УДК37.035:004.85

СОЦИАЛИЗАЦИЯ ЛИЧНОСТИ во Всемирной паутине

Диана Александровна Богданова,
старший научный сотрудник Института кибернетики и образовательной информатики Федерального исследовательского центра «Информатика и управление» Российской академии наук, кандидат педагогических наук

С приходом Интернета исчезли множественные пространственно-временные барьеры — и в общении люди перестали быть привязанными только к тем, кто физически находится в непосредственном окружении: появилась возможность устанавливать мобильные связи по всему миру. Технологии проникли в различные аспекты повседневной жизни. Сейчас не принято разделять жизнь на онлайн и настоящую, потому что онлайн — это тоже настоящая жизнь. Однако вместе с технологиями пришёл и довольно внушительный список рисков, связанных с их использованием. И взрослым пользователям Всемирной паутины, и молодёжи, входящей в сетевое пространство, необходимо помнить о том, что жизни онлайн и офлайн, тем не менее, имеют существенные различия: нельзя действовать в Сети, опираясь на представления, сформировавшиеся в реальной жизни.

• *интернет-безопасность* • *цифровые следы* • *управление сетевой репутацией* • *кража идентичности* • *сетевое мошенничество* • *катфишинг* • *аутентификация в социальной сети* • *дезинформация*

Человек в Интернете

Миллионы людей по всему миру сталкиваются с проблемой: как разумно существовать в условиях, когда в Интернете записывается всё — и ничто не забывается, когда каждая фотография в Интернете, обновление статуса, запись в «Твиттере» или

запись в блоге, сделанная нами, о нас или от нашего имени, могут быть использованы мошенниками, сохранены навсегда и много лет спустя оказать негативное влияние на текущую ситуацию.

Каждый раз, выходя в Интернет и действуя там, мы оставляем, подобно следам на мокром песке, цифровые отпечатки деятельности, так называемые «цифровые следы». Можно сказать, что «цифровые следы» — это информация о конкретном человеке, которая существует в Интернете в результате его онлайн активности[1]. Например, вся деятельность в социальных сетях на различных платформах, постановка «лайков», написание комментариев — это всё «цифровые следы». Цифровые следы, которые человек оставляет, в дальнейшем могут оказывать влияние на его жизнь, поэтому важно понять, как ими управлять. Проще управлять формированием активной части цифрового следа, особенно в социальных сетях. В этом случае не следует заниматься такой деятельностью, о которой мы не хотим, чтобы люди узнали. Некоторые придерживаются позиции, что им нечего скрывать, поэтому нет смысла беспокоиться о цифровых следах. В реальности такой подход ошибочен[2]. В Сети располагается огромное количество третьих лиц, занимающихся сбором информации. Пишем ли мы твит, ставим ли лайки или просто просматриваем страницы — происходит негласный сбор информации, которая используется с коммерческими целями и имеет коммерческую стоимость. На цифровых следах зарабатывают структуры, с которыми люди не знакомы и никогда не вступали ни в какие отношения, и их деятельность никак нельзя проконтролировать. И даже если нечего скрывать, всегда существует какая-то часть информации, не подлежащая распространению перед широкой аудиторией. Медицинской информацией поделимся в семье, но не обязательно на работе. Или, например, следы могут быть поданы в ином контексте или неверно истолкованы. Или, например, верующий человек не хочет рассказывать об этом широкой аудитории. Не существует простого механизма, позволяющего запретить сбор информации, или, например, влиять на то, что можно распространять, а что — нет. Некоторые правительства отслеживают, что публикуется в социальных сетях — и дело в отдельных случаях может закончиться даже лишением свободы. Однако цифровые следы имеют и позитивную сторону. Оставляя положительный цифровой след, пользователь укрепляет имидж. И когда кто-то при поиске в Интернете найдёт только хорошие следы, это выгодно для пользовательского имиджа. Кроме того, участие в профессиональных сообществах, форумах, общение с другими специалистами в конкретной области может подчеркнуть сильные стороны пользователя и его индивидуальность.

