СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(2–20.03)

2016 № 5

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(2–20.03)
№ 5

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

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

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2016

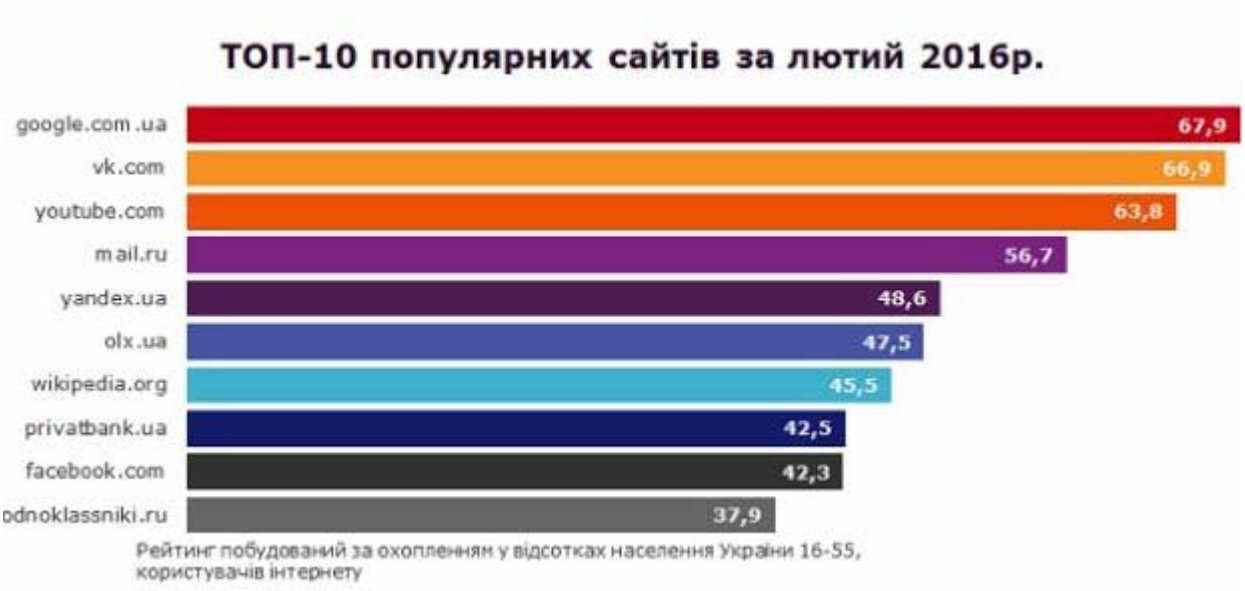
ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

15.03.2016

Google, «ВКонтакте» та YouTube – чим українці користувалися у лютому

За даними дослідження CMeter компанії TNS, у лютому в трійці лідерів залишилися Google.com.ua, Vk.com, YouTube.com. З ТОП-10 випала Rozetka.com.ua – замість неї 10-е місце посіли Odnoklassniki.ru, пише Телекритика.



У лютому трохи знизився інтерес до погоди, завдяки чому Sinoptik.ua перемістився в рейтингу з 13-го на 15-е місце.

Також зросли показники Prom.ua, що може бути пов’язано з купівлею подарунків на День закоханих і 8 Березня.

Збільшилася аудиторія Privatbank.ua, завдяки чому він обігнав Facebook.com.

При дослідженні використовували лічильники, інтегровані в сайти та встановлені у фреймі банерної мережі та панель, що фіксує контакт користувачів з контентом. Дані об’єднуються в режимі реального часу, що гарантує відсутність втрат даних.

***

10.03.2016

Эксперт спрогнозировал, как будут развиваться самые популярные соцсети в будущем

Прогнозы – дело неблагодарное, однако не делать их, значит не анализировать текущее состояние рынка социальных сетей. Каждый раз, когда

вы задумываетесь о том, что будет с Facebook или «ВКонтакте» завтра, вы тем самым активизируете и корректируете собственную стратегию участия и продвижения в сети.

Об этом в своем блоге на «Обозревателе» пишет Р. Калинин, координатор «Антикоррупционного движения», информирует Экономические известия.

«Поэтому давайте немного проанализируем, что сейчас происходит на основных площадках и чем они могут нас удивить в будущем, как с точки зрения посещаемости, так и технологическими новинками.

“ВКонтакте” сеть № 1 в странах бывшего СНГ. Сервис, в самом начале полностью скопировавший идею у Facebook, сейчас создает собственную идею. Изначально “русскоговорящий” он стал альтернативой иностранному Facebook.

Более 13 млн, по данные Factum Group, украинцев в сутки посещают эту сеть. Более 80 млн посещают сеть во всем мире. Официальная статистика.

Аудитория сети продолжает расти. В худших раскладах запас прочности не менее чем на 5 лет.

Преимущества сети: удобный интерфейс и простая регистрация. Т.е. низкий порог входа.

В последнее время появились новые механизмы рекламы – ретаргетинг и продвижения постов, что делает сеть более привлекательной для рекламодателей.

Было много разговоров, что с уходом основателя “ВКонтакте” П. Дурова – сеть умрет, однако этого не случилось, так как он заложил правильные механизмы инерции – спрыгнуть с тысяч бесплатных песен, фильмов (пиратских), интересных групп и сообществ теперь сложно.

Facebook – социальная сеть № 1 в мире по своей популярности и № 3 по популярности в Украине. Насчитывает более 1,5 млрд пользователей в мире. Сеть более сложная для пользователя, чем “ВКонтакте”, ввиду гораздо большего количества разработчиков, инженеров и финансовой основы. Имеет более интеллектуальную аудиторию. Накопленный массовый сегмент подталкивает зарегистрироваться в Facebook, если тебя еще там нет. Скорее всего, большинство друзей или знакомых уже там и предпочитают общение именно через Facebook.

В перспективе 2–3 лет Facebook займет законное 2 место в бывших странах СНГ после “ВКонтакте”.

Самый большой запас прочности в мировом формате. Facebook принадлежат Instagram и WhatsApp (в свое время очень актуальные покупки были – на перспективу). Если тренд социальных сетей сменится, то WhatsApp поможет комфортно чувствовать себя в эпоху мобильных. Плюс Facebook продолжает активно развивать свой Messenger, который является аналогом WhatsApp и Viber. То есть Facebook уже сидит на двух стульях и активно развивает внутреннюю технологическую конкуренцию.

Аудитория Facebook растет ежедневно огромными темпами и, в ближайшее время, не планируется отток людей, т. к. люди очень рефлективные

пользователи. И если он сидит тут 5 лет и у него здесь большинство друзей, то бросить и перейти на что-то более удобное очень сложно.

“Одноклассники” на сегодняшний день находятся на 2 месте среди украинских пользователей. Более 8,5 млн украинских пользователей посещают эту сеть в день. Но постепенно сеть теряет свою аудиторию. Изначально разработчиками была сделана ставка на взрослую аудиторию, и сложно долгое время удерживать высокие позиции. Новая аудитория приходит плохо, т. к. выросла на продукте конкурента. Нет тенденции, что пользователь “ВКонтакте” или Facebook доживает до 37 лет, закрывает аккаунт и регистрируется в “Одноклассниках”. Он привык, оброс друзьями, связями и никуда он не уйдет. Приток пользователей пока идет лишь из-за того, что взрослая аудитория осваивает интернет и идет в социальные сети. Менеджеры “Одноклассников” это понимают и купили домен “ОК”, чтобы перестроиться на молодежь. Думаю, задумка не удалась. В долгосрочной перспективе рост аудитории уменьшится. Обе компании “ВКонтакте” и “Одноклассники” принадлежат одной корпорации – Mail.ru, а значит “ВКонтакте” не будет “убивать” “Одноклассников” и они займут 3-4 место по посещаемости среди украинской аудитории.

“Мой мир”

Плохая статистика и тенденции. В планах компании Mail.ru передать своих пользователей “ВКонтакте” и “Одноклассникам”, что вполне логично с точки зрения бизнеса и затрат.

Instagram

Сомнительное будущее. С одной стороны, система интересная, люди ей пользуются, но как из этого сделать бизнес модель до сих пор еще не ясно. Бурный рост закончился. Эффект новизны прошел. Многие уже “наигрались” и им надоело смотреть одни фотографии и короткие ролики. Однако есть запас прочности, как минимум еще на пару лет.

Twitter

В настоящее время эту сеть посещают около 4 млн уникальных украинских пользователей в день. Однако в связи с ростом других социальных сетей перед ними стоит выбор – или стать клоном Facebook или остаться в своей нише. Twitter для людей мини-репортёров, которые хотят постоянно что-то публиковать. Доходит до того, что люди начинают публиковать каждый свой шаг. На это тоже находится своя целевая аудитория, которая готова это читать, но она становится все менее многочисленной. Чтобы выжить, Twitter нужно остаться в своей нише, при том, что компания стабильно показывает многомиллиардные убытки, несмотря на сотни миллионов пользователей во всем мире. Будет сложно конкурировать с другими сетями. В Twitter добавили графику, но тут есть Instagram, они добавили большую возможность для общения, но тут есть Facebook, можно постить видео, но для этого есть YouTube. Их спасает то, что в настоящее время в Twitter зарегистрировано наибольшее количество известных людей, звезд и президентов.

Главный тренд – смартфоны и мобильный доступ.

Люди привыкли к онлайну. Если раньше нужно было пойти и сесть за компьютер, то сейчас достаточно достать из кармана смартфон. Подумал и сразу зашел в Google и что-то нашел или написал в социальной сети.

Месенджеры заняли новую нишу и пока не отъели аудиторию у социальных сетей. Пользователь, зарегистрировавшись в месенджере, вряд ли перестанет пользоваться любимой социальной сетью. При этом в месенджеры уже начинают добавлять функционал социальных сетей: аватар, формат групп в Viber и формат каналов в Telegram.

Такие тенденции на сегодняшний день. И как всегда бывает в сфере IT – все может измениться за один год. На этом рынке нет гарантии, что при наличии финансирования и количества пользователей, завтра ты не окажешься на обочине истории. Кто сейчас вспоминает про MySpace или где былая слава Yahoo? Все меняется со скоростью света, что только добавляет интереса к интернет-бизнесу!»

***

10.03.2016

Социальные сети: Место для позерства или место, которое поможет заработать деньги?

Молодежь придает большое значение социальным сетям и отводит им значимую роль в своей жизни. В то время, когда начали появляться первые социальные сети, регистрация в них привлекала людей в первую очередь тем, что это давало возможность общаться с теми людьми, общение с которыми несколько проблематично в реальной так сказать жизни. С того времени прошло уже достаточное количество лет, и у многих восприятие социальных сетей поменялось, пишет HiTech-News.ru. Так что же современный пользователь Интернета видит в этих самых социальных сетях?

Конечно, нельзя сказать, что момент общения сегодня отсутствует. Как и раньше, социальные сети позволяют нам найти людей, жизненные пути с которыми разошлись по каким бы то ни было причинам. Но при этом страница в социальной сети может стать источником дохода. Для последнего необходимо лишь раскрутить свою страницу. Общение, которое нам дарят социальные сети, с некоторых пор ушло с первой позиции. Многие люди, которые создают аккаунты и группы, преследуют две цели: заработок и самоутверждение. Последнее больше свойственно молодому поколению, которое ошибочно считают, что удачные фотографии, которые иллюстрируют красивую жизнь, могут создать положительный и социально одобряемый имидж. А если быть точнее, то можно сказать, что в этом есть доля правды, однако мнение общественности, которое формируют социальные сети, ни коем образом не влияет на качество и уровень жизни. Тем самым можно сказать, что социальные сети иногда могут задавать неправильные ориентиры для некоторых представителей молодежи, которых достаточно много.

Среднее поколение достаточно часто расценивает социальные сети как инструмент, способный принести доход. И эта мысль имеет под собой достаточное основание, так как не секрет, что создатели популярных групп в сетях и владельцы популярных аккаунтов, зарабатывают деньги на рекламе. Но можно использовать свою популярность в сети и по-другому, продвигая на своей странице то, чем вы занимаетесь оффлайн.

Можно сказать, что лишь старшее поколение в большинстве своем регистрируется в социальных сетях исключительно для общения. В связи с этим очень интересно будет посмотреть на то, как обстоят дела в социальных сетях лет через тридцать, когда молодежь станет уже старшим поколением.

***

2.03.2016

Yahoo! обесценит купленный за 1,1 млрд долларов сервис Tumblr

Yahoo! может произвести обесценивание нематериальных активов сервиса микроблогов Tumblr, приобретенного интернет-гигантом в 2013 г. за 1,1 млрд долл. Об этом сообщает информационное агентство «Рейтер» со ссылкой на заявление Yahoo, пишет InternetUA.

Основанный в 2007 г. сервис Tumblr позволяет вести микроблоги, публикуя в них статьи, видеоконтент и изображения различных тематик. По состоянию на ноябрь 2015 г. в Tumblr зарегистрировано более 260 млн блогов.

Ранее в феврале 2016 г. Yahoo! объявила об отчислении 230 млн долл. в резервы в связи обесценением активов Tumblr и начала изучать стратегические варианты дальнейшего развития своего интернет-бизнеса.

В I квартале 2016 г. компания намерена потратить на реструктуризацию, которая, в частности, предполагает сокращение рабочих мест, от 64 до 78 млн долл.

К концу 2016 г. Yahoo! собирается уменьшить численность персонала на 15 % и закрыть офисы в Дубае, Мехико, Буэнос-Айресе, Мадриде и Милане.

***

2.03.2016

Facebook изменил алгоритм ленты, отдав предпочтение прямым трансляциям.

Социальная сеть размещает их в топе, вместо обычных видео и архивных фидов. Напомним, два месяца тому Facebook запустил функцию прямых трансляций для всех пользователей. В своем заявление компания отметила, что пользователи проводят в три раза больше времени, просматривая прямые трансляции по сравнению с сохраненными трансляциями. Нововведение позволит пользователям более активно взаимодействовать с видео, размещать вопросы или комментарии. Идея повторяет интеграцию Periscope с Twitter, объединив трансляции с лентой, пишет Marketing Media Review.

***

10.03.2016
Грищенко Д.
Google+ снова ждут перемены. Но есть ли смысл?

На днях в сети появилась информация о том, что основатель крупнейшего мирового имиджборда 4chan К. Пул назначен «волшебником» по части Google+. В компании анонсировали его будущую работу над переосмыслением этого проекта и других продуктов этой мегакорпорации, предназначенных для пользователей социальных сетей, пишет IGate.

Сам К. Пул прокомментировал это вполне радужно, заявив в своем блоге, что с радостью поделится своим многолетним опытом, приобретенным за дюжину лет создания онлайн-сообществ, с такой удивительной компанией, как Google.

Это далеко не первый раз, когда Google заговаривает о необходимости «что-то сделать» с сервисом. Так, можно вспомнить высказывание разработчика и сооснователя поисковой системы С. Брина, заявившего, что он не является особо общительным человеком и «…это, видимо, изначально было моей ошибкой – работать над чем-то, имеющим отношение к социальности».

Сегодня мы расскажем вам о том, почему же так происходит и что мешает амбициозному проекту Google развиваться.

Согласно различным данным, в Google+ от 2 до 2,5 млрд пользовательских аккаунтов. При этом активными пользователями сети являются от 300 до 450 млн человек. Немало. Однако не так уж много. По крайней мере, за Facebook Google+ пока не угнаться.

Проблема в функционале?

Когда речь заходит о непопулярности сервиса, в первую очередь приходит мысль о проблемах с его функционалом. Однако у Google+ с этим, похоже, нет никаких проблем.

Структура Google+ складывается из трех типов виртуальных пространств – личных пользовательских блогов, многопользовательских сообществ по интересам и, наконец, из ряда облаков тэгов, объединяющих посты одной тематики.

Основной фишкой Google+ является разделение личного блога на «круги», в которые можно добавлять своих подписчиков (в один или несколько сразу), таким образом наделяя их правом определенно ограниченного доступа к публикуемой информации. Исходно в Google+ уже включено несколько стандартных кругов (работа, друзья, семья и пр.), но можно создавать и свои собственные.

Можно добавлять и редактировать посты, публиковать фотографии (с подписями в виде популярных «мемов» или «демотиваторов»), видео, делиться интересными постами, найденными в сети. Google+ также позволяет отслеживать активность пользователей в вашем блоге как с помощью почтовых уведомлений, так и с помощью мобильной связи. Казалось бы весь

необходимый функционал в наличии. Однако такого активного пользовательского интереса, как тот же Gmail, он по-прежнему не вызывает.

Проанализировав удобство сервиса, можно лишь продолжать удивляться. Сервис удобен в использовании, не перенасыщен «ненужным», навязчиво предлагаемым функционалом, воплощен в классическом для Google минималистическом стиле. И все же, его редко используют ради развлечения.

Почему?

Говоря о слабой активности пользователей Google+ по сравнению с аудиторией Gmail или YouToube – стоит понимать, что это в первую очередь именно социальная сеть, а не рабочий инструмент и не развлекательный видеоресурс. А социальные сети предполагают высокую интеграцию с реальной жизнью пользователя, при этом зачастую во вне его профессиональной сферы деятельности.

В последнее время в больших социальных сетях высокой популярностью среди публичных лиц стали пользоваться так называемые «публичные» страницы, на которых размещаются лишь так называемые «официальные» факты биографии. А личные страницы либо полностью закрыты для всех остальных пользователей, либо ведутся «под замок» с доступом для очень ограниченного круга лиц.

Все потому, что интегрированность соцсетей в современные СМИ с каждым годом все полнее. Даже в этом материале вы уже увидели пост в Twitter.

Что же мы видим в Google+? Социальная сеть напрямую привязана к нашему аккаунту в Gmail, который в 90 % случаев является рабочим инструментом, по которому мы ведем серьезную деловую переписку с потенциальным работодателем. И от компрометирующих фотографий с последней вечеринки с друзьями, где мы решили расслабиться и повалять дурака, его отделяет всего 1 клик. А Google+ еще и предлагает ему добавить вас в свои круги, так как переписка уже вышла за пределы 1–2 ни к чему не обязывающих писем.

Неловко вышло…

Можно, конечно, не публиковать на своей странице в Google+ таких фотографий, ограничиваясь только той информацией, которую вы хотели бы видеть привязанной к своему рабочему аккаунту. Однако в этом случае сервис становится не полноценной социальной сетью – а скорее эдакой «многофункциональной визиткой», целью которой является высветить вас в наиболее благополучном свете. И летят туда деловые фото, отчеты о презентациях, успешных проектах, влиятельных знакомствах, – но не реальная жизнь. Что мы, собственно, и видим в статистике.

2,5 млрд пользовательских «визиток» Google+ – удобных, красивых, полезных на самом деле. И всего пятая (если не шестая) часть активно ведущихся аккаунтов, часть из которых, к слову, все равно остается преимущественно «деловой».

Куда идти?

Если рассматривать возможные пути развития Google+ как социальной сети – можно отметить два основных направления, одно из которых уже завоевало внимание основного (и единственного) конкурента – Facebook. Это «корпоративная социальная сеть» и «независимая социальная сеть» (ничем, кроме удобства, по сути от того же Facebook не отличающаяся).

И первые шаги в этом плане уже сделаны.

Так, 27 июля 2015 г. Google отменила требование об обязательной привязке аккаунта в Google+ ко всем остальным продуктам компании, пообещав, что вскоре наличие аккаунта в этой социальной сети перестанет быть «обязательным». Также велись разговоры о планах корпорации по изменению самой сути сервиса, однако до недавнего момента далее разговоров дело не заходило.

Что ж, посмотрим, что сможет сделать с этим сервисом такой специалист как К. Пул. Возможно, уже в ближайшем будущем Google+ нас приятно удивит.

***

13.03.2016

Google запустил новую социальную сеть Create на основе Google

Американский поисковик Google запустил новую социальную сеть Create на основе Google. Новшество позиционируется своими создателями в качестве площадки для творческих людей с богатой фантазией, которые смогут с помощью ресурса рассказывать о себе и знакомиться с единомышленниками, пишет U-News.

Американские разработчики воспользовались его возможностями, чтобы создать нечто новое. Именно новый проект и получил название Create. Как сообщают его создатели, ресурс будет являться идеальным местом для творческих людей со всего мира.

Основа работы Create будет зиждиться на выставлении разнообразных интересных изображений, которые и будут оцениваться пользователями. Что примечательно, так это политика руководства Create: только часть избранных пользователей получит свои аккаунты в новой соцсети после того, как желающий сможет уверить специальную комиссию в собственной креативности.

***

11.03.2016

Соцсеть Facebook оформила патент на распознавание интернет-жаргона

Популярная социальная сеть Facebook некоторое время назад оформила патент на распознавание интернет-жаргона. Программа будет заносить новые

слова, аббревиатуры и неологизмы в специальный виртуальный словарь, пишет HiTech-News.ru.

В социальной сети Facebook появился специальный виртуальный «социальный словарь», который будет фиксировать новые слова, фразеологизмы, аббревиатуры, часто используемые в сети. Таким способом создатели соцсети хотят научиться распознавать интернет-жаргон.

Все слова и фразеологизмы будут заноситься в словарь по решению пользователей соцсети Facebook путем специальных опросов. Представители соцсети также отметили, что любые заинтересованные компании могут воспользоваться платной подпиской на обновления данного словаря.

Неологизмами станут считаться слова, которые будут наиболее часто использоваться людьми, проживающими в одном регионе и разговаривающими на одном языке.

***

7.03.2016

«ВКонтакте» масштабно обновила Android-приложение

«ВКонтакте» выпустила большое обновление клиента для платформы Android. Разработчики полностью обновили дизайн приложения и добавили новые функции. Примечательно, что, исключив в прошлом году аудиоплеер из версии для iOS, «ВКонтакте» не только оставила музыкальный проигрыватель в новой версии Android, но и похвасталась улучшениями в его дизайне, пишет InternetUA.

Самое полезное улучшение в обновленном клиенте – новый принцип обновления ленты. Теперь свежие записи подгружаются автоматически, и читать их можно обычным пролистыванием ленты вверх. При этом остались и возможность обновить ленту вручную, и кнопка для перехода к самым свежим записям. Также время от времени в ленту добавляют блок с людьми, которых может знать пользователь или на которых решит подписаться.

Ссылки в записях теперь открываются во встроенном браузере. По словам разработчиков, это быстрее и зачастую удобнее, чем запускать браузер отдельным приложением. При этом всегда можно в два клика открыть ту же ссылку в стороннем браузере.

Изменения в профилях заметнее всего: в самом верху пользователя встречает большая фотография его владельца. Ниже – основная информация вроде количества друзей, места проживания и места работы. Там же есть ссылка на более подробную информацию.

Есть и изменения в сообщениях. Кнопка «Новое сообщение» внизу теперь разворачивает топ-5 друзей пользователя и предлагает создать беседу.

Кроме того, социальная сеть изменила внешний вид просмотрщика фотографий и аудиоплеера.

О сроках релиза обновленного клиента «ВКонтакте» для iPhone и iPad не сообщается.

***

7.03.2016

Instagram разрабатывает свое универсальное приложение

Так уж сложилось, что официальный клиент Instagram для смартфонов с Windows – это вечная «бета», устаревшее приложение, которое никогда не обновляется. Если бы не общепризнанное стороннее приложение 6tag, то любителям обмениваться фото и видео пришлось бы совсем туго. Изменится ли такое положение вещей? Да, по-видимому, да! И это, вероятно, не займет много времени, пишет InternetUA.

Итальянскому ресурсу WindowsBlogItalia удалось заполучить в свои руки бета-версию нового официального клиента, написанного в формате универсального приложения. Приложение разрабатывается с использованием инструмента Project Islandwood, а потому является обычным портом версии Instagram для iOS.

В настоящее время Instagram для Windows 10 Mobile находится на стадии закрытого тестирования, так что установить его могут лишь избранные, но публичная версия может быть выпущена относительно быстро. Что касается неисправностей в текущей версии, то источник отмечает сбои при попытке открыть галерею, при использовании камеры и т. д.

Более интересно отметить, что, будучи портом версии для iPhone, Instagram для Windows 10 Mobile наследует все возможности оригинального приложения. По той же причине его интерфейс не очень соответствует канонам дизайна операционной системы от Microsoft. Но не исключено, что по мере продвижения работы разработчики приведут в порядок и визуальную составляющую.

***

10.03.2016

Доступна бета-версия Facebook Messenger для Windows 10

В магазине Windows появилась бета-версия (порт с iOS) универсального приложения Facebook Messenger, которая предлагает большинство функций, присутствующих в версии Messenger для мобильных устройств. В настоящее время приложение поддерживает x86-архитектуру, т. е. его можно установить только на устройства под управлением настольной версии Windows 10, пишет InternetUA.

Особенности приложения:

– поддерживаются уведомления, так что вы никогда не пропустите ни одного сообщения;

– информация о новых сообщениях на динамической плитке;

– возможность отправки фото, видео, файлов GIF и много другого;

– поддержка стикеров в разговорах;

– возможность узнать, когда люди увидели ваше сообщение;

– можно создавать группы, давать им имена и устанавливать фото;

– переадресация сообщений или фотографий, которые не являются частью разговора;

– поиск людей и групп.

