О НЕКОТОРЫХ АСПЕКТАХ ИСПОЛЬЗОВАНИЯ СОЦИАЛЬНЫХ СЕТЕЙ В ПРЕПОДАВАНИИ
SOME ASPECTS OF USE SOCIAL NETWORKS IN TEACHING

Богданова Диана Александровна
ИПИ ФИЦ ИУ РАН, Москва, Россия

Ключевые слова: Социальные медиа, безопасное поведение в сети, кража идентичности, романтическое мошенничество.

Резюме. Приводятся базовые правила безопасного поведения в социальных сетях, рассматриваются реальные ситуации с кражей идентичности, приводится пример законодательного регулирования проблемы в Евросоюзе.

Keywords: Social media, social networks safety, identity theft, romantic scam.

Summary. The basic rules of safe behavior in social networks are given, the real situation of identity theft considered, an example is given of legislative regulation of the problems in the European Union.

Социальные медиа стали неотъемлемой частью современной жизни. По результатам исследований, проведенных в 2014 году американской компанией Pew Research, три четверти взрослого населения США используют социальные медиа. Среди молодежи эти показатели несколько выше. По результатам опросов, опубликованных Министерством связи Великобритании в 2014 году, подростки 11-14 лет только 3% своего времени, потраченного на общение, пользуются телефоном. Остальное общение проходит в сетях или через сервисы мгновенного обмена сообщениями. У взрослых картина несколько иная, но и у них на телефонные разговоры тратится лишь около 35% от общего времени, потраченного на общение. Какое определение можно дать социальным медиа? Если задуматься, практически весь Web уже можно считать социальным. Почти каждый сайт, который мы посещаем, на котором делаем покупки или заказываем услугу, предлагает оставить комментарий, написать мнение или предлагает поделиться в Facebook-е, Вконтакте или Твиттере. Даже Википедия имеет свой социальный аспект в виде форума. Институт информационных технологий Юнеско дает довольно лаконичное, но емкое определение: «Социальные медиа на основе использования технологий дают возможность общения, иными словами, социальные медиа — это медиа для социального взаимодействия» [1].

Многие преподаватели примкнули к социальным медиа в той или иной степени, для профессиональной деятельности или личного общения. С профессиональной точки зрения это может способствовать развитию рабочих контактов, повышению уровня профессиональных знаний или послужить основой для образовательных проектов. Стали появляться инициативы по продвижению учебных заведений в социальных сетях [2]. Что касается личного использования, то здесь преподаватели так же, как и их студенты, имеют семьи, родственников, друзей, с которыми они поддерживают общение, обмениваются новостями. И именно в связи с некоторой двойственностью пребы-

вания себя в сети преподавателю имеет смысл проявлять в своих действиях повышенную предусмотрительность и дальновидность: какие посты можно размещать, с кем можно общаться, кого можно зачислять в «друзья», делая, таким образом, некоторую часть своей личной жизни видимой. Иными словами, возникает необходимость разделить профессиональное общение преподавателя и общение с друзьями и близкими, то есть, его профессиональную и личную жизнь в информационной среде. Предлагаемый перечень простых правил, скорее всего, не потребуется молодым преподавателям — опытным пользователям информационно-коммуникационных технологий, но может оказаться полезным «новичкам», не очень уверенным пользователям.

- Социальные сети, такие, например, как “Вконтакте”, имеют целый ряд параметров конфиденциальности. Однако зачастую в соответствии с настройками по умолчанию данные пользователя остаются открытыми, и его можно легко найти через поисковые системы такие, как Яндекс или Google. Поэтому для начала очень важно проверить настройки и сделать страничку доступной только для друзей, чтобы информация о пользователе: данные, фотографии и т.д., не могли увидеть посторонние.
- Лучше размещать на своей странице только нейтральную информацию, стараясь избегать материалов, которые могут быть истолкованы неоднозначно. На Западе уже стало нормой, когда при приеме на работу сотрудники HR-отделов проводят поиск и анализ Интернет-историй соискателей.
- Следует принимать запрос на регистрацию в друзьях только в том случае, если человек лично известен и/или есть желание иметь его в своих друзьях. Обязательно следует интересоваться настройками безопасности друзей в сети.
- У бывших студентов могут быть друзья среди студентов сегодняшних, поэтому лучше не принимать запросы на регистрацию в друзьях от студентов и молодых людей (или их родителей) — коллег. Если младшие члены семьи зарегистрированы в списке друзей и при этом имеют друзей среди студентов, никогда не следует забывать о том, что то, что написано, будет видимым не только для ваших друзей.
- Следует помнить об осторожности: например, “Вконтакте” написанный на стене друзей текст, может быть увиден и посторонними людьми: все зависит от настроек конфиденциальности владельца стены.
- Следует помнить о том, что фотообменные сайты зачастую не имеют настроек конфиденциальности по умолчанию.
- Следует хранить свои профессиональные материалы отдельно от личных. Для личных дел в Интернете, таких, например, как покупки онлайн, лучше создать отдельную учетную запись электронной почты.
- При заполнении различных регистрационных форм он-лайн желательно отвечать только на «необходимые» вопросы, а не на все только потому, что об этом спросили: ведь не известно, для кого эти данные.
- Если возникло подозрение, что кто-то выдает себя за вас в социальной сети и т. п., следует сразу же сообщить об этом службе

поддержки этой социальной сети. Подобные действия являются нарушением правил.

На этом аспекте хотелось бы остановиться подробнее. Кража идентичности (незаконное использование чужих личных данных) получила широкое распространение в Интернете: крадутся номера банковских карт, банковских счетов, номера карт социального страхования, фотографии с личных страничек и т.д. Этот аспект имеет непосредственное отношение не к преподаванию, а к преподавателям. Здесь хотелось бы привести две истории, реальных людей, преподавателей — профессиональных контактов автора. Доцент, коллега автора, неожиданно узнал от своих студентов, что он появился в «Вконтакте» с довольно странной информацией о себе, где, например, среди своих друзей «он» упоминал Усаму бен Ладена, и просился в «друзья» к своим студентам. Была размещена его фотография, сделанная во время лекции. Страничка, очевидно, была создана одним из недовольных студентов, просуществовала она около полугода, а затем была удалена. Вторая история — профессора А.С. из университета Реджины (Канада). В 2013 году автору довелось учиться на МООС «Социальные медиа в образовании», организатором которого был этот профессор. Он активный сторонник теории коннективизма, и курс был организован в соответствии с этой теорией. У него есть аккаунты в Твиттере, Facebook-е и Linkedin-е, еще он ведет блог. Есть все основания считать, что профессор — грамотный пользователь социальных сетей. Произошедшая с ним история описана в его блоге. Вот уже на протяжении нескольких лет мошенники используют его фотографии для романтических (любовных) афер (romantic scam). Стоит отметить, что профессор обладает довольно приятной внешностью. Мошенники, используя его фотографии, фотографии его детей, размещенные на его странице в Facebook-е, создают фальшивые странички, с другим именем и фамилией, заводят по переписке романтические отношения с женщинами и обманным путем выманивают у них крупные суммы денег. Впоследствии, когда обман вскрывается, обманутая жертва начинает поиски, и находит ни в чем не виноватого профессора, предъявляя к нему претензии. Современные сервисы позволяют легко манипулировать внешностью (http://msqrd.me/products, faceswaplive.com/), что мы уже имели возможность наблюдать в развлекательных телевизионных программах. Однако недавно объявленная разработка Стэнфордского университета [3] может быть использована мошенниками для подтверждения аутентичности персонажа, за которого они себя выдают. Персонаж, чье изображение будет использовано, удаленно управляется актером, движения мышц лица которого, повторяются персонажем. Довольно часто для проверки аутентичности нового знакомого, ему предлагают пообщаться по Скайпу. Это — проверка реальности образа на странице в социальной сети. С помощью такого сервиса мошенник, управляя мимикой персонажа, может создать у собеседника впечатление, что он общается с реальным человеком. Если собеседник не знает голоса персонажа, то он вряд ли сможет распознать обман. Следует отметить, что обращения профессора в Facebook с указанием фальшивых аккаунтов пока что к результату не приве-

ли. Более того, по обращениям мошенников, Facebook дважды закрывал аккаунт профессора. И, чтобы статус-кво восстановить, ему пришлось дважды отправлять копию своего паспорта для доказательства аутентичности. Таким образом, следует признать, что, хотя существуют рекомендации обращаться в службу поддержки сети, обращения далеко не всегда приводят к желаемому результату. Поэтому есть смысл самим предпринимать превентивные меры предосторожности. Что это может быть? Во-первых, защита фотографии, планируемой к размещению в соцсети, с помощью бесплатных программ водяных знаков(watermarks), доказывающих право собственности (приложения существуют и для IOS, и для Android). Специалисты говорят, что водяные знаки можно удалить, но это очень трудоемкая работа, и на фотографии признаки удаления останутся [4]. Можно периодически проверять, не использует ли кто вашу фотографию, для чего воспользоваться обратным поиском Google. Для этого необходимо выбрать опцию Images, в строке поиска выбрать изображение камеры, загрузить фотографию, которую необходимо проверить. Google вернет каждый случай использования фотографии, если таковой будет обнаружен. Однако в силу настроек приватности этот поиск не может гарантировать абсолютного результата. Как сообщает портал финской государственной телерадиокомпании «Yle» [5], в соответствии с директивой ЕС, обязательной для исполнения во всех странах Евросоюза, с осени 2016 года вступит в силу закон, согласно которому за ложный профиль в социальных сетях можно получить штраф. В самой Финляндии кража идентичности станет уголовным преступлением с 4 сентября. Автору не удалось найти информации об аналогичных законодательных актах в России.

Таким образом, использование социальных сетей предоставляет большие возможности для общения, в образовательном плане способствует организации обучения на ином, более привычном для современного поколения уровне, однако содержит массу опасностей, во избежание которых совершенно необходимо предпринимать все возможные меры предосторожности.

Список использованной литературы

1. [Электронный ресурс] Режим доступа: iite.unesco.org/pics/publications/en/files/3214685.pdf (дата обращения: 10.04.2016).

2. Апостолова, Т.М., Савва, С.С. Социальные сети и имидж университета [Электронный ресурс] Режим доступа: http://www.tehnosfera-edu.ru/publ (дата обращения: 10.04.2016) .

3. Real-Time Face Capture and Reenactment of RGB Videos[Электронный ресурс] Режим доступа: http://www.graphics.stanford.edu/~niessner/thies2016face.html (дата обращения: 10.04.2016).

4. Chastain, S. What is a watermark? How can I add a watermark to my photos? [Электронный ресурс] Режим доступа: http://graphicssoft.about.com/od/glossary/f/watermark.htm (дата обращения: 11.04.2016).

5. [Электронный ресурс] Режим доступа:http://yle.fi/uutiset/news/ (дата обращения: 12.04.2016).