В качестве первого шага пользователю следует проанализировать, какой информацией он делится[3]. Нельзя быть уверенными в том, что другие будут обращаться с чужими постами так, как бы хотелось авторам. Поэтому, прежде чем разместить что-нибудь онлайн, имеет смысл прочитать это дважды. Если возникли сомнения относительно того, как это может повлиять на автора или его друзей, не следует спешить с отправкой, лучше отложить её.

Во-вторых, следует всегда выходить из Сети; использовать псевдонимы; держать пароль в секрете — относясь

---

[1] DigitalFootprins [Электронный ресурс] / Kidsmart: aChaildnetwebsite // Режим доступа: http://www.kidsmart.org.uk/digitalfootprints/(дата обращения: 19.10.2017).

[2] *Богданова Д.А.* О создании и мониторинге цифровой идентичности / В сборнике: Современные информационные технологии в образовании материалы XXVIII Международной конференции 2017. — С. 120–122.

[3] Building and keeping a positive digital identity. A Practical Approach for Educators, Students and Parents[Электронныйресурс] / ISTE. Whitepaper, 2015 // Режим доступа: https://www.iste.org/resources/product?ID=3689&name=Building+and+Keeping+a+Positive+Digital+Identity (дата обращения: 22.11.2017).

к нему как к зубной щётке, которой никто ни с кем не будет пользоваться совместно и будет менять её регулярно. Также следует напоминать о том, что сетевые настройки приватности не гарантируют полной защиты размещённой информации. Бывает так, что сети меняют правила, а иногда у сетей появляются новые владельцы. В качестве примера можно привести Instagram и Facebook. Поэтому, помня о настройках конфиденциальности в социальных сетях, следует тщательнее подходить к отбору размещаемой информации, сознавая, что конфиденциальность очень уязвима и зависима от грамотного и аккуратного поведения самого пользователя: лучшие настройки — это, собственно, поведение пользователя, его самоконтроль.

В-третьих, следует хорошо подумать, кому размещаемая информация предназначается, с кем ею можно делиться. Принимая это решение, можно воспользоваться правилом «первой полосы»: хотелось бы увидеть эту информацию на первой полосе газеты или на домашней странице каждого из своих знакомых? Если ответ отрицательный, тогда следует воздержаться от её размещения.

В-четвёртых, желательно проанализировать размещаемую информацию ещё по одному критерию. Для этого лучше представить, что цифровой след остаётся в Сети навсегда. То, что в данный момент кажется смешным или актуальным, может выглядеть нелепым и сформировать отрицательное впечатление через несколько лет. Поэтому написанное давно может случайно возникнуть много лет спустя и начать преследовать пользователя.

Например, согласно опросу компании Microsoft, 75% американских рекрутеров признали, что компании требуют проверять кандидатов по их онлайн занятиям, и многие просматривают целый ряд сайтов, тщательно изучая претендентов в социальных сетях, по фото и видеообменным сайтам, персональным страницам, блогам, онлайновым играм, обращая внимание и на «историю». Семьдесят процентов рекрутеров при этом сообщили, что им приходилось отказывать кандидатам из-за информации, найденной в Интернете, например, неприличных фотографий, сделанных, в том числе, много лет назад, или членства в предосудительных группах. Или другие примеры: 16-летняя британская девушка, уволенная с работы за жалобы на Facebook: «Мне так скучно!»; 66-летний канадский психотерапевт, которому было отказано во въезде в США за публикацию 30-летней давности в философском журнале об экспериментах с ЛСД — подобные примеры множатся с каждым днём. При этом следует помнить и о том, что злоумышленник может воспользоваться украденной информацией или украденным именем в собственных целях — и это может нанести ущерб сетевой репутации невиновного человека.