***

8.03.2016

Соцсеть «Одноклассники» готовится к монетизации собственных видеосервисов

Социальная сеть «Одноклассники» планирует полностью монетизировать свои видеосервисы в конце 2016 – в начале 2017 г., пишет Inshe.tv.

Об этом заявил накануне руководитель российской компании А. Федчин на пресс-конференции в Москве, сообщает ТАСС.

В настоящее время социальная сеть Odnoklassniki.ru (OK.ru) активно развивает свои видеосервисы. Ранее компания запустила сервис групповых трансляций в режиме реального времени и приложение для Smart TV.

Как отмечается, в конце апреля 2016 г. «Одноклассники» планируют запустить приложение для смартфонов, которое позволит вести онлайн-трансляции в соцсети. Сейчас на рынке уже есть такие сервисы, в том числе американские Periscope (принадлежит Twitter) и Snapchat.

Аудитория «Одноклассников» по состоянию на январь составляет 51 млн человек в сутки (по Liveinternet). Месячная мобильная аудитория насчитывает 64 % от общего числа активных пользователей. Ежедневно видеоплатформой соцсети пользуются 20 млн уникальных пользователей с количеством просмотров в 300 млн.

***

14.03.2016

Сидорин С.

«Одноклассники» представили приложение для Smart-TV «ОК Видео»

Российская социальная сеть «Одноклассники» предоставила пользователям возможность просмотра онлайн-телевидения. На днях соцсеть представила приложение для Smart-TV под названием «ОК Видео». Благодаря приложению пользователи смогут просматривать на телевизионном экране не только контент, загруженный другими людьми, но и различные фильмы, предоставляемые организациями-партнерами, пишет HiTech-News.ru.

Приложение «ОК Видео» будет самостоятельно выбирать качество воспроизводимого контента в зависимости от скорости соединения с Интернетом, разрешения видео и диагональ экрана. При этом пользователь может сам регулировать качество видеозаписи вплоть до максимального разрешения – Ultra HD (4K).

Первое время «ОК Видео» работает лишь на телевизорах Samsung и доступно для скачивания в интернет-магазине Samsung Smart TV. В будущем разработчики планировать адаптировать приложение для работы на телевизорах других производителей.

***

7.03.2016

До кінця століття Facebook перетвориться на віртуальний цвинтар

Згідно з недавніми аналізами статистики Facebook, до кінця цього століття соцмережа перетвориться на найбільший у світі віртуальний цвинтар, пише bublbe.com з посиланням на інтернет-портал Daily Mail.

Відмова Facebook від автоматичного видалення мертвих користувачів призведе до того, що їх стане більше, ніж живих. Експерти також дійшли висновку, що зростання кількості користувачів соцмережі скоро значно сповільниться.

За розрахунками вчених, до 2098 р. кількість сторінок померлих користувачів перевищить кількість живих людей, які спілкуються на сайті. Проблема в тому, що адміністрація Facebook не видаляє із соціальної мережі сторінки користувачів у разі їхньої смерті. Дослідники припускають, що в майбутньому позиція компанії щодо цього питання навряд чи зміниться. Представники Facebook відмовилися від коментарів з приводу заяви вчених.

Подібна політика адміністрації Facebook викликає постійну хвилю обурення з боку родичів і друзів померлих людей, які, крім усього іншого, продовжують отримувати від них сповіщення

***

15.03.2016

Яровая М.

Wire – тот же Skype, но без рекламы, который шифрует не только переписку, но и звонки

Сооснователи Skype создали конкурента своему же детищу по принципу «быстрее, сильнее, выше». Сервис Wire – это те же голосовые и видеозвонки, групповые чаты, только без рекламы и с end-to-end шифрованием всех разговоров, переписок и файлов. Сервис доступен в веб-версии и в качестве отдельного десктопного приложения для Windows и Mac. Также у Wire имеются приложения для мобильных платформ iOS и Android, пишет AIN.UA.

Интерфейс и юзабилити Wire мало чем отличается от большинства мессенджеров. В нем аналогично отображаются ссылки на сайты, социальные сети, видео из YouTube и других подобных сервисов. Регистрация в Wire требует верификации по email, и пока у сервиса нет проблем с выбором имени пользователя.

Шифрование в Wire реализовано на базе открытого кода, который может проанализировать любой желающий. По словам разработчиков, на сегодня Wire – единственный сервис, который шифрует не только переписку, но и разговоры, видео, групповые чаты. Если верить сравнительной таблице на сайте сервиса, новый мессенджер и VoIP-сервис даже более защищен, чем Telegram.

Wire создали разработчики Skype во главе с сооснователем сервиса Я. Фрисом, который стал исполнительным председателем и соинвестором в новом стартапе. Компания зарегистрирована в Швейцарии, там же находится и офис.

Традиционное швейцарское уважение к личной информации и частной переписке нашло отображение и в сервисе: в Wire не продают персональные данные пользователей рекламодателям. Бизнес-модель для Wire пока не нашли. По словам основателей, сейчас цель сервиса – как можно быстрее набрать обороты и пользовательскую базу. А о способах монетизации разработчики подумают позже.

Напомним, end-to-end шифрование – это когда информация шифруется на устройстве-отправителе и расшифровывается на устройстве-получателе без участия сервера. То есть сам сервис не «видит» ваши сообщения и не сможет раскрыть их содержимое даже по требованию спецслужб. Только участники переписки будут иметь к ней доступ. Эту технологию используют большинство современных мессенджеров, в том числе WhatsApp и Telegram.

***

16.03.2016

Instagram вводит новые «правила» для фотографий

Сервис размещения фотографий Instagram поменяет принципы формирования ленты новостей, передает «Укринформ». Лента будет формироваться с помощью алгоритма, учитывающего несколько факторов. Среди них – вероятность того, что пользователю понравится фотография или видео, связи с аккаунтом, где была размещена публикация, а также время публикации, пишет МОСТ-ДНЕПР.

Изменения алгоритма будут происходить постепенно. В ближайшие месяцы Instagram перейдет на формирование ленты только на основе популярности фотографий и видео, потом алгоритм будет усложнен.

На сегодняшний день лента формируется в хронологическом порядке. В будущем принципы появления формирования ленты будут похожи на те, что применяются в Facebook. «Возможно, вы будете удивлены, узнав, что в среднем люди пропускают 70 процентов своих лент. Поскольку Instagram вырос, стало сложнее отслеживать все фотографии и видеозаписи, которые выкладывают люди. Это значит, что вы очень часто не видите наиболее важные посты», – сообщили в Instagram.

***

15.03.2016

Samsung готовит к запуску социальную сеть

Южнокорейская компания Samsung готовит к запуску социальную сеть Waffle, говорится в сообщении компании, пишет Украинские реалии.

Главная особенность этой соцсети – коллективное создание контента: пользователи могут делать совместные коллажи, присоединяя к уже загруженным друзьями изображениям свои фотографии, рисунки и подписи. Контент в сервисе будет представлен в виде «коллективного граффити», которое по виду напоминает вафли, откуда и название сервиса, пишет Samsung.

Waffle разработана подразделением Samsung под названием C-Lab (разрабатывает и тестирует новые сервисы). Она была представлена на американском медиафестивале SXSW 2016. Приложение еще находится в разработке, beta-версия доступна для устройств на операционной системе Android.

Samsung может закрыть проект Waffle летом 2016 г., если он не оправдает ожиданий, сообщил американский сайт the Verge со ссылкой на представителя компании. Однако в случае его популярности компания запустит полноценный мобильный сервис как на Android, так и на iOS.

На рынке уже существуют социальные сети, главным контентом которых являются фотографии пользователей, среди них – Instagram и Snapchat. Ресурс Mashable уже охарактеризовал новинку как «мультиплеерный Snapchat».

***

14.03.2016

Большинство украинцев узнают новости из интернет-СМИ, а не из печатных, – опрос

Опрос Института Горшенина, проведенный с 8 по 17 февраля, свидетельствует о том, что подавляющее большинство граждан Украины получает информацию о ситуации в государстве из программ украинского телевидения, пишет МОСТ-ДНЕПР.

Респондентам было предложено назвать не более трех основных источников, из которых они чаще всего получают информацию о событиях в стране. Были получены следующие результаты:

– украинские телеканалы – 88,0 %;
– разговоры с родными, друзьями, знакомыми – 31,9 %;
– украинские новостные интернет-сайты – 29,9 %;
– местные печатные издания – 15,1 %;
– всеукраинские печатные издания – 12,5 %;
– радиоканалы FM-диапазона (радиоприемник) – 9,5 %;
– социальная сеть «ВКонтакте» – 8,5 %;
– российские телеканалы – 8,0 %;

– социальная сеть Facebook – 7,2 %;
– российские новостные интернет-сайты – 5,8 %;
– социальная сеть «Одноклассники» – 5,3 %;
– стационарная радиоточка (проводное радио) – 5,1 %;
– зарубежные новостные интернет-сайты – 4,3 %;
– зарубежные телеканалы – 1,5 %;
– социальная сеть Twitter – 1,2 %;
– другие источники – 0,5 %;
– меня не интересуют новости – 1,8 %.

Всего согласно выборке, с учетом основных социально-демографических характеристик населения Украины, было опрошено 2000 респондентов в возрасте от 18 лет, во всех регионах Украины (без учета населения оккупированных территорий АР Крым, Донецкой и Луганской областей). Квотами были регион проживания, пол и возраст респондентов. Погрешность репрезентативности исследования не превышает +/-2,2 %

***

18.03.2016
Бовкун О.
Twitter с 15 апреля закрывает десктопный клиент TweetDeck

Социальная сеть Twitter с 15 апреля планирует закрыть десктопный клиент TweetDeck для операционной системы Windows. Попасть на приложение теперь можно будет через отдельный веб-сайт, пишет HiTech-News.ru.

Помимо прочего, в связи с новыми изменениями, доступ ко всем версиям TweetDeck значительно облегчается: зарегистрированные пользователи смогут автоматически попасть в приложение. В заявлении пресс-службы компании также содержатся инструкции относительно доступа к TweetDeck через панель задач браузера Chrome.

***

18.03.2016
Twitter змінив алгоритм формування стрічки для всіх користувачів

Twitter зробив за замовчуванням алгоритм формування новинної стрічки на основі переваг користувачів. Щоб повернутись до попереднього, хронологічного, варіанта видачі, необхідно внести зміни до налаштувань, пише UkrainianWatcher.

Новий алгоритм Twitter ввів ще на початку лютого, але він не вмикався за замовчуванням для користувачів. Головна його ідея полягала в тому, щоб відображати твіти не в хронологічному порядку, а на основі інтересів користувачів.

***

19.03.2016

Американские ученые создали распознающую «пьяные» твиты нейросеть

Американские ученые разработали нейросеть, способную распознавать в Twitter посты, написанные в состоянии алкогольного опьянения. Кроме того, полученная математическая модель может определять, где авторы «пьяных» постов находились в момент их написания. Об этом сообщает InternetUA со ссылкой на MIT Technology Review.

Для создания нейросети специалисты из Рочестерского университета в течение года собирали твиты, в которых используется «алкогольная» лексика. Анализ около 11 тыс. постов помог установить, является ли автор сообщения тем, кто пьет спиртное, и был ли твит написан непосредственно во время употребления напитка.

Ученые также решили определить, откуда пользователи чаще всего пишут «пьяные» твиты. Чтобы понять, находился ли автор поста дома, анализировалось употребление специфической «домашней» лексики (например «диван» или «ванна»). Кроме того, использовались данные геолокации.

В дальнейшем авторы исследования хотят научить нейросеть определять пол, возраст, этническую принадлежность и иные особенности по записям в Twitter. Ученые считают, что это поможет в изучении влияния алкоголя на здоровье.

***

16.03.2016

YouTube запускает функцию мгновенного просмотра закэшированного видео

Видеохостинг YouTube приступил к тестированию Accelerator – возможности мгновенного просмотра закэшированного видео, пишет InternetUA.

Первой страной, где данная функция будет опробована, станут Филиппины.

На старте программа предложит пользователям подключиться к 12 точкам доступа (их расположение можно посмотреть на карте), где они, независимо от интернет-соединения, смогут посмотреть 100 тыс. самых популярных в стране видео. Ролики, которые можно посмотреть мгновенно, будут отмечены специальным значком.

Когда данная возможность появится в других странах, пока неизвестно.

***

20.03.2016

Twitter не будет менять стандарт твитов в 140 символов

Сервис микроблогов Twitter не будет изменять ограничение на твиты в 140 символов, несмотря на слухи. Об этом сообщает Bloomberg, пишет InternetUA.

«Все остается. Это хорошее ограничение для нас, помогает быть кратким», – отметил глава Twitter Д. Дорси.

В январе сообщалось, что разработчики Twitter планируют увеличить количество возможных символов для публикации записей до 10 тыс. знаков.

***

13.03.2016

В блогах WordPress появится поддержка «мгновенных статей» Facebook

Пользователи, постоянно читающие новости через Facebook, наверняка не раз сталкивались с так называемыми «мгновенными статьями» (Instant Articles), позволяющими очень быстро загружать материалы на мобильных устройствах. Пока такая возможность доступна лишь ограниченному числу издательств, но с 12 апреля технология станет доступна всем, включая блогеров. Facebook объединилась с корпорацией Automattic, известной благодаря созданию сервиса WordPress, чтобы позволить блогерам по всему миру делиться в социальной сети своими статьями, которые будут загружаться в 10 раз быстрее, чем обычно, пишет InternetUA.

В частности, две компании объединили усилия для создания плагина с рядом встроенных в него инструментов, позволяющих подготовить блог на базе WordPress к глобальному запуску «мгновенных статей». Среди этих инструментов – возможности, позволяющие блогерам публиковать автоматически проигрываемые видеоролики и создавать галереи с функцией увеличения изображений простым нажатием на них пальцем. Все эти инструменты позволят сделать публикации в блогах куда более привлекательными.

Для Facebook это очень важный шаг, особенно если учесть, что на WordPress работает более четверти сайтов в Интернете. Компания заверила, что её плагин будут поддерживать все стандартные шаблоны, однако также предупредила, что если владелец сайта изменял свои шаблоны, то ему придётся настроить плагин для его оптимальной работоспособности.

***

18.03.2016

Бондаренко А.

Запуск магазина ботов Facebook может стать самым значимым событием со времен App Store

Если раньше о том, что боты становятся основным технологическим трендом, говорили аккуратно и как бы между делом, то в последние пару месяцев это стало притчей во языцех. Таким образом колонка Т. Хедфилда на TechCrunch о появлении магазина ботов Messenger Bot Store становится манифестом грядущих перемен, пишет AIN.UA.

Мы уже описывали предсказания на этот год, которые сходятся с мыслями Т. Хедфилда. Похоже, в апреле, на конференции F8, все станет на свои места – если Facebook представит Messenger Bot Store.

Если Facebook таки анонсирует магазин на F8, как многие предсказывают, это будет, возможно, наиболее важным событием в технологической индустрии с того момента, как Apple презентовали App Store и SDK iPhone в марте 2008 г.

Тогда даже С. Джобс не мог предположить, насколько большое влияние окажет, как он описывал, «новое приложение, которое позволяет пользователям искать, покупать и скачивать приложения от других компаний прямо на их iPhone».

К тому моменту как открылся App Store (в июле 2008 г.), iPhone был приблизительно у 6 млн пользователей по всему миру. Количество владельцев удвоилось к концу года, и каждый последующий год продажи этих смартфонов удваивались и удваивались. Экосистема App Store – в рамках которой работает более 1,5 млн iOS-приложений – стала предвестником новой эры «мобайл».

В настоящее время у Facebook Messenger 800 млн ежемесячных пользователей – число, превышающее количество пользователей iPhone на момент запуска App Store более чем в 100 раз. Нынешняя база пользователей Messenger вообще превышает общее количество когда-либо проданных iPhone. У мессенджеров больше активных пользователей, чем у социальных сетей.

В январе появились первые слухи о секретном Chat SDK от Facebook для создания ботов под Messenger. Когда и если Facebook представит Bot Store, это станет «концом начала» новой эры: переписка как платформа. Диалоговые интерфейсы изменят способ взаимодействия с миром миллиардов пользователей.

С чего начиналась переписка как платформа

Появление нынешней волны интереса к «переписке как платформе» можно проследить в начале прошлого года. В марте 2015 г. Magic, ассистент по покупкам на базе SMS, был самой желанной компанией демо-дня Y Combinator, и поднял 12 млн долл. от Sequoia. В последующие месяцы GoButtler, практически идентичный сервис, поднял 8 млн долл. от General Catalyst и Operator поднял 10 млн долл. от Greylock. Внезапно все заговорили о битве на новом технологическом рубеже.

Летом информационное пространство взорвала новость о том, что Facebook M, построенный на искусственном интеллекте, позволит пользователям Messenger совершать покупки, бронировать места в ресторанах, билеты на самолеты – и все это в рамках диалогового интерфейса.

П. Дуров анонсировал расширение Telegram Bot Store, а Т. Ливингстон заявил, что Kik станет «западным WeChat». К концу года Slack анонсировал Slack App Directory, поддержанную 80 млн долл. инвестиций на рост экосистемы, а Google, по слухам, разрабатывает собственных чат-ботов.

«Ботовая» лихорадка

С тех пор постоянно говорят о поиске самого крутого бота. Все только начинается, но мы уже видим венчурные инвестиции под боты вроде Howdy, Assi.st, Hyper, Scout, Luka и Rep. Параллельно другие стартапы, такие как Pandorabots и Prompt, концентрируются на создании инструментов для разработчиков ботов.

Некоторые из топовых инвесторов Долины делают ставки. Ф. Либин из General Catalysr описывает ботов как «наиболее важный технологический тренд года», А. Венгер из Union Square Ventures описывает эту новую эру как «Ботовая лихорадка» (более привлекательная фраза, чем «Ботагеддон»). Всего пару дней назад Д. Лилли из Greylock затвитил, что «процент питчей от ботов и/или ИИ-компаний достигает 100 %». Инвесторы, глядящие в будущее, вроде Б. Ветца, Д. Морина, С. Шаха и Н. Ейала тоже очень заинтересованы.

Боты – это новые приложения

Messenger Bot Store повлияет не только на предпринимателей и инвесторов, но и на разработчиков и дизайнеров. С. Лессин, CEO Fin, говорит, что рост диалоговых интерфейсов приведет к «фундаментальному сдвигу в типах приложений и стиле разработки».

К. Мессина как-то удачно предсказал, что 2016 г. будет «годом диалоговой коммерции», но бот-платформа Messenger идет дальше коммерции.

Переписка станет командной строкой реального мира – в то же время она будет отличаться от командной строки, с которой мы знакомы. Учитывая последние достижения в обработке человеческой речи, синтаксис общения с ботами будет куда менее грубым, нежели командная строка в последние десятилетия.

В какой-то момент с ботами можно будет общаться обычным языком, часто такую модель называют «невидимыми приложениями». Как говорит Д. Либов из USV, «просто потому что оболочкой является мессенджер, это не значит, что внутри приложения построены на тексте». Т. Штольфа говорит, что существует «неисследованный потенциал насыщения диалоговых интерфейсов богатыми графическими элементами».

Если 800 млн пользователей Facebook откроют для себя ботов в Messenger после F8, это подтвердит слова всех тех, кто говорит, что боты – это новые приложения.

Но поверх этого нужно строить целую экосистему, сродни по масштабам с App Store. Если вы сможете легко взаимодействовать с Dominos, United Airlines и Capital One через Messenger, будет ли у вас желание продолжать пользоваться их нативными приложениями? Нынешний ландшафт ботов очень напоминает Интернет в 1995-м или мобильные приложения в 2008 г.

Остается еще один важный вопрос: как скоро другие мессенджеры, вроде WhatsApp, тоже откроют свои платформы для разработчиков? Будет ли это похоже на OpenTable, с созданием ботов под каждую отдельную платформу или появятся какие-то кроссплатформенные стандарты разработки? И, что еще более важно, в каких случаях переписка может оказаться более удобным решением, чем традиционные нативные приложения?

Д. Либов прав в своем наблюдении, что «интерес разработчиков в переписках/ботах намного, намного опережает интерес пользователей на данный момент». Но если предсказания Т. Ливингстона верны, то все изменится на F8 12 апреля.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

14.03.2016

Структурні підрозділи Мукачівського виконкому «вийшли» у соцмережі

Структурні підрозділи міськвиконкому зареєстровані в мережі Facebook, повідомляє Інформаційно-аналітичний сайт Zaholovok.com.ua.

Це зроблено заради комунікацій із громадськістю та інформування про роботу підрозділів.

Так, створено сторінки 13 структурних підрозділів міськради та міськвиконкому. Зокрема, у мережі вже є: відділ по роботі з депутатами та постійними комісіями, юридичний відділ, відділ з питань внутрішньої політики, відділ у справах молоді та спорту, відділ культури, відділ охорони здоров'я, управління освіти, управління праці та соціального захисту населення, управління містобудування та архітектури, управління економіки та транскордонного співробітництва, фінансове управління, управління міського господарства, управління комунальної власності та ЦНАП, пише Мукачівська міськрада.

***

14.03.2016

У соцмережах закликають підписати петицію про заборону російського контенту

Петиція українських митців про заборону російського контенту зібрала 47 % необхідних підписів за половину відведеного терміну, пише Західна інформаційна корпорація.

Про це йдеться на сторінці Бойкоту російського кіно у Facebook.

Організатори закликають усіх блогерів та публічних осіб, усі патріотичні рухи та організації, усі проукраїнські ЗМІ та журналістів підтримати цю петицію й залучити якомога більше людей до її підписання.

«Якщо ми не активізуємося, то вона (петиція. – Ред.) не встигне набрати голосів. Наша аудиторія в соцмережах – тисячі. Поки ми боремося за кожен голос, проросійські медіа рясно засівають рашаконтент серед мільйонів українців. Тому кожен, хто знає про цю петицію, має її підписати», – повідомляють на сторінці.

Подається текст петиції, докладна інструкція з підписання петиції та інформація для тих, хто не вірить у петиції.

***

19.03.2016

Папа Римский завел аккаунт в Instagram

Папа Римский Франциск завел аккаунт в Instagram и опубликовал в нем первую фотографию. Об этом предстоятель Римско-католической церкви сообщил в своем официальном аккаунте в Twitter, пишет InternetUA.

«Я начинаю новое путешествие в Instagram, чтобы идти с вами по пути доброты и милосердия бога», – сообщил Франциск.

В комментарии к фотографии он написал «Молитесь за меня» на девяти языках.

На аккаунт в Instagram за три часа его существования подписалось более 422 тыс. человек.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

2.03.2016

Facebook заплатит знаменитостям за видеотрансляции

Facebook начнет платить известным людям за использование сервиса прямых видеотрансляций Live. В продвижении сервиса поучаствуют актеры, комики, телезвезды и знаменитые интернет-персоны, пишет InternetUA со ссылкой на Re/Code.

Всего к продвижению проекта планируется привлечь около 100 знаменитостей, сообщила операционный директор Facebook Ш. Сандберг. Предполагается, что они станут использовать Live на регулярной основе, а доход от рекламы в их трансляциях будет делиться между компанией селебрити по аналогии с тем, как это уже делает YouTube.

В Facebook считают, что в долгосрочной перспективе проект поспособствует росту рекламных доходов. Представители соцсети отметили, что пока только изучают способы монетизации сервиса, но обратили внимание на то, что Live является приоритетом для главы компании М. Цукерберга.

***

3.03.2016

Число активных рекламодателей Facebook превысило 3 миллиона

Facebook объявил, что число активных рекламодателей на площадке превысило 3 млн. При этом большая часть из них – это представители малого и среднего бизнеса. 70 % из этих компаний находится за пределами США. Самым быстрорастущим рынком является Юго-Восточная Азия, а в число самых быстроразвивающихся стран вошли Вьетнам, Египет, Индонезия, Перу и Турция, сообщает МедиаБизнес со ссылкой на searchengines.ru.

Топ-5 стран по абсолютному росту рекламодателей в сравнении с прошлым годом составили США, Бразилия, Великобритания, Италия и Австралия.

Страницы в Facebook ведут более 50 млн малых предприятий. Ежемесячно пользователи оставляют на них более 2,5 млрд комментариев, а свыше 1 млрд человек подписаны на новости как минимум одной компании. В России более 39 % пользователей следят за обновлениями небольших компаний. Среди владельцев страниц преобладают представители трёх типов бизнеса: услуги, местные торговые предприятия и интернет-торговля.

Чтобы отметить успех этих компаний Facebook запускает новый инструмент – Your Business Story (История вашего бизнеса) yourbusinessstory.fb.com. Он позволит предпринимателям создать короткое видео о своём бизнесе и рассказать о его результатах. В ролики можно загрузить фотографии со страницы компании, добавить музыкальное сопровождение и поделиться ими со своей аудиторией.

В Facebook также рассказали, что более 1 млн рекламодателей настраивает рекламу прямо с мобильного устройства, а свыше 20 млн компаний с активными страницами используют приложение Pages Manager.

***

16.03.2016

Секреты успешного контента в соцсетях от Buzzsumo

Сервис Buzzsumo опубликовал исследование о том, как брендам повысить эффективность работы с Facebook и увеличить охват публикаций в Facebook. Исследование базируется на анализе 1 млрд постов, размещенных в январе 2016 г. в пабликах 3 млн брендов, включая как небольшие, так и всемирно известные компании, пишет МедиаБизнес.

Среди ключевых рекомендаций:

- ✓ лучше всего публиковать посты между 22.00 и полуночью, а также в воскресенье;
- ✓ сопровождать посты иллюстрациями и вопросами;
- ✓ включать в посты линки (оптимально – ссылки на статьи от 1000 до 3000 слов), а также ограничивать посты по размеру (короткие посты читаются лучше длинных);
- ✓ видео, загруженные напрямую в Facebook, обеспечивают лучшее вовлечение, чем ссылка на видео YouTube;
- ✓ посты с хештегами имеют меньшее вовлечение аудитории, чем без хештегов;
- ✓ у фото, загруженных в Facebook через Instagram, на 23 % больше взаимодействий, чем у фото, размещенных в Facebook напрямую.

***

9.03.2016

Facebook Atlas позволил брендам учитывать данные об офлайн-продажах в рекламных кампаниях

Кросплатформенный рекламно-аналитический сервис Facebook Atlas ввел функцию Offline Actions, которая позволит маркетологам загружать данные о покупках с мест продаж и анализировать их в контексте рекламных кампаний, сообщает МедиаБизнес со ссылкой на sostav.ua.

Опция должна дать рекламным специалистам понимание того, какой эффект они получают от кампаний в Facebook в своих офлайн-продажах.

Также Facebook добавил метрику Path to Conversion, которая позволит маркетологам понять, какая именно реклама – мобильная или десктопная – способствует продажам. Например, эта функция поможет сравнить эффект от двух мобильных объявлений с мобильной рекламой, сопровождающейся десктопной промокампанией.

«Это дает представление о том, как реальные люди (а не куки) просматривают рекламу с разных устройств», – объясняет вице-президент по рекламе в Facebook Б. Боланд. Данные нововведения помогут оптимизировать кампании – как до запуска так и в период проведения.

К концу марта в Facebook Atlas будет доступна видеореклама.

***

15.03.2016

10 порад для SMM та журналістики даних від Socialbakers

Socialbakers – всесвітньо відома аналітична компанія з Чехії, яка досліджує соціальні мережі, SMM та все, що з цим пов’язано. Існує безліч унікальних інструментів для роботи з даними в Інтернеті, однак не всі з них є достатньо відомими. Й. Шлерка, співзасновник Socialbakers, розповідає про

деякі з них та ділиться власними секретами роботи з інформацією. До вашої уваги – 10 порад для ефективнішої праці в мережі, пише UkrainianWatcher.

1. Машина часу

Існує корисний сервіс Archive.org з досить цікавою опцією Wayback Machine, яка дасть змогу здійснити своєрідну подорож в минуле. Цей ресурс щодня робить скріншоти різних сайтів в мережі. І якщо ви хочете глянути, як виглядала головна сторінка якого-небудь сайту (а особливо це цікаво для ЗМІ) 2, 5 чи навіть 7 років тому – просто введіть у спеціальне поле його адресу. Деколи скріншоти є доступними для кожного дня, деколи – раз на місяць, залежно від популярності сайту. Відвідати можна навіть ті сторінки, яких вже давно не існує – вся інформація запам'ятовується в мережі. Більше того – ресурс зберігає оригінальну структуру сайту, тому можна клікати на посилання, розміщені на його головній, та переглядати їх.

2. Пошук документів

Дуже часто в документах можна знайти багато корисної інформації, зокрема про посадових чи публічних осіб. Наприклад, адреси електронних скриньок чи навіть номери їхніх телефонів, якщо пощастить. Інформація може зберігатись у документах Word, таблицях Excel чи навіть презентаціях Power Point – Google знайде все, що існує в мережі. Для цього після ключової фрази пошуку (наприклад, «Яценюк +380») слід додати ext:doc/xls/ppt/pdf/… (в залежності від того, який тип документа вам потрібен) – і пошуковик видасть результати лише за вашим конкретним запитом, якщо вони є.

3. Розширений пошук

Для того, щоб зробити свої пошуки в мережі більш ефективними, в Google існує опція Advanced Search. Вона дозволяє максимально деталізувати свій запит й знайти саме те, що потрібно. Результати пошуку можна фільтрувати за мовою, регіоном, наявністю або відсутністю ключових слів, конкретним сайтом, відвіданими сторінками, часом публікації тощо. Таким чином, відсіяти усе зайве й зробити запит якомога конкретнішим буде значно легше.

4. Хвиля трендів

Google Trends – чудовий сервіс, з допомогою якого ви можете відслідковувати активність тих чи інших пошукових запитів. Наприклад, задавши в пошук War in Ukraine, можна помітити, що тема України у світі вже давно не на першому місці. Статистика Google також показує «найактивніші» країни та міста, період, кількість запитів та ін. Крім того, можна відсортувати дані за регіоном чи окремими відрізками часу й таким чином отримати якомога детальнішу інформацію з красивим графіком. Для журналістів (зокрема аналітиків) цей ресурс є корисним для моніторингу того, як змінюються зацікавлення людей певними темами чи персонами. Особливо цікаво спостерігати за динамікою змін у передвиборчий період – на основі статистики Google можна зробити висновки про ріст популярності політиків серед електорату.

5. Сповіщення

Припустимо, ви цікавитесь виборами у США й періодично пишете про це журналістські матеріали. Однак постійно відслідковувати новини західних ЗМІ забирає багато часу й втомлює. Тут у пригоді стане ще один сервіс – Google Alerts, який сам присилатиме вам сповіщення про нові публікації з ключовими словами. Параметри відбору новин ви задаєте самі: можна вибрати мову, джерела інформації, частоту та кількість звітів тощо. І вказавши, скажімо, Donald Trump, ви будете щодня отримувати на електронну скриньку з обраних вами джерел найсвіжіші новини, пов'язані з Д. Трампом. Все просто.

6. **Люди в соцмережах**

Facebook пропонує цікавий сервіс, який називається Audience Insights. Першочергово така опція створювалась для компаній, які хочуть рекламувати свої товари через Facebook, але вона дає чудові можливості також і журналістам – для аналізу поведінки суспільства в соцмережах. Фільтрувати свої запити можна як завгодно – за конкретним населеним пунктом, за віком, статтю, зацікавленнями, соціальним статусом, освітою, сімейним станом тощо. Таким чином можна дізнатись, що найбільше цікавить людей певної категорії та краще дослідити центральну аудиторію свого ЗМІ. Крім того, за допомогою Audience Insights можна моніторити поведінку не лише своїх, а й чужих підписників. Ідеться про сторінки медіа, політиків, брендів, партій, кого завгодно. Це дасть краще розуміння того, ким є їхня аудиторія та що від неї можна очікувати. Щоб побачити статистику якої-небудь сторінки, слід просто ввести у полі Interests (внизу правої панелі) її назву – і Facebook розповість про її прихильників усе, що знає.

7. **Всі лайки в одному місці**

Якщо ви займаєтесь SMM чи дослідженнями соціальних медіа, є один сервіс, який стане для вас незамінним – це Netvizz. Він орієнтований на Facebook і агрегує дані з різних його секцій (групи, сторінки, пошук), збирає та сортує їх. Netvizz пропонує користувачам декілька функцій. Link stats, наприклад, досліджує й показує загальну кількість зібраних лайків, поширень та коментарів до конкретного лінку. Тому якщо вас, скажімо, цікавить, наскільки популярним є ваш матеріал у Facebook, Netvizz покаже вам статистику. Функція Page data є більш складною, проте дає повнішу інформацію. За допомогою неї можна сформувати статистику постів сторінки – в одній таблиці сервіс покаже вам всю активність навколо останніх 10, 50, 100 чи більше записів. Це дуже зручно, адже ви отримаєте загальну картину лайків, поширень та коментарів, не докладаючи майже ніяких зусиль. Після проведеного аналізу Netvizz збирає дані в таблицю формату .tab. Утім, зазвичай такі файли не відкриваються на комп'ютері, тому щоб переглянути документ, необхідно перейменувати його на .tsv й завантажити на Google Drive.

8. Відеомоніторинг

Якщо ви активно ведете свій YouTube-аккаунт, спробуйте скористатись сервісом YouTube Data tools. Він пропонує декілька функцій – показує відео, які YouTube радить після перегляду вашого контенту, створює повну статистику вашого каналу тощо. Окремо слід виділити опцію Video info and

comments. З її допомогою можна зібрати в одному місці всі коментарі під відео з інформацією про їхніх авторів, таким чином відслідковуючи тролів та аналізуючи свою комунікацію з аудиторією. Для SMM-ників така функція буде безцінною, адже вона суттєво економить час.

9. Демографія

Дуже часто журналістам, які пишуть аналітичні матеріали, важко знайти достовірну статистику для того, щоб додати своєму тексту повноти. Соціологічні дані з різних країн світу можна отримати на сайтах OECD (Organisation for Economic Co-operation and Development) http://www.oecd.org/ та Eurostat http://ec.europa.eu/eurostat. Ці ресурси надають найсвіжішу інформацію щодо рівня освіти, зарплат, безробітності, політичної активності, задоволеності життям та багатьох інших факторів, які впливають на суспільні процеси.

10. Більше ресурсів!

Для тих, хто постійно працює з аналізом інформації та потребує більше інструментів для цього, є спеціальний сайт digitalmethods.net. Зліва на головній сторінці є вкладка Tools; клікнувши на неї, ви отримаєте перелік різноманітних онлайн-сервісів для роботи з інформацією в Інтернеті. Тут є ресурси для моніторингу соціальних мереж, для збору й сортування інформації з Вікіпедії, для роботи з Google та багато інших.

***

12.03.2016

Instagram набрал 200 тыс. рекламодателей по всему миру

Число рекламодателей, продвигающих свои товары и услуги в популярном мобильном приложении Instagram, достигло 200 тыс. Большинство из них – представители малого и среднего бизнеса. Быстрый рост числа рекламодателей связан с тем, что осенью прошлого года сервис интегрировался с инфраструктурой Facebook и открыл рекламную платформу для рекламодателей в 200 странах мира, пишет UBR со ссылкой на content-review.com.

В недавнем интервью газете Financial Times главный операционный директор Instagram М. Левин подчеркнула, что соцсеть будет и дальше реализовывать свой рекламный потенциал за счет использования ресурсов материнской компании Facebook и привлечения небольших рекламодателей из разных стран. «До сих пор вы могли наблюдать в основном как большие бренды и большие рекламодатели используют рекламу для связи с пользователями. Я думаю, что в 2016 г. рекламироваться начнут гораздо больше представителей малого бизнеса», – сказала она.

Аудитория Instagram перевалила за 400 млн и продолжает увеличиваться. Однако ложку дегтя в медовые показатели приложения добавили исследователи из компании Locowise. Они утверждают, что на фоне растущего числа юзеров и рекламодателей в Instagram падает показатель вовлеченности, то есть, доли пользователей, отреагировавших на увиденную в ленте рекламу. В

январе кликнули по рекламному посту или поставили ему «лайк» только 0,95 % от общей аудитории приложения. Это очень низкий показатель для Instagram, в 2015 г. он варьировался в пределах от 2,8 % до 1,36 %.

Справедливости ради, показатели вовлеченности в Facebook еще ниже – 0,46 %, а в Twitter и вовсе 0,09 %. Так что даже на фоне снижения интереса аудитории к рекламным постам Instagram остается наиболее эффективным среди глобальных социальных сетей. Это объясняется тем, что рекламные посты в Instagram максимально интегрированы в ленту пользователей и мало отличаются от публикаций самих юзеров.

***

10.03.2016

Соцсети не могут похвастаться большими продажами

Продажи, которые генерируют фан-страницы в социальных сетях, покрывают расходы на их ведение. Об этом сообщает директор по маркетингу интернет-магазина одежды и обуви LeBoutique Юлия Шилова, пишет UBR.

«Мы для себя рассматриваем страницы в социальных сетях как репутационную составляющую, без которой современной компании не обойтись. Также для нас это элемент обслуживания клиентов: многие наши клиенты предпочитают задавать вопросы по поводу заказов именно в личных сообщениях в социальных сетях. Это как кулер с водой в центре выдачи», – заявляет Ю. Шилова.

По ее словам, каждая из социальных сетей имеет свою специфику и свою аудиторию. Даже одни и те же люди в разных социальных сетях ведут себя по-разному.

Эксперт уточнила, что работа с социальными сетями определяет, что мы продаем и кому. Кроме того, важно учитывать особенности медиапотребления в данной конкретной сети и разделять работу с развитием сообществ в социальной сети и рекламу в сети. «Однозначно, для нашего интернет-магазина не работают Twitter, просто потому что там нет нашей аудитории. И LinkedIn, потому что в этой сети аудитория проводит не так много времени, да и занята в основном деловыми вопросами. В нашем случае сложно пока раскачать Instagram – тут вопрос в том, как соединить нашу модель шопинг-клуба и специфику сети», – объясняет Ю. Шилова.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

7.03.2016

Ученый объяснил зависимость людей от соцсетей эволюционным процессом

Чрезмерная зависимость от социальных сетей вроде Twitter или Facebook и мобильных устройств является частью эволюционного процесса, под который подстраивается человеческий мозг, заявил профессор кафедры психологии общества из Университета Бристоля Б. Худ, пишет Newsland.

Б. Худ связывает распространение технологий мгновенной связи и популярность Facebook и Twitter с тем, что человек эволюционировал как «социальное животное», передает RT со ссылкой на газету Bristol Post.

«Неудивительно, что многие из нас буквально прикованы к социальным сетям, ведь наш мозг тысячу лет готовился к уровню общения, который предоставляют Twitter и Facebook», – заявляет ученый.

Б. Худ считает, что человеческий мозг начал уменьшаться около 20 тыс. лет назад, в конце ледникового периода. Большинство ученых полагают, что этот процесс связан с изменением климата и рациона, однако профессор Б. Худ считает, что к таким переменам в физиологии человеческого мозга привело распространение оседлого образа жизни.

Б. Худ, написавший целый ряд книг по когнитивистике, утверждает, что размер мозга не стоит привязывать к более высокому интеллекту, однако он имеет влияние на общение между членами общества.

Профессор считает, что когда люди начали переходить к более оседлому образу жизни, образ мышления от индивидуального желания «перехитрить всех и каждого» перешел к более коллективному мышлению, которое устранило необходимость обладать сразу всей доступной информацией каждому индивиду в отдельности.

Таким образом, люди эволюционировали в «прирожденных сплетников», а современные социальные сети лишь удовлетворяют эту естественную потребность, говорит Б. Худ.

Он подчеркивает, что каждый «лайк» в соцсети Facebook и ретвит в Twitter вызывает выброс эндорфинов, вызывая чувство удовлетворения. «Это очень сильно подыгрывает нашему естественному желанию получать одобрение от широкого круга людей», – заключает Б. Худ.

***

6.03.2016

Как с помощью Facebook узнать режим сна человека?

Исследователь и программист из США С. Янсен (Soren Louv-Jansen) разработал программу, которая определяет режим сна активных пользователей Facebook. «Многие люди заходят в Facebook сразу после пробуждения и непосредственно перед отходом ко сну. Это даёт возможность определить их режим сна», – заявил разработчик в интервью Mail Online, пишет InternetUA.

Суть программы С. Янсена состоит в том, что она регулярно заходит в Facebook и считывает, кто в списке друзей сейчас онлайн. Автор изучил приложение Facebook Messenger, и нашёл в ней записи времени последнего посещения социальной сети участников списка друзей. По его словам, любой желающий может авторизоваться на сайте Messenger.com, выбрать в контекстном меню браузера View Source или аналогичную опцию, и найти там строку кода, указывающую на время последнего посещения.

«Создав простой сервис, который заходит на Facebook каждые 10 минут, я могу точно знать, когда мои друзья пользуются Facebook», – заявил С. Янсен. Создатель выложил исходный код программы в репозиторий GitHub.

«Я не пытаюсь шпионить за друзьями. Я хочу, чтобы люди понимали, что они оставляют цифровой след всюду, куда заходят», – говорится в интервью С. Янсена.

***

10.03.2016

Facebook стал виртуальной контрацепцией – исследование «The Telegraph»

По данным Управления национальной статистики Англии, с появлением социальных сетей частота беременностей среди девочек в возрасте до 18 лет в Англии и Уэльсе снизилась на 45 %. На сегодняшний день статистика подростковой беременности самая низкая за последние 50 лет, пишет FaceNews.

Сенсационное снижение вызвало множество теорий. Многие даже решили, что наконец-то стали окупаться занятия по вопросам полового воспитания. Но также есть люди, которые полагают, что молодежь просто тратит меньше времени в непосредственной близости друг от друга из-за социальных сетей – это явление, которое стало глобальным в 2007 г., после того, как сеть Facebook распространилась за пределы университетских городков.

Также появились предположения, что снижение подростковой беременности сопровождается признаками исправления других традиционно рискованных вариантов поведения, таких как распитие спиртного и употребления наркотиков.

Ситуацию прокомментировала специалист из Консультативной службы по вопросам подростковой беременности К. Мерфи.

«Доступ к противозачаточным средствам и половое воспитание, без сомнения, сыграли свою роль в снижении уровня подростковых беременностей, но вообще я согласна с предположением профессора Патона об эффекте социальных медиа. Резкое снижение случаев употребления подростками алкоголя, например, может снизить вероятность незащищенного секса. К тому же, подростки все чаще общаются в Интернете, ограничивая возможности для сексуальной активности», – сказала К. Мерфи.

***

18.03.2016

Открытие: Instagram делает еду вкуснее

Согласно данным нового исследования, проведенного специалистами из университетов Сент-Джозеф и Сан-Диего, выкладывание фотографий блюд в Instagram или пролистывание таких изображений усиливает удовольствие, получаемое от еды. Ученые говорят: кулинарное искусство развивается, как и вкусовые рецепторы человека. Многие экспериментируют с иностранной кухней и делятся фотографиями необычных блюд с другими, пишет Newsyou.

В исследовании приняли участие более 120 человек, пишет Zee News. Исследователи выяснили: если человек фотографировал блюдо перед едой, то он оценивал его выше. Правда, только в тех случаях, когда блюдо было достаточно вкусным. Специалисты полагают, что фотографии продуктов способны заставить людей питаться правильно.

А вот ученые из Оксфордского университета считают: демонстрация еды в СМИ и соцсетях способствует распространению эпидемии ожирения. Кулинарные шоу и фото в Instagram делают нас одержимыми едой. Они пробуждают чувство голода чаще, чем следует. Это «визуальный голод», который связан не с тем, что мы хотим есть, а с нашим восхищением красивыми и аппетитными блюдами.

Маніпулятивні технології

2.03.2016

Как украинский международный интернет зависит от России

Известный украинский интернет-предприниматель (управляющий партнер GrowthUP Group) Д. Довгополый написал в Facebook, что, по его опасениям, международный трафик многих (сотен) украинских интернет-провайдеров проходит через российских транспортных операторов. В своем конкретном примере он указал на МТС Украина (Vodafone) и интернет-провайдера Фринет.

Это, как считает Д. Довгополый, делает украинский внешний трафик зависимым от запретов и интернет-цензуры Роскомнадзора, пишет МедиаБизнес.

Могут ли российские законы в какой-то степени влиять на украинский международный Интернет?

Надо сказать, что действительно, большая часть нашего международного трафика идет с востока. Экс-директор Датагруп (крупнейший украинский игрок на рынке оптового интернет-трафика) М. Смелянец говорит, что около 50 % украинского трафика идет по российским магистральным линиям из Украины прямо в Москву и Санкт-Петербург.

Объясняется это в первую очередь тем, что российские сайты по-прежнему пользуются среди украинцев популярностью. В частности, по данным рейтинга исследовательской компании Gemius за январь этого года, в топ-10 наиболее посещаемых в Украине сайтов попали социальная сеть «ВКонтакте», поисковик Yandex, почтовый сервис Mail.ru, а также соцсеть «Одноклассники».

Как утверждает технический директор сети Ланет А. Марчук, по умолчанию интернет-трафик сам выбирает себе маршрут. «Русский трафик идет через Россию. Весь другой – через Франкфурт, Амстердам и т. п.», – подчеркивает он. Менеджер добавляет, что транзитом через Россию в Украину может идти разве что азиатский трафик. Но его очень немного. Естественно, можно искусственно перенаправить весь поток международного трафика только через Москву. Но, поясняет А. Марчук, это будет невыгодно экономически. И украинские провайдеры на это вряд ли пойдут.

Несмотря на большую зависимость от российских интернет-сайтов, с точки зрения доступа к мировому Интернету Украина чувствует себя вполне независимо. В первую очередь за счет географического положения. Наша страна граничит на западе с европейскими странами и имеет десятки межграничных магистральных переходов в разных местах. Только у одного Укртелекома более десяти физических пограничных переходов с семью странами. Поэтому даже чисто гипотетически Россия не сможет ограничить нам интернет-доступ в мир или миру – доступ в Украину. Для сравнения Казахстан, который зажат между Россией и Китаем, не имеет такого разнообразия международных каналов. Поэтому доступ этой страны в мир может быть осложнен непосредственно на границе.

Представители магистральных операторов с российскими корнями открещиваются от того, что могут повлиять на украинский международный трафик...

Хотя, как утверждают представители украинских операторов, нюансы с украинским трафиком, идущим в Россию и через нее, все-таки сохраняются. «По идее, на транзитный трафик никакие внутренние ограничения стран, через которые идет транзит, распространяться не должны. Но всякое случается», – рассказывает начальник отдела по связям с общественностью МТС Украина (Vodafone) В. Рубан. По ее словам, если оператор сталкивается с подобными ситуациями, он настраивает маршрутизацию через другого провайдера.

М. Смелянец добавляет, что он знает о случаях, когда украинский трафик в России «резался». Точно так же, как и запрещенный у нас трафик становился доступным в России.

***

1.03.2016

70 % россиян имеют доступ к интернету, но подвержены пропаганде – эксперт

93 % россиян считают основным источником информации теленовости, пишет Телекритика.

Как рассказал генеральный директор Киевского института социологии В. Паниотто в интервью «Лига.Нет», люди подвержены пропаганде, но называют ее при этом личной точкой зрения.

«Сегодня, в отличие от Советского Союза, который пытался обрезать любую альтернативную информацию, у 70 % россиян есть полный доступ к информации по Интернет – и все равно пропаганда побеждает», – отмечает эксперт.

Он говорит, что его компания проводила четыре исследования на Майдане, он сам не раз был там, общался со знакомыми и постоянно отслеживал информацию на телевидении и в сети. «И когда мой московский коллега, вместо того чтобы спросить у меня, что же происходит, объясняет мне, что в действительности происходило на Майдане, причем объясняет убежденно, не сомневаясь в своей правоте, – это просто смешно, если бы не было так печально», – рассказывает В. Паниотто.

Одной из причин подверженности пропаганде эксперт называет монополизацию средств массовой информации, огромные массивы однородной непротиворечивой информации, проверять достоверность которой у людей нет времени.

***

3.03.2016

В России заподозрили Telegram в пропаганде терроризма

Мессенджер П. Дурова Telegram подозревают в содействии террористам ИГ. В Генеральную прокуратуру РФ поступили жалобы о том, что посредством мессенджера распространяются экстремистские материалы, пишет IGate.

Автором одной жалобы является М. Григорьев, глава Фонда исследования проблем демократии, заместитель председателя комиссии по гармонизации межнациональных и межрелигиозных отношений.

«Наш фонд неоднократно выявлял в Telegram террористические каналы. В них не только ведется пропаганда терроризма, но и распространяются инструкции по изготовлению взрывчатых веществ, пособия по ведению

диверсионной работы», – отметил М. Григорьев. По его словам, запросы на закрытие этих каналов остаются без ответа.

М. Григорьев подчеркивает, что посредством мессенджера любой может свободно получить информацию о том, как изготовить взрывчатку, а также прочитать пособие по диверсионной работе. Зная об этом, руководство Telegram не пытается пресечь распространение таких материалов.

Вторую жалобу составил К. Гринченко, глава «МедиаГвардии» МГЕР. Согласно его данным, в мессенджере зарегистрировано около двух сотен аккаунтов, на которых пропагандируют терроризм.

***

3.03.2016

Малайзийцы начали нелегально торговать редкими животными в Facebook

В закрытых группах Facebook, зарегистрированных в Западной Малайзии, ведется незаконная торговля редкими животными. Информацию об этом опубликовала экологическая организация Traffic, пишет InternetUA.

За последние пять месяцев на 14 малайзийских страницах соцсети были выставлены на продажу 300 диких зверей – в частности, малайские медведи, гиббоны, выдры и бинтуронги. Большинство животных принадлежит к местной фауне, что свидетельствует о спросе на них в качестве домашних питомцев, делают выводы исследователи Traffic. Охота на ряд этих зверей и торговля ими запрещены малайзийским законодательством.

Группы Facebook, приспособленные для нелегальной торговли, насчитывают почти 68 тыс. участников, среди которых идентифицированы 106 продавцов. В настоящее время организация Traffic продолжает расследование в сотрудничестве с представителями Facebook.

***

13.03.2016

Госдеп США рад троллям из России

Государственный департамент США считает присутствие российских троллей на своих платформах приятным вызовом, а также приветствует освещение своей деятельности на российском ТВ, каким бы оно ни было. Об этом «Газете.Ru» рассказала заместитель помощника государственного секретаря США в Бюро по связям с общественностью М. Уэйлан, пишет InternetUA.

«Мы рады, что российское ТВ стало одним из самых главных потребителей нашей информации, другой вопрос, что эта информация используется не по назначению. Но это тоже часть нашего присутствия в медийном пространстве», – отметила чиновница.

По ее словам, российские тролли обожают инстаграм Госдепа и другие онлайн-платформы американского дипломатического ведомства. «Тролли – это большой вызов на таких площадках, как Facebook. Конечно, мы бы хотели видеть там настоящий диалог, но вместо него полоса комментариев подчас превращается в набор фраз, по которым очень легко можно определить тролля», – добавила М. Уэйлан.

Вместе с тем даже присутствие троллей Госдеп считает положительным знаком. «За нами следят, это хорошо. Но мы хотели бы заглушить этот шум и привлекать настоящих людей для разговора. У нас есть политика, запрещающая удалять негативные комментарии – это часть демократии, это часть того, кто мы есть», – подытожила М. Уэйлан.

Зарубіжні спецслужби і технології «соціального контролю»

2.03.2016

Жителя Чернигова посадили на пять лет за сепаратизм и вербовку в соцсетях

Деснянский районный суд города Чернигова вынес приговор уроженцу областного центра, который через социальные сети распространял сепаратистские материалы и антиукраинскую пропаганду. Об этом сообщает пресс-центр СБУ, пишет InternetUA.

Как отмечается, по указанию представителей самопровозглашенной террористической организации «ЛНР», черниговчанин размещал в одной из российских соцсетей пропагандистские материалы с призывами к поддержке и финансированию незаконных террористических формирований, вербовке новых боевиков, созданию так называемой «Новороссии».

Также сообщается, что украинские силовики задержали сепаратиста летом 2015 г. После этого досудебное расследование установило, что житель Чернигова неоднократно в июне прошлого года в соцсети «ВКонтакте» умышленно и из корыстных побуждений распространял материалы с призывами к совершению действий с целью изменения границ территории или государственной границы Украины в нарушение порядка, установленного Конституцией Украины.

Таким образом, черниговский суд признал мужчину виновным по ст. 110 Уголовного кодекса Украины (распространение материалов с призывами изменения границ территории или государственной границы Украины) и назначил наказание в виде лишения свободы сроком на пять лет.

***

5.03.2016

В Константиновке на Донетчине задержали админа сепаратистской группы в соцсетях

В Константиновке Донецкой области сотрудники СБ Украины задержали информатора террористов. Об этом сообщает пресс-служба ведомства, передает InternetUA со ссылкой на ИА «Вчасно».

По указанию боевиков, задержанный создал в социальных сетях группу, где обсуждалась ситуация в регионе, перемещение украинских военных, а также пропагандировались идеи «русского мира» и «Новороссии».

Полученные от участников группы данные информатор пересылал представителям террористической организации «ДНР».

Открыто уголовное производство по ст. 258-3 Уголовного кодекса Украины.

Продолжаются неотложные оперативно-следственные действия.

***

8.03.2016

За пост в соцсети украинца оштрафовали на 8500 гривен

Рассмотрев дело № 591/442/16-к, суд признал виновным в совершении преступления, предусмотренного ч. 3 ст. 109 Уголовного кодекса – публичных призывах к насильственному свержению конституционного строя и к захвату государственной власти через СМИ владельца страницы в социальной сети «ВКонтакте», пишут Херсонские Вести.

Как сообщает «Юрлига», суд пришел к выводу, что интернет-страница использовалась как средство массовой информации. Поскольку обвиняемый признал свою виновность, суд утвердил соглашение с прокурором, оштрафовав преступника на 8500 грн.

***

4.03.2016

СБУ може знімати інформацію з Viber і WhatsApp, – Ситник

Використовуючи можливості СБУ, абсолютно реально знімати інформацію з месенджерів Viber і WhatsApp, пише Espreso.tv.

Про це в інтерв'ю «Дзеркало тижня» заявив глава НАБУ А. Ситник.

«Зняти інформацію і з Viber, і з WhatsApp, використовуючи можливості СБУ, – реально», – сказав А. Ситник.

За його словами, «у СБУ є свої мотиви не допомагати нам (НАБУ. – Ред.)». «Загроза тероризму і необхідність загального контролю. Однак ні перше, ні друге не змінює нашої позиції з цього приводу. Тим більше в ситуації, м'яко кажучи, частих випадків незаконного зняття інформації з каналів зв'язку самими працівниками СБУ», – розповів А. Ситник.

Директор НАБУ має підозру, що депутати «навряд чи найближчим часом зроблять нам (НАБУ. – Ред.) такий подарунок».

«Занадто багатьом ми наступаємо на хвіст», – заявив А. Ситник.

***

13.03.2016

В Турции заблокировали доступ к соцсетям

Суд в Анкаре заблокировал доступ к социальным сетям, в том числе Twitter и Facebook, после публикации в них фото и видео последствий теракта в центре турецкой столицы. Об этом сообщают вечером в воскресенье, 13 марта, турецкие телеканалы NTV и CNN Turk, пишет InternetUA.

Решение принято на основании того, что пользователи соцсетей начали публиковать фото и видео с жертвами теракта.

Ранее Высший совет Турции по телевидению и радио принял решение ограничить освещение теракта. В частности, в эфире не должны появляться место событий и жертвы взрыва.

***

14.03.2016

У Німеччині заборонили використовувати кнопку «Like» на сайтах, бо вона нелегально передає інформацію

Питання приватності все більше турбує користувачів Європи. Днями суд у Німеччині ухвалив рішення, згідно з яким веб-сайти повинні отримувати попередню згоду користувачів, перш ніж розміщувати на своєму сайті кнопку Like соціальної мережі Facebook, пише UkrainianWatcher.

Річ в тім, що кнопка Like, розміщена на сайті, відсилає інформацію про користувача соціальній мережі Facebook навіть якщо він в ніякий спосіб не взаємодіяв з нею. Через це суд вважає, що це порушує права користувачів, адже інформація про них передається від сайту третій стороні (соцільній мережі) без згоди користувача.

Судовий розгляд ініціювала організація із захисту прав споживачів і стосувався він німецького рітейлера Peek&Cloppenburg. Інтернет-магазину тепер загрожує штраф 250 тис. євро.

Наразі рішення суду стосується виключно інтернет-магазинів, але всі інші сайти, у тому числі медійні, у такий самий спосіб передають третім сторонам інформацію про користувача, тому можна очікувати нові судові рішення.

Це вже не перше рішення такого типу. Два місяці тому в Німеччині визнали незаконною функцію пошуку друзів у Facebook.

***

14.03.2016

Дуров не вважає за потрібне давати владі доступ до даних через загрозу тероризму

Засновник російської соціальної мережі «ВКонтакте», а нині керівник месенджера Telegram П. Дуров не вважає, що технологічні компанії повинні

давати владі необмежений доступ до даних своїх користувачів заради боротьби з терористами, пише MediaSapiens.

Про це він заявив під час інтерв'ю в програмі «60 хвилин» американського телеканалу CBS.

П. Дуров, зокрема, охарактеризував позицію Telegram з цього питання. Він наголосив, що месенджер був задуманий як винятково приватний засіб спілкування. За його словами, неможливо дати владі доступ до одних каналах і не дати до всіх інших. Крім того відкрити доступ до жодних повідомлень Telegram неможливо зокрема й через особливості шифрування.

П. Дурову відомо, що учасники екстремістських організацій можуть використовувати Telegram для власної пропаганди та координації. Однак він вважає, що доступ до цієї інформації не вирішить проблеми.

«Це світ технологій, і їх неможливо зупинити. ІДІЛ може створити свій додаток протягом місяця, якщо захоче», – зазначив керівник Telegram. П. Дуров також додав, що їх працівники намагаються попередити спілкування екстремістів через месенджер.

***

10.03.2016

В Твери блогера судят за репост материала и картинки о Крыме

В Твери началось рассмотрение по существу уголовного дела в отношении пользователя социальной сети «ВКонтакте» А. Бубеева. Он обвиняется в публичных призывах к осуществлению экстремистской деятельности (ч. 2 ст. 280 УК РФ) и к осуществлению деятельности, направленной на нарушение территориальной целостности РФ (ч. 2 ст. 280.1 УК РФ), сообщила NEWSru.com адвокат подсудимого С. Сидоркина, пишет NEWSru.com.

По ее словам, поводом для уголовного преследования послужили репост А. Бубеевым материала «Крым – это Украина» публициста Б. Стомахина и картинки на эту же тему на собственной странице в соцсети «ВКонтакте».

«Сегодня в суде огласили обвинительное заключение. Также суд отклонил наше ходатайство о возвращении дела прокурору для устранения грубых нарушений», – заявила адвокат. Она отметила, что сам А. Бубеев вину не признал. Он считает, что его преследуют за убеждения.

Ранее А. Бубеев уже был осужден за репосты аналогичных материалов и картинок. В августе 2015 г. он был приговорен за возбуждение ненависти или вражды (статья 282 УК РФ) к 10 месяцам лишения свободы с отбыванием наказания в колонии-поселении.

Об истории А. Бубеева писал портал «Открытая Россия». В статье, в частности, отмечалось, что последние пару лет в России пользователей соцсетей все чаще привлекают к уголовной ответственности по экстремистским статьям за размещенные на странице материалы. В одной только Твери с начала 2015 г. по статьям об экстремизме было привлечено к ответственности

более 20 человек, многие из которых студенты тверских вузов, утверждается в материале. При этом поводом для повышенного интереса правоохранителей может стать обычный лайк или комментарий к какой-нибудь картинке или статье, отмечает автор.

***

10.03.2016

Британські спецслужби отримали доступ до даних 22 тис. бойовиків ІДІЛ

Спецслужби Великобританії отримали доступ до особистих справ 22 тис. іноземних найманців, які воюють на боці терористичного угруповання «Ісламська держава», пише LB.ua.

Допоміг спецслужбам бойовик-дезертир, який викрав електронний носій із секретною інформацією. Вкрадені файли містять імена, адреси і дані родичів 22 тис. найманців ІДІЛ.

«Цей витік оцінено як серйозний удар по ІД, оскільки він дає доступ до життєво важливих розвідданих про воєнний стан в Іраку та Сирії», – наголошує видання.

Згідно з даними, у лавах терористичної організації воюють громадяни більш ніж 50 країн. Понад 70 % із них родом з арабських країн.

Раніше американські спецпризначенці захопили в полон іракця, який очолював програму ІД зі створення власної хімічної зброї.

***

15.03.2016

В Днепропетровской области СБУ задержала организатора «пророссийского подполья»

Сотрудники Службы безопасности Украины задержали в городе Терновка Днепропетровской области местного жителя, который через социальные сети пытался создать «пророссийское подполье» в регионе.

Об этом ИА «МОСТ-ДНЕПР» сообщили в пресс-службе УСБУ в Днепропетровской области.

Мужчина в июне 2014 г. находился на территории Донецка, где установил контакт с представителями террористической организации «ДНР» и получил задание организовать на территории западного Донбасса поддержку действий боевиков.

«Вернувшись домой, сообщник террористов через российские социальные сети начал вербовать местных жителей к незаконным вооруженным формированиям боевиков. Он также распространял материалы антиукраинского характера, популяризировал действия террористов «ДНР/ЛНР» и призвал к сопротивлению силам антитеррористической операции», – отметили в спецслужбе.

Во время обыска сотрудники спецслужбы изъяли у злоумышленника компьютерную технику с доказательствами агитации и пропаганды террористических организаций.

Открыто уголовное производство по ч. 1 ст. 258-3 Уголовного кодекса Украины. Продолжаются неотложные оперативно-следственные действия для установления всех сторонников создания «пророссийского подполья» в Днепропетровской области.

***

16.03.2016

СБУ викрила активіста, який займався проросійською пропагандою на Житомирщині

Співробітники Управління СБУ в Житомирській області припинили поширення в Інтернеті антидержавної пропаганди на підтримку агресії Російської Федерації проти України очільником місцевого осередку однієї з громадських організацій (яка займає проросійську позицію). Про це повідомила прес-група УСБ України в Житомирській області, пише InternetUA.

«Через свою сторінку у соцмережі лідер громадської структури підтримував тісні контакти із бойовиками сепаратистських незаконних воєнізованих формувань, активно розміщував на ній статті та посилання на повідомлення, у яких обґрунтовувалися ідеї необхідності федералізації України на кшталт псевдодержавних утворень «ДНР/ЛНР» з подальшим курсом на об’єднання із Росією на правах “молодшого брата”», – ідеться в повідомленні.

Пропагуванням федералізму і сепаратизму серед інтернет-користувачів він не обмежувався – у розмовах зі своїми знайомими він підтримував агресивну зовнішню політику РФ стосовно України та нав’язував їм антиукраїнські погляди.

Служба безпеки України офіційно попередила громадського діяча, що у випадку подальшого поширення ним аналогічних матеріалів та продовження антиукраїнської пропаганди його дії кваліфікуватимуться за статтями 110 та 258-2 Кримінального кодексу України.

Протиправний контент із адміністрованих ним сторінок у соціальній мережі він видалив добровільно.

***

17.03.2016

Иран заблокировал международную версию «Яндекса» и «ВКонтакте» из-за несоответствия ценностям

В Иране заблокировали международную версию российского поисковика «Яндекс» – yandex.com, свидетельствуют данные ресурса blockediniran.com. При этом региональные сайты компании, в том числе yandex.ru, доступны,

пишет «Коммерсантъ» со ссылкой на пресс-атташе посольства России в Иране М. Суслова, пишет InternetUA.

«Иранская сторона считает, что там находится информация, не отвечающая их ценностям. Хотя yandex.ru работает. Есть специальная служба, которая занимается просмотром сайтов, она принимает решения о блокировке того или иного ресурса», – сообщил М. Суслов, пресс-атташе России в Иране

По словам М. Суслова, в Иране заблокировано много сайтов, среди которых «ВКонтакте», Twitter и Facebook. Он отметил, что многие жители страны обходят блокировку с помощью VPN-сервисов. В «Яндексе» и «ВКонтакте» подтвердили факт блокировки сайтов на территории Ирана.

«Это не приоритетный для нас рынок», – отметил представитель поисковика в разговоре с «Коммерсантом».

Источник издания, близкий к российскому правительству, говорит, что вопрос блокировки «Яндекса» поднимался на встрече главы Минкомсвязи РФ Н. Никифорова и министра связи и информационных технологий Ирана М. Ваези.

По итогам этой встречи М. Ваези заявил о договорённости, подразумевающей открытие офиса «Яндекса» в Иране. Однако представители компании тогда сообщили vc.ru, что у поисковика нет планов по открытию новых офисов.

По данным «Коммерсанта», российские интернет-компании заинтересованы в том, чтобы проблема ограничения доступа к их сайтам в Иране снова была поднята на высоком уровне. «Мы уже написали письма в посольство Ирана и иранское надзорное ведомство по телекоммуникации и связи. Кроме того, рассчитываем, что проблема будет поднята во время визита в Иран первого вице-премьера И. Шувалова», – сообщил изданию источник, близкий к одной из компании.

***

16.03.2016

Жителям ОАЭ грозит штраф за публикацию в соцсетях фото и видео стихийных бедствий

Власти ОАЭ предупредили местных жителей, что распространение слухов и размещение негативных фото и видео во время дождей, аварий и пожаров на сайтах социальных сетей повлекут за собой уголовное наказание, сообщает Gismeteo.

Согласно законам, отмечают власти, такие действия наказуемы, они сеют путаницу и панику в обществе, а также влияют на репутацию страны и усилия государственных ведомств относительно сохранения и защиты жизни и имущества.

«Во время недавних сильных дождей в ОАЭ некоторые люди вели себя безответственно на сайтах социальных сетей, – идет речь в сообщении властей. – Они делились фотографиями и видео несчастных случаев, которые

произошли в течение дождливых дней, и распространяли слухи об обвалах и людях, тонущих в дождевой воде, тем самым создавая панику среди общественности».

Нарушители будут приговорены к лишению свободы сроком от одного до трех месяцев или будут вынуждены оплатить штраф.

***

10.03.2016

Сноуден назвал чушью заявления ФБР и рассказал, как спецслужбы могут взломать iPhone террориста

Бывший сотрудник американских спецслужб Э. Сноуден, обнародовавший данные о слежке спецслужб США в мировом масштабе, считает, что не только у Apple есть ключи к личным данным, которые хранятся в iPhone. Об этом он заявил на конференции The Intercept, пишет InternetUA.

«ФБР говорит, у Apple имеются “эксклюзивные технологические средства” для разблокирования этого телефона, – сказал Э. Сноуден в рамках видеомоста, посвящённого теме демократии и развитию гражданского общества. – При всём уважении это чушь».

Э. Сноуден считает, что у самой ФБР есть технические средства для взлома iPhone. Он считает, что спецслужбы не были бы так настойчивы в этом вопросе, если бы не несли ответственности за упущенный шанс получить доступ к смартфону самостоятельно.

«Все, что нужно сделать ФБР, чтобы обойти функцию удаления данных после 10 ввода попыток пароля – скопировать флеш-накопитель (который включает Effaceable Storage). Затем они могут бесконечно подбирать пароль, так как у них будет возможность восстанавливать память NAND flash из резервной копии», – сказал Э. Сноуден.

«ФБР достаточно отсоединить чип от материнской платы, подключить его к устройству для чтения и записи NAND flash и сделать копию всех данных. Затем они могут вернуть чип и начать процесс подбора паролей. Если так случится, что функция автоудаления данных включена и чип Effaceable Storage удалит ее, они могут извлечь чип и перенести на него оригинальную информацию. Если они хотят делать это много раз, они могут подключить test socket к материнской плате, что ускорит процесс замены чипов», – пояснил он.

Ранее Э. Сноуден высказал мнение, что власти США добиваются от Apple полного доступа ко всем iPhone. Хотя спецслужбы говорят лишь об одном конкретном устройстве, бывший сотрудник американских спецслужб уверен, что цель ФБР – получить полный доступ ко всем смартфонам Apple, находящимся в обращении.

***

13.03.2016

СМИ: в ШАБАК разработан алгоритм, помогающий выявлять террористов в Facebook

10 канал ИТВ сообщил, что Общая служба безопасности совместно с разведкой Израиля и штабом Центрального военного округа разработали алгоритм, позволяющий выявлять потенциальных террористов в сети Facebook. Благодаря новому методу были предотвращены десятки терактов, пишет NEWSru.co.il.

В сообщении телеканала отмечалось, что в течение полугода службы безопасности Израиля искали способ борьбы с «террором одиночек», когда потенциальные террористы, не состоящие ни в одной организации, действуют спонтанно. Однако недавно службам безопасности удалось создать алгоритм анализа сообщений, публикуемых в социальных сетях, и, в первую очередь, в Facebook.

В репортаже 10 канала не было никаких технических подробностей, раскрывающих механизм работы системы. Лишь говорилось, что система выдает сигнал предупреждения в случае, если находит в публикациях «опорные слова или фразы», например, «я отомщу евреям», «евреи разрушают Аль-Аксу» и т. д. Предупреждение получают в ШАБАК и отделе сбора информации при штабе Центрального округа.

10 канал также сообщил, что подобным алгоритмом пользуются палестинские спецслужбы для выявления потенциальных террористов.

Проблема захисту даних. DDOS та вірусні атаки

5.03.2016

Что расскажет о человеке страница в соцсети

Социальные сети собирают и хранят огромные массивы информации о пользователе. При этом тот может даже не подозревать, что о нем может стать известно другим, ведь заниматься настройками конфиденциальности слишком утомительно. О владельце страницы могут рассказать и другие детали, пишет InternetUA.

В первые годы существования соцсетей регистрация в них была делом личным, можно было создавать массу аккаунтов для различных целей, регистрировать «фейки» и фактически с нуля рисовать виртуального «человека». Со временем правила регистрации стали жестче, потребовались и почта, и номер телефона.

Однако в настоящее время соцсети – это необходимость. Это в первую очередь инструмент общения, получения информации и, наконец,

социализации в широком смысле. Немаловажную часть занимают и развлечения, которых также предостаточно. Здесь и видео, и игры, и развлекательные паблики и группы.

Первое время социальные площадки использовались сугубо для личных целей. Если нужна деловая сторона вопроса – добро пожаловать в LinkedIn.

Регистрируя аккаунт в социальной сети (не в различных сервисах, блогах или приложениях) и каждый день его обновляя, человек не создает выдуманный портрет, а проецирует свой настоящий образ. Если в Instagram можно загружать, например, лишь фотографии с вечеринок и дальних поездок и создать, таким образом, ореол успешности, то обычная социальная площадка посредством других косвенных факторов все-таки раскроет истинную суть более или менее верно.

Тем временем данными другого человека могут интересоваться не только спецслужбы или сотрудники отделов HR, но и так называемые сталкеры, следящие за каждым действием жертвы в соцсети. Их намерения могут быть как минимум странными и даже причинять реальный вред.

В противовес «сталкерам» существуют и «виртуальные параноики», которые 10 раз подумают перед тем, как опубликовать фотографию или добавить информацию в раздел «О себе». Других подобная открытость, наоборот, не отпугивает – они готовы делиться с миром каждым шагом, что, в свою очередь, также может отпугивать подписчиков и «друзей».

Одним из чувствительных видов информации, который сопровождает выкладываемые в соцсети снимки, является местоположение.

Включенные геотеги при публикации позволят узнать местонахождение автора фотографии всем желающим. Кроме того, «ВКонтакте» и Instagram по фотографиям с геометками формируют целую карту, на которой отображаются все места планеты, посещенные пользователем. Также и новый сервис Twitter Periscope позволяет любому человеку увидеть, где находится ведущий трансляции.

Любые публикации в соцсетях по умолчанию доступны для всех пользователей, будь то друзья или случайные гости. Также и основная личная информация расскажет много о пользователе. Если в описании указаны места обучения и проживания в хронологическом порядке, то в результате получается и вовсе краткая автобиография. Кроме этого, при стандартных настройках страница в соцсети индексируется и поисковыми системами.

Достаточно много об интересах, политических взглядах и видах деятельности могут подробно рассказать группы и паблики, в которых состоит пользователь.

Существует и закрытая информация, которой владеет только соцсеть. Анализируя деятельность пользователя, она создает свой портрет, который пригодится рекламодателям. В отличие от контекстной рекламы, которая опирается на конкретный читаемый материал, таргетированная реклама зависит от виртуального портрета человека. Например, если пользователь интересуется техникой и подписывается на страницы о гаджетах, то и реклама будет

предлагать ему приобрести тот или иной смартфон или планшет. И, конечно, мобильные приложения соцсетей всегда знают, где находится пользователь.

В современных реалиях практически невозможно не оставлять следов в сети неискушенному пользователю. На случай, если человек все-таки окончательно решит уйти с социальных площадок, существует даже несколько сервисов, которые облегчат задачу.

Портал AccountKiller, например, обещает удалить всю информацию из Facebook, а также из многих других социальных площадок. Тем не менее в комментариях пользователи сервиса пишут о том, что возможность войти в аккаунт после его «удаления» – это совсем не то, что обещает сервис.

Сайт justdelete.me – это набор активных ссылок на удаление из тех или иных соцсетей, форумов или онлайн-магазинов. При этом каждая ссылка обладает своим цветом. Зеленый цвет обозначает то, что удалиться с этой площадки очень просто, желтый – несколько труднее, красный – очень тяжело. Черный цвет говорит о том, что стереть свой аккаунт и информацию окончательно невозможно. Зеленым, например, подсвечена ссылка на удаление из «Одноклассников» или «ВКонтакте», а черным – удаление из Netflix.

Как бы то ни было, даже полное исчезновение из Instagram, Twitter, «ВКонтакте», Facebook, «Одноклассники» и прочих площадок не позволит избавиться от информации, которую Интернет уже знает о пользователе. Кэш поисковых систем запоминает все, поскольку он делает слепок каждой новой частички информации, и ему совсем не обязательно иметь под рукой новый активный источник.

***

15.03.2016

Facebook, Google и Snapchat планируют усилить шифрование данных

Корпорации Google, Snapchat и Facebook планируют внедрять технологии шифрования для улучшения безопасности данных своих пользователей, пишет InternetUA.

На фоне скандала, связанного с противостоянием Apple и ФБР по поводу взлома смартфона террориста из Сан-Бернардино, корпорации заявили о желании усилить шифрование данных.

Как сообщает издание, в течение нескольких недель Facebook планирует внедрить технологию шифрования для голосовых звонков внутри собственного мессенджера WhatsApp. Также планируется усиление безопасности в мессенджере Facebook Messenger.

Компания Google заявила о желании усилить защиту электронной почты. Snapchat занимается улучшением защиты сообщений пользователей.

***

3.03.2016

Даже малозначительные web-приложения могут привести к утечке конфиденциальных данных

На сегодняшний день многие крупные компании значительно недооценивают риск использования уязвимых веб-приложений в корпоративной среде. В большинстве случаев сотрудники службы информационной безопасности предприятий устраняют критические угрозы для наиболее важных программ. Однако любое ненадежное веб-приложение может представлять опасность для корпоративных систем, отмечает эксперт И. Колошенко в статье на портале Dark Reading, пишет InternetUA.

В настоящее время наиболее легким способом осуществления APT-атаки является фишинговая рассылка. Как правило, сотрудники организаций без опаски переходят по ссылкам в электронных сообщениях на корпоративных веб-сайтах. В результате злоумышленники могут получить доступ на систему компании без необходимости приобретения эксплоитов для уязвимостей в iOS или Adobe Flash.

В качестве примера опасности недооценки риска уязвимых веб-приложений, специалист привел атаку на небольшой швейцарский банк, осуществленную в прошлом году. Злоумышленники взломали одно из «малозначительных» приложений, похитили персональные данные и потребовали выкуп в размере 10 тыс. евро за неразглашение информации. Руководство финорганизации отказалось выполнить требование киберпреступников. В результате данные оказались опубликованными в сети. Хотя большинство записей данных не принадлежали клиентам банка, инцидент все равно нанес ему значительный репутационный ущерб.

В другом случае злоумышленники перевели средства со счетов частной европейской клиники (название не разглашается) на подконтрольные им счета. Преступники смогли получить доступ к деньгам, изменив несколько номеров банковских счетов, содержащихся в запросе предложения (документированный запрос организации, заинтересованной в приобретении каких-либо товаров или услуг), созданный для новый сотрудников.

Как показывают данные примеры, даже не особо важное приложение может представлять риск для безопасности корпоративной системы. Эксперт рекомендует организациям проводить регулярные проверки своих веб-сайтов и приложений, обращая особое внимание на защищенность программ с возможностью доступа извне.

***

2.03.2016

Обнаружен новый вредонос, предположительно разработанный Hacking Team

Исследователи безопасности обнаружили новый вид вредоносного ПО для OS X, предположительно разработанный Hacking Team. Вредонос используется в качестве дроппера и загружает на компьютер систему удаленного управления Hacking Team Remote Control System (RCS), пишет InternetUA.

Как сообщил ИБ-специалист SentinelOne П. Вилака, код дроппера похож на код Hacking Team RCS, и в обоих продуктах содержатся одинаковые элементы. Сложно определить, был ли вирус разработан собственно Hacking Team либо сторонними хакерами, использовавшими исходный код продуктов компании. Напомним, в июле 2015 г. неизвестные киберпреступники взломали корпоративную сеть организации и опубликовали в открытом доступе более 400 ГБ данных.

Два варианта вредоносного кода были загружены на VirusTotal. На момент написания новости дроппер не детектировался ни одним антивирусом.

По сравнению с более ранними версиями дропперов от Hacking Team вредонос начал использовать нативную систему шифрования в OS X и собственный упаковщик. Дроппер также использует технологии по обходу отладки.

Правозащитные организации обвиняют Hacking Team в продаже шпионского ПО государствам с репрессивным правительством. Как следует из полученных в результате взлома данных, компания сотрудничала с властями Азербайджана, Бахрейна, Египта, Эфиопии, Казахстана, Марокко, Нигерии, Омана, Саудовской Аравии и Судана.

***

2.03.2016

Масштабный анализ показал уязвимость продуктов Netgear и D-Link

Группа исследователей сетевой безопасности обнаружила серьёзные уязвимости в более чем десятке беспроводных маршрутизаторов и точках доступа производства компаний Netgear и D-Link. Помог им в этом открытым фреймворк для динамического анализа встроенных прошивок устройств. Фреймворк FIRMADYNE автоматически запускает прошивку на основе Linux для встроенных устройств в эмуляторе и производит ряд тестов, в том числе проверку на устройчивость перед известными эксплоитами, пишет InternetUA

Исследователи использовали фреймворк FIRMADYNE на примерно 23 тыс. образах прошивок от 42 производителей устройств. Фреймворк сумел извлечь 9486 образа и в 887 из них обнаружил уязвимость как минимум к одному из 74 известных эксплоитов. Было также найдено 14 ранее неизвестных уязвимости в 69 прошивке 12 устройств. Ряд уязвимостей нашли в продуктах от Netgear и D-Link.

Веб-интерфейс шести устройств Netgear содержит несколько страниц, доступных без авторизации, дающих за счёт этого доступ к командной строке. Уязвимость обозначена как CVE-2016-1555 и может привести к получению

контроля над устройством, особенно если оно настроено на управление через Интернет. Уязвимы модели Netgear WN604, WN802Tv2, WNAP210, WNAP320, WNDAP350 и WNDAP360.

Netgear WN604, WNAP210, WNAP320, WND930, WNDAP350 и WNDAP360 также включают в себя веб-страницы с доступом без авторизации, которые показывают пин-код в режиме Wi-Fi Protected Setup (WPS). Веб-сервер семи устройств D-Link обладает уязвимостью переполнения буфера, итогом её использования может стать удалённое выполнение кода. Затронуты модели D-Link DAP-2310, DAP-2330, DAP-2360, DAP-2553, DAP-2660, DAP-2690 и DAP-2695. Три устройства D-Link и три Netgear показывают пароли и данные администратора через протокол Simple Network Management Protocol (SNMP). Это модели D-Link DAP-1353, DAP-2553, DAP-3520, Netgear WNAP320, WNDAP350 и WNDAP360.

***

2.03.2016

Немецкое антимонопольное ведомство начало расследование в отношении Facebook

Федеральное антимонопольное ведомство ФРГ начало расследование против компании Facebook, а также ее немецкой «дочки» Facebook Germany в связи с возможным использованием данных пользователей для показа рекламы, сообщает ТАСС со ссылкой на пресс-релиз ведомства (InternetUA).

«Ведомство имеет подозрения, что Facebook благодаря условиям договора о личных данных пользователей злоупотребляла своим возможным доминированием на рынке социальных сетей», – отмечается в сообщении.

Представители антимонопольного ведомства пояснили, что для таких компаний, как Facebook, получающих доход от рекламы, крайне важно, как прописано пользовательское соглашение. По мнению чиновников, социальная сеть «в большом объеме» и «из самых разных источников» получает личные данные своих пользователей, что позволяет рекламодателям вставлять контекстную рекламу, адаптированную под каждого конкретного человека.

Пользователи Facebook соглашаются с условиями договора, где прописана вся процедура, однако они вряд ли представляют, какие последствия будет иметь это согласие. «Есть серьезные сомнения в том, что такие действия допустимы, особенно с учетом действующего законодательства в области защиты данных», – говорится в сообщении.

В свою очередь представитель Facebook выразил уверенность, что компания найдет общий язык с антимонопольщиками и ответит на все поставленные вопросы, сообщает Reuters.

Соцсеть столкнулась с растущим давлением со стороны правоохранительных и антимонопольных органов Европы, обеспокоенных тем, как она обращается с пользовательскими данными. Ведется общее расследование на уровне Евросоюза, регуляторы Франции, Бельгии,

Нидерландов, Испании ранее открыли разбирательства на национальном уровне.

***

4.03.2016

Очередной сайт знакомств взломан, в даркнете продают данные 27 млн пользователей

На хакерских форумах Hell был замечен дамп базы данных популярного сайта знакомств Mate1.com. Неизвестный хакер продает информацию о 27 млн пользователей ресурса за 20 биткоинов (около 8400 долл.), пишет InternetUA.

Злоумышленник утверждает, что сумел взломать MySQL-сервер Mate1, откуда и скачал полный дамп. Исходно на руках хакера оказались данные о почти 40 млн пользователей (хотя счетчик на Mate1 утверждает, что на сайте 31,5 млн пользователей), но после того как взломщик удалил из базы все дубликаты и ботов, их число сократилось до 27 млн.

В отличие от прошлогоднего взлома «сайта для измен» Ashley Madison, этот случай менее страшен, так как хакер заполучил в свое распоряжение только email-адреса и незашифрованные пароли пользователей ресурса. Никаких личных данных, которые помогли бы деанонимизировать клиентов сайта, база не содержит.

Впрочем, утечку 27 млн паролей тоже вряд ли можно назвать хорошей новостью. Как известно, люди очень часто используют один и тот же пароль на разных ресурсах.

На подлинность базу уже проверили журналисты издания Vice Motherboard. 498 из 500 протестированных ими адресов действительно связаны с аккаунтами Mate1.com. Впрочем, регистрация на сайте не требует подтверждения через почту, так что аккаунты могли быть зарегистрированы и на чужие (подставные) ящики.

Руководство Mate1 пока никак не комментирует ситуацию, предпочитая хранить молчание.

***

3.03.2016

Хакеры «Исламского государства» взломали не тот Google

Группа хакеров из террористической группировки «Исламское государство» (ИГ) сообщила о взломе Google, однако позже выяснилось, что кибератаке подвергся не популярный поисковик, а сайт с похожим названием. Об этом информирует The Independent, пишет InternetUA.

О готовящейся кибератаке на Google террористы заявили в мессенджере Telegram. Спустя несколько часов взломанным оказался сайт Addgoogleonline.com, зарегистрированный на гражданина Индии. На этом сайте

стали транслироваться песни ИГ на французском языке, появилась символика организации и знак «Hacked By: CCA» («Взломано армией Киберхалифата»).

В тот день боевики также атаковали 35 британских веб-сайтов. Среди них был ресурс по продаже ламината и мебели, а также сайт инструктора по японским танцам.

The Independent добавляет, что британские порталы были взломаны террористами в качестве мести за убийство уроженца Англии, джихадиста Ю. Хусейна, который погиб в результате авиаудара США в 2015 г.

***

2.03.2016

Google разработал технологию, позволяющую лучше защитить почту Gmail

Крупные компании как никто другой нуждаются в защите конфиденциальной информации от утечек. Стоит каким бы то ни было фактам о производственном процессе, планах на будущее или другой области деятельности предприятия просочиться в сеть, как у компании начинаются серьёзные проблемы. Для предотвращения подобных инцидентов Google представляет новую технологию Data Loss Prevention (DLP) для Gmail, призванную свести риск утечки информации к нулю. Получив обновление, Gmail сможет проводить оптическое сканирование документов с последующим распознаванием символов. Таким образом, сервис удостоверится, что прикрепленные файлы не содержат никаких конфиденциальных или сугубо личных сведений, пишет IGate.

Защитные детекторы на бизнес-платформе Google и раньше обладали функцией сканирования содержания, однако его функциональность была сильно ограничена. Теперь же по завершении сканирования программа автоматически проверит соответствие содержимого документов составленным администратором черному и белому спискам. Это поможет избежать как случайной отправки нежелательных сведений по ошибке, так и злонамеренного разглашения конфиденциальной информации недобросовестными сотрудниками. В настоящее время сервис DLP доступен исключительно платным подписчикам Google Apps Inlimited.

***

2.03.2016

Microsoft представила облачный сервис для защиты от хакерских атак

Портфель решений Microsoft для защиты данных пополнился новым облачным сервисом. Он позволяет узнавать, была ли на корпоративную сеть совершена атака, и восстановить защиту. Новый сервис работает только в Windows 10, и в Microsoft полагают, что это послужит дополнительным

стимулом для перехода организаций на последнюю версию операционной системы, пишет Центр информационной безопасности.

Microsoft представила облачный сервис Windows Defender Advanced Threat Protection, который, как полагают в компании, станет дополнительным стимулом для перехода на Windows 10 коммерческих клиентов.

Windows Defender Advanced Threat Protection («защита от сложных угроз безопасности») предназначен для выявления уже совершенных атак на корпоративные сети и оказания помощи системным администраторам в принятии ответных мер. То есть он помогает ликвидировать последствия тогда, когда все другие уровни защиты сети хакерами были преодолены.

Windows Defender ATP послужит дополнительным стимулом перехода на Windows 10, потому что в любых других версиях операционной системы Windows он не поддерживается. Является ли новый сервис бесплатным, в компании не уточнили.

Windows Defender ATP способен обнаруживать следы вторжений и помнить их в течение шести последних месяцев, он сообщает: посредством чего была совершена атака и на какие устройства, почему не сработали средства защиты. Далее сервис дает рекомендации – какие шаги необходимо предпринять для восстановления защиты и ликвидации последствий.

Анонимная информация поступает в облако Windows Defender ATP с многочисленных источников: более 1 млрд Windows-устройств, 2,5 трлн веб-страниц и 600 млн узлов проверки репутации. Кроме того, ежедневно сюда стекаются результаты анализа более 1 млн подозрительных файлов.

Сервис использует машинное обучение. И так как эта технология не дает стопроцентной точности, указания Windows Defender ATP носят рекомендательный характер, уточнил исполнительный вице-президент Microsoft Windows and Devices Group Т. Мейерсон. Администраторы вольны самостоятельно принимать решение о принятии мер, оценив доступную им информацию, добавил он.

Как рассказали в Microsoft, в настоящее время сервис проходит закрытое тестирование на 500 тыс. устройствах под управлением Windows 10. В течение 2016 г. компания планирует предоставить возможность участия в тестировании большему количеству организаций. Однако в Microsoft не уточнили, когда именно. Срок полномасштабного запуска нового сервиса тоже неизвестен.

В Microsoft считают, что Windows Defender ATP поможет организациям эффективнее бороться с хакерами, атаки которых становятся все более сложными и профессиональными.

«Только в 2015 г. были обнаружены тысячи атак на корпоративные сети. По нашим данным, в среднем организациям требуется более 200 дней на то, чтобы обнаружить следы вторжения, и около 80 дней на то, чтобы восстановить защиту. В среднем устранение последствий одной атаки обходится организациям в 12 млн долл., но еще больше страдает их репутация», – сказал Т. Мейерсон.

***

3.03.2016

Атака DROWN поставила под угрозу треть всех сайтов, работающих с HTTPS

Проект OpenSSL представил обновленные версии 1.0.2g и 1.0.1s, в которых была устранена опасная уязвимость CVE-2016-0800. Данная брешь позволяет злоумышленнику провести межпротокольную атаку, которой исследователи дали имя DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). Проблема актуальна для сайтов, работающих с протоколами SSLv2 и TLS, то есть ставит под угрозу около 33 % всех сайтов и почтовых серверов Интернета, пишет InternetUA.

Проблему обнаружила и помогла устранить сводная команда из 15 человек, в которую вошли ученые из университетов Германии и США, а также специалисты в области информационной безопасности. На официальном сайте уязвимости представлен их подробный доклад.

Исследователи обнаружили в SSLv2 уязвимость, на базе которой сумели построить атаку, во многом копирующую Bleichenbacher-атаку на RSA, известную с 90-х годов. Смысл данной методики в том, что перед установкой зашифрованного соединения клиент случайным образом выбирает ключ сессии, который зашифровывает RSA и отправляется серверу. Таким образом клиент проходит валидацию, и устанавливается защищенное HTTPS-соединение. Атака Bleichenbacher позволяет узнать оригинальный RSA-ключ, основываясь лишь на ответах сервера: простом «да/нет», которое сервер отвечает за запрос «это RSA-ключ сессии?». Эксперты сумели обойти защиту, добавленную в SSLv2, для предотвращения подобных атак и нашли новый способ реализации атаки Bleichenbacher.

«При обычном раскладе злоумышленнику понадобится отследить 1000 TLS-хендшейков, инициировать 40 0000 SSLv2-соединений, и совершить 2^50 оффлайновых операций для расшифровки 2048-битного шифротекста RSA TLS», – пишут исследователи.

Несмотря на такие числа, суперкомпьютер для реализации атаки не потребуется. В докладе сказано, что в среднем для расшифровки сессионного 2048-битного ключа RSA понадобится 8 часов работы облака Amazon EC2, что обойдется атакующему примерно в 440 долл. Но есть и более дешевый и быстрый способ: если добавить в уравнение недавно обнаруженные в OpenSSL уязвимости CVE-2016-0703 и CVE-2015-3197, на расшифровку шифротекста TLS у обычного ПК уйдут считанные минуты. Этого вполне хватит для осуществления man-in-the-middle атаки на любой современный браузер.

Также исследователи отмечают, что под угрозой находятся не только ресурсы, использующие SSLv2 и TLS. Простого отключения SSLv2 можно оказаться недостаточно, если сайт использует сертификат или RSA ключ совместно с другим сервером: распространенные примеры, это почтовые серверы SMTP, IMAP и POP, а также вторичные HTTPS-серверы веб-

приложений. Если отключив SSLv2 на сайте, администратор сайта забудет сменить RSA-ключи и позаботиться о смежных ресурсах, они будут по-прежнему уязвимы перед DROWN.

В докладе сказано, что в наши дни около 17 % всех HTTPS-серверов в мире до сих пор разрешают SSLv2-соединения, хотя протокол SSLv2 давно устарел. Помимо них, из-за совместного использования ключей, еще 17 % HTTPS-серверов оказываются под ударом, что суммарно дает 33 % уязвимых серверов. Это приблизительно 11,5 млн сайтов, включая ресурсы Yahoo, Weibo, Alibaba, xHamster, DailyMotion, BuzzFeed, Flickr, StumbleUpon, 4Shared и так далее.

Всем настоятельно рекомендуется обновиться до OpenSSL 1.0.2g и 1.0.1s. Проверить свои ресурсы на уязвимость перед DROWN можно на официальном сайте атаки. Также, помимо официального доклада исследователей, можно почитать статью М. Грина – известного криптографа и профессора университета Д. Хопкинса.

***

4.03.2016

Рекламные троянцы атакуют пользователей OS X

Вредоносные программы для компьютеров Apple на сегодняшний день распространены не столь широко, как троянцы для ОС Windows и Android, но вместе с тем злоумышленники не обходят своим вниманием владельцев таких машин, пишет ITnews.

Большинство современных вредоносных программ, способных работать в OS X, предназначены для несанкционированного показа рекламы в окне браузера. Не стали исключением и новые троянцы семейства Mac.Trojan.VSearch, обнаруженные в марте специалистами компании «Доктор Веб».

Атака троянцев семейства Mac.Trojan.VSearch на компьютер Apple начинается с установщика приложений, детектируемого Антивирусом Dr.Web как Mac.Trojan.VSearch.2. Он распространяется под видом различных утилит и программ – например, проигрывателя Nice Player. Пользователь может сам скачать его с различных веб-сайтов, предлагающих бесплатное ПО для OS X.

Сразу после запуска установщика в его окне отображается традиционное приветствие. По нажатии на кнопку Continue Mac.Trojan.VSearch.2 должен показать пользователю список компонентов, устанавливаемых помимо приложения, которое он хотел получить с самого начала. В этом списке пользователю обычно предоставляется возможность выбрать необходимые модули, однако на практике этого не происходит: инсталлятор сразу переходит к окну с предложением указать папку установки, при этом он настроен таким образом, будто пользователь сам отметил флажками все предложенные варианты. Среди компонентов, которые Mac.Trojan.VSearch.2 устанавливает на зараженный компьютер, был замечен троянец Mac.Trojan.VSearch.4, а также

множество других опасных и нежелательных программ, в частности MacKeeper (Program.Mac.Unwanted.MacKeeper), ZipCloud (Program.Mac.Unwanted.ZipCloud) и Mac.Trojan.Conduit.

После установки на атакуемом компьютере Mac.Trojan.VSearch.4 обращается к серверу злоумышленников и выкачивает оттуда специальный скрипт, который подменяет в настройках браузера поисковую систему по умолчанию, устанавливая в качестве таковой сервер Trovi. С помощью этого скрипта троянец может скачать и установить на инфицированный «мак» поисковый плагин для браузеров Safari, Chrome и Firefox, детектируемый Антивирусом Dr.Web как нежелательное приложение Program.Mac.Unwanted.BrowserEnhancer.1. И, наконец, эта вредоносная программа загружает и устанавливает в системе троянца Mac.Trojan.VSearch.7.

Попав на инфицированный компьютер, Mac.Trojan.VSearch.7 в первую очередь создает в операционной системе нового пользователя (который не отображается в окне приветствия OS X) и запускает специальный прокси-сервер, с помощью которого встраивает во все открываемые в окне браузера веб-страницы сценарий на языке JavaScript, показывающий рекламные баннеры. Помимо этого, вредоносный сценарий собирает пользовательские запросы к нескольким популярным поисковым системам.

Специалистам компании «Доктор Веб» удалось установить, что в общей сложности на принадлежащие киберпреступникам серверы за время их существования поступило 1 735 730 запросов на загрузку вредоносных программ, при этом было зафиксировано 478 099 уникальных IP-адресов обращавшихся к этим серверам компьютеров. Указанная цифра позволяет сделать определенные предположения о масштабах распространения угрозы. Все представители семейства Mac.Trojan.VSearch успешно детектируются Антивирусом Dr.Web для OS X и потому не представляют опасности для наших пользователей.

***

3.03.2016

Хакеры разработали новые методики показа вредоносных рекламных объявлений

Злоумышленники создают все более сложные схемы по показу и распространению вредоносных рекламных объявлений. Как сообщается в отчете Malwarebytes под названием Operation Fingerprint, хакеры разработали технику, позволяющую проверять компьютеры потенциальных жертв с помощью встроенных в рекламный баннер сниппетов, пишет МедиаБизнес со ссылкой на bin.ua.

Новый подход позволяет авторам наборов эксплоитов действовать более активно, не опасаясь обнаружения со стороны исследователей безопасности. Метод достаточно дешев: 1000 просмотров вредоносных объявлений будут стоить лишь порядка 19 центов.

«Разработчикам вредоносного ПО больше не надо перенаправлять пользователей на вредоносные сайты, распространяющие пакеты эксплоитов. Теперь обнаружить уязвимости на системе жертвы можно с помощью объявлений на легитимных ресурсах. На страницу, распространяющую набор эксплоитов, будут перенаправлены лишь жертвы, использующие уязвимое ПО», – сообщается в отчете Malwarebytes.

Ежедневно злоумышленники используют несколько сотен сокращенных с помощью сервиса goo.gl ссылок для перенаправления пользователей на вредоносные ресурсы. Хакеры запустили более 100 поддельных рекламных доменов и десятки рекламных сетей. Более 42 % всех инфицирований, произошедших в прошлом году из-за вредоносных объявлений, произошли в США.

***

4.03.2016

Интернет-вирус начал вымогать деньги от имени белорусского КГБ

В сети появился вирус, вымогающий деньги от имени Комитета государственной безопасности Республики Беларусь. Об этом сообщает Tut.by, пишет InternetUA.

Вредоносная программа блокирует компьютер пользователя и перенаправляет его на сайт, требующий в течение 12 часов заплатить штраф за просмотр порно в размере 500 тыс. белорусских рублей. Логотип госоргана расположен в левом верхнем углу страницы.

В феврале в Минской области были заключены под стражу трое россиян, подозреваемых в создании аналогичного вируса. Программа требовала внести штраф за просмотр порно от имени МВД, передает БЕЛТА.

В милиции отмечают, что, несмотря на задержание предполагаемых хакеров, вирус продолжает свою вредоносную деятельность в Интернете, пишет Tut.by.

***

10.03.2016

Вірус вперше зміг обійти захист комп'ютерів Apple

Програма під назвою KeRanger шифрує дані на заражених комп'ютерах, а потім просить користувачів заплатити викуп у цифрових валютах, щоб отримати електронний ключ для доступу до їх даних. Таким чином, вірус став першим, що зумів обійти захист комп'ютерів Apple, передає УНН із посиланням на Reuters, пише Від і дО.

«Це перший випадок поразки комп'ютерів Apple дійсно функціонує програмою, вона шифрує дані і вимагає у користувачів оплати», – коментує інцидент директор з кібербезпеки компанії Palo Alto Networks Р. Олсон.

Хакери поширили шкідливе програмне забезпечення за допомогою його завантаження на інтернет-сайт програми Transmission, яка призначається для передачі даних через торрент-трекер BitTorrent, замаскувавши його під нову версію програми. Після установки на комп'ютер вона перебуває в режимі очікування протягом трьох днів, а потім шифрує призначені для користувача файли, вимагаючи за них викуп у розмірі 1 біткоіна (близько 400 дол.).

Наразі шкідливу програму видалили із сайту, також користувачі можуть завантажити нову версію Transmission, автоматично видаляє встановлений на комп'ютер вірус, замаскований під неї.

Своєю чергою представники компанії Apple зазначили, що фірма повинна вжити всіх необхідних заходів, щоб запобігти подальшому поширенню шкідливої програми.

***

11.03.2016

Как спасти переписку от взлома в сети, – советы экспертов

В нынешнее время через Интернет можно взломать практически любое устройство, подключенное к сети. Эксперты рассказали, как можно обезопасить свою переписку в сети от взлома, информирует Экономические известия.

1. Установите на телефон программы, способные мониторить память устройства: что именно у вас установлено, какие ресурсы потребляет. Это позволит вовремя заметить, что какая-то программа работает в Интернете без вашей санкции. Например, что делает сейчас в сети ваша игра, которую вы установили, но не пользуетесь ею в данный момент.

2. Никогда не проходите тесты и опросы в соцсетях. Таким образом вы сами даете доступ к данным своего профиля и своих друзей. То есть расширяете область поражения вирусом, который может быть запущен по сети по полученным контактам.

3. В мобильном Интернете надо следить, на каком именно сайте вы находитесь. Внимательно проверяйте адрес в адресной строке. Внешне этот сайт может быть очень похож на популярный или нужный вам, а на самом деле это клон. Вы, к примеру, нажимаете кнопку Play и в результате оформили подписку на услуги мобильного контента, который втихую будет снимать с вашего мобильного телефона деньги.

4. Менять пароль соцсетей – мало. Легче всего взламывается ваша электронная почта, привязанная к страничке. Поэтому меняйте чаще пароль почты.

5. Лучше не привязывать номер мобильного к страничке в соцсетях, поскольку умельцы могут взломать ваш аккаунт через сим-карту с номером телефона. Просто изготовят клон карточки, быстро зайдут на страничку и поменяют пароли.

***

9.03.2016

Хакери атакували «Єлисаветградський тиждень»

Хакери на кілька днів заблокували сайт інтернет-видання «Єлисаветградський тиждень», пише Week.

«Було видалено близько 20 файлів, що відповідають за роботу ядра сайту. Навряд чи вони видалились самі собою», – прокоментував «Єлисаветградському тижню» один із системних адміністраторів.

На сьогодні роботу сайту повністю відновлено.

Редакція інтернет-видання пов'язує атаку хакерів з тим, що сайт у процесі перейменування Кіровограда активно виступає у підтримку назви Єлисаветград.

***

10.03.2016

Fortinet запускает глобальную программу оценки киберугроз

Fortinet представила новую программу оценки киберугроз Cyber Threat Assessment Program (CTAP), пишет ITnews.

Цель программы – предоставить организациям подробные сведения о типах и количестве киберугроз, которые могут проникнуть в корпоративные сети в обход существующих средств защиты.

Программа является частью более масштабной стратегии компании Fortinet и отдела исследования угроз FortiGuard Labs и направлена на интеграцию рекомендательной функции в комплексную платформу безопасности. Реализуя программу, клиенты получат более достоверное представление об изменяющихся во времени киберугрозах.

Программа предназначена для обнаружения ранее неизвестных угроз и разработки стратегий их устранения

Компания Fortinet совместно с партнерами разработала бесплатную программу оценки угроз для организаций. В ходе подготовки к проведению процедуры оценки в сети клиента устанавливается высокопроизводительный брандмауэр нового поколения FortiGate, который проверяет внутрисетевой трафик приложений на наличие нарушений, вредоносного ПО и приложений, при помощи которых злоумышленники могут получить доступ к файлам конфиденциальных данных и нанести компании-клиенту значительный ущерб. По окончании периода сбора данных с помощью средства FortiAnalyzer создается подробный отчет об угрозах, содержащий сведения о трафике приложений, производительности пользователей, использовании сети, общей подверженности сети риску и сопутствующих деловых рисках. Также отчет содержит подробное описание мер по устранению угроз.

В прошлом брандмауэры гораздо более эффективно обнаруживали сетевые угрозы, так как трафик можно было классифицировать в соответствии

с протоколами, а стратегии злоумышленников не были столь изощренными, – говорит Д. Мэддисон, первый вице-президент отдела продуктов и решений Fortinet. – В настоящее время количество угроз, созданных специально для обхода традиционных брандмауэров, неуклонно растет. Наша новая программа CTAP разработана для быстрого обнаружения угроз, которые не удалось перехватить другим средствам защиты. С ее помощью клиенты смогут добиться повышения эффективности систем безопасности и снизить деловые риски».

Программа Fortinet CTAP незаменима для организаций, которые все еще полагаются на устаревшие системы безопасности, малоэффективные против современных динамических кибератак, осуществляемых по нескольким направлениям. В результате реализации программы тщательного анализа существующих и потенциальных угроз клиенты получают достоверное представление о рисках, угрожающих их сетям, а компания Fortinet и ее партнеры рекомендуют меры по снижению этих рисков. Таким образом, теперь компании-клиенты могут быть спокойны за сохранность важнейших ресурсов.

Слабыми местами многих компаний являются социальные сети и Application Control; чаще всего объектами атак становятся учреждения финансового обслуживания

В течение последних четырех месяцев программа CTAP была реализована сотнями компаний-клиентов Fortinet в США. Данные составленного по результатам анализа отчета позволяют сделать следующие выводы:

1. Независимо от размера и организационной формы, компании сталкиваются с огромным количеством серьезных угроз: число атак, которым подверглись сети, превышает 32,14 млн. В сети продолжают распространяться такие печально известные образцы вредоносного ПО, как Conficker, Nemucod и ZeroAccess. В ходе анализа было обнаружено 5230 экземпляров Conficker, 4220 экземпляров Nemucod и 3210 экземпляров ZeroAccess.

2. Трафик социальных сетей и мультимедийных потоков составляет 25,65 % всего сетевого трафика. Это повышает риск поражения корпоративных сетей и конфиденциальных данных при помощи скрытых загрузок, социальной инженерии и вредоносной рекламы. Наибольший объем трафика приходится на долю социальной сети Facebook – 47,27 % трафика социальных сетей. В то же время 42,29 % трафика потокового содержимого проходит через сервис YouTube.

3. В ходе реализации Application Control администраторы постоянно сталкиваются со сложностями. Рост объема трафика в одноранговых сетях (в основном это обмен данными с помощью протокола Bittorrent и сетевые игры) способствует попаданию в сеть вредоносного содержимого, для распространения которого используются приложения и файлы, загружаемые с популярных сайтов. В процессе внедрения политик Application Control в корпоративных сетях необходимо соблюдать меры предосторожности.

4. Так как хищение финансовых данных в результате проникновения в сети банков и финансовых организаций приносит злоумышленникам наиболее значительный доход, именно эти организации чаще всего становятся объектами атак: на их долю приходится более 44,6 % акций киберпреступников. Для проникновения в сети финансовых учреждений и перемещения внутри них злоумышленники используют молниеносные атаки, изощренные трояны и стратегии поражения сетей.

«Организации постоянно подвергаются кибератакам. Количество направлений атак резко увеличилось, используемые злоумышленниками экосистемы стали более продвинутыми. Чтобы защитить ИТ-ресурсы в этих условиях, компании должны проявлять особую бдительность, – говорит Д. Мэддисон. – Программа оценки киберугроз Fortinet предназначена для тщательного анализа трафика в корпоративных сетях и поиска индикаторов нарушений. В результате реализации программы клиент получает рекомендации по снижению риска и повышению эффективности работы сети».

***

15.03.2016

Хакеры взломали компанию, которая предоставляет защиту от DDoS-атак

Неизвестные атаковали калифорнийскую компанию Staminus Communications, предоставляющую услуги хостинга и защиты от DDoS-атак. Злоумышленники уже опубликовали на Hastebin похищенные персональные данные клиентов компании, пишет Украинский телекоммуникационный портал.

11 марта в официальном Twitter компании появилось сообщение о том, что из-за некоего маловероятного стечения обстоятельств, инфраструктура Staminus временно вышла из строя. Как выяснилось позже, причиной сбоя в работе хостинга стал отнюдь не отказ оборудования, а спланированная кибератака. В выходные сотрудники Staminus были вынуждены вообще приостановиться работу сервиса.

Оказалось, что проникшие в систему хакеры сумели перехватить управление практически всей инфраструктурой хостинга, а затем принялись сбрасывать настройки сетевого оборудования до заводских, что сводило на нет все усилия сотрудников компании. Вскоре на Reddit появилось сообщение о взломе и TOR-ссылки на дамп украденных у компании Staminus данных. Хакеры рассказали об атаке почти художественно, в формате занимательного ezin’a.

Оказывается, им удалось не только поиздеваться над персоналом Staminus, но и похитить базу, содержащую логины, хешированные пароли и email-адреса клиентов компании. Что особенно плохо: дамп содержит реальные имена людей и данные об их банковских картах (в формате обычного текста). Также среди украденной информации можно найти заявки в саппорт, логи

серверов, логи чатов, основную БД Staminus и даже исходные коды некоторых сервисов компании, в частности Intreppid – сервиса защиты от DDoS. К сожалению, подлинность этих данных прессе уже подтвердили многие клиенты Staminus, нашедшие в дампе данные о себе. staminus-580x578 Взломщики не смогли удержаться от сарказма и сопроводили публикацию дампа «советами по работе ИБ-компании». В стиле «Вредных советов», злоумышленники перечислили уязвимости, которые позволили им осуществить взлом Staminus:

***

15.03.2016

Популярные сайты стали жертвами Angler

Десятки тысяч пользователей могли стать жертвами вымогательских или других вредоносных программ после появления определенных рекламных объявлений на популярных сайтах. Вредоносная реклама связана с серверами, распространяющими наборы эксплоитов Angler, сообщают эксперты Trend Micro и Trustwave, пишет InternetUA.

По словам исследователей, в ходе кампании злоумышленники распространяют бэкдор под названием BEDEP, позволяющий загружать на компьютер другое вредоносное ПО. Исследователи Trustwave наблюдали в некоторых случаях распространение вредоносами бэкдора BEDEP и вымогательского ПО TeslaCrypt.

Как оказалось, хакеры получили контроль над доменом brentsmedia[dot]com, использовавшегося в свое время для рекламы в Интернете. BrentsMedia была законной компанией, и хакеры решили воспользоваться ее хорошей репутацией.

Вредоносные объявления были размещены от имени двух рекламных интернет-компаний. Одна из них удалила вредоносное ПО сразу после получения уведомления от Trustwave, а с другой связаться не удалось.

Владельцы сайтов не могут остановить распространение вредоносов, поскольку за рекламу отвечают не они. Несмотря на заметный прогресс в обнаружении вредоносных объявлений, до совершенства еще далеко. Размещение рекламы на сайте с высоким траффиком дает злоумышленнику возможность заразить много компьютеров в короткий промежуток времени.

***

16.03.2016

В Украине создадут Национальный координационный центр кибербезопасности

П. Порошенко подписал указ, которым ввел в действие решение Совета национальной безопасности и обороны от 27 января о стратегии кибербезопасности Украины.

Об этом ИА «МОСТ-ДНЕПР» сообщили в пресс-службе главы государства.

«Целью Стратегии кибербезопасности является создание условий для безопасного функционирования киберпространства, его использования в интересах личности, общества и государства», – отмечается в сообщении.

Стратегия предусматривает комплекс мероприятий, приоритетов и направлений, в частности, – создание и адаптацию госполитики, направленной на развитие киберпространства и достижения совместимости с соответствующими стандартами ЕС и НАТО, формирование конкурентной среды в сфере электронных коммуникаций, предоставление услуг по защите информации и киберзащиты.

Согласно документу, основу национальной системы кибербезопасности составят Министерство обороны, Госслужба специальной связи и защиты информации, Служба безопасности, Национальная полиция, Национальный банк, а также разведывательные органы.

Кроме того, СНБО поручил Кабинету Министров вместе с СБУ, Службой внешней разведки и при участии Национального института стратегических исследований утвердить в двухмесячный срок план мероприятий на 2016 г. по реализации Стратегии.

Также совет решил создать Национальный координационный центр кибербезопасности как рабочий орган СНБО.

***

15.03.2016

За два останніх роки держсайти України зазнали 179 хакерських атак – Держспецзв'язку

Державна служба спеціального зв'язку та захисту інформації України повідомила, що хакери здійснили 179 спроб втрутитися в роботу сайтів органів державної влади та державних підприємств впродовж 2014–2015 рр., пише MediaSapiens.

***

10.03.2016

Сервери Адміністрації Президента часто стають об'єктами кібератак хакерів з РФ

Російські хакери регулярно вчиняють кібератаки на комп'ютери та сервери в Адміністрації Президента України з метою отримання інформації або зараження вірусами, пише iPress.ua.

«Є конкретні віруси, сигнатури, з якими доводиться боротися. І це сьогоднішні реалії», – сказав заступник глави АП Д. Шимків. За його словами, для боротьби з такими атаками держава повинна створювати спеціальні

підрозділи, з навчанням яких можуть допомогти IT-компанії. «IT-галузь володіє всіма необхідними для цього знаннями», – підкреслив заступник глави АП.

У той самий час директор асоціації «IT України» В. Валєєв зазначив, що компанії, які входять до складу асоціації, готові надати таку допомогу.

В асоціацію входить близько 45 IT-компаній, найбільшими серед яких є: EPAM Systems, SoftServe, Luxoft, GlobalLogic та Ciklum.

За словами директора Львівської міськради з інновацій Я. Мірило, аналогічну допомогу в підготовці фахівців з комп'ютерної безпеки готова надати некомерційна організація ICT Competence Center, співзасновником якої вона є.

***

17.03.2016

Сайт телеканала «Херсон плюс» подвергался DDoS-атакам

Сайт телеканала «Херсон плюс» больше 10 дней подвергается DDoS-атаки. Об этом ИМИ сообщил директор телеканала В. Косюк, пишут Херсонские Вести.

Как он заявил, атака началась 4 марта, когда на сайте телеканала был обнародован видеосинхрон председателя Херсонского областного совета А. Путилова. Чиновник на форуме учителей рассказал о своем видении реформы системы образования, на что получил немало критических замечаний и комментариев.

«И уже в 13:00 на сайте телеканала "Херсон плюс" была начата DDoS-атака, пик которой пришелся на 19:00. Всего во второй половине дня 4 марта на сайт телеканала "Херсон плюс" было 42 804 фиктивных обращений, в момент пика – 4700 фиктивных обращений в час. Сайт за это время отдал трафика более 50 ГБ», – рассказал В. Косюк.

Сейчас активность хакеров значительно уменьшилась, сообщил директор телеканала. «Но не из-за того, что они плохо выполняют свою задачу, а потому, что мы используем сервис CloudFlare, который является одним из мировых лидеров по защите от DDoS-атак», – рассказал он.

***

18.03.2016

Symantec предупредила об уязвимостях в своем антивирусном продукте

Компания Symantec предупредила о наличии трех уязвимостей в антивирусном решении Symantec Endpoint Protection (SEP), пишет Центр Информационной Безопасности.

Эксплуатация ошибок позволяет авторизованному пользователю повысить привилегии на системе и выполнить произвольный код. Две уязвимости содержатся в консоли управления SEP. Первая (CVE-2015-8152)

позволяет осуществить XSS-атаку, вторая (CVE-2015-8153) – внедрить SQL-код. Проэксплуатировав проблемы, авторизованный пользователь может повысить привилегии на системе.

Третья ошибка, (CVE-2015-8154), затрагивает драйвер SysPlant.sys и может быть проэксплуатирована для обхода защитных механизмов SEP, предотвращающих выполнение недоверенного кода на системе.

Как указывается в предупреждении Symantec, успешный обход защиты может привести к выполнению произвольно кода с привилегиями пользователя на целевой системе. Злоумышленник может получить доступ к устройству, обманом заставив авторизованного пользователя перейти по вредоносной ссылке или открыть вредоносный документ.

Компания устранила вышеуказанные уязвимости в выпуске SEP 12.1-RU6-MP4 и рекомендует пользователям обновиться до данной версии продукта.

***

18.03.2016

Вредоносное ПО AceDeceiver атакует iOS-устройства без джейлбрейка

Исследователи Palo Alto обнаружили новое семейство вредоносного ПО для iOS-устройств без джейлбрейка, получившее название AceDeceiver. В отличие от других вредоносов для мобильной платформы от Apple, обнаруженных за последние два года, AceDeceiver не использует сертификаты, пишет Центр информационной безопасности.

Вредоносное ПО способно устанавливаться на систему жертвы, обходясь без цифровой подписи. AceDeceiver эксплуатирует ошибки в механизме технических средств защиты авторских прав (DRM), и, даже если Apple удалит его из App Store, вредонос будет по-прежнему распространяться благодаря новому вектору атак.

По словам исследователей, они впервые столкнулись с ПО для iOS, использующим уязвимости в DRM-технологии FairPlay от Apple для установки на устройства без джейлбрейка вредоносных приложений.

Данная техника под названием FairPlay Man-In-The-Middle (MITM) применяется пиратами для распространения нелицензионных программ еще с 2013 г., однако для дистрибуции вредоносного ПО она используется впервые.

Владельцы мобильных устройств от Apple могут загружать приложения из App Store через установленный на Mac клиент iTunes, а с компьютера – на смартфон или планшет. С целью подтвердить факт покупки для каждой устанавливаемой программы iOS-устройство запрашивает код авторизации. Для осуществления атаки FairPlay MITM злоумышленник приобретает в App Store приложение, а затем перехватывает и сохраняет код авторизации. Далее создается десктопное ПО, имитирующее действия клиента iTunes и заставляющее iOS-устройство «думать», будто приложение было приобретено жертвой.

Используя данную технику, пользователь может бесплатно загружать платные программы, а злоумышленник – устанавливать вредоносное ПО без ведома жертв.

***

9.03.2016

В iOS обнаружили четыре уязвимости, позволяющие обойти пароль на iPhone

Пользователь iPhone и iPad может обойти парольную защиту с помощью специально составленных запросов к голосовому помощнику Siri. Об этом сообщает Securitylab со ссылкой на исследование Evolution Security GmbH, пишет Центр информационной безопасности.

Специалисты компании обнаружили четыре уязвимости в iOS, с помощью которых злоумышленники могут обойти пароль на гаджетах. Эксплуатация брешей безопасности позволяет получить доступ к штатным приложениям в ОС.

Как заявил исследователь Б. Меджри, ошибки присутствуют в операционной системе в течение последних трех месяцев. Каждая уязвимость может быть проэксплуатирована с помощью специально составленного запроса к голосовому помощнику Siri.

Так, злоумышленник может попросить ассистента открыть несуществующее приложение. В результате голосовой помощник откроет магазин приложений App Store, откуда злоумышленник может выйти на главный экран устройства в обход процедуры аутентификации.

Аналогичные уязвимости были обнаружены в приложениях Часы и Календарь. Программы позволяют пользователям открывать ссылки в приложении Weather Channel. Если данное ПО не установлено, пользователь будет перенаправлен в App Store. Эксплуатация уязвимости позволит злоумышленнику обойти процедуру аутентификации.

Исследователь связался с Apple и сообщил о наличии уязвимостей в iOS еще в начале года. Компания до сих пор не выпустила исправления и не сообщила, когда ошибки будут устранены.

***

18.03.2016

На устройствах Nexus обнаружили уязвимость в системе безопасности

Функция Factory Reset Protection (сброс к заводским настройкам) является дополнительной мерой защиты в случае потери или кражи Android-устройства, позволяющей стереть все личные данные, включая аккаунт Google, системные настройки, фотографии, музыку и документы. Однако на устройствах линейки Nexus, работающих на необновлённой версии Android 6.0 Marshmallow или

бета-версии Android N, эту защиту можно с лёгкостью обойти. В теории, если кто-то нашёл или украл девайс, то без пароля от аккаунта Google он не сможет сделать сброс и спокойно пользоваться девайсом. В реальности – защиту Factory Reset Protection можно обойти, совершив несложную комбинацию действий, пишет InternetUA.

Видеоблогер под ником RootJunky нашёл уязвимость в стандартных клавиатуре, диалере и приложении обмена сообщениями на Nexus-устройствах, которая позволяет обойти защиту Factory Reset Protection.

Такая же проблема присутствует в первой сборке Android N, которую уже протестировал всё тот же RootJunky. Он снова проделал это на своём Nexus 6P.

Хорошая новость для всех владельцев устройств линейки Nexus заключается в том, что в мартовском обновлении системы безопасности данная уязвимость уже была исправлена. Именно поэтому рекомендуется устанавливать эти апдейты сразу же после их выхода.

***

20.03.2016

ФБР предупредило о растущем риске кибератак на «умные» автомобили

Федеральное бюро расследований США совместно с Министерством транспорта и Национальным управлением по безопасности движения (National Highway Traffic and Safety Administration) опубликовало предупреждение о растущих рисках кибератак на «умные» автомобили, пишет InternetUA.

Современные транспортные средства часто оснащены технологиями, предоставляющими новые возможности для обеспечения безопасности, экономии топлива и пр. Подключенные к Интернету автомобили становятся более уязвимыми для потенциальных кибератак, указывается в сообщении.

В документе опубликован ряд рекомендаций, направленных на минимизацию рисков потенциальных киберугроз. В частности, ведомства советуют следить за выходом обновлений для программного обеспечения авто, не производить никаких несанкционированных изменений в ПО, а также не подключать ненадежные устройства к сети машины и не предоставлять незнакомцам физический доступ к транспортному средству.

***

13.03.2016

Исследователь обнаружил способ осуществления атаки на автобусы

Исследователь безопасности Х. Норте обнаружил способ осуществления кибератак на автобусы, подключенные к Интернету и оснащенные телематическими системами и модемами. Успешное осуществление атаки позволит хакеру перехватить управление транспортным средством, пишет InternetUA.

«К Интернету подключены тысячи телематических систем, не требующих аутентификации. Управление осуществляется через веб-интерфейс или сессию Telnet», – сообщил ИБ-специалист. Хакер с минимальным уровнем подготовки может осуществить атаку на подобные системы и узнать местоположение и скорость транспортного средства или изменить маршрут передвижения.

Для упрощения атаки злоумышленники могут просмотреть подробные сведения о телематических системах в интернете. К тому же большинство подобных систем с открытым доступом можно найти в Shodan. Например, исследователь смог обнаружить 733 телематические системы с открытым доступом по порту 73.

«Устройство подсоединено к схеме зажигания, аккумулятору и прочим компонентам транспортного средства. Страшно представить, что хакеры могут сделать с автомобилем», – отметил специалист. Х. Норте решил не проводить полноценную атаку, поскольку компрометация целого автобуса могла бы привести к непредвиденным последствиям.

***

9.03.2016

Adobe устранила ряд уязвимостей в продуктах Reader и Acrobat

В рамках мартовского «вторника обновлений» компания Adobe выпустила бюллетени безопасности для продуктов Reader и Acrobat, а также приложения Adobe Digital Editions, предназначенного для чтения электронных книг. В данном наборе отсутствуют ставшие привычными патчи для Flash, однако Adobe пообещала представить новую версию медиаплеера уже в «ближайшие дни», пишет InternetUA.

В прошлом месяце в Adobe Flash Player было устранено в общей сложности 22 уязвимости. В основном ошибки были связаны с нарушением целостности памяти или использования после освобождения. Мартовский выпуск получился гораздо скромнее – производитель устранил всего три уязвимости в Reader и Acrobat и одну проблему в Adobe Digital Editions.

Ошибки в Reader/Acrobat были обнаружены участниками проекта Zero Day Initiative компании HP. Две уязвимости CVE-2016-1007 и CVE-2016-1009 связаны с повреждением памяти, третья (CVE-2016-1008) – существует из-за ошибки обхода директории. Эксплуатация данных проблем позволяет удаленному пользователю скомпрометировать систему. Уязвимыми являются следующие продукты:

– Adobe Reader XI 11.0.14 и более ранние версии;

– Adobe Acrobat XI 11.0.14 и ниже;

– Adobe Acrobat Reader DC 15.006.30119 (трек Classic) / 15.010.20059 (трек Continuous) и более ранние версии;

– Adobe Acrobat DC 15.006.30119 (трек Classic) / 15.010.20059 (трек Continuous).

Уязвимость CVE-2016-0954 в Adobe Digital Editions (версия 4.5.0 и более ранние) также связана с повреждением памяти. Эксплуатация ошибки позволяет удаленное выполнение кода. В настоящее время нет информации об активной эксплуатации ошибки. Производитель рекомендует пользователям обновиться до версии 4.5.1.

***

11.03.2016

ISC предупреждает об опасной уязвимости в DHCP

Организация Internet Systems Consortium (ISC) объявила о скором выходе обновленных версий протокола DHCP. В патче будет устранена уязвимость, позволяющая удаленному злоумышленнику вызвать отказ в обслуживании, пишет InternetUA.

Об уязвимости CVE-2016-2774 стало известно в понедельник, 7 марта. Поскольку сервер ISC DHCP не ограничивает количество открытых соединений, злоумышленник может открыть неограниченное число TCP-соединений. Последствия от эксплуатации уязвимости могут быть разными, но чаще всего, по данным ISC, будет происходить отказ в обслуживании. Сервер может прекратить принимать запросы от клиентов, прекратить прием клиентов OMAPI или исчерпать количество свободных сокетов. Также может быть затруднена работа параллельно запущенных служб.

До выхода исправления операторам серверов рекомендуется принимать подключения к коммуникационным каналам DHCP лишь от доверенных хостов. ISC также предлагает ограничить подключения к порту управления OMAPI или полностью отключить данный порт.

Уязвимость будет исправлена в DHCP версий 4.1-ESV-R13 и 4.3.4. Выход обновлений состоится не позже конца нынешнего месяца.

***

7.03.2016

Террористы могут воспользоваться услугами хакеров для похищения нефти

Нефтяные и газовые компании должны максимально подготовиться к возможным хакерским атакам, сообщает The Guardian со ссылкой на ИБ-эксперта компании ERPScan А. Полякова. Злоумышленники могут атаковать предприятия нефтегазовой отрасли ради похищения ценной продукции или с целью осуществления терактов. В настоящее время, когда цены на нефть низкие, и компании всеми силами пытаются урезать расходы, вопрос кибербезопасности стоит особенно остро, заявил А. Поляков на конференции RSA в Сан-Франциско, пишет InternetUA.

По словам эксперта, на предприятиях нефтегазовой отрасли используется множество критических процессов, являющихся потенциальной мишенью для

хакеров. В подобных компаниях, начиная нефтяными вышками и заканчивая автозаправочными станциями, повсеместно используется программное обеспечение, способное стать целью для кибератак.

Работа каждого звена отрасли в значительной степени зависит от различного оборудования – датчиков давления, температуры и уровня горючего и масла, мониторов, позволяющих следить за всевозможными процессами и т. д. Практически все они работают под управлением бизнес-приложений от таких компаний, как SAP и Oracle. Подключенное к Интернету ПО злоумышленники могут атаковать удаленно.

А. Поляков продемонстрировал, как с помощью используемой в одной из нефтяных компаний программы для мониторинга ему и его коллегам удалось осуществить атаку на грузовой отсек танкера с нефтью и незаметно опустошить его. По словам А. Полякова, можно незаметно не только опустошить, но и наполнить хранилище. Данный способ наверняка придется по вкусу террористическим организациям, легализирующим доход от незаконных продаж нефти.

«Нас было всего трое парней, несколько месяцев занятых поиском уязвимостей, а у них [террористов] гораздо больше возможностей», – отметил А. Поляков.

***

5.03.2016

Опасные вирусы, которые можно подцепить в марте

Компьютерные вирусы развиваются и видоизменяются, практически не уступая по скорости своим биологическим собратьям. Каждый день в сети появляются новые и более совершенные угрозы. IGate собрал информацию о наиболее серьезных и интересных вирусах, которые могут угрожать пользователям компьютеров и мобильных устройств в марте 2016 г., пишет InternetUA.

Triada для Android

Эксперты по кибербезопасности обнаружили троян Triada всего пару дней назад. По их словам, ни с чем подобным они прежде не сталкивались. Дело в том, что этот вредонос является первым в истории трояном для операционной системы Android, который способен, подобно вирусу для Windows, внедрять свой код в другие приложения. Вирус использует для внедрения системный процесс Zygote, который является неотъемлемой частью самой операционной системы Android.

Также важно отметить, что Triada имеет модульную структуру. С одной стороны, это усложняет обнаружение следов заражения. С другой, злоумышленники имеют возможность отправлять на устройство жертвы только те компоненты, которые соответствуют поставленной задаче. На данный момент наиболее распространена версия Triada, которая перехватывает микротранзакции. К примеру, пользователь хочет оплатить какой-либо

внутриигровой предмет. Но вирус перехватывает и модифицирует исходящие и входящие данные. В результате платеж пользователя уходит разработчикам вируса, хотя пользователь до последнего уверен, что провел оплату корректно. Вирус Triada на сегодняшний день можно считать самым опасным вредоносом для Android.

Ocean Lotus для OS X

Еще один интересный вирус недавно был обнаружен экспертами компании AlienVault. Это – новая модификация уже известного трояна Ocean Lotus. Впервые этот вредонос был обнаружен еще в 2012 г., но пару недель назад в сети была найдена его обновленная и более опасная версия. Следует уточнить, что Ocean Lotus относится к достаточно редкому семейству вирусов для операционной системы OS X. Эксперты сравнили старую и новую версии трояна. Старая обнаруживается любым из существующих ныне антивирусов. Но новую не находит ни один из них. Цель вируса достаточно проста – он крадет пользовательские данные, включая список недавно открытых документов, и передает их злоумышленникам. Что намерены делать с этими данными разработчики Ocean Lotus, достоверно неизвестно. В 2012 г. вирус был использован для кражи данных правительственных организаций и научных институтов.

Android/Clicker

На днях компания ESET раскрыла одно из крупнейших заражений в истории магазина Google Play. Эксперты обнаружили десятки приложений, зараженных разнообразными модификациями трояна Android/Clicker. Как следует из названия, вирус ориентирован на устройства под управлением Android.

Действие вируса можно считать относительно безобидным. Вирус ничего не крадет, но периодически открывает в браузере порносайты, накручивая, таким образом, их трафик. Впрочем, это может серьезно навредить пользователю, использующему 3G-подключение с ограниченным трафиком.

За последние несколько месяцев злоумышленники загрузили в Google Play несколько сотен зараженных приложений. Одно лишь число модификаций Android/Clicker в магазине достигло 343. Количество установок превысило 1,2 млн.

Тот факт, что махинация раскрылась, вовсе не отменяет возможности того, что в ближайшее время злоумышленники продолжат «пропихивать» в Google Play модифицированные версии трояна. Потому пока единственный способ уберечься от заражения – внимательно изучать отзывы о том или ином приложении. Как правило, пользователи, столкнувшиеся с Android/Clicker, оперативно сообщают о нем в комментариях к приложению.

Acecard для Android

С Acecard для Android лучше не шутить. Этот вредонос не отличается безобидностью и считается одним из самых опасных. Дело в том, что приложение крадёт данные банковских карт и учётные данные для доступа к онлайновым и мобильным сервисам. При этом оно изнутри смартфона

подменяет их официальные сайты поддельными фишинговыми страницами. Кроме того, троян способен перехватывать банковские SMS для проведения транзакций.

Модификации Acecard были замечены даже в официальном магазине приложений Google Play. Некоторые версии вредоноса до сих пор не обнаруживаются никакими антивирусными программами. Троян был замечен практически во всех странах мира, но особенно сильно он распространён в Австралии, Австрии, Германии, России и Франции.

***

15.03.2016

Советы по безопасности от легендарного хакера К. Митника

Практически каждому знакомо имя К. Митника, легендарного хакера, прославившегося чередой громких взломов в 80-х и 90-х годах. В свое время он был самым разыскиваемым киберпреступником мира, но в XXI в. перешел на другую сторону баррикад. Сегодня К. Митник занимается обеспечением компьютерной безопасности. В настоящее время он занимает должность главного менеджера по взлому (Chief Hacking Officer) в компании KnowBe4, пишет InternetUA.

В 2015 г. бывший хакер выпустил книгу «Искусство невидимости» (Art of Invisibility), в которой он делает акцент на социальной инженерии. По его словам, эксплуатируя человеческий фактор и играя на тонкостях психологии, можно взломать систему быстрее, чем при помощи любых сверхсовременных технических средств. «Взломать человека намного проще, чем компьютер, поскольку компьютеры следуют инструкциям, а люди – поддаются эмоциям», – утверждает К. Митник.

Используя свои знания социальной инженерии, экс-хакер дает несколько советов по обеспечению безопасности разнообразных устройств.

Смартфоны

По словам К. Митника, все люди ленивы. Это дает хакерам огромное преимущество. Не международной конференции по кибербезопасности К. Митник подсматривал за тем, как ведущие эксперты отрасли разблокируют свои смартфоны. Практически все они используют пароль из четырех цифр. Это – минимальная длина, которую можно установить. Хакер уверен, если бы система позволяла создавать еще более короткие пароли, этой возможностью пользовались бы, невзирая на угрозу безопасности.

Сам К. Митник использует не какой-то специализированный сверхзащищенный смартфон, а iPhone в стандартной комплектации. По его словам, поведение пользователя более важно для безопасности, чем аппаратные или программные средства. В качестве основного пароля для смартфона К. Митник использует длинную буквенно-цифровую комбинацию, а обычную блокировку экрана снимает с помощью сканера отпечатка пальца Touch ID.

Однажды при въезде в США от хакера потребовали разблокировать смартфон. Тогда К. Митник просто выключил устройство. При этом Touch ID перестал работать, поскольку для включения смартфона нужно ввести основной пароль. Смысл такого действия в том, что суд США имеет право потребовать от пользователя разблокировать iPhone отпечатком пальца, но не имеет права требовать раскрытия основного пароля. Потому иногда знание нюансов закона страны может помочь сохранить свои данные в секрете.

Компьютеры и ноутбуки

В некоторых случаях ограничение прав неопытного пользователя может быть для него благом. В качестве примера К. Митник приводит историю собственной матери. Когда она пользовалась компьютером под управлением Windows, хакеру приходилось раз в неделю приезжать к ней и вычищать из компьютера тонны вирусов.

Тогда К. Митник купил матери Mac и заблокировал установку приложений из неавторизированных источников. Теперь, даже если она проходит по фишинговой ссылке и загружает зараженный файл, вирус не может «укорениться» в системе. Само собой, от целенаправленного взлома это не спасет, но от наиболее примитивных и массовых методов социальной инженерии, вроде поддельных веб-страниц, защитить может.

Направления атаки

По словам К. Митника, кибербезопасность – это не то, что можно настроить один раз и навсегда забыть. Обеспечение безопасности требует от каждого пользователя разумности и внимательности. В идеале, каждый должен быть немножко параноиком.

В доказательство своих слов на прошлогодней конференции CeBIT в Германии К. Митник продемонстрировал ряд приемов взлома, о которых рядовые пользователи могут не догадываться. К примеру, бытует мнение, что флешки становятся безопасными, если в системе отключить для них автозапуск. Тем не менее, К. Митник показал, как с помощью зараженной флешки можно взять систему под полный контроль даже при отключенном автозапуске. По словам хакера, USB-носители априори небезопасны, потому с неизвестными флешками следует обращаться с крайней осторожностью.

Широкая публика недооценивает серьезность угрозы, исходящей от PDF-файлов. К. Митник утверждает, что с помощью зараженного документа этого формата система также может быть взята под контроль.

Особо опасны с точки зрения социальной инженерии общественные точки доступа Wi-Fi. Люди склонны доверять проверенным общественным заведениям, но не учитывают, что их можно подделать. По словам К. Митника, злонамеренный хакер может прийти в интернет-кафе со своим роутером и изменить имя собственной точки доступа так, чтобы оно совпадало с именем местного Wi-Fi. При этом огромное количество посетителей заведения при попытке подключиться к Интернету установит соединение с компьютером злоумышленника.

***

14.03.2016

Эксперты исследовали способы сокрытия деятельности хакеров

Компания Damballa опубликовала отчет, проливающий свет на деятельность киберпреступников. Эксперты объяснили, как киберпреступникам удается оставаться необнаруженными в течение долгого времени, пишет InternetUA.

Специалисты в течение восьми месяцев изучали дроппер Pony, оснащенный средствами для сокрытия деятельности киберпреступников. Как выяснилось, хакеры использовали лишь несколько IP-адресов на каждого провайдера. Подобная осторожность позволяла злоумышленникам дольше оставаться незамеченными.

За период наблюдения хакеры использовали 281 домен и более 120 IP-адресов, принадлежащих 100 различным провайдерам. В сезон отпусков и зимних праздников соотношение доменов к IP-адресам резко увеличивалось.

Хакеры также изменяли вид вредоносного ПО, загружаемого с помощью дроппера. В мае 2015 г. Pony распространял банковский троян Dyre, но уже через четыре месяца дроппер загружал на компьютеры жертв Vawtrak.

Исследователи также изучили способы сокрытия деятельности хакеров от правоохранителей и ИБ-экспертов на примере трояна Destover. Как выяснилось, при инфицировании ПК вредоносом злоумышленники используют две утилиты setMFT и afSET, позволяющие избежать обнаружения и расширить вектор атаки. В результате троян становится сложнее обнаружить – в большинстве случаев специалисты не могут обнаружить ни троян, ни дополнительное ПО.

***

14.03.2016

Эксперты обнаружили новый метод DDoS-атак с использованием протокола TFTP

Группа исследователей из Эдинбургского университета им. Непера (Edinburgh Napier University) обнаружила новый вектор DDoS-атак. Как известно, для усиления так называемого «отражения» DDoS-атак часто используются DNS или NTP, однако эксперты выявили способ эксплуатации для подобных целей протокола TFTP (Trivial File Transfer Protocol), пишет InternetUA.

По словам экспертов, злоумышленники могут использовать уязвимости в публичных TFTP-серверах для запуска масштабных DDoS-атак с отражением. Простое сканирование показало наличие 599,6 тыс. публично доступных TFTP-серверов (TFTP использует порт 69). По словам исследователей, коэффициент усиления атак данного типа гораздо выше по сравнению с другими протоколами и может достигать 60.

«Обнаруженная уязвимость позволяет злоумышленникам использовать публичные TFTP-серверы для усиления трафика так же, как и в атаках другого типа. При наличии определенных условий объем трафика может быть увеличен в 60 раз», – рассказал один из авторов исследования Б. Сиклик в беседе с изданием The Register.

TFTP представляет собой упрощенную версию протокола FTP (File Transfer Protocol) и обычно используется в локальных сетях. Основное назначение TFTP – обеспечение простоты реализации клиента. В связи с чем он используется для загрузки бездисковых рабочих станций, обновлений и конфигураций в «умные» сетевые устройства и т. д.

В настоящее время нет информации об инцидентах с эксплуатацией данной уязвимости, однако на российских и китайских сайтах уже появлялись публикации на эту тему, предупредил Б. Сиклик.

***

8.03.2016

Новый Android-троян симулирует взаимодействие с пользователями

В сети появился новый вариант существовавшего ранее трояна, который научился имитировать поведение пользователей, что должно приносить доход его владельцам. Новый троян получил название Golem и является разновидностью семейства Ghost Push, последние сведения о котором датируются прошлым сентябрём. Ghost Push обладает способностью рутировать устройства и используется в приложениях сторонних разработчиков, чаще всего для отображения рекламы, пишет InternetUA.

Разница между Golem и Ghost Push в новой функциональности, которая позволяет обойти встроенную функцию Android Input, о чём сообщает компания Cheetah Mobile. Она известна такими приложениями, как Battery Doctor, Clean Master, CM Browser, CM Security и CM Launcher.

Инструмент Input предустановлен на Android-устройства и даёт разработчикам возможность выполнять процедуры автоматического тестирования, имитируя поведение пользователей, вроде ввода с клавиатуры и сенсорного экрана. Выполнив рут устройства, Golem скачивает на него приложения, запускает их и симулирует взаимодействие. Жертвами уже стали 40 тыс. пользователей, и это число продолжает расти. Из них большинство живут в Юго-Восточной Азии, в странах вроде Индии, Индонезии и Филиппин.

Результатом заражения трояном Golem является замедление работы устройств и более быстрое истощение заряда аккумулятора. Удаление трояна требует загрузки аппарата в безопасном режиме. Кроме того, Cheetah Mobile предлагает приложение Stubborn Trojan Killer для устранения этого трояна и Ghost Push.

***

6.03.2016
Wired: Как хакеры отключили электричество в Украине

23 декабря 2015 г. на значительной территории Ивано-Франковской области отключилось электричество. Без света остались более 230 тыс. человек. Компания «Прикарпатьеоблэнерго» заявила, что «систему фактически хакнули». Это оказалось правдой. Издание Wired рассказывает о сложной и очень продуманной атаке, в ходе которой хакерам удалось проникнуть в систему и отключить три десятка подстанций, пишет InternetUA.

Оператор одного из центров управления подстанциями около 15:30 заметил, как курсор на его мониторе дернулся, хотя сам он не шевелил мышкой. Курсор двинулся в сторону переключателя, отвечающего за рубильник на одной из подстанций. И дернул его. Оператор схватил мышь, но курсор его не слушался. Оператора выкинуло из системы управления подстанциями.

Как говорит специалист по безопасности Роберт Ли из компании Dragos Security, ко взлому хакеры готовились не меньше полугода. Сначала они внедрили на компьютеры программу Blackenergy 3. Для этого они использовали старый способ: пользователям сети отправляли фишинговые письма с файлами Microsoft Word, которые при открытии предлагали установить макрос. Тот, в свою очередь, вызывал вредоносную программу.

Внутренние сети распределительных центров были хорошо отделены от системы управления подстанциями при помощи файерволов. Wired отмечает, что защита была лучше, чем в американских компаниях, управляющих американской электросетью. Тем не менее, хакерам удалось ее взломать. Они получили данные пользователей для подключения к системе управления подстанциями через VPN и могли подключаться под видом добросовестных пользователей.

На изучение того, как устроена сеть распределительных центров и как она связана с системой управления подстанций, у злоумышленников ушло несколько месяцев. За это время они также написали новую прошивку для конвертеров на подстанциях, которые получают сигнал через Интернет и передают его рубильникам. Как отмечают эксперты, это был первый взлом, когда перепрошивалось непосредственно оборудование.

При начале атаки хакеры отключили источники бесперебойного питания у двух из трех распределительных центров, в сеть которых у них был доступ. После этого они запустили гигантский поток звонков в колл-центр «Прикарпатьеоблэнерго», чтобы жители не могли сообщить об отключении энергии. Одновременно они отключили 30 подстанций и перепрошили там конвертеры таким образом, что операторы перестали видеть их состояние удаленно. Переключить рубильник стало возможно только физически. Кроме того, на компьютерах операторов хакеры запустили программу, которая сделала невозможной перезагрузку.

Таким образом, операторы остались без компьютеров и без возможности включить рубильники удаленно. Свет восстановили через шесть часов. До сих пор рубильники на подстанциях невозможно переключить удаленно, только физически. Энергетикам придется заменить конвертеры, испорченные хакерами. Wired отмечает, что в США последствия такой атаки были бы куда серьезнее: там на подстанциях рубильники нельзя переключить руками.

Украинские власти считают, что за атакой стоит Россия. Reuters также указывал, что программу Blackenergy ранее использовали российские хакеры. В пользу того, что следы ведут в Россию, говорит время отключения энергии: это произошло вскоре после того, как украинские активисты обесточили Крым. Тем не менее, специалисты, опрошенные Wired, не смогли точно сказать, кто стоит за атакой. В принципе, хакеры могли взломать украинскую энергосистему, а потом продать свои наработки России.

Возможно, обесточивание Ивано-Франковской области было связано с планами Украины национализировать энергоактивы, принадлежащие российскому олигарху, связанному с В. Путиным. В тексте не называется его имя, но, известно, что энергетический бизнес в Украине, в частности, ведет Е. Гинер. Ему частично принадлежит компания VS Energy, в чьей собственности находится «Севастопольэнерго» и «Одессаоблэнерго».

***

4.03.2016

Исследователь безопасности обнаружил уязвимость в дроне

Немецкий студент Н. Роддей смог перехватить управление неназванной моделью беспилотного летательного аппарата. Как сообщает CNET, будущий специалист обнаружил несколько уязвимостей в дроне и смог успешно подменить отправляемые устройству команды. Н. Роддей сотрудничал с неназванным изготовителем беспилотников для увеличения степени безопасности продукта, пишет InternetUA.

Во время полета дроны получают команды с наземного центра управления. Данные передаются по каналу XBee. Н. Роддею удалось перехватить и подменить транслируемые команды на собственные. Уязвимость может быть проэксплуатирована удаленно.

По словам исследователя, беспилотники других производителей также могут быть уязвимы к данной атаке. Речь идет о дронах, использующих аналогичную микросхему для управления полетом.

Компания, позволившая Н. Роддею протестировать дрон, приступила к разработке исправления. Обновление будет выпущено в ближайшее время.

Итоги исследования Н. Роддея были представлены на конференции по кибербезопасности RSA, прошедшей в среду, 2 марта, в Сан-Франциско, США.

***

11.03.2016

Осторожно: новый Android-троян крадет данные из банковских приложений

Активное распространение троянской программы Spy.Agent.SI было зафиксировано экспертами компании ESET. Разработчик антивирусного ПО утверждает, что троян успешно обходит двухфакторную аутентификацию и крадет данные из банковских приложений, пишет InternetUA.

Троян маскируется под мобильное приложение Flash Player и после загрузки запрашивает доступ к функциям администратора устройства. Таким образом он защищает себя от удаления со смартфона или планшета под управлением Android.

Данные об устройстве жертвы вредоносное ПО каждые 25 секунд отправляет на удаленный сервер. Разработчики трояна, по словам экспертов, получают название модели смартфона, его IMEI, данные об активации прав администратора и используемом языке.

После этого троянская программа выполняет поиск в памяти Android-девайса банковских мобильных приложений. С удаленного сервера она загружает поддельные экраны ввода логина и пароля, которые появляются поверх реальных и блокируют их до ввода действительных логина и пароля пользователем.

Личная информация отправляется на удаленный сервер, откуда совершается попытка входа в банковский аккаунт. Параллельно приложение перехватывает на зараженном устройстве SMS-сообщение с одноразовым паролем, который выдается банком.

Эксперты отмечают, что троян быстро развивается, и каждую новую модификацию обнаружить всё сложнее. В настоящее время разработчики вредоноса сконцентрировались на клиентах 20 крупнейших банков Турции, Австралии и Новой Зеландии, но не исключено, что вскоре атаки будут перенаправлены на другие страны.

Защититься от вредоносного ПО можно, своевременно обновляя банковские приложения и используя надежный антивирус. Кроме того, крайне опасно переходить по подозрительным ссылкам и скачивать приложения не из официальных магазинов.

***

14.03.2016

Злоумышленники активно распространяют вымогательское ПО Locky

Вымогательское ПО Locky, обнаруженное в феврале нынешнего года специалистами Palo Alto Networks, стало одним из самых распространенных

семейств вредоносов, использующихся в спаме. Об этом сообщают ИБ-специалисты компании TrustWave. По их словам, более 18 % из 4 млн нежелательных сообщений электронной почты содержали вредоносное вложение, загружающее Locky, пишет InternetUA.

Об аналогичных результатах сообщают и прочие ИБ-компании. По данным Fortinet, 16,4 % из 18 млн сообщений, перехваченных системой защиты Fortinet Intrusion Prevention System, содержали вложение, необходимое для загрузки вымогательского ПО. Остальные письма в основном распространяли трояны-вымогатели TeslaCrypt и CryptoWall.

Locky распространяется через ботнет, ранее использовавшийся для передачи вредоносного ПО Dridex. Вначале сообщения содержали вредоносный документ Word с макросом, загружающим вымогательское ПО. Теперь же спам содержит обфусцированный JavaScript-сценарий, при запуске инициализирующий закачку и запуск Locky. По данным исследователей McAfee, подобным образом злоумышленники пытаются обойти антивирусную защиту.

Locky шифрует и добавляет расширение *.locky к файлам на системе. Для восстановления доступа к информации пользователь должен отправить злоумышленнику определенную сумму средств в биткоинах. Для обмена ключами в памяти используется C&C-инфраструктура.

***

18.03.2016

Хакеры Anonymous обнародовали номер телефона и страховки Трампа

Международная хакерская группа Anonymous выложила в сеть персональные данные претендента на пост президента США Д. Трампа. Об этом сообщает The Mirror, пишет InternetUA.

Газета опубликовала видео, в котором хакеры назвали «истинные» цели претендента на президентский пост и указали ссылку на приложение Pastebin, в котором разместили телефонный номер Д. Трампа и номер его страхового свидетельства.

16 марта группа Anonymous пообещала развязать тотальную войну против республиканца. Хакеры завили, что увеличат количество DDoS-атак на сайты американского миллиардера и выведут из строя ресурсы, задействованные в его предвыборной кампании. Киберпреступники анонсировали также публикацию личных данных Д. Трампа. Anonymous призвали всех членов объединения «взяться за оружие» и направить его против республиканца.

Anonymous атакуют сайты Д. Трампа с декабря 2015 г.

***

7.03.2016

Отсутствие проверки подлинности обновлений подвергает риску безопасность пользователей

Общим слабым звеном практически любого программного обеспечения, обладающего механизмом обновления, являются ключи шифрования, пишет ИБ-эксперт Л. Ридж в статье на портале ArsTechnica. При помощи вредоносного обновления злоумышленник может заполучить ключи и полностью скомпрометировать целевую систему, пишет InternetUA.

По словам специалиста, атакующий может обманом заставить жертву установить вредоносную версию какого-либо ПО и получить контроль над системой. Успешное проведение атаки зависит от двух факторов: возможности отправки вредоносного обновления и способности убедить жертву в его подлинности. Проникнув в систему, атакующий может заполучить любые ключи шифрования или другую незашифрованную информацию, доступную для вредоносного приложения.

Как отмечает Л. Ридж, бэкдоры позволяют злоумышленникам выполнять различные действия, к примеру, расшифровать зашифрованные данные или выполнить произвольный код на целевой системе. Успешное выполнение атаки возможно только при наличии определенных условий, однако в результате преступники могут завладеть любыми данными, в том числе ключами шифрования и записями с микрофона или камеры устройства.

По словам Л. Риджа, данная проблема затрагивает практически все широко используемые системы обновления. Значительное количество производителей только в последние годы начали реализовывать проверку подлинности обновлений, однако даже алгоритмы компаний, применяющих подобную практику на протяжении десятилетий, являются ненадежными, отмечает эксперт.

***

6.03.2016

Китай запланировал усовершенствовать национальную кибербезопасность

Китай намерен участвовать в создании правил международной кибербезопасности и борьбе с киберпреступностью, пишет InternetUA со ссылкой на «Синьхуа».

Данные меры указаны в новом пятилетнем плане развития страны в период с 2016 по 2020 г.

Согласно документу, Китай намерен принимать активное участие в создании правил международной кибербезопасности, борьбе с киберпреступностью, а также разработке технологий и стандартов кибербезопасности.

Отмечается, что власти страны намерены более тщательно управлять и национальным киберпространством. Согласно 13-й пятилетке, необходима дальнейшая реализация и усиление контроля за национальной безопасностью.

Не менее важна, говорится в плане, реализация политики страны в области безопасности в таких сферах, как политика, территориальная целостность, экономика, общество, ресурсы и др. Будет усовершенствована и система цензуры, которая также является частью плана по обеспечению национальной безопасности Китая.

***

17.03.2016

Сломанный принтер помог хакерам украсть у ЦБ Бангладеш 100 миллионов долларов

Ошибка в работе принтера не позволила сотрудникам Центрального банка Бангладеш заметить атаку хакеров. Об этом сообщило в среду, 16 марта, агентство Bloomberg со ссылкой на направленное в полицию заявление регулятора, пишет InternetUA.

5 февраля один из управляющих ЦБ З. Худа заметил, что принтер, распечатывающий подтверждения о переводе средств в рамках системы SWIFT, перестал работать в автоматическом режиме, как сказано в документе. Мужчина попытался распечатать подтверждения вручную, но безуспешно. «Мы решили, что это рядовая проблема», – объяснил он. В этот день у сотрудников регулятора был выходной – Бангладеш – преимущественно мусульманская страна, а 5 февраля пришлось на пятницу.

В субботу З. Худа столкнулся с еще одной проблемой: приложение, обменивающееся информацией со SWIFT, не работало. Когда оно было перезапущено, удалось распечатать подтверждения о транзакциях. Выяснилось, что Федеральный резервный банк Нью-Йорка направил в Бангладеш сообщения о 46 сомнительных переводах.

15 марта глава ЦБ Бангладеш А. Рахман покинул свой пост из-за хакерской атаки. Отмечалось, что после инцидента А. Рахман не сообщил правительству о пропаже денег.

О пропаже 100 млн долл. регулятор сообщил 9 марта. Близкие к ЦБ Бангладеш источники сообщали, что украденные деньги были переведены на Филиппины и Шри-Ланку. Центральный банк выяснил, что средства поступили по крайней мере в три филиппинских казино для отмывания.

***

6.03.2016

Морские пираты грабили корабли с помощью хакера

Как описано в последнем отчете Data Breach Digest компании Verizon, команда RISK Team, занимающаяся безопасностью данных, исследовала и решила проблему морского перевозчика с пиратами, пишет InternetUA.

Судоходная компания рассказала о регулярных набегах мелких пиратов. Морские грабители прибывали со сканерами штрих-кодов, искали конкретные ящики, забирали дорогостоящий груз, а потом уплывали прочь. Ввиду вышеперечисленных событий, было принято решение нанять RISK Team для отслеживания возможных источников утечки информации.

Как оказалось, пираты обратились за помощью к хакеру. Злоумышленник взломал не обновлявшуюся систему управления контентом сайта судоходной компании и получил доступ к ее базе данных. Используя скомпрометированную БД, хакер получил доступ к товарно-транспортным накладным и будущим расписаниям отгрузок. С помощью похищенной информации пираты отслеживали маршруты судна и планировали атаки, а затем идентифицировали ящики и забирали дорогостоящий груз.

К счастью, хакер не был специалистом. Verizon упоминает об использовании злоумышленником веб-оболочки, которая не поддерживает SSL, то есть, все выполняемые команды были записаны в журнале веб-сервера.

RISK Team смогла создать график всех действий хакера и точно определить интересовавшие его сведения. Исследователи безопасности также отметили безуспешную попытку злоумышленника получить доступ к другим серверам компании. Они оказались провальными даже после получения доступа к различным учетным записям и паролям. Помимо всего, признаком отсутствия навыков было использование домашнего IP-адреса вместо прокси или VPN.

Verizon помогла судоходной компании блокировать IP-адрес хакера, удалить веб-оболочку, восстановить сервер, сбросить пароли для всех взломанных учетных записей, а также обновить CMS.

***

14.03.2016

Исправленную в 2013 году уязвимость в Java по-прежнему можно успешно эксплуатировать

Плохие новости для пользователей Java – выпущенный компанией Oracle в 2013 г. патч оказался неэффективным. Как сообщают эксперты компании Security Explorations, уязвимость CVE-2013-5838 («Ошибка 69») так и не была окончательно исправлена, поэтому злоумышленники могут эксплуатировать ее и в последних версиях ПО, пишет InternetUA.

Oracle присудила данной ошибке рейтинг 9,3 из 10, поскольку она позволяет неаутентифицированному пользователю удаленно скомпрометировать систему. По словам экспертов, компания неверно оценила степень распространенности уязвимости. Согласно уведомлению Oracle за октябрь 2013 г., ошибка может эксплуатироваться только для обхода песочниц

приложений, использующих технологию Java Web Start, и песочниц Java-апплетов. Как сообщают эксперты, данная информация не соответствует действительности.

«Мы доказали, что “Ошибка 69” может успешно эксплуатироваться в серверном окружении и в приложениях Java на хостинге Google App Engine», – сообщили исследователи.

В 2013 г. Security Explorations представила PoC-код для данной ошибки. По словам главы компании А. Говдяка, после выхода исправления уязвимость по-прежнему можно эксплуатировать – достаточно лишь изменить четыре символа в PoC-коде и использовать свой HTTP-сервер, выдающий ошибку «404» при определенных запросах.

Новый PoC-код может использоваться для эксплуатации уязвимости в последних доступных версиях Java, включая Java SE 7 Update 97, Java SE 8 Update 74 и Java SE 9 Early Access Build 108.

Намерена ли Oracle выпускать экстренное обновление, или планирует подождать планового релиза, пока неизвестно.

***

14.03.2016

Власти Германии предупредили о возможных атаках российских хакеров на энергосистемы страны

Федеральное ведомство по охране конституции Германии (Bundesamt für Verfassungsschutz, BfV) разослало различным немецким торговым ассоциациям письмо с предупреждением о возможной масштабной кибератаке на энергокомплекс страны со стороны хакерской группировки Sofacy. Как сообщает немецкое издание Tagesspiegel, по оценкам экспертов, в худшем случае последствием атаки может стать сбой в работе электростанций, пишет InternetUA.

В настоящее время атаки Sofacy/APT 28 являются «одной из наиболее активных и агрессивных кампаний в виртуальном пространстве», указывается в сообщении BfV. Предположительно, группа Sofacy, также известная под именами APT28, Pawn Storm, Fancy Bear и Sednit, ответственна за кибератаку на Бундестаг в мае 2015 г. Тогда хакеры взломали 14 правительственных серверов и похитили 16 ГБ данных. По данным издания, за Sofacy стоят две российские спецслужбы – ФСБ и Главное разведывательное управление (ГРУ).

***

20.03.2016

Новая уязвимость позволяет за 15 секунд получить контроль над смартфоном

Наверняка вы помните о Stagefright, одной из самых опасных уязвимостей Android, выявленной в последнее время. Исследователи в области

безопасности из Израиля обнаружили новый эксплойт на основе Stagefright, который позволяет полностью передать злоумышленникам контроль над смартфонами LG, HTC и Samsung всего за 15 секунд. Эксплойт получил название Metaphor, пишет InternetUA.

«Метафора» позволяет вредоносной программе попасть на устройство, после чего она может копировать и удалять данные на устройстве. Злоумышленники также смогут получить контроль над камерами, микрофонами и GPS-приемником смартфона.

Как можно стать жертвой Metaphor? Пользователь может получить в виде сообщения ссылку на видео, которое вызывает перезагрузку встроенного медиаплеера. После этого скрипт на странице собирает все возможные данные и отправляет их на сервер, на котором хранится видео. Сервер в ответ отдает другой видеофайл, содержащий в себе вредоносную программу, которая и осуществляет контроль над устройством.

Согласитесь, перезагрузка приложения для просмотра видео не кажется чем-то необычным и обычно не вызывает подозрений у пользователей смартфонов на Android. Злоумышленникам даже не нужно, чтобы вы смотрели видео. Вредоносное ПО может быть заложено в информацию о названии или длине видео, которую считывает устройство.

Уже сегодня исследователи в области безопасности смогли заразить Nexus 5, Galaxy S5, LG G3 и HTC One на версиях Android до 4.0 включительно, а также на Android 5.0 и 5.1. Считается, что другие версии ОС не подвержены атаке.

***

19.03.2016

Мошенники используют LinkedIn для усыпления бдительности потенциальных жертв

Злоумышленники изобрели новый способ усыпления бдительности потенциальных жертв, помогающий сделать их более восприимчивыми к вредоносным рассылкам. Для данной цели мошенники используют социальную бизнес-сеть LinkedIn, сообщает InternetUA со ссылкой на портал Computing.

По словам руководителя IT-отдела юридической компании BLM Э. Юэн, на ее организацию была совершена одна из подобных фишинговых атак. В ходе атаки злоумышленники пытались выманить деньги посредством электронных писем и телефонных звонков, якобы от одного из партнеров компании. Как оказалось, мошенники связались с партнером на сайте LinkedIn и воспользовались полученной информацией для осуществления фишинговой атаки.

В настоящее время фишинг входит в список самых серьезных угроз для организаций в Великобритании наряду с DDoS-атаками. По словам эксперта компании Mimecast О. Скотта-Коули, из-за простоты в реализации фишинг становится все более распространенным методом атаки. Для ее осуществления

не нужно обладать особыми техническими навыками, достаточно просто прикрепить к письму приобретенное на подпольном рынке вредоносное ПО.

Как отмечает О. Скотт-Кроули, люди привыкли доверять почтовым сервисам, в чем и кроется проблема. Мошенники используют данное доверие и обманом пытаются заставить пользователей перейти по вредоносным ссылкам. В результате злоумышленники получают возможность перевода значительных средств со счета жертвы на подконтрольные им счета.

***

7.03.2016
Юлия Гринь
Кто такие Anonymous и против чего они борются?

В последнее время активизировалась деятельность хакерской группировки Anonymous, которая противостоит членам ку-клукс-клана и террористам ИГИЛ. Кто же они такие – эти Anonymous, откуда они взялись и за что борются – попытаемся выяснить вместе! – пишет Hyser.

Кто они и откуда

Можно бесконечно долго рассуждать о том, откуда взялась сама концепция анонимного борца «за все хорошее против всего плохого», но так и не прийти к однозначному ответу. Пожалуй, корни этой славной традиции теряются в глубине веков. Но если говорить конкретно о современном движении Anonymous, то его идея зародилась еще в 2003 г. в разделе /b/ на имиджборде 4chan – полностью анонимном веб-форуме. Раздел /b/ – единственная категория форума, где отсутствуют какие-либо правила. В этом канале царит первозданный хаос и находят отражение диаметрально противоположные стороны человеческой натуры. Абсолютно серьезные дискуссии о квантовой механике и астрофизике, культуре и искусстве здесь могут соседствовать с контентом, от которого обыватель, незнакомый с темной стороной сети, содрогнется от ужаса и омерзения. Не удивительно, что идея анонимных стражей интернет-свободы была выкована и отполирована именно в кипящем «первичном бульоне».

Ошибочно воспринимать Anonymous как некую ограниченную группу лиц с установленной иерархией и лидерами. Anonymous – в первую очередь, идея, которая предполагает, что интернет должен быть максимально свободным и открытым для всех без исключения. Согласно философии Anonymous, ни спецслужбы, ни государства, ни корпорации не имеют права присваивать себе киберпространство и вмешиваться в него, устанавливая цензуру или иные ограничения.

Такая идея изначально не предполагает никакой жесткой структуры или постоянного состава. Само собой, когда речь идет о резонансных взломах с похищением и обнародованием информации, за этим могут стоять вполне определенные хакеры. Но когда на какой-либо «проштрафившийся» объект совершается мощная скоординированная атака силами десятков тысяч

возмущенных пользователей, то каждый из этих пользователей – Anonymous, по крайней мере, до завершения акции.

Операции Anonymous координируются на анонимных имиджбордах, вроде уже названного 4chan, в социальных сетях, общественных каналах мессенджеров и IRC. Существуют отдельные ресурсы вроде AnonOps, где желающие могут не только спланировать свои действия, но и получить инструкции о том, как именно помочь общему делу. В общем, Anonymous представляет собой некое самоорганизующееся общественное сознание Интернета.

Борьба и цели Anonymous

Хотя концепция движения Anonymous возникла еще в 2003 г., первая массовая акция датируется 2008 г. Тогда Церкви саентологии попыталась добиться удаления из сети интервью с Т. Крузом, где тот раскрывал некоторую информацию об этой закрытой организации. Интернет-общественность восприняла этот акт как попытку установления цензуры. На Церковь саентологии обрушился град DDoS-атак, спама (в том числе, бумажного), пранков и критики. Люди в масках Гая Фокса, одного из символов Anonymous выходили на реальные протесты. Эти события способствовали широкому распространению информации о движении Anonymous и его популяризации.

Вскоре после этого борьба Anonymous приобрела и политические оттенки. Когда в 2010 г. по фиктивному обвинению в изнасиловании был арестован основатель Wikileaks Д. Ассанж, интернет-общественность снова активизировалась. Тогда гнев Anonymous был направлен на все организации, прямо или косвенно ответственные за любые ограничения свободы в Интернете, преследования пиратов и Д. Ассанжа. Так, в ходе операции «Расплата» были взломаны платежные системы PayPal, Mastercard, Visa, ресурсы банка PostFinance, сайты шведского правительства и нескольких сенаторов США. Крепко досталось даже Amazon, который ранее «выселил» ресурс WikiLeaks с одного из своих серверов.

После этого Anonymous произвели еще множество успешных операций, атакуя всех, кто, по мнению движения, этого заслуживает: от авторитарных правительств до распространителей детской порнографии.

Интересно, что одна из наиболее успешных операций Anonymous была связана с Украиной. Когда в начале 2012 г. правительство В. Януковича попыталось остановить работу EX.UA, крупнейшего файлообменника страны, это вызвало справедливый гнев общественности. Активисты «положили» сайты Президента, Кабинета Министров, МВД, Службы безопасности Украины, Верховной Рады. Кроме того, люди вышли на реальные акции протеста. Всё это вынудило правительство пойти на попятную и вернуть EX.UA в строй. Спустя два года Anonymous помогали украинцам бороться с властями в ходе Революции достоинства, снова атакуя правительственные ресурсы.

В 2015 г. движение Anonymous активизировалось особенно сильно. Объявление войны террористической группировке ИГИЛ и последующее разоблачение 5,5 тыс. аккаунтов боевиков стало одной из самых масштабных

акций прошлого года. Впрочем, следует признать, что какая-либо религиозная или национальная дискриминация чужда Anonymous. Так, активисты атакуют боевиков ИГИЛ, но когда Д. Трамп выступает с агрессивными высказываниями против всех мусульман, Anonymous незамедлительно атакует и его.

В общем, никем не контролируемое общественное движение Anonymous борется против какой-либо дискриминации и ограничений, будь то попытка установления религиозной диктатуры на Востоке или ужесточение закона об авторском праве на Западе. У общественного сознания, порожденного самой сетью, есть свое собственное видение мира и справедливости. Это можно восхвалять и считать высшей формой общественной самоорганизации. Это можно ненавидеть и считать проявлениями хаоса и анархизма. Но чего делать совершенно нельзя, так это игнорировать Anonymous. Потому что, если верить лозунгу движения, Anonymous – это Легион, который ничего не прощает и ничего не забывает.

***

16.03.2016

Главные источники вирусов в Интернете

За последние лет 10–15 инновационные технологии прочно вошли в нашу жизнь. Мы уже слабо представляем, как жили когда-то без мобильных телефонов, компьютеров, социальных сетей и электронной почты. С одной стороны, такой ИТ-бум – это прекрасно, все вышеперечисленные «блага цивилизации» дают нам доступ к информации, о которой мы ранее и подумать не могли. Но, с другой – растущая интернет-зависимость провоцирует и рост угроз, которые поджидают нас в сети, пишет Hyser.

Для того чтобы донести важность ИТ-гигиены, мы подготовили подборку главных каналов, которые используют злоумышленники для распространения вредоносного кода.

Мобильные гаджеты

В 2016 г., по прогнозам компании Ericsson, общее число подключенных смартфонов достигнет 5,6 млрд. Это практически по одному мобильному устройству на каждого взрослого человека на планете. Однако у такой любови к мобильным гаджетам есть печальные последствия.

Мы используем смартфоны для выполнения финансовых операций, в том числе для приобретения товаров и услуг и отправки различных платежей. При этом, как правило, мы в меньшей степени уделяем внимание безопасности мобильных устройств. Быстрое принятие и доверие к мобильным технологиям не остались незамеченными киберпреступниками. Разработчики используют мобильные устройства для монетизации своих угроз, как никогда раньше.

«До 2011 г. было немного программ для мобильных устройств. Массированное внедрение мобильных устройств, как в корпоративном секторе, так и индивидуально, спровоцировало появление буквально миллионов

мобильных зловредов», – говорит Д. Эмм, старший антивирусный эксперт Kaspersky Lab.

По подсчетам компании Pulse Secure, в 2014 г. было обнаружено почти миллион вредоносных приложений. При этом самыми уязвимыми являются пользователи Android, 97 % всех новых угроз создаются для этой платформы. Среди них программы-вымогатели, шпионские программы, просто вредоносные приложения. Зараженный смартфон может рассылать платные SMS и спам, звонить на платные номера, через него злоумышленники могут подслушивать, а то и подглядывать за вами.

Совет: Устанавливайте мобильные приложения только из официальных источников. Обновляйте мобильное ПО. Настройте права приложений.

USB

USB-устройства для хранения данных могут таить в себе огромную угрозу. Помимо той информации, которую вы записываете на устройство, на флешках может содержаться вредоносное и шпионское программное обеспеченье.

«На съемных накопителях передаются не только данные, но и вредоносное ПО. Эти механизмы активно используются для распространения вредоносных программных кодов», – подтверждает Д. Эмм.

Принцип работы USB-зловредов заключается в том, что при подключении флешки к зараженному компьютеру вредоносная программа модифицирует загрузочный файл Autorun.inf, который определяет параметры автозапуска таким образом, чтобы путь к запускаемой автоматически программе ввел именно на исполняемый модуль вируса. В результате вредоносное ПО на съемном устройстве автоматически запускается при подключении к компьютеру и сразу же заражает компьютер.

Примечательно, что в качестве носителя вируса могут выступать не только привычные нам флешки, но и фотоаппараты, смартфоны, планшеты, плееры.

Совет: Не подключайте чужие флешки к своему компьютеру без предварительной проверки на вирусы.

Почта

Электронная почта уже давно перестала быть простым каналом коммуникации.

По данным Kaspersky Lab, во II квартале 2015 г. доля спама в мировом почтовом трафике составила 53,5 %. Украина в списке стран-источников спама занимает третье место, после США и России.

«Электронная почта также используется для распространения вредоносного ПО. Мы знаем, что молодежь электронной почтой не очень пользуется, но на предприятиях по-прежнему активно используется корпоративная почта, через которую распространяется приложения или ссылки на зараженные сайты», – поясняет антивирусный эксперт.

Один из примеров зловредных писем – фишинговые письма, когда вас, как пользователя почты, пытаются обманным путем вынудить перейти по

ссылке, ведущей на зараженный сайт, или открыть зараженное вложение. Такое письмо могут прислать от имени вашего банка или сотрудника. Фишеры рассчитывают, что на поддельной веб-странице пользователь введет свои конфиденциальные данные, которые сразу же будут доступны киберпреступникам.

Совет: Не открывайте подозрительные письма и их вложения. Если очень надо, то проверьте содержимое письма на вирусы. Не переходите по подозрительным ссылкам, которые есть в письме от адресата, которому вы не доверяете.

Веб-браузеры

Браузеры являются главным окном во Всемирную паутину, что делает эти программы одними из самых ненадежных. Уязвимости браузеров и плагинов успешно используются так называемыми эксплойтами.

Эксплойт – это форма вредоносного кода (по сути, последовательность команд), которая использует существующие дыры в защите программы, чтобы получить несанкционированный доступ к системе или нарушить ее функциональность. Посредством эксплуатирования слабых мест злоумышленники могут украсть личные данные, в том числе пароли к банковским системам, использовать компьютер в качестве элемента ботнета для рассылки спама или выполнения DDoS-атак.

По словам Д. Эмма, подхватить вирус можно просто посетив веб-сайт, на который загружено вредоносное ПО. «Те, кто заходят на инфицированную веб-страницу, автоматически заражают свои компьютеры. Разумеется, если они не установили вовремя обновления», – отмечает эксперт. Простое обновление браузера и популярных плагинов, таких как Adobe Flash, Adobe Acrobat и Java, исправляет известные уязвимости.

Совет: Регулярно обновляйте браузер и плагины. Не заходите на сайты, вызывающие сомнения. Проверяйте веб-страницы на подлинность перед вводом конфиденциальной информации на них.

Соцсети

Социальные сети – сравнительно новый инструмент доставки вирусов к пользователям, обладающий рядом преимуществ по сравнению с почтой и браузерами.

Доступность, скорость, масштабность – эти условия привлекают не только пользователей соцсетей, но и киберпреступников.

Во-первых, пользователи достаточно откровенно ведут себя в социальных сетях, неосознанно передавая все козыри в руки киберпреступников. Отсюда развитие социальной инженерии, взломы и преследования. Во-вторых, в соцсетях информация распространяет почти мгновенно. И в-третьих, соцсети обеспечивают огромное покрытие – количество пользователей исчисляется миллиардами.

«Социальные сети используют для сбора информации для целевых атак и распространению вредоносного ПО в широких масштабах. Они как воры-

карманники, которые орудуют в толпе. А толпа сегодня – это социальные сети», – говорит Д. Эмм.

Только в отличие от реальной жизни, мы еще не научились держать виртуальный кошелек при себе.

Совет: Личные данные должны оставаться личными. Не открывайте доступ к данным на своей страничке незнакомцам. Ограничьте круг друзей.

***

3.03.2016

Военная разведка США: Антивирус Касперского открывает двери для кибератак

Разведывательное управление Министерства обороны США предупреждает, что хакеры российского правительства могут проникнуть в американские системы управления промышленными процессами, используя коммерческое антивирусное программное обеспечение, сообщает Inshe.tv со ссылкой на интернет-издание Washington Free Beacon.

В частности речь идет об использовании антивируса, разработанного российской компанией «Лаборатория Касперского», в американских энергетических и коммунальных компаниях. Оно может сделать системы управления промышленными процессами и так называемые системы оперативно-диспетчерского управления (SCADA) уязвимыми.

По информации Washington Free Beacon, представители военного командования призвали министра обороны Э. Кратера принять меры по защите ключевой инфраструктуры от кибератак на системы управления промышленными процессами.

Разведывательное управление Минобороны опасается, что, если электросети, системы водоснабжения и другие ключевые инфраструктуры США закупят и будут использовать программное обеспечения «Лаборатории Касперского», то хакеры российского правительства могут получить доступ к программному обеспечению промышленности и особым программам удаленного контроля, которые управляют электросетями, нефте- и газопроводами, системами водоснабжения, системами сбора и отведения сточных вод и дамбами.

Высокопоставленные чиновники США заявили, что российские и китайские хакеры уже проводили разведывательные операции для проведения кибератак, в случае если в будущем между государствами возникнет конфликт.

Американские военачальники считают, что угроза для безопасности индустриальных систем США очень серьезна и Пентагону следует разработать электронную систему, которая позволит выявлять уязвимые места в оборонных компьютерных сетях.

Министерство национальной безопасности установило, что с 2010 по 2015 г. угроза кибератак на ключевые инфраструктуры возросла в семь раз.

Кроме того, директор Национальной разведки Д. Клэппер обнародовал информацию о том, что российские специалисты по ведению кибервойны разрабатывают технические средства для удаленного доступа к системам управления промышленными процессами в ключевых инфраструктурах.

Основатель «Лаборатории Касперского» Е. Касперский заявил, что его компания работает со многими правительствами Европы, Азии, Ближнего Востока, а также с правительством России. Но от разведывательных и шпионских служб компания старается «держаться подальше». «Мы – компания безопасности, поэтому мы должны быть независимыми и нейтральными», – подчеркнул Е. Касперский.

Вместе с тем сообщается, что Е. Касперский несколько лет проработал в советском институте военных исследований. Критики отмечают, что, помогая западным правительствам обнаруживать вредоносные программы, «Лаборатория Касперского» «с меньшим усердием» выявляет хакерские попытки российского правительства, пишет Washington Free Beacon.

***

11.03.2016

Составлен рейтинг стран по уровню защиты от кибератак

С каждым днем все чаще случаются кибератаки. Однако некоторым странам киберпреступления не так опасны как другим. Сотрудники Университетов Мэриленда и Виргинии провели анализ уязвимости разных стран, и на основе полученных данный выпустили книгу под названием «Уязвимость 44 Наций в отношении кибератак», пишет Novoston.

Согласно этим данным, США оказалось на 11 месте по уровню безопасности, в то время как скандинавские страны (Дания, Норвегия и Финляндия) оказались на самых верхних строчках рейтинга. Специалисты к числу самых уязвимых отнесли Китай, Индию, Россию, Саудовскую Аравию и Южную Корею.

Данное исследование проводилось на протяжении двух лет, в ходе которого ученые провели анализ около 20 млрд автоматически сформированных отчетов, собранных из 4 млн персональных компьютеров в год по всему миру. В основе рейтингов легло количество кибернетических атак в каждой стране, а также количество нападений на каждый, отдельно взятый компьютер.

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.