Ежемесячный информационно-правовой бюллетень «СМИ и право», №88 (99), сентябрь, 2013г.

Издается Национальной ассоциацией независимых СМИ Таджикистана (НАНСМИТ)

Республика Таджикистан, г. Душанбе, проспект Рудаки, 137.

тел/факс: (992 37) 221-37-11, 224-88-23;

Электронная почта: coordinator@nansmit.tj

Предназначен для всех журналистов, нуждающихся в юридической поддержке, а также для всех лиц, заинтересованных в развитии свободных СМИ и журналистики в Таджикистане.

Поддержка данного издания осуществляется Национальным фондом в поддержку демократии (NED, США) в рамках Проекта поддержки независимых СМИ Таджикистана.

В этом номере:

Новые медиа и информационная безопасность журналиста

Диана Рахманова,

Институт Новых медиа, Бишкек, Кыргызстан

Что такое Новые медиа? Интерактивные электронные издания и новые формы коммуникации производителей контента с потребителями, отличающиеся от традиционных, также любая медиа продукция, являющаяся интерактивной и распространяемая цифровыми методами относятся к новым медиа. Этим термином обозначают процесс развития цифровых, сетевых технологий и коммуникаций.

К новым медиа можно соотнести - блоги, социальные сети, чаты, форумы, он-лайн конференции, электронные редакции, видео порталы и тд.

Развитие цифровых, сетевых технологий и коммуникаций наряду с положительными изменениями в информационном пространстве также имеет ряд опасностей. Опасность, в частности, проявляется в виде краж финансовых средств (веб-кошельки, кредитные карты), кража личных данных пользователей цифровых технологий (личные данные, документы) и физическое обнаружение человека (геолокация, IP адреса и т.п.).

Таким образом, пользуясь новыми медиа, мы не должны допускать такие технические риски как, кражу и подбор паролей, кражу персональных данных, распознавание IP –адреса и установление личности, кражу данных с компьютера пользователей и др.

В тоже время имеет место и кража данных посредством доступа к устройствам передачи как кража оборудования (ноутбуки и флешки), посредством систем оперативно-розыскных мероприятий и блокирование доступа к сети и отдельным ресурсам.

Мы не должны забывать также о законодательных рисках, которые состоит из следующих аспектов:

- Легализация СОРМ (разрешение на контроль траффика со стороны правоохранительных органов);
- Регулирование деятельности СМИ, Интернета, свободы слова и свободы самовыражения;
- Криминализация клеветы, домыслов и «покушения на конституционный строй»;

Каким образом можно обеспечить безопасность в виртуальном пространстве? Для обеспечения безопасности, необходимо предпринимать комплекс технических, инфраструктурных и законодательных мер, которые могут обеспечить эффективное обнаружение кибератак и противодействие им.

На наш взгляд, противодействие кибератакам можно осуществить с учетом реальных ситуаций. Вот некоторые советы:

- Законодательные и инфраструктурные риски кибербезопасности журналиста при работе в Сети зависят от усилий (лоббирование и

эдвокаси) всего гражданского сообщества;

- Проведение эффективных кампании по обходу блокировок может минимизировать попытки ограничение доступа к Интерет ресурсам;
- Личная техническая безопасность должно быт приоритетом в деятельности журналиста;
- Необходимо повышение потенциала создателей контента в сфере их информационной безопасности.

Вместе с тем, все пользователи информационно- коммуникационных технологий должны знать и следовать таким советам как, шифрование данных (http – https), пользоваться надежной почтой и более сложными паролями. Не менее важно осознать ценности персональной информации, хранимой в учетных записях, особенно в почте и меньше пользоваться твердыми носителями (флешки, диски и т.д.);

Выводы и советы к активным пользователям новых медиа:

- Привязывайте учетные записи к номеру телефона;
- Используйте разные сложные пароли к доступу на разные ресурсы;
- Блокируйте доступ к вашим компьютерам и гаджетам с помощью паролей и экранов блокировок;
- Храните как можно больше информации он-лайн под псевдонимом;
- Развивайте свои знания в сфере кибербезопасности.

Урегулирование Интернета: попытки, результаты и последствия

Мухаммади Ибодуллоев

Общественный Фонд ГИПИ, г.Душанбе

Среда интернета сегодня является весьма разнообразной. Интернет позволяет нам обучаться и дает знания, способствует открытию или продвижению бизнеса, предоставляет информацию. В тоже время Интернет является средством связи и дает огромные возможности развлечения пользователям. Он способствует уменьшению расходов связанных с распространением информации позволяя охватить неограниченное количество ее получателей. Благодаря возможностям интернета можно обеспечить интерактивность и выход за национальные границы, как при получении информации, так и при её распространении.

Исходя из всего, что сказано выше задаемся вопросом - нужно ли регулировать Интернет?

В пути регулирования Интернета мы столкнемся рядом проблем технического и юридического характера. Проблемы в юридической сфере в первую очередь указывают на определение национальных границ, что порождает очередной вопрос – каким образом?

Технические проблемы охватывают разработку соответствующих индикаторов, также создание и внедрение технологий.

В тоже время, регулирование Интернета влечет за собой ряд последствий, таких как недостаточное развитие зоны и содержания/контента, недостаточное развитие человеческих ресурсов и информационная безопасность.

Попытки урегулирование Интернета в Таджикистане начались давно. В январе 2006 года в целях улучшения сферы Интернет распространилась информация о создании Единого коммутационного центра (ЕКЦ) в интернет издании http://www.centrasia.org/. Позже прошла презентация проекта создания ЕКЦ Министерством связи РТ и обсуждение проекта в СМИ (январь - март 2006).

Обращая внимание на аргументы «против» Мобильной связи (МС) можно сделать такие выводы, как трудности управления соединениями и эксплуатацией, плохое качество обслуживания абонентов, высокие эксплуатационные расходы и низкую надежность сети. В тоже время можем перечислить целый ряд аргументов «за» Мобильной связи - легкость в управлении, высокую надежность и низкие затраты, гарантийное качество обслуживания абонентов, также оптимизация и упрощение соединений между операторами.

После долгих споров, этот вопрос так и не был решен. Второй этап истории с ЕКЦ началась в феврале 2009 года, когда Министерство транспорта и коммуникаций РТ повторно представил проект создания «Единого коммутационного центра электрической связи» на утверждение в Правительство Республики. В ответ на этот шаг операторы мобильной связи направили открытое письмо Президенту страны. В письме отмечалось, что реализация данного проекта в конечном итоге может привести к пагубным последствиям. ЕКЦ сведет на нет все достижения по развитию телекоммуникационной сферы и рыночных отношений в этой области за последние двадцать лет. 25 февраля 2009 года все игроки рынка ИКТ собрались за стол переговоров, чтобы обсудить проект "Единого коммутационного центра электрической связи". Тем не менее, вопрос создание ЕКЦ не увенчался успехом.

Можно ли Интернет соотнести к СМИ? Интернет является лишь инструментом распространения и доступа к информации, следовательно, нельзя его отнести к СМИ. Обращая внимание на негативную информацию в Интернете, мы должны понять, что это не проблема, а его последствие. Следовательно, надо работать над самой проблемой. И вопрос регулирование Интернета должен касаться в большей степени инфраструктуру, а не контента/содержания информационных ресурсов.

Относительно блокировок веб-ресурсов в Таджикистане можно вспомнить, что первые были зафиксированы в 2003 и 2007 годах. Первый случай был в 2003 году накануне референдума во время выборов. Позже осенью 2010г. наблюдались блокировки нескольких СМИ. Весной и летом 2012 года были блокированы СМИ и социальные сети (март, июнь, июль). Последние годы наблюдается блокировки

новой тенденции - снижение уровня сигнала при входе на определенные ресурсы, также блокировка широкополосного доступа и вход через мобильный Интернет.

Возвращаясь к вопросам регулирования можно поставить вопрос иначе: Саморегулирование лучше, чем регулирование? В мире имеется богатый опыт саморегулирование Интернета. Исходя из этого, в Таджикистане также принят **Этический кодекс электронного гражданина (эТИКет).**

Этический кодекс электронного гражданина (эТИКет)

Этического кодекса электронного гражданина — результат совместной деятельности заинтересованных сторон с целью развития отечественного контента Интернет и практики его саморегулирования в Республике Таджикистан. Проект разработан группой отечественных экспертов, как одна из инициатив по повышению информационной культуры общества.

Для разработки проекта, рабочая группа изучила национальный и международный опыт по саморегулированию на примере управление доменного имени страны, «Этические нормы журналистской деятельности», управление Интернетом на глобальном уровне и «Press Council» Боснии и Герцеговины.

Экспертная группа состоит из представителей структурных подразделений Исполнительного аппарата Президента Республики Таджикистан, государственных органов и общественных организаций. Проект разработан при поддержке Интерньюс Нетворк, Института «Открытое Общество» Фонд Содействия и Организации по Безопасности и Сотрудничеству в Таджикистане.

Состав рабочей группы по разработке проекта Этического кодекса:

- Структурные подразделения Исполнительного аппарата Президента Республики Таджикистан:

1. Информационно-аналитический отдел
2. Отдел транспорта и коммуникаций
3. Юридический отдел
4. Информационно-технический центр
5. Сектор информационно-коммуникационных технологий

- Учреждения и организации:

1. Национальный центр законодательства при Президенте Республики Таджикистан
2. Служба связи при Правительстве Республики Таджикистан
3. Ассоциация операторов мобильной связи Таджикистана
4. Национальная Ассоциация независимых средств массовой информации Таджикистана
5. Общественный фонд ИНДЕМ
6. Общественный фонд Гражданская инициатива политики Интернет
7. Ассоциация Интернет Сервис Провайдеров

Мы, члены цифрового информационного общества, принимая этический кодекс электронного гражданина, выступаем за то, чтобы этические нормы реальной жизни полностью соблюдались и в виртуальном пространстве.
Нормы настоящего кодекса претворяются при общении по мобильному телефону и во всемирной сети Интернет.
Сокращенный вариант настоящего акта – эТИКет, составлен из слов «мобикэт» и «нетикэт», вместе обозначающие этикет пользования информационно-коммуникационными технологиями.

1. При пользовании и претворении информационно-коммуникационных технологий (ИКТ) общественные интересы должны превалировать .
2. Позитивное мышление, позитивное общение, позитивные деяния, независимо от местонахождения и времени, обязательны.и в виртуальном пространстве.
3. Соблюдение и уважение прав и свобод человека, национальных законов, международных правовых актов и в виртуальном пространстве обязательны.
4. Этика общения должна соблюдаться и при использовании ИКТ, пользователь обязан представиться и коротко и внятно объяснить причину своего обращения.
5. Соблюдение прав и этики использования первоисточников обязательны и при пользовании ИКТ.
6. Уважение норм государственного языка и национальных традиций обязательны и в виртуальном пространстве.
7. Длительное громкое общение по телефону и другими средствами связи в общественных местах недопустимо.
8. Неприемлемо использование посредством ИКТ неприятных (режущих слух) звуков, нецензурных слов и громкое прослушивание музыки в общественных местах.
9. ИКТ должны использоваться, не нарушая покоя и не нанося вреда здоровью людей.
10. Нельзя использовать оборудование и технологические средства других пользователей без их разрешения.
11. Использование ИКТ для преследования, оскорблений, клеветы, провокаций, паники, из корысти, местничества и других недопустимых побуждений - неприемлемо .
12. Уважение интеллектуальной собственности обязательно, плагиат и с использованием ИКТ запрещается.
13. Слова и информацию другого человека (пользователя) нельзя искажать и/или сокращать.

14. Посредством ИКТ нельзя распространять спам.
15. Личная информация человека и в виртуальном пространстве является неприкосновенной, использование её без разрешения пользователя недопустимо.
16. Ущемление прав пользователя по национальному, языковому, религиозному, расовому и гендерному признакам и в виртуальном пространстве запрещается.
17. Злоупотребление недостаточными технологическими знаниями и навыками других пользователей недопустимо.
18. Защита прав и интересов несовершеннолетних и нуждающихся является приоритетной задачей в пространстве ИКТ.
19. Запрещается использование неэтичных и незаконных комментариев к информации других пользователей.
20. Каждый человек (пользователь) несет ответственность за распространенную им информацию.
21. Каждый человек (пользователь) несет ответственность за нарушение этики в виртуальном пространстве ИКТ.

(Источник: http://cipi.tj/)

Как создавать и хранить надежные пароли?