Защита сетевой репутации

В настоящее время для защиты сетевой репутации необходимо выполнять целый спектр различных действий[4]. Рассмотрим, что рекомендуется делать сегодня для самостоятельного управления репутацией лицам, не являющимся продвинутыми пользователями Интернета.

1. Поискать себя в Интернете. «Погуглить» имя во Всемирной паутине, а также воспользоваться его поиском в Googleimage. Установить оповещение Googlealert на имя, чтобы отслеживать новый материал, который, возможно, будет появляться. Можно будет получать уведомления, отправляемые, например, один раз в день.

2. Купить себе доменное имя. Существуют разные мнения относительно того, сколько усилий и денег следует в это вложить. Одни рекомендуют захватывать множество доменных имён — imya.com, imyafamiliyaonline.com, imyafamiliyablog.com и т.д., утверждая,

[4] *Frederiksen L.* The visible expert profile: Ian Brodie / L. Frederiksen [Электронныйресурс] // Hinge. — 2015. July 15. — Режим доступа: https://hingemarketing.com/blog/story/visible-expert-profile-ian-brodie (дата обращения: 12.10.2017).

что чем больше имён удастся получить, тем лучше. Другие считают такой подход чрезмерным. Лучше выбрать одно доменное имя и приложить некоторые усилия для создания контента, который будет жить на сайте. Здесь можно разместить ту информацию о себе, какую пользователь посчитает необходимым. Здесь можно также размещать интересные статьи и комментарии к ним.

3. Разместить всё содержание в одном месте. Есть несколько сайтов, которые сейчас позволяют это сделать. Среди них, например, WordPress и About.me. Можно также «присоединить» доменное имя к этим сайтам. Это означает, что любой, кто зайдёт на imya.com, будет перенаправлен на страницу About.me или на страницу WordPress. Это удобно, потому что WordPress, например, предлагает хорошо разработанные шаблоны, что позволяет организовать материал таким образом, что сайт будет похож на разработанный профессионалом, без необходимости нанимать дизайнера.

4. Присоединиться к социальным сетям. Как известно основные — социальные сети (доступные в России) — это Facebook, Twitter, Google+, «ВКонтакте». Даже если по внутреннему ощущению нет времени для активного присутствия в них, всё же следует присоединиться и стремиться найти время для того, чтобы заполнить профили. Можно не быть очень активным, но и не быть полностью спящим. Желательно добавлять новый контент не реже одного раза в месяц. Это можно делать очень просто, например, размещая ссылку на статью с указанием в коротком комментарии, почему это интересно.

5. Оптимизировать присутствие в социальных сетях. Необходимо заполнить страницы в социальных сетях настолько полно, насколько возможно, настраивая URL-адрес, и повторяя имя там, где это необходимо. Также желательно использовать полное имя, а не псевдоним или фразу, которая выглядит броско. На большинстве веб-сайтов можно установить связь с другими.

6. Держать частное частным. Сейчас многие молодые люди знают, что неразумно публиковать фотографии, пьющего алкоголь или танцующего полуодетым. Многие также сознают, что не смогут контролировать фотографии, размещаемые друзьями. Совершенно необходимо установить параметры конфиденциальности для всего контента, которым есть желание поделиться только с избранной группой друзей и членами семьи. Однако Facebook и другие сайты постоянно меняют правила конфиденциальности. А друзья могут разместить «неудачные» снимки без согласия изображённых на них лиц.

Поэтому не следует размещать личные фотографии, не предназначенные для широкого просмотра. То же относится и к публикации фотографий маленьких детей, играющих, например, сидя голыми в ванне. Ведь у этих фотографий есть шанс появиться, когда дети подрастут. И они их точно не порадуют. Как считают дети Евросоюза, родители не должны размещать в Сети их детские фотографии прежде, чем получат на это разрешение самих детей. Продолжая эту цепь рассуждений, возникает естественный вопрос: что же тогда безопасно и разумно размещать? Альтернатива — создание двух профилей: одного для «аутсайдеров», