростом выявления трояновшифровальщиков, ориентированных на бухгалтерский сектор предприятий. Злоумышленники используют методы социальной инженерии, которые позволяют убедить пользователя запустить зараженную программу или открыть файл, тем самым заразив свой ПК «вирусом», который зашифрует на нем все файлы.

19 % всех атак на персональные ПК украинских пользователей осуществлялись с помощью программ данного типа. Стоит отметить, что эти

данные свидетельствуют о некотором снижении активности в Украине троянских программ (в III квартале 2014 г. – 33 % от всех угроз) в общей массе вирусных угроз.

Самые распространенные

Наиболее активными за III квартал 2015 г. были ниже представленные семейства вредоносного программного обеспечения. Следует отметить, что некоторые из них начали использоваться в разы больше при том, что за аналогичный период 2014 г. их «популярность» была близка к нулевой.

Adware.Agent.Win32 – большое семейство рекламного вредоносного ПО, которое устанавливается на компьютер втайне от пользователя и проявляет свою активность в виде навязчивых всплывающих окон с рекламой или подменой результатов поиска.

Adware.Eorezo.Win32 – данные приложения обладают скрытым функционалом, таким, как показ всплывающей рекламы, открытие дополнительных окон в браузере и перенаправление пользователя на рекламные сайты, и сайты с вредоносным программным обеспечением. Также, втайне от пользователя, на компьютер загружаются другие рекламные модули.

Adware.CrossRider.Win32 – семейство кросплатформенного рекламного ПО. В основном Adware.Crossrider используется для черного SEO, то есть для раскрутки или повышения рейтинга сайта, за счет перенаправления на него пользователей заразившихся Adware.Crossrider .

Adware.ConvertAd.Win32 – навязчивое рекламное программное обеспечение. При просмотре веб-страниц показывает квадратные всплывающие окна с рекламой. Кроме того на страницах могут появляться баннеры с рекламой, а ссылки подменяются на рекламные. Кроме того на компьютер пользователя будут загружаться другие программы рекламного характера.

Trojan.Black.Win32 – семейство вредоносных программ упакованных протектором Themida. Протектором может быть упакованная любая троянская программа ***(Вирусные угрозы в III квартал 2015 года: украинцев атакуют Adware и трояны // UBR.UA (http://ubr.ua/ukraine-and-world/technology/virusnye-ugrozy-v-iii-kvartal-2015-goda-ukraincev-atakuut-adware-i-troiany-366301). – 2015. – 18.11).***

***

ИБ-исследователи из Proofpoint опубликовали информацию о вредоносном ПО, детектированном экспертами как AbaddonPOS, целью которого являются PoS-терминалы. Специалисты выявили вредонос Vawtrak, загружающий TinyLoader, загрузчик, который использовал собственный протокол для передачи полезной нагрузки с C&C-сервера. Затем TinyLoader загружал другой загрузчик в виде шелл-кода, который, в свою очередь, инфицировал систему вредоносным ПО AbaddonPOS.

Специалисты пояснили, что набор эксплоитов Angler или инфицированный документ Microsoft Office могут поставлять вредоносные программы, используя сложные методы обхода систем безопасности.

AbaddonPOS считывает все процессы в поисках данных кредитных карт. Как только вредонос обнаруживает искомые данные, они отправляются на C&C-сервер с помощью реализованного двоичного протокола.

Напомним, на прошлой неделе стало известно о том, что исследователи из Trustwave выявили вредоносное ПО для PoS-терминалов, которое оставалось необнаруженным по крайней мере в течение четырех лет. Вредонос, который исследователи назвали Cherry Picker, обходил обнаружение благодаря сложной технике.

По словам экспертов, вредоносное ПО для PoS-терминалов – весьма распространенное явление в США в последние несколько лет. Тем не менее, внедрение технологии EMV может способствовать защите кредитных карт от AbaddonPOS, Cherry Picker и других PoS-вредоносов ***(Эксперты обнаружили очередной вредонос для PoS-терминалов // InternetUA (http://internetua.com/eksperti-obnarujili-ocserednoi-vredonos-dlya-PoS-terminalov). – 2015. – 18.11).***

***

Независимый исследователь B. Амин и главный архитектор лаборатории Elastica Cloud Threat Labs A. Суд обнаружили брешь в «умных» коммутаторах серии DGS-1210 Gigabit Smart Switches производства D-Link. Эксплуатация бреши позволяет атакующему получить удаленный неавторизованный доступ к файлам регистрации и конфигурации на сервере или в флеш-памяти устройства.

Как пояснили эксперты в беседе с журналистами издания SecurityWeek, конфигурация коммутаторов такого типа позволяет хранить резервные копии файлов, в том числе журналы, файлы прошивки и конфигурационные файлы на веб-сервере или в флеш-памяти устройства. Проблема заключается в том, что в коммутаторах не реализованы надлежащие процедуры авторизации и аутентификации, что позволяет злоумышленнику получить доступ к резервным данным и корневой папке сервера, просто имея в наличии IP-адрес целевого устройства.

Получив доступ, атакующий может просмотреть и похитить всю информацию об устройстве, в том числе данные о настройках, имя пользователя и т. д. К примеру, для того, чтобы узнать детали конфигурации, достаточно загрузить ее на другой коммутатор, приобретенный на рынке. По словам исследователей, файлы журналов содержат в себе информацию о клиентах с доступом к устройству, а также другие данные, связанные с инфраструктурой. Компрометация сетевых коммутаторов может иметь серьезные последствия в связи с тем, что у злоумышленника есть возможность получить контроль над трафиком, предупреждают B. Амин и A. Суд.

В настоящее время исправление безопасности недоступно, несмотря на то что специалисты проинформировали D-Link об обнаруженной ими уязвимости еще в начале октября текущего года ***(В коммутаторах D-Link DGS-1210***

обнаружена уязвимость // InternetUA (http://internetua.com/v-kommutatorah-D-Link-DGS-1210-obnarujena-uyazvimost). – 2015. – 18.11).

***

Системы управления контентом в три раза чаще подвергаются кибератакам по сравнению с другими веб-приложениями. Особо остро проблема касается популярной платформы WordPress, говорится в докладе ИБ-компании Imperva.

По данным специалистов, CMS наиболее уязвимы к атакам, в которых используются техники удаленного выполнения команд и удаленного включения произвольных файлов.

«Данные фреймворки в основном представляют собой ПО с открытым исходным кодом, что позволяет разработчикам регулярно создавать дополнительные плагины, не обращая внимания на безопасность. Такая модель разработки приводит к росту числа брешей в CMS-приложениях. Особенно, если речь идет о WordPress, которая, помимо прочего, еще и создана на базе PHP», – отмечается в отчете Imperva.

Что касается приложений, разработанных для сферы здравоохранения, в основном они подвержены XSS-уязвимостям, которые эксплуатируются в 57 % атак. По словам специалистов, XSS-атаки являются одним из наиболее распространенных способов хищения персональной информации пользователей медицинских приложений.

Отмечается, что различные программы уязвимы к разным типам атак. К примеру, туристические, развлекательные и финансовые сервисы чаще всего подвергаются атакам удаленного включения файлов. IT-сфера и приложения для online-шопинга уязвимы к атакам по HTTP, а гостинично-ресторанный сектор – к атакам типа «Обратный путь в директориях» ***(Сайты на базе WordPress атакуют чаще всего // InternetUA (http://internetua.com/saiti-na-baze-WordPress-atakuuat-csasxe-vsego). – 2015. – 18.11).***

***

Министр финансов Великобритании Д. Осборн опасается, что террористы в настоящее время могут готовить кибератаки на инфраструктуру городов, больницы, электрические сети и системы контроля воздушного трафика. А потому стране необходимо усилить защиту киберпространства и создать «элитные наступательные кибервойска».

Поэтому расходы на эти нужды будут удвоены и составят 2,9 млрд дол. до 2020 г. Финансирование распределят между Центром правительственной связи и британскими военными. Кибервойска займутся отдельными хакерами, группами преступников и боевиков, враждебными странами, сообщает Gizmodo ***(Элитные кибервойска Британии вступят в борьбу с «Исламским государством» // InternetUA (http://internetua.com/elitnie-kibervoiska-britanii-vstupyat-v-borbu-s--islamskim-gosudarstvom). – 2015. – 19.11).***

***

«Лаборатория Касперского» опубликовала результаты исследования, в ходе которого изучалось поведение детей в Интернете и отношение их родителей к обеспечению информационной безопасности.

Сообщается, что половина взрослых – 53 % – обеспокоена тем, что их ребенок может увидеть в сети нежелательный контент. Причем каждый 10-й родитель уверен в том, что это уже произошло.

Кроме того, взрослых волнует вопрос общения детей с опасными незнакомцами: на эту проблему указали 44 % родителей. Такие собеседники могут оскорблять ребенка, выманивать у него конфиденциальную информацию, предлагать реальные встречи.

В то же время именно средства интернет-коммуникаций (социальные сети, веб-почта и чаты) являются самой распространенной детской активностью в сети – результат 77 %. Также дети заходят в Интернет ради компьютерных игр (11 %) и для оплаты покупок в интернет-магазинах или платежных системах (4 %). В меньшей степени среди малолетних пользователей популярны другие активности, такие как поиск пиратских программ, видео, музыки, принципов работы блокирующих программ, поставленных родителями, и способов их обхода и пр.

Исследование также показало, что, несмотря на большое количество рисков, каждый пятый взрослый не предпринимает никаких защитных мер, чтобы оградить своего ребенка от сетевых угроз. Только 22 % респондентов сообщили, что установили средства родительского контроля ***(Большинство родителей обеспокоены доступностью нежелательного контента для их детей // IGate (http://igate.com.ua/lenta/11489-bolshinstvo-roditelej-obespokoeny-dostupnostyu-nezhelatelnogo-kontenta-dlya-ih-detej). – 2015. – 20.11).***

***

Независимый исследователь безопасности из Бразилии Б. Родригес обнаружил бэкдор в кабельных модемах Arris. Компания уже проинформирована о проблеме и сейчас работает над устранением уязвимости. По словам эксперта, устройства легко обнаружить при помощи поисковой системы Shodan, таким образом ему удалось отследить более 600 тыс. уязвимых устройств.

Отмечается, что модемы Arris класса SOHO (предназначенные для применения в небольших и домашних офисах) содержат незадокументированную библиотеку libarris_password.so, функционирующую в качестве бэкдора, который позволяет получить удаленный доступ к устройству привилегированным пользователям с кастомными паролями.

Впервые о проблеме в модемах ARRIS стало известно в 2009 г. Тогда был обнаружен бэкдор, который позволял удаленно получить доступ к девайсам при помощи сгенерированного пароля администратора.

В этом случае Б. Родригес обнаружил похожий бэкдор, затрагивающий скрытую административную оболочку, реализованную в модемах Arris. Так

называемый «ежедневный пароль ARRIS» (ARRIS password of the day) представлет собой удаленный бэкдор, который для генерации пароля использует канал, зашифрованный с помощью алгоритма DES. Как выяснил эксперт, пароль основан на последних пяти цифрах серийного номера модема.

По просьбе производителя исследователь не раскрыл всех подробностей об уязвимости, но опубликовал PoC-видео с примером атаки. В настоящее время не известно о случаях эксплуатации данной бреши ***(В 600 тыс. кабельных модемах Arris обнаружен бэкдор // InternetUA (http://internetua.com/v-600-tis--kabelnih-modemah-Arris-obnarujen-bekdor). – 2015. – 22.11).***

***

ИБ-исследователи из Heimdal Security обнаружили, что новая модификация банковского трояна Dyreza теперь направлена на устройства на базе Windows 10 и браузер Microsoft Edge. Вредонос собирает личные данные пользователя, а затем отправляет их на свои серверы.

Dyreza или Dyre «убивает» серию процессов, связанных с системой безопасности для того, чтобы быстрее проникнуть в систему и увеличить свою производительность. Стоящие за вредоносом злоумышленники используют спам-кампанию, известную под названием spray & pray, в которой Dyreza отправляется случайным жертвам.

Новый вариант Dyreza не только инфицирует компьютеры с целью хищения финансовой информации, вредонос также объединяет зараженные машины в ботнет. Согласно данным ИБ-исследователей, в настоящее время Dyreza успел инфицировать 80 тыс. компьютеров. Вредонос может внедрять код в такие браузерные процессы, как chrome.exe, chromium.exe», «firefox.exe, iexplore.exe и microsoft edge.

В числе уязвимых для Dyreza продуктов оказались Windows 7, 7 SP1, XP, 8, 8.1, Server 2003, Vista SP2, Vista, Vista SP1 и 10 IP. Новый штамм вредоноса получил модуль «aa32», предназначенный для 32-битных систем, или «aa64» – для 64-битных. Модуль внедряет себя в процесс spoolsv.exe для того, чтобы постоянно прерывать связанные с безопасностью процессы. Чаще всего Dyreza инфицирует системы с помощью загрузчика Upatre.

Эксперты считают, что новая модификация Dyreza активизировалась в настоящее время в связи с грядущими праздниками и «Черной пятницей» для того, чтобы собрать максимальное число конфиденциальных данных ***(Банковский троян атакует Windows 10 и Microsoft Edge // InternetUA (http://internetua.com/bankovskii-troyan-atakuet-Windows-10-i-Microsoft-Edge). – 2015. – 22.11).***

***

Ранее в этом году ряд крупных ИБ-компаний опубликовали отчеты о хакерской группе, известной под такими именами, как APT28, Sofacy, Fancy Bear, Sednit или Operation Pawn Storm, которая предположительно связана с

российским правительством. Согласно недавнему отчету Microsoft, Pawn Storm не единственная крупная APT-группа в киберпространстве. Техногигант выявил вредоносную деятельность еще одного предприятия, которое получило название Strontium.

Расследование Microsoft показало, что Strontium впервые проявила себя еще в 2007 г. Жертвами хакеров стали государственные органы, военные организации, в особенности НАТО, дипломаты, журналисты и политические деятели. Ранее в этом году специалисты выяснили, что APT-группа осуществляет фишинг-кампании, ориентированные на пользователей продуктов от Microsoft, с целью хищения их учетных данных Outlook. Strontium отправляет фишинг-письма перед запланированными техногигантом важными конференциями, а также распространяет вредоносные ссылки через соцсети.

Согласно отчету Microsoft, жертвами этих злоумышленников становятся небольшие группы людей, все атаки являются целевыми, поэтому эксперты предполагают, что Strontium спонсируется государством. В своих кампаниях хакеры эксплуатируют уязвимости нулевого дня в таких продуктах, как Flash, Java, Microsoft Word и Internet Explorer ***(Microsoft предупреждает о крайне опасной APT-группе // InternetUA (http://internetua.com/Microsoft-preduprejdaet-o-kraine-opasnoi-APT-gruppe). – 2015. – 22.11).***

***

Согласно данным ИБ-исследователей из Malwarebytes, злоумышленники снова начали использовать набор эксплоитов Blackhole. К слову, прошло почти два года с последнего известного инцидента, связанного с Blackhole. Этот набор эксплоитов был очень популярен в свое время – около 75–80 % всех киберугроз были связаны с Blackhole. Однако все изменилось после ареста его создателя.

Напомним, набор эксплоитов BlackHole предназначен для эксплуатации уязвимостей в программном обеспечении, которое доступно в Интернете через плагины браузера – Java, Adobe Reader и Flash Player. Разработчик Blackhole, который в сети использовал псевдоним Paunch, был арестован в России. Набор эксплоитов предположительно был продан или арендован другими киберпреступниками для создания хакерских инструментов.

В недавнем происшествии, связанном с Blackhole, злоумышленник допустил серьезную ошибку – оставил сервер, на котором была размещена вся инфраструктура набора эксплоита, открытым в Интернете. Именно так Malwarebytes удалось выяснить, что Blackhole снова используется. Эксперты не совсем понимают тактику хакеров, так как этот набор эксплоитов считается устаревшим, поэтому размер и число кибератак будут незначительными ***(Хакеры снова используют набор эксплоитов Blackhole // InternetUA (http://internetua.com/hakeri-snova-ispolzuuat-nabor-eksploitov-Blackhole). – 2015. – 21.11).***

***

Компания «Доктор Веб» исследовала троян-шифровальщик для ОС Linux Linux.Encoder.2. Об этом CNews сообщили в «Доктор Веб».

Несмотря на то что данная вредоносная программа была добавлена в вирусные базы Dr.Web под вторым номером, исторически она появилась раньше, однако в течение длительного времени не попадала в поле зрения аналитиков антивирусных компаний. Более того, недавно одна из компаний-разработчиков антивирусного ПО опубликовала исследование другого трояна, названного ею Linux.Encoder.0. Предположительно, он является самым первым в этой группе шифровальщиков, Linux.Encoder.2 начал распространяться чуть позже, в сентябре – октябре 2015 г., а уже затем появился Linux.Encoder.1.

По информации «Доктор Веб», модификацию Linux.Encoder.2 от Linux.Encoder.1 отличает то, что она использует другой генератор псевдослучайных чисел, для шифрования применяет библиотеку OpenSSL (а не PolarSSL, как в Linux.Encoder.1). Шифрование троян осуществляет в режиме AES-OFB-128, при этом происходит повторная инициализация контекста каждые 128 байт, то есть через 8 блоков AES. Также в Linux.Encoder.2 имеется ряд других существенных отличий от альтернативной реализации этого энкодера.

Как указали в компании, все известные на сегодняшний день утилиты, предназначенные для расшифровки файлов, не удаляют внедренный злоумышленниками на инфицированный сервер шелл-скрипт, которым впоследствии могут воспользоваться киберпреступники для повторного заражения системы. Поэтому специалисты службы технической поддержки «Доктор Веб» помогают всем обратившимся за помощью в расшифровке файлов пользователям очистить систему от посторонних вредоносных объектов и обезопасить ее от возможных атак с использованием этого скрипта в будущем.

Сигнатура Linux.Encoder.2 добавлена в вирусные базы «Антивируса Dr.Web для Linux». Специалисты «Доктор Веб» разработали методику расшифровки файлов, поврежденных в результате действия этой вредоносной программы. Услуги по расшифровке файлов оказываются только обладателям коммерческих лицензий на антивирусные продукты Dr.Web. Компания при этом не дает полной гарантии расшифровки всех поврежденных в результате действия энкодера файлов ***(Обнаружен очередной троян-шифровальщик для Linux // InternetUA (http://internetua.com/obnarujen-ocserednoi-troyan-shifrovalsxik-dlya-Linux). – 2015. – 21.11).***

***

В четверг, 19 ноября, «Фонд электронных рубежей» (Electronic Frontier Foundation, EFF) совместно с Visualizing Impact запустил проект Onlinecensorship.org. Проект представляет собой платформу, на которой будет публиковаться информация о материалах, подвергшихся цензуре в социальных сетях – что было заблокировано, кем и почему. По мнению EFF, проект

поможет определить, по каким принципам осуществляется модерация пользовательского контента в социальных медиа, и где нарушается право на свободу слова.

На Onlinecensorship.org пользователи смогут самостоятельно сообщать об удалении своего контента из Facebook, Google+, Twitter, Instagram, Flickr и YouTube. Эта информация будет каталогизироваться и анализироваться с целью обнаружения тенденций в удалении пользовательских материалов и выявлении, как это влияет на определенные группы людей.

«Мы хотим знать, как социальные медиа соблюдают свои условия использования. Собранные нами данные помогут повысить осведомленность общественности о том, как эти компании регулируют свободу слова, – сообщила соучредитель проекта Д. Йорк. – Мы надеемся, что компании отреагируют на это, усовершенствовав свои правила и сообщив об используемых ими механизмах и процессах» ***(Новый проект EFF позволит пользователям сообщать о цензуре в соцсетях // InternetUA (http://internetua.com/novii-proekt-EFF-pozvolit-polzovatelyam-soobsxat-o-cenzure-v-socsetyah). – 2015. – 21.11).***

***

Кибератаки стали оказывать влияние на реальную жизнь людей и организаций

Развитие сетевого взаимодействия и появление большого числа потенциально уязвимых устройств с неизбежностью привело к тому моменту, когда кибератаки стали оказывать влияние на реальный мир. Такой вывод содержится в отчете по информационной безопасности за III квартал 2015 г. Hazards Ahead: Current Vulnerabilities Prelude Impending Attacks, представленном компанией Trend Micro, мировым разработчиком решений для информационной безопасности. В отчете показано, что прорехи в информационной безопасности и лазейки в мобильных платформах, а также использующие эти уязвимости вредоносные программы подвергают риску уже не только конфиденциальную информацию, но и физическую безопасность, сообщили CNews в Trend Micro. Кроме того, такие пробелы в безопасности подготавливают потенциальную почву для более масштабных событий, которые, по мнению компании, могут произойти в 2016 г.

«Эволюция кибератак уже подошла к тому этапу, когда они стали оказывать влияние на реальную жизнь людей и организаций, – отметил Р. Гинес, CTO, Trend Micro. – Большое число уязвимостей в программном обеспечении и нарушения в защите данных, которые были выявлены в этом квартале, подвергали риску утечки весьма конфиденциальную и потенциально опасную информацию, которая могла бы быть потом продана в Deep Web».

Масштабные утечки данных этого квартала, такие как инцидент с Ashley Madison, спровоцировали целую серию атак с последующей публикацией конфиденциальной информации в публичное пространство и вызвали последствия гораздо более серьезные, чем просто сбой в работе сервиса.

Киберпреступники использовали украденную информацию для вымогательства и шантажа, что стало настоящей катастрофой как для владельца сайта знакомств компании Avid Life Media, так и для более чем 30 миллионов его пользователей. Сообщалось даже о случаях суицида среди пострадавших из-за последствий, которые оказала эта атака на их личную жизнь.

Большое количество инцидентов в этом квартале произошло в организациях здравоохранения, включая атаку на больничную сеть Калифорнийского университета (UCLA Health) в Лос-Анджелесе. В результате атаки были скомпрометированы данные о 4,5 млн пациентах UCLA Health. По информации Trend Micro, личная или медицинская информация о пациенте оказалась на втором месте по «популярности» среди утечек данных различных категорий. Этот случай является наглядным примером того, почему отрасль здравоохранения остается привлекательной целью для киберпреступников.

Злоумышленники продолжают проявлять интерес к пользователям мобильных устройств, используя уязвимости в платформах iOS и Android. Обнаружение таких уязвимостей в Android лишь подчеркнуло необходимость интегрированного подхода к стратегии по безопасности. В то же время оптимизированные инструменты по созданию приложений развенчали миф о том, что благодаря закрытости системы платформа iOS может избежать подобных атак, подчеркнули в компании.

«Аналитики Trend Micro отмечают, что кибератаки больше не носят изолированный характер, – отметил Т. Келлерман, Chief Cybersecurity Officer, Trend Micro. – Для того чтобы уменьшить число возможных атак и снизить риски, предприятия должны сосредоточиться на предотвращении вторжений и бороться с повторным заражением. Интеграция систем обнаружения нарушений с системами их предотвращения является ключевым решением для того, чтобы как можно быстрее остановить проникновение хакеров в сеть. “Ожидать атаку, чтобы противостоять ей” – это девиз информационной безопасности в 2016 году».

Согласно данным исследования Trend Micro, утечка данных была использована для проведения дальнейших атак и вымогательств. Успешные атаки против Hacking Team и Ashley Madison значительно повлияли на сферу безопасности и обработки данных.

В то же время обнаружение уязвимостей в двух мобильных платформах подчеркнуло наличие проблем в обеих экосистемах. В ответ на обнаружение целой череды уязвимостей в Android корпорация Google, наконец, анонсировала программу регулярного обновления системы безопасности своей мобильной платформы.

Тактика «широкого охвата» в атаках на PoS-терминалы оказывает все более сильное влияние на малый бизнес. Атаки, отмеченные в III квартале, связанные, в том числе, с уязвимостями платежных терминалов, использовали такие «старые» техники, как спам, вредоносные макросы, наборы эксплойтов и ботнеты, отметили в компании.

Основной целью кампаний кибершпионажа стали политики. Анализ последних данных показал, что, например, под прицелом группы хакеров Pawn Storm оказались не только американские, но и российские организации.

Среди инструментов, которыми пользовались злоумышленники в III квартале 2015 г., наибольшей популярностью пользовался набор эксплойтов Angler Exploit Kit. По данным Trend Micro, рост числа его использований по сравнению с прошлым кварталом составил 34 %. Авторы Angler Exploit Kit заметно обновили свой набор эксплойтов за последний квартал. Это привело к тому, что преступники использовали эти разработки для распространения вредоносных программ.

В новом исследовании также поднимается вопрос уровня безопасности устройств с подключением к Интернету. Исследования показали, что злоумышленники могут получить контроль над такими устройствами, что может повлечь за собой опасные последствия, указали в компании ***(Кибератаки стали оказывать влияние на реальную жизнь людей и организаций // InternetUA (http://internetua.com/kiberataki-stali-okazivat-vliyanie-na-realnuua-jizn-luadei-i-organizacii). – 2015. – 21.11).***

***

Некоторые пользователи Twitter оказались подвержены спаму со стороны неизвестных лиц, поскольку размещали свои личные данные в сети, сообщает The Verge. Для борьбы с этим нужно оставить сообщение в Twitter для Э. Сноудена «Meow, I <3 catfacts» («Мяу, я люблю факты о котах»).

Так как пользователи размещают в социальных сетях личную информацию, такую как свой адрес, электронную почту или фотографии водительского удостоверения, то это может быть использовано против них. Заинтересованные пользователи удаляют свои телефонные номера и отправляют интересные факты о кошках другим пользователям в надежде научить их безопасному использованию Интернета.

Процесс поиска номера и отправки сообщения автоматизирован с помощью двух этапов. На первом этапе с помощью API соцсети, используя ключевые слова, осуществляется поиск номера телефона, а на втором – отправка сообщения с помощью бесплатного сайта. «Когда Сноуден вошел в Twitter, он выразил благодарность кошкам», – сказал создатель проекта ***(Для борьбы со спамом пользователи твиттера будут мяукать // InternetUA (http://internetua.com/dlya-borbi-so-spamom-polzovateli-tvittera-budut-myaukat). – 2015. – 21.11).***

***

Ранее в этом месяце исследовательская фирма Lookout выявила на Android-смартфонах новое семейство троянцев – Shedun, Shuanet и ShiftyBug, которые практически невозможно удалить. Вирусы обходят механизмы защиты Android, получают права администратора и проникают глубоко в систему и осаждают пользователя надоедливой рекламой.

Более того, вредоносное ПО перемещает зараженное приложение в системный раздел, что позволяет ему «выжить» даже в случае сброса аппарата до заводских настроек. В Lookout внимательнее изучили троянцев и выяснили, что разновидность Shedun оказалась самой хитрой и опасной.

«Shedun, относящийся к семейству рекламного троянского ПО, гораздо более изощренный, чем многие думают. Помимо получения root-доступа, Shedun эксплуатирует Android Accessibility Service (AAC, “Специальные возможности Android”) во вредоносных целях, выяснила Lookout», – написал в блоге представитель компании М. Бентли, отметив, что такие случаи чрезвычайно редки.

Shedun сканирует установленные на Android-смартфон приложения на предмет предоставленных им разрешений в AAC. Далее, используя функции сервиса, предназначенные для пользователей с ограниченными физическими возможностями, троянец читает текст на экране, прокручивает список разрешений и нажимает на кнопку «Установить», причем никакого физического взаимодействия с пользователем не требуется.

Shedun, а также Shuanet и ShiftyBug проникают на Android-устройства под видом официальным приложений (Facebook, Snapchat, WhatsApp, Twitter и других), скачиваемых из сторонних магазинов. Образцов вируса в официальном магазине Google Play обнаружено не было – Shuanet заражает только смартфоны, у которых разрешена установка программ из альтернативных источников ***(«Неубиваемый» вирус сам устанавливает программы // InternetUA (http://internetua.com/neubivaemii--virus-sam-ustanavlivaet-programmi). – 2015. – 20.11).***

***

После серии хакерских атак на правительственные сети США Вашингтон намерен создать новую армию. Пентагон работает над проектом под названием «План X» стоимостью 125 млн дол., который должен помочь мгновенно опознавать интернет-атаки.

В течение четырех лет проект создаст целый спектр новых интернет-возможностей. По словам бывшего министра обороны США Ч. Хейгла, проект подразумевает создание современного кибероружия с помощью настоящих профессионалов. По плану, в 2016 г. планируется подготовить 6 тыс. военных хакеров, тесно сотрудничающих с американской разведкой и военачальниками.

Таким образом, в армии США впервые за последние 30 лет появится новая военная специальность. Летом 2015 г. первая группа военных уже начала обучение в «Кибер-школе» на военной базе Форт Гордон в Джорджии.

Самая большая проблема виртуальной войны – это тот факт, что она происходит не на земле, не в воздухе и не на воде, а в принципе невидима, и жертва хакерской атаки либо вообще ее не замечает, либо замечает поздно. В Пентагоне и в ведомствах по сетевой безопасности эксперты вынуждены долго расшифровывать коды, чтобы заблаговременно опознать проникновение в

систему. Ежедневно правительственные сети США сканируются по миллиону раз, так как нет системы мгновенного обнаружения нарушителя.

Этот пробел должен исправить «План X»: в будущем будет достаточно одного взгляда на экран, чтобы в реальном времени увидеть слабые места или атаку. С помощью графики, 3D-визуализации и анимации невидимое станет видимым.

До сих пор власти США хранят молчание о возможном возмездии за атаки, приписываемые китайским и российским хакерам. Однако Россия фактически воспринимается как главный военный враг, технологическая структура которого находится под прицелом американцев ***(Пентагон создаст новую «армию хакеров» // ЗапорожьеИнфо (http://zpinfo.cinfoo.com/news-55567.html). – 2015. – 23.11).***

***

Компания Microsoft недавно опубликовала доклад Security Intelligence Report volume 19, рассмотрев последние тенденции в сфере программной безопасности как собственных продуктов, так и приложений других производителей. Во второй половине 2014 г. число найденных в продуктах Microsoft уязвимостей составляло 209, в первой половине нынешнего года это значение возросло до 266 (+27,3 %).

Хотя это и негативная тенденция, график показывает, что у остальных производителей дела идут ещё хуже, несмотря даже на снижение числа найденных в них за рассматриваемый период уязвимостей. Веб-браузеры, операционные системы и встроенные приложения оказались самыми защищёнными, тогда как на остальные приложения приходится 55,6 % открытых уязвимостей.

Microsoft пишет, что число открытий уязвимостей в таких приложениях за минувшее полугодие снизилось почти вдвое, но они всё равно остаются наиболее распространёнными. В частности, было найдено множество связанных с протоколом SSL уязвимостей на Android в магазине Google Play Store.

Естественно, в Microsoft говорят о повышении безопасности операционных систем Windows за последние годы, в частности, в Windows 10. Новая система блокирует эксплоиты, затрудняя несанкционированный доступ к данным пользователей, а в браузере Edge нельзя ставить дополнения, вроде панелей инструментов, не прошедшие процедуру проверки в Microsoft ***(Доклад Microsoft говорит о числе программных уязвимостей за первое полугодие // InternetUA (http://internetua.com/doklad-Microsoft-govorit-o-csisle-programmnih-uyazvimostei-za-pervoe-polugodie). – 2015. – 23.11).***

***

Компания Google может удаленно сбрасывать пароли на всех смартфонах и планшетах, которые работают на Android версий от 1.0 до 4.4. Правда, это происходит только по решению суда в тех случаях, когда полиции необходимо

получить к данным на мобильном устройстве подозреваемого, а он отказывается добровольно сообщить пароль.

Судя по опубликованной недавно компанией Google статистике, смартфонов и планшетов, на которые установлен Android 2.2-4.4 – 74,1 %. Остальные работают на более новых версиях Android, в которых, как правило, используется полное шифрование накопителя. Благодаря такому шифрованию взламывать устройства удаленно бесполезно – их содержимое все равно нельзя будет просмотреть, не зная пользовательский пароль.

По сведениям Wall Street Journal, в конце прошлой недели власти США обратились к Apple, Google и Microsoft с требованием предоставить доступ к зашифрованной переписке пользователей. Причиной такого требования стала серия терактов в Париже, после которой вновь обострился вопрос о том, могут ли американские компании предоставлять услуги по переписке, которую не могут перехватить и прочитать правоохранительные органы.

Осенью прошлого года попытки Минюста и ФБР убедить Apple, Google и Microsoft в необходимости ослабить защиту шифрованием на смартфонах и планшетах были безуспешны. Американские корпорации, напротив, обратились к властям США с просьбой разрешить использовать более сильное шифрование. До сих пор Белый дом не вмешивался в этот конфликт и не занимал сторону ни корпораций, ни Минюста с ФБР.

Как считаете, правоохранительные органы должны иметь возможность читать всю вашу переписку? Думаете, это поможет им в борьбе с терроризмом? ***(Стоит ли жертвовать тайной переписки ради безопасности? // InternetUA (http://internetua.com/stoit-li-jertvovat-tainoi-perepiski-radi-bezopasnosti). – 2015. – 24.11).***

***

На вопрос журналиста издания ZDNet З. Уиттакера, почему приложения Skype, WhatsApp и Yelp очень часто обращаются к списку контактов, представители компаний Microsoft, Facebook и Yelp, которым принадлежат сервисы, не смогли дать конкретный ответ. З. Уиттакер использовал приложение DTEK на смартфоне BlackBerry Priv для того, чтобы узнать, как часто и как долго программами осуществляется доступ к такой информации, как местоположение пользователя, контакты, текстовые сообщения, микрофон и камера.

Skype чаще всех просматривал контактый список, отметил З. Уиттакер. Почти каждые несколько часов сервис обращался к контактам пользователя. Согласно DTEK, в течение трех дней Skype просмотрел контактный лист 3 484 раза, WhatsApp -2 449, а Yelp – 165. Также эти сервисы при установке получают разрешение на доступ к микрофону, камере и прочей личной информации пользователя, которая затем ими проматривается.

З. Уиттакер выяснил, что Facebook Messenger за три дня просмотрел контакты 78 раз, Pinterest – 11, Dropbox – 8, а Instagram, которое принадлежит Facebook, – всего 3 раза. Непонятно, загружают ли сервисы информацию на

свои серверы, или просто просматривают ее. Например, Skype и WhatsApp сохраняют данные на своих серверах, а потом иногда просматривают другую информацию пользователя, когда тот находится в сети.

По словам представителя Skype, «сервис регулярно просматривает контактный лист, чтобы телефонная книга приложения могла соответствовать реальным данным». Facebook никак не отреагировала на вопрос Уиттакера. Yelp до сих пор ищет подходящий комментарий. Согласно заявлению представителей сервиса, контакты нужны не для того, чтобы рекламировать Yelp знакомым пользователя, сервис также не хранит данные своих клиентов ***(Skype и WhatsApp крайне часто просматривают контакты пользователя // InternetUA (http://internetua.com/Skype-i-WhatsApp-kraine-csasto-prosmatrivauat-kontakti-polzovatelya). – 2015. – 25.11).***

***

Исследователи из компании Malwarebytes обнаружили вариант ПО, устанавливающего нежелательную рекламу на компьютере пользователя. После более подробного анализа программа, получившая наименование Vonteera, была классифицирована как троян в связи с некоторыми модификациями, которые она осуществляет на инфицированной системе.

В ходе анализа эксперты заметили, что вредонос добавляет в общей сложности 13 сертификатов в категорию «Недоверенные сертификаты» в хранилище сертификатов Windows. В их числе сертификаты для антивирусных компаний ESS Distribution, Avast, AVG Technologies, Avira, Baidu, Bitdefender, ESET, Lavasoft, Malwarebytes, McAfee, Panda Security, ThreatTrack Security и Trend Micro. Таким образом троян обеспечивает себе защиту от обнаружения антивирусными решениями. Более того, пользователь не сможет загружать файлы с сайтов, использующих данные сертификаты. Созданный трояном сервис appinf.exe предназначен для проверки наличия сертификатов и их восстановления в случае удаления пользователем.

Оказавшись на целевой системе, Vonteera создает в планировщике Windows Task Scheduler несколько задач для отображения рекламных баннеров через равные промежутки времени. Также троян создает новую службу appinf.exe и модифицирует ярлыки для рабочего стола, панели задач и пускового меню для интернет-обозревателей Internet Explorer, Firefox, Chrome, Opera и Safari. Таким образом, при запуске одного из этих приложений загружается скрипт, предназначенный для рандомизации перенаправлений пользователя во время работы с браузером.

В случае с Internet Explorer троян добавляет новый модуль Browser Helper Object (BHO). Если используется Google Chrome, Vonteera эксплуатирует ключ ExtensionInstallForcelist, определяющий список приложений и расширений, которые устанавливаются «по-тихому», и получают все запрашиваемые разрешения. Эти программы не могут быть деинсталлированы пользователем ***(Троян Vonteera использует сертификаты для отключения антивирусов //***

InternetUA (http://internetua.com/troyan-Vonteera-ispolzuet-sertifikati-dlya-otkluacseniya-antivirusov). – 2015. – 25.11).

***

По данным исследователей, две трети наиболее популярных Android-приложений скрыто передают данные на удаленные серверы. Согласно отчету «Скрытые коммуникации мобильных приложений» (Covert Communication in Mobile Applications) экспертов Массачусетского технологического института и компании Global InfoTek, проблема в той или иной мере затрагивает продукты Gameloft, Unity3d и grillgames.

Примечательно, что это подключение приложений к серверам абсолютно бесполезно для пользователей. Около половины трафика связана с аналитическими данными, используемыми, к примеру, Twitter и Pandora. Предназначение остального объема трафика остается неизвестным.

Из отчета исследователей:

«Аналитические сервисы собирают информацию о производительности приложения, сбоях в работе и использовании, а также об определенных действиях пользователя в самой программе. Эти данные нужны разработчикам, однако нигде не уточняется, какая именно информация и в каких объемах собирается.

По факту, некоторые приложения начинают собирать аналитическую информацию еще до своей активации. К примеру, Twitter, Walmart и Pandora начинают сбор информации, как только загрузится смартфон, и периодически продолжают это делать, пока он включен, даже если сами по себе эти приложения не используются вовсе. В большинстве случаев единственным способом отключить передачу этих данных является деинсталляция программы».

После того как исследователи внесли в код некоторые изменения и отключили передачу информации, пять приложений перестали работать. Эксперты обнаружили, что в трех четвертях случаев передачи данных использовался компонент com.google, совершавший порядка 2000 звонков (половина из всех исследуемых) ***(Популярные Android-приложения скрыто передают данные разработчикам // InternetUA (http://internetua.com/populyarnie-Android-prilojeniya-skrito-peredauat-dannie-razrabotcsikam). – 2015. – 24.11).***

***

Исследователи по безопасности американской компании Damballa нашли больше информации об атаке на компьютерные системы Sony Pictures, в результате которой в сеть «утекли» внутренние сообщения и документы компании, сообщает BusinessInsider.

Как заявляют исследователи, одним из инструментов хакерской атаки был так называемый метод setMFT. Он может быть использован хакером, чтобы изменить даты, связанные с некоторыми файлами. Вторым

инструментом был afset, который использовался для того, чтобы скрыть атаку от экспертов ***(Исследователи обнаружили, как атакующие Sony хакеры оставались незамеченными // InternetUA (http://internetua.com/issledovateli-obnarujili--kak-atakuuasxie-Sony-hakeri-ostavalis-nezamecsennimi). – 2015. – 24.11).***

***

Персональные компьютеры Dell содержат уязвимость, позволяющую злоумышленникам получать доступ практически к любым данным пользователя, передаваемым через Интернет, путем создания поддельных сайтов с поддельными сертификатами.

Неограниченные возможности перехвата

Уязвимость в персональных компьютерах Dell предоставляет хакерам возможность направлять пользователей на поддельные сайты с поддельными сертификатами, получая доступ к их паролям, электронной почте, банковским и другим данным. В качестве примеров исследователи уже создали поддельные сертификаты google.com и bankofamerica.com, заставив веб-браузер считать подлинными сайты, которые ими не являются.

Сообщения об уязвимости появились на сайте Reddit, на интернет-форумах и в Twitter. О ее наличии сообщили владельцы компьютеров Dell XPS, Precision и Inspiron. В Dell подтвердили наличие проблемы, не уточнив, ограниченна ли она какими-либо линейками. В компании сказали просто: «Уязвимость в наших компьютерах».

Суть уязвимости

Компания Dell предустанавливает на компьютеры самоподписанный корневой сертификат eDellRoot, который может подписывать сторонние сертификаты. Он комплектуется закрытым ключом, который помечен как неэкспортируемый. Однако при помощи ряда инструментов исследователям удалось получить копию этого ключа. Более того, как выяснилось, на всех поставляемых компьютерах Dell и сертификат, и закрытый ключ полностью идентичны.

«Атакующий по сети может использовать eDellRoot для того, чтобы подписать свои собственные поддельные сертификаты для реальных веб-сайтов. Пользователь будет находиться в полном неведении, пока не проверит цепочку сертификатов сайта. Кроме того, eDellRoot может быть использован для подписывания приложений, предназначенных для запуска на компьютере жертвы», – пояснил пользователь Reddit rotorcowboy, один из первых обнаруживший уязвимость.

Реакция Dell

Dell опубликовала сообщение на своем сайте, подтвердив наличие проблемы. Компания выпустила инструкцию по удалению сертификата eDellRoot. Эту процедуру пользователи должны выполнить самостоятельно, хотя они могут воспользоваться и специальным инструментом, который

компания планирует выпустить в конце ноября 2015 г. Он выполнит поиск eDellRoot на компьютере и самостоятельно удалит сертификат.

Сертификат eDellRoot предназначен для службы технической поддержки Dell. Он позволяет ей дистанционно узнавать модель компьютера. Это ведет к сокращению времени обслуживания, пояснили в Dell. «eDellRoot не собирает какие-либо пользовательские данные», – добавили в компании.

Похожая проблема у Lenovo

В феврале 2015 г. похожая проблема была обнаружена в компьютерах Lenovo. Как выяснилось, устройства поставлялись с предустановленным приложением Superfish, относящимся к категории нежелательного рекламного ПО. Взломав данное приложение, злоумышленники также могли перехватывать пользовательские данные ***(«Дыра» в компьютерах Dell дает хакерам карт-бланш // InternetUA (http://internetua.com/dira--v-kompuaterah-Dell-daet-hakeram-kart-blansh). – 2015. – 25.11).***

***

Миллионы ничего не подозревающих пользователей Facebook раскрыли свою персональную информацию, пройдя невинный на первый взгляд развлекательный тест. Разработчик приложения, корейская компания Vonvon, отрицает все обвинения и выступает в защиту своего продукта.

По данным сайта comparitech.com, порядка 16 млн пользователей соцсети были одурачены тестом под названием «Какие слова вы чаще всего используете на Facebook?», который собирает большие объемы персональных данных.

«Этот “тест”, созданный компанией Vonvon.me, привлек свыше 16 млн человек всего за несколько дней. Звучит здорово, правда? Как бы не так! 16 млн человек согласились предоставить компании практически всю личную информацию о себе и даже не догадываются об этом», – заявил П. Бишофф из comparitech.com.

П. Бишофф отметил, что политика конфиденциальности Vonvon проливает некоторый свет на то, что происходит с собранными пользовательскими данными. Регистрируясь в приложениях компании, пользователь дает согласие на передачу своей персональной информации «третьим сторонам». Согласно политике конфиденциальности, передача данных осуществляется «анонимно и без возможности идентификации личности».

По словам П. Бишоффа, Vonvon оставляет за собой право продавать информацию пользователей кому угодно с целью получения выгоды. Компания уверяет, что не передает данные без согласия, однако, проходя тест, пользователь уже автоматически дает свое разрешение, при этом не ознакомившись с политикой конфиденциальности.

«Хуже всего, что Vonvon снимает с себя ответственность за дальнейшее использование информации третьими сторонами, которые могут делать с ней всей, что взбредет в голову», – заявил эксперт.

Тем не менее, по заявлениям представителей компании, Vonvon только получает доступ к учетной записи пользователя с целью подсчитать результаты теста. «Мы не сохраняем личную информацию, в том числе электронные адреса, списки контактов, фотоальбомы и пр. Мы никогда не храним ничего такого в своих базах данных. Если пользователь хочет опубликовать результаты теста на своей странице, они сохраняются на серверах Facebook, а не на наших», – заявили в Vonvon ***(Развлекательный тест собрал данные 16 млн пользователей Facebook // InternetUA (http://internetua.com/razvlekatelnii-test-sobral-dannie-16-mln-polzovatelei-Facebook). – 2015. – 27.11).***

***

Специалисты швейцарской ИБ-компании High-Tech Bridge обнаружили критическую уязвимость в системе управления интернет-магазинами Zen Cart (версия 1.5.3 и, возможно, ниже). Отметим, что на базе данной платформы работает более 3,5 тыс. веб-сайтов.

Пока эксперты не раскрывают подробностей о бреши, но, судя по информации, размещенной в опубликованном компанией бюллетене безопасности, речь идет о внедрении PHP-кода, что является довольно серьезной уязвимостью. Путем ее эксплуатации злоумышленники могут взломать веб-серверы и получить доступ к данным пользователей. Кроме того, для всех серверов, работающих под управлением Zen Cart, существует высокий риск инфицирования вредоносным ПО.

Эксперты High-Tech Bridge уже проинформировали о проблеме разработчиков Zen Cart. В настоящее время компания никак не комментирует ситуацию. Полная информация о бреши будет доступна с 16 декабря текущего года.

По словам гендиректора High-Tech Bridge И. Колошенко, критические уязвимости в популярных коммерческих платформах – явление довольно редкое. Обычно такие веб-приложения подвержены уязвимостям типа XSS или CSRF, а также более серьезным брешам, для эксплуатации которых, тем не менее, требуются специфические условия или другие уязвимости ***(Обнаружена критическая уязвимость в платформе Zen Cart // InternetUA (http://internetua.com/obnarujena-kriticseskaya-uyazvimost-v-platforme-Zen-Cart). – 2015. – 26.11).***

***

Миллионы дебетовых и кредитных карт американцев были скомпрометированы с помощью сложного вредоносного ПО, которое получило название ModPOS. Вредонос инфицировал PoS-системы в различных точках розничной торговли (названия пострадавших заведений не указываются) в США. Ущерб от продолжительной кибератаки составил миллионы долларов. Согласно данным расследования, злоумышленники начали свою вредоносную кампанию еще в 2013 г.

«Это PoS-вредонос на стероидах. Мы проанализировали подобные программы, выявленные за последние восемь лет, и не обнаружили ничего подобного. Это самый сложный вредонос для PoS-систем, по крайней мере, за последнее время», – отметил старший директор ИБ-компании iSight Partners С. Уорд.

Эксперт отметил, что его команде потребовалось около трех недель для того, чтобы «обезвредить» один из трех модулей ядра ModPOS. Для сравнения, подобные манипуляции с вредоносом Cherry Picker заняли у экспертов всего 30 минут. Проделанная вирусописателями работа очень впечатлила ИБ-экспертов, которых поразил уровень сложности ModPOS и его способность оставаться незамеченным.

По словам С. Уорда, злоумышленники потратили уйму времени и денег на каждый модуль ядра, который ведет себя, как руткит. Это делает его трудно выявляемым и устраняемым. Из-за использования хакерами антикриминалистических инструментов многие предприятия в Восточной Европе не смогут обнаружить атаку. ИБ-эксперты уже предупредили компании о возможном инфицировании их PoS-систем ***(Обнаружен самый сложный PoS-вредонос // InternetUA (http://internetua.com/obnarujen-samii-slojnii-PoS-vredonos). – 2015. – 26.11).***

***

Исследователи немецкой компании Payload Security впервые обнаружили вымогательское ПО с интерфейсом на иврите. Инфицировав систему, вредонос подменяет обои рабочего стола заявлением с требованием выкупа и флагом Израиля. Очевидно, шифровальщик распространяется на подпольных форумах и нацелен на пользователей, говорящих на иврите.

По словам исследователей, вредонос puzevomy.exe скрывает свое присутствие на системе, подавляя вывод сообщения об ошибках. Среди необычных характеристик эксперты выделили импорт подозрительных API и получение данных о поддерживаемых языках. Шифровальщик детектируется как вредоносное ПО многими антивирусными решениями ***(Обнаружено первое вымогательское ПО с интерфейсом на иврите // InternetUA (http://internetua.com/obnarujeno-pervoe-vimogatelskoe-po-s-interfeisom-na-ivrite). – 2015. – 26.11).***

***

Активисты-хакеры Ghost Security Group заявили о том, что обнаружили данные боевиков террористической организации «Исламское государство», использующих виртуальную валюту биткоин для денежных переводов и финансирования. Об этом сообщает Fox News.

Один из основателей компании Kronos Advisory М. Смит сказал, что хакерам удалось обнаружить несколько таких счетов. На одном из них они обнаружили сумму в 3 млн дол.

По его словам, активисты сами связались с ним и передали эту информацию. Он отметил, что хакеры заявили о желании «Ghost Security Group внести свой вклад в борьбе с терроризмом».

Один из активистов отметил, что виртуальная валюта составляет 1–3 % общего дохода ИГ. Тем не менее, отмечается в тексте, для проведения теракта и не нужно больших финансовых вложений, а биткоины опасны именно тем, что их перевод никак не контролируется ***(Хакеры нашли боевиков «Исламского государства» среди пользователей биткоинов // InternetUA (http://internetua.com/hakeri-nashli-boevikov--islamskogo-gosudarstva--sredi-polzovatelei-bitkoinov). – 2015. – 26.11).***

***

Google обновила статистику по использованию европейскими гражданами «права на забвение», сообщает searchengines.ru

По данным компании, за период с 29 мая 2014 г. по 25 ноября 2015 г. было получено 348085 запросов на удаление из поисковой выдачи 1 234 092 URL-адресов. Из уже рассмотренных обращений Google удовлетворил 441 032 (42 %).

По количеству удалённых ссылок лидирует Facebook. За социальной сетью следует поисковая система profileengine.com, у которой был контракт на индексацию профилей Facebook с 2007 по 2010 г. Третье и четвёртое место занимают сервисы Google.

Напомним, что Европейский суд подтвердил право пользователя «быть забытым» поиском Google 13 мая 2014 г.

В настоящее время активисты требуют введения «права на забвение» в США ***(Facebook лидирует по числу удалённых через «право на забвение» ссылок // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45421/118/lang,ru/). – 2015. – 26.11).***

***

26 листопада телеканал «112 Україна» піддався масованій DDos-атаці, у результаті якої сталися збої в роботі сайту 112.ua.

Про це повідомила прес-служба телеканалу.

Ефір мовника не постраждав і продовжив роботу у звичайному режимі. Технічні фахівці компанії відбили три атаки і відзначили, що в майбутньому також можливі подібні дії хакерів.

«Метою подібних спланованих дій хакерів є виведення з ладу обладнання телеканалу. Зараз всі системи відновлені, прийняті різноманітні заходи для подальшого посилення захисту компанії», – зазначили в прес-службі ***(На канал «112 Україна» здійснили DDos-атаку // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/na_kanal_112_ukraina_zdiysnili_ddosataku/). – 2015. – 26.11).***

***

Демонстрация рекламы в мобильных приложениях для многих разработчиков уже давно стала одним их главных источников заработка.

Однако такой способ получения прибыли все чаще берут на вооружение не только добропорядочные производители ПО, но и киберпреступники, создающие для этого всевозможные вредоносные программы. Одной из них стал обнаруженный специалистами компании «Доктор Веб» троянец Android.Spy.510, который устанавливает на Android-смартфоны и планшеты нежелательный программный модуль, показывающий рекламу поверх большинства запускаемых приложений.

Android.Spy.510 распространяется в модифицированном вирусописателями изначально безобидном мультимедийном проигрывателе, который злоумышленники назвали «AnonyPlayer». Троянская версия плеера обладает всеми функциями оригинала и полностью работоспособна, поэтому у потенциальных жертв не должно возникнуть никаких подозрений относительно его возможной опасности.

После установки и запуска Android.Spy.510 собирает и передает на управляющий сервер ряд конфиденциальных данных, включая логин пользователя от учетной записи Google Play, информацию о модели зараженного смартфона или планшета, версии SDK операционной системы, а также о наличии в ней root-доступа. Затем троянец пытается инсталлировать скрытый в его ресурсах дополнительный программный пакет, который содержит основной вредоносный функционал, необходимый злоумышленникам. Для этого Android.Spy.510 демонстрирует специальное сообщение, в котором говорится о необходимости установить приложение AnonyService, якобы обеспечивающее анонимность пользователей и предотвращающее получение конфиденциальной информации третьими лицами. В действительности же данная программа не предоставляет подобного функционала и является рекламным модулем, внесенным в вирусную базу Dr.Web как Adware.AnonyPlayer.1.origin.

Сразу после запуска Adware.AnonyPlayer.1.origin запрашивает у владельца мобильного устройства доступ к специальным возможностям операционной системы (Accessibility Service), после чего переходит в режим ожидания и начинает нежелательную деятельность лишь спустя несколько суток с момента своей инсталляции. Это сделано с целью уменьшения вероятности обнаружения пользователем источника нежелательной активности на зараженном устройстве.

По прошествии заданного времени Adware.AnonyPlayer.1.origin благодаря имеющимся в его распоряжении функциям Accessibility Service начинает отслеживать все происходящие в системе события и ожидает момента, когда жертва запустит какое-либо приложение. Как только это происходит, модуль немедленно приступает к выполнению своей главной задачи – показу рекламы ***(Рекламное Android-приложение «подставляет» другие программы // ITnews***

(http://itnews.com.ua/news/79116-reklamnoe-android-prilozhenie-quotpodstavlyaetquot-druqie-programmy). – 2015. – 27.11).

***

Согласно данным VPN-провайдера Perfect Privacy, некоторые VPN-сервисы могут быть использованы злоумышленником для выяснения реального IP-адреса жертвы. По словам экспертов, пострадавшими от вредоносной деятельности могут оказаться и пользователи BitTorrent. Уязвимость затрагивает те сервисы, которые поддерживают перенаправление портов.

Успешная атака требует нескольких условий: злоумышленнику необходимо быть в той же VPN-сети, что и жертва, а пользователь должен подключиться к подконтрольному хакерам ресурсу. Заставив обманным путем жертву открыть вредоносный файл, злоумышленник, который способен перенаправить порт, может увидеть ее реальный IP-адрес.

«Пользователь VPN-сервисов, подключаясь к своему VPN-серверу, использует маршрут по умолчанию с реальным IP-адресом, как того требует подключение к VPN. Именно в этом и заключается главная проблема», – отметили эксперты из Perfect Privacy.

Специалисты протестировали девять VPN-провайдеров, пять из которых оказались уязвимы к описанной выше атаке. Эксперты уже уведомили представителей сервисов о существующей проблеме. К сожалению, по словам Perfect Privacy, у них не было возможности проверить работу и остальных VPN-провайдеров.

«Пострадать от такой атаки могут и пользователи клиента BitTorrent, которые обращаются к VPN для загрузки контента. Вполне вероятно, защитники правообладателей могут использовать такой тип атаки в борьбе с пиратством», – рассказали в Perfect Privacy ***(Брешь в VPN ставит под угрозу пользователей BitTorrent // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2015/11/27/VPN-flaw.html). – 2015. – 27.11).***

***

Согласно прогнозу ИБ-компании Lookout Security, в следующем году коммерческие предприятия столкнутся с ростом кибератак с эксплуатацией уязвимостей в iOS-устройствах. Мобильные гаджеты постепенно приобретают функционал, присущий персональным компьютерам, к примеру, у планшета Apple iPad Pro появилась клавиатура, поясняют в компании.

«Мы не считаем, что атаки из App Store станут нормой. Тем не менее, мы ожидаем рост числа атак на корпоративные iOS-устройства, учитывая хранимые на них большие объемы данных и тот факт, что посредством мобильных гаджетов можно получить доступ к другой важной информации», – отмечают эксперты Lookout.

Вероятнее всего, кибератаки будут комбинированными и включать использование вредоносных приложений, эксплуатацию уязвимостей в

легитимных программах и операционных системах, а также социальную инженерию.

Также специалисты считают, что пользователи по-прежнему будут создавать себе неприятности, устанавливая слабые пароли на сайтах и в учетных записях.

Одним из способов решения этой проблемы является повсеместная реализация двухфакторной аутентификации, и в будущем году использование и доступность этой функции будет расти. «В настоящее время пароли являются, пожалуй, самой основной проблемой в Интернете. Слабые пароли, использование одних и тех же паролей на различных сайтах и восстановленные пароли, которые могут получить лица с доступом к электронной почте пользователя, делают их своеобразной ахиллесовой пятой даже для тех, кто серьезно относится к собственной безопасности», – добавляют в Lookout ***(Эксперты прогнозируют рост атак на iOS-устройства в 2016 году // Центр Інформаційної Безпеки (http://www.bezpeka.com/ru/news/2015/11/27/iOS-attacks-growth-in-2016.html). – 2015. – 27.11).***

***

Двойной удар: как атакуют Linux-серверы и заметают следы

Сценарии современных сетевых атак порой напоминают детектив. Подозрение сначала падает на невиновных, а злодей успешно маскируется до тех пор, пока за него сообща не возьмутся профессионалы. Эксперты компании Check Point опубликовали отчет о расследовании инцидента с использованием нового метода атак на Linux-серверы. В нём приводится анализ тактики злоумышленников и использованных ими вредоносных программ, а также даются советы по защите от них.

В июле этого года с группой расследования инцидентов Check Point связался крупный заказчик, который обнаружил странные действия в файловой системе на одном из своих серверов DNS BIND, работавшим под управлением ОС Linux. Странность заключалась в большом числе специфических файлов, записанных в системных каталогах.

В результате анализа эксперты установили, что ранее в том же месяце сервер подвергся брутфорсу учетных записей SSH. Его особенность состояла в том, что атакующих IP-адресов было очень много, и почти все они принадлежали китайским подсетям. Стандартные методы бана по IP оказались неэффективны. Каждый узел успевал перебрать лишь несколько паролей, но благодаря массированной атаке через несколько дней был получен рутовый доступ.

Используя рут, атакующие внедрили на сервер троян XOR.DDoS и бэкдор Groundhog. Они «зомбируют» заражённые машины, делая их частью ботнета, который в дальнейшем используется для проведения масштабных DDoS-атак и других целей.

Эксперты отмечают мастерство авторов этих вредоносных программ и целенаправленность выполненной атаки. Большинство других троянов и бэкдоров распространяются хаотично, инфицируя любые уязвимые системы независимо от их роли. Эти же заражали только серверы под управлением Linux с потенциальным доступом к скоростным каналам. Высокая пропускная способность каждого из заражённых серверов в ботнете даёт возможность проводить DDoS-атаки небывалой интенсивности.

Интересно, что на момент расследования инцидента троян XOR.DDoS уже был известен, а вот Groundhog стал открытием. В результате анализа стало очевидно, что они имеют много общего на уровне конфигурации, методов защиты и способов коммуникации. Глубокое изучение их кода позволяет сделать вывод, что троян и бэкдор имеют общее происхождение. «С большой вероятностью, XOR.DDoS и Groundhog – это разные модули одного семейства вредоносных программ, созданных одним автором», – поясняет руководитель отдела реагирования на инциденты Check Point Д. Уайли.

Согласно предыдущим расследованиям, брутфорс SSH часто начинался в подсети, принадлежащей китайской компании HEE THAI LIMITED (AS63854). В апрельском отчёте упоминается о блокировании её трафика и лишении ботнета возможности наступления. Однако последнее исследование Check Point показало, что злоумышленникам удалось перевести свой ботнет-трафик в подсеть CHINANET, чьи сервера расположены в провинции Цзянсу.

Дальнейший анализ логов заражённого сервера и мониторинг его активности подтвердил, что злоумышленники недавно сменили подсети. Они перестали использовать те же IP-адреса, что и для начального брута SSH. Согласно данным, собранным в ходе расследования службой Check Point ThreatCloud, это был не единственный случай заражения, а управляемая распределенная кампания, направленная на серверы по всему миру.

Процедура заражения серверов состояла из двух основных этапов: брута SSH и инфицирования набором из трояна и бэкдора. Сначала выполнялось внедрение XOR.DDoS. Этот троянец чаще всего используется в современных DDoS-атаках, поддерживая такие распространённые методы, как SYN Flood, ACK Flood и DNS amplification. Цели и параметры атак ему передаёт C&C-сервер, с которым XOR.DDoS поддерживает расширенное взаимодействие: он может принимать и отправлять файлы, исполнять скрипты и устанавливать другие вредоносные компоненты. Шифрование соединения с C&C сводится к банальной процедуре XOR, отражённой в названии трояна.

Однако для успешного наполнения ботнета мало заразить очередной сервер. Троян может быть обнаружен, а пароль доступа изменён в любой момент, поэтому злоумышленники также использовали функции бэкдора Groundhog, чтобы обеспечить себе постоянный доступ. Его основная задача состоит в удалённом управлении конфигурацией сервера, приёме командных сообщений и файлов, которые он также может запускать на исполнение. Для маскировки связь с C&C происходит через разные порты TCP: 22, 80, 443 и другие. Groundhog использует предопределенный домен

GroUndHog.MapSnode.CoM (211.110.1.32), в честь которого он и получил свое название.

Оказавшись на сервере, трояны совершают несколько действий, обеспечивающих их повторную активацию в случае перезагрузки. Скрипт автозагрузки создаётся в папке /etc/init.d. Другой скрипт размещается по адресу /etc/cron.hourly/gcc.sh и применяется для ежечасной проверки наличия троянов в системе. Еще один скрипт отвечает за принудительное включение всех сетевых интерфейсов и применяется для запуска ранее загруженных вредоносных файлов.

В современных атаках часто используются сразу несколько вредоносных программ. Каждая из них по отдельности выглядит очередным трояном, сетевым червём или бэкдором, специализирующимся на определенном типе целей – от смартфонов и домашних ПК до маршрутизаторов и высокопроизводительных серверов. Однако их умелое сочетание открывает для атакующих совершенно иные возможности построения ботнетов и выполнения целенаправленных атак.

Расследования последних инцидентов показывают, что ботнеты стали наиболее совершенным средством проведения DDoS-атак. Входящие в их состав узлы – лишь инфицированные машины, чьи владельцы обычно не знают о несанкционированном использовании их мощностей. Поэтому не следует воспринимать их как инициаторов атаки. Чтобы найти её настоящий источник, надо восстановить всю цепочку событий. Сложно выявить реальных кукловодов – тех, кто наполнял ботнет заражёнными узлами для последующей продажи C&C или личного использования.

Специалисты CheckPoint отмечают, что в последнее время изменился характер известных киберугроз и возникло множество новых. Крупные организации всё чаще становятся жертвами целенаправленных атак, среди которых основную массу составляют масштабные DDoS-атаки повышенной сложности. Из-за распределённого характера и применения в них заражённых серверов с высокоскоростными каналами, такие атаки трудно блокировать классическими низкоуровневыми инструментами.

«Мы считаем, что современные элементы управления безопасности могут предотвратить такую атаку, – комментирует Д. Уайли. – Мониторинг логов, блокировка повторяющихся логинов, ограничение удаленного доступа, использование NGFW и другие меры существенно снижают возможности атакующей стороны» ***(Двойной удар: как атакуют Linux-серверы и заметают следы // InternetUA (http://internetua.com/dvoinoi-udar--kak-atakuuat-Linux-serveri-i-zametauat-sledi). – 2015. – 23.11).***

***

Производители встраиваемых устройств не тестируют их безопасность

Большое количество маршрутизаторов, DSL-модемов, VoIP-телефонов, IP-камер и других встраиваемых устройств содержат уязвимости, что указывает на недостаток тестирований безопасности со стороны производителей. К

такому выводу пришли эксперты исследовательского центра EURECOM (Франция) и Рурского университета в Бохуме (Германия) на основе анализа сотен образов прошивки, находящихся в общественном доступе.

Для начала исследователи собрали 1925 образов прошивки на основе Linux устройств от 54 производителей, однако им удалось запустить веб-сервер только для 246 из них. Целью экспертов было обнаружение уязвимостей путем динамического анализа веб-интерфейсов управления пакетов прошивки, проведенного с помощью инструментов с открытым исходным кодом. В результате было обнаружено 225 брешей в 46 анализируемых образах.

Также было проведено отдельное исследование, предполагавшее извлечение кода веб-интерфейса и размещение на общем сервере, так что его можно было протестировать без эмуляции непосредственной среды прошивки. У этого теста есть свои недостатки, однако он был успешно проведен в отношении 515 пакетов прошивки, в 307 из которых были обнаружены уязвимости.

Помимо вышеописанных тестов, с помощью другого инструмента с открытым исходным кодом эксперты провели статический анализ извлеченного из образов прошивки PHP-кода. В результате в 145 образах было обнаружено 9046 уязвимостей.

С помощью статического и динамического анализа в веб-интерфейсах 185 уникальных пакетов прошивки исследователи выявили опасные бреши, позволяющие выполнять команды, осуществлять SQL-инъекции и межсайтовый скриптинг. Эти уязвимости являются лакомым куском для злоумышленников, и возникает вопрос, почему сами производители не обнаружили и не исправили их? Не исключено, что они просто не проводят такие тестирования, а если и проводят, то недостаточно тщательно ***(Производители встраиваемых устройств не тестируют их безопасность // InternetUA (http://internetua.com/proizvoditeli-vstraivaemih-ustroistv-ne-testiruuat-ih-bezopasnost). – 2015. – 27.11).***

***

DARPA разрабатывает систему оповещения о кибератаках на энергосети

На протяжении длительного времени разработка систем защиты для национальной энергетической системы США является ключевой целью для многих частных компаний и правительственных организаций. Тем не менее, по мнению ряда экспертов, энергетический сектор по-прежнему является уязвимым для кибератак.

В настоящее время Агентство передовых оборонных исследовательских проектов (Defense Advanced Research Projects Agency, DARPA) разрабатывает систему под названием RADICS (Rapid Attack Detection, Isolation and Characterization), которая будет обнаруживать и автоматически реагировать на кибератаки, осуществленные на инфраструктуру США.

Как пишет издание Networkworld, в агентстве заинтересованы в системе, которая предупреждает о предстоящих атаках и способна оперативно оценивать

ситуацию, изолировать сеть, а также характеризовать угрозы. DARPA пока не раскрывает подробностей о том, что представляет собой новая система, пообещав предоставить больше информации в ходе пресс-конференции, которая пройдет 4 декабря этого года.

В прошлом DARPA уже предлагала свои решения для обеспечения безопасности энергетической инфраструктуры. Так, в 2012 г. была представлена программа HACMS (High-Assurance Cyber Military Systems), направленная на разработку киберфизических систем высокого уровня, которые могут применяться в любых сферах – от внедрения в SCADA-системы до использования в различной компьютерной технике (принтеры, маршрутизаторы, мобильные телефоны и пр.).

Цель проекта заключалась в разработке набора инструментов с открытым исходным кодом, интегрированных в программное обеспечение, которое найдет широкое применение как в коммерческом, так и военном секторах ***(DARPA разрабатывает систему оповещения о кибератаках на энергосети // InternetUA (http://internetua.com/DARPA-razrabativaet-sistemu-opovesxeniya-o-kiberatakah-na-energoseti). – 2015. – 29.11).***

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Касаткіна** Тетяна

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

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, просп. 40-річчя Жовтня, 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
www.nbuv.gov.ua/siaz.html

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.