- ·How-To Booklet

Люди привыкли защищать важную информацию с помощью ключей. Ключ от квартиры, ключ зажигания в автомобиле, PIN-код банковской карточки, пароль к электронному почтовому ящику, и так далее. Есть ключ — есть доступ. Можно построить сложную систему запоров, задвижек, замков, сейфов, но если все это открывается единственным универсальным ключом, который висит на крючке у входной двери, грош цена такой системе безопасности.

Чтобы обеспечить своей информационной безопасности, вам необходимо придумать надежный пароль для работы с компьютером. Каким должен быть хороший пароль? По мнению экспертов по кибербезопасности пароли должны быт:

- **Достаточно длинным.** Хотя бы 8-10 символов. Иногда компьютерные программы используют целые парольные фразы.
- **Неочевидным.** Грубую ошибку совершает тот, кто выбирает в качестве пароля личную информацию, например, номер телефона или кличку любимой собаки. Эти данные могут быть известны другим людям, а значит, им несложно подобрать пароль. В фильме "Идеальное преступление" весь план главного героя в исполнении Майкла Дугласа развалился в один момент из-за того, что он выбрал для своего личного сейфа ужасный пароль — дату собственной свадьбы.
- **Уникальным.** Не используйте один и тот же пароль снова и снова. В противном случае удачный подбор — и все ваши сайты, дневники, сообщения на форумах достанутся злоумышленнику. Общее правило: каждому ресурсу — свой пароль.
- **Обновляемым.** Пароль — не надпись на памятнике. Меняйте его время от времени. Случается, что человек так привыкает к паролю, что не хочет с ним расставаться. Пароль не меняется месяцы, а то и годы. Чем дольше хранится пароль, тем выше вероятность, что его в конце концов узнают те, кому не следовало.
- **Приватным.** Некоторые наклеивают листочки с паролями на монитор. Наверное, у вас нет этой вредной привычки. Но если пароль все-таки стал известен другим людям (*скомпрометирован*), смените его как можно скорее. Не стоит хранить пароли в открытых текстовых файлах, документах Word, словом, в таких "контейнерах", которые с легкостью откроет и прочтет всякий.

Для обеспечения надежности пароля можно пользоваться некоторыми хитростями. Вот несколько примеров:

- Меняйте регистр. Как вам, например, такой пароль: "сЕмнадцать мгнОвений вЕсны"? (Каждая первая гласная в слове дана в верхнем регистре).

- Используйте не только буквы и цифры, но и другие значки, например, точки, дефисы. Иногда можно удачно заменить букву цифрой, скажем, так: "30л0тые ябл0ки с0лнца". Здесь буквы "О" заменены нулями (а буква "З", кстати, цифрой "3").

- Попробуйте мнемонические выражения. Что такое, к примеру, "КПЧУУРЗЯСФО"? Кажется, что бессмыслица, а на самом деле — начальные буквы слов стихотворения "Ворон" Эдгара По (предлоги опущены): "Как-то в полночь в час угрюмый, утомившись от раздумий, задремал я над страницей фолианта одного".

Даже если вы забудете свои записи, такой пароль вы без большого труда сможете восстановить по памяти (если, конечно, помните первую строчку "Ворона", а если нет, кто мешает использовать строчку из вашего любимого произведения?).

"Парольные" программы

Пара-тройка сайтов, любимый форум, почтовый клиент — везде нужны пароли. Если вы активно работаете на компьютере, счет идет на десятки. Запомнить все пароли невозможно!

Некоторые записывают пароли в текстовый файл, а затем шифруют его с помощью криптографической программы. Но можно, использовать специальную программу для создания и хранения паролей. Одна из таких программ — KeePass. Пароли хранятся в защищенной базе данных. По сути дела, вам нужно запомнить единственный пароль, который дает вход в саму программу KeePass (пароль,

конечно, должен быть надежным). Программа помогает создавать пароли, упорядочивать их (так, что ими становится удобно пользоваться). KeePass может работать с USB-флешки, ее удобно носить с собой.

(Адаптировано из https://securityinabox.org/ru/)

Защита паролем

Общие замечания
I. Не полагайтесь на пароли Windows, надеясь, что они защитят ваши данные. Эти пароли нетрудно вскрыть.
II. Пароль должен быть длиной минимум 8 символов (пройдет время, и мы будем советовать не менее 9!). Можно использовать в качестве пароля короткое предложение.
III. Хороший ход – записать пароли и хранить их в надежном месте. Плохое решение – использовать простые и легкие для угадывания пароли(1).
IV. Используйте цифры, буквы в разных регистрах и небуквенные символы.
V. Не используйте один и тот же пароль в двух разных системах.
VI. Не придумывайте паролей, которые непосредственно связаны с вашей частной жизнью или интересами.
VII. Не делайте ваши пароли достоянием гласности.
VIII. Меняйте пароли каждые 3-6 месяцев.
IX. Помните, что в Интернете распространяется немало программ, которые способны "вытащить" на белый свет пароль Windows, ключ к шифрованию беспроводной связи и почти любой другой пароль.

Хорошие пароли много значат для безопасности компьютера. Пароль играет роль барьера, ограничивающего доступ к той или иной "двери", будь то учетная запись электронной почты, вход в локальную сеть или онлайновый банковский счет. Пароль по смыслу похож на дверной ключ. Можно иметь несколько ключей для дома, офиса, машины, сейфа. Все эти замки – разные. Нужна целая связка ключей, чтобы иметь возможность пользоваться ими. Это создает препятствия злоумышленникам. Даже если вор подберет какой-то один ключ, он не сможет отпереть им другие замки. А они становятся все более сложными и дорогими. Их собирают из множества частей, и все для того, чтобы затруднить вскрытие. То же касается паролей. Это своего рода замки к вашим информационным хранилищам. Современные компьютерные системы таковы, что информация может обладать куда большей ценностью, чем содержимое шкатулки или сейфа. Значит, ваши пароли должны обеспечивать не меньшую степень защиты, чем самые дорогие замки.

В мире цифровых угроз, где мы с вами живем, пароль – важнейшая часть любой системы. История учит, что пароли нередко оказывались легкой добычей для хакеров и прочих злоумышленников, которые покушаются на информационные системы.

Взлом

Можно ли скомпрометировать пароль? Да, и несколькими способами. Например, можно просто подглядеть, как некто набирает свой пароль на клавиатуре. А можно установить программу-перехватчик, которая будет отслеживать нажатия на клавиши и передавать эти сведения "хозяину". Бдительный пользователь способен оградить себя от этих бед. Присматривайтесь к тому, что происходит вокруг, регулярно запускайте анти-шпионские и антивирусные программы, не забывайте их обновлять.

Сбор данных

Чтобы подобрать пароль, злоумышленник может задаться целью собрать персональные данные о его владельце. Довольно часто люди выбирают в качестве паролей то, что легко запомнить: год рождения, имя кого-то из членов семьи или друга, место рождения, название любимой футбольной команды и т.д. Злоумышленник аккуратно собирает такие данные. Он присматривается к вашему рабочему месту, обращает внимание на книги в шкафу. Почему мы выбираем простые пароли (по крайней мере, выбирали до сегодняшнего дня)? Потому что человеку трудно запомнить множество разных паролей, с которыми у него не возникает никаких ассоциаций. Но простой пароль легко "сдается" злоумышленнику, если у того есть персональные данные его владельца. Сегодня это самый распространенный способ получить доступ к информационной системе (и настойчивые хакеры нередко им пользуются).

Многие сайты в Интернете позволяют восстановить забытый пароль, если вы ответите на заранее определенный "секретный вопрос". По какой-то необъяснимой причине список типичных "секретных вопросов" так или иначе касается вашего имени, клички животного, названия школы, девичьей фамилии матери. Вроде бы, зачем напрягать память, когда можно запросто набрать хорошо знакомый ответ на несложный вопрос и получить пароль по e-mail? Увы, это сильно упрощает жизнь не только нам, но и злоумышленнику. Если вы натолкнетесь на такой странный механизм "обеспечения безопасности" (то есть, вам предложат ответить на простой вопрос о вашей частной жизни), откажитесь. Если без этого никак не получается завершить процедуру регистрации, проявите фантазию и придумайте какую-нибудь абракадабру. Но не полагайтесь на такой способ восстановления забытого пароля..

Социотехника

Есть довольно хитрые методы выуживания пароля у человека. Существуют целые сценарии. Телефонный звонок, вы снимаете трубку, и на другом конце провода раздается вежливый голос: "Здравствуйте, это ваш провайдер Интернета. Мы устанавливаем новый сервер и проявляем заботу об информации клиентов. Мы не хотим, чтобы вы потеряли электронную почту. Пожалуйста, напомните, какой у вас пароль?" Или же какой-то тип представляется сотрудником из другого отдела вашей компании: ему нужен пароль для доступа к общему ящику электронной почты. А единственный человек, знающий пароль, увы, тяжело болен, поэтому...

Такие приемы называются "социотехника". Есть множество примеров того, как люди раскрывали важную информацию (и подвергали риску своих знакомых и свой бизнес), поддавшись на обман. Хакеры широко применяют социотехнику, чтобы получить доступ к

интересным для них ресурсам.

Ни в коем случае не раскрывайте компьютерную информацию (особенно пароли и коды доступа) по телефону, если вы не можете подтвердить личность собеседника.

Метод перебора

Пароль можно угадать, если задаться целью перебрать все возможные комбинации: взять электронный словарь и проверять слова подряд. На первый взгляд кажется, что это весьма трудоемкая задача. Для человека – да, а для компьютера – считанные секунды. Если вы используете в качестве паролей правильно написанные слова, то за минуту-другую такой пароль может быть взломан методом перебора.

Давайте угадаем: может быть, вы используете в качестве пароля первую строчку из всемирно известной песни? Сегодня едва ли не все стремительно переводится в цифровую форму. Возникают целые электронные сборники литературных произведений. Вооружившись таким сборником, злоумышленник представляет серьезную угрозу для ваших паролей. Подумайте дважды перед тем, как выбрать в качестве пароля осмысленную фразу, комбинацию слов или законченное предложение.

Некоторые системы парольной защиты устойчивы к методу перебора, например, банкомат и мобильный телефон. Хотя ваш пароль, в сущности, состоит всего из нескольких цифр, система заблокируется после трех неверных попыток отгадывания пароля.

Создаем пароли

Мнемонический метод

Есть немало способов придумать пароль, который трудно вскрыть и легко запомнить. Популярный метод – мнемонический. В этом случае мы используем какой-либо прием, облегчающий запоминание, например, рифму или акроним.
Заменяем слова на первые буквы (существительные – в верхнем регистре). Можно проявить фантазию:

За двумя зайцами погонишься, ни одного не поймаешь: z2Zp-1-p

Вот как этот метод работает в английском языке (даже смайлику нашлось применение):

Are you happy today?: rU:-)2d?

Это самые простые примеры. Всегда можно придумать свой способ кодирования цифр и слов. Попробуйте сами. **Замечание**: вряд ли стоит копировать приведенные выше примеры паролей.

Полезные программы

Что еще можно сделать для совершенствования ваших паролей? Использовать специальную программу, которая позволяет их создавать. Она случайным образом генерирует последовательность букв и цифр и может хранить их в защищенном формате. Вы будете иметь по-настоящему трудные пароли, не истязая при этом свою память. Неплохое решение! Программы для создания паролей обычно маленькие, их можно держать на дискете или флэш-диске.

Пароли можно разложить по категориям. Чтобы перенести пароль из вашего хранилища в прикладную программу, удобно пользоваться обычным буфером памяти. Пароли дополнительно защищены шифром. Таким образом, единственный пароль, который вам по-настоящему надо знать – это ключ к этому шифру.

Конечно, придется потратить немного времени, чтобы внести все пароли в такую программу. Но затраты окупятся сторицей.

Пароль нередко становится первым и самым важным способом обеспечения безопасности ваших данных. Его можно сравнить разве что с дверным ключом. Работать без пароля – все равно, что оставлять дверь распахнутой на ночь. Может, никто и не заберется к вам в квартиру, а может, вам не повезет; кто знает? Подумайте о том, насколько надежные пароли вы создаете и где их храните. См. также такие программы, как PasswordSafe (http://passwordsafe.scoureforge.net) и Keypass (http://keypass.scourceforge.net).

(Источник: Адаптировано из https://equalit.ie/esecman/russian/chapter2_2.html)

Как журналисты могут использовать Storyful MultiSearch?

Наташа Тайнс, IjNet

Поиск информации в социальных сетях становится общей практикой в журналистике. Наглядным примером такой ситуации может служить то, как сильно редакции полагаются на видео гражданских журналистов во время освещения конфликта в Сирии.

С увеличением количества социальных медиа-платформ журналисты всё более нуждаются в возможности просматривать всё большее количество сайтов и сетей для получения последней информации и поиска контента, который они могли бы использовать. Этот процесс может занимать много времени и создает технические проблемы, так как большое количество открытых вкладок браузера может вывести

некоторые браузеры из строя.

Storyful, идентифицирующий себя как "новостную ленту социальных медиа", недавно предложил решение этой проблемы: приложение с открытым исходным кодом “Storyful MultiSearch", которое позволяет журналистам одновременно выполнять поиск на нескольких платформах социальных медиа.

Этот инструмент - расширение браузера Google Chrome. После загрузки в углу браузера появится лого с изображением увеличительного стекла. Ввод одного ключевого слова в поле поиска, которое открывается в правом углу браузера при клике на увеличительное стекло, немедленно даёт результаты с Twitter, Twitter videos, Twitter images, Tumblr, Instagram, Storyful News, Storyful Viral и Spokeo. Результаты отображаются в отдельных вкладках браузера, число которых в настоящее время ограничено восемью.

По словам Маркхэма Нолана, главного редактора новостных сервисов Storyful, с момента запуска в начале сентября более 850 пользователей добавили это расширение к своим браузерам. "Мы получили отзывы в числе прочих от журналистов Wall Street Journal и Аль-Джазира, которые говорят, что это большая помощь", - сказал он IJNet .

Storyful MultiSearch сперва был протестирован членами команды Storyful. Как сказал в пресс-релизе Адам Томас, директор Storyful по развитию бизнеса, организация сделала это расширение общедоступным, чтобы облегчить жизнь журналистам. "Наши журналисты часто используют этот инструмент, который не только экономит время на поиск информации о последних новостях, но и помогает в работе над материалами, которые должны быть опубликованы не так срочно".

Сам инструмент имеет некоторые ограничения. Одно из них – то, что он не даёт журналистам возможности искать в Facebook. Однако, в настоящее время ни одна программа не делает этого. "В Интернете практически не существует вебсайта, дающего возможность открытого поиска в Facebook, - сказал IJNet технический директор Пол Уотсон - OpenStatusSearch.com [который был полезным инструментом для журналистов] перестал работать. Поиск на самом сайте facebook.com не даёт результатов, полезных для журналистов”.

Кроме того, инструмент в настоящее время работает только в одном браузере: Chrome.

"Портирование на другие браузеры – задача нетривиальная, и мы надеемся, что те, кто хочет использовать это расширение в Firefox, или Safari, или Internet Explorer, обратятся к разработчикам в своих редакциях, чтобы они сделали ответвление от доступных в открытом коде исходников", - сказал Уотсон.

Storyful надеется вскоре предложить вниманию журналистов и другие инструменты. "У нас есть и другие расширения браузера, которые мы хотим открыть, а также другие библиотеки и инструменты, - сказал Уотсон и добавил, что создание такого рода проектов, это "возвращение сообществу того, что мы используем в нашем коммерческом коде" (новостной бизнес Storyful построен вокруг проверки социального медиа-контента командой журналистов и исследователей, среди их клиентов такие гиганты, как New York Times, Channel 4 News, ABC, France24, Reuters и Bloomberg).

Также Storyful недавно запустил проект Open Newsroom project на Google + , который позволяет подписчикам этой группы работать вместе над проверкой циркулирующего в сети медиа-контента.

Скачать расширение Storyful MultiSearch можно здесь. Для получения исходного кода нажмите сюда.

Наташа Тайнс – работающий на двух языках цифровой журналист из Вашингтона, округ Колумбия. Она - основатель Tynes Media Group, предлагающей различные решения в области медиа для клиентов по всему миру. Ранее она работала в Международном центре для журналистов, где занималась разработкой и управлением программой интерактивного обучения и программой для Ближнего Востока. Также она работала журналистом и редактором на Ближнем Востоке в течение более чем десяти лет, сотрудничала с с Аль-Джазира, Jordan Times и Arabia Online. Вы можете ознакомиться с её мыслями на тему журналистики, цифровых СМИ и ситуации на Ближнем Востоке на ее веб-сайте, следить за ней в Twitter или связаться с ней по электронной почте ntynes (at) gmail.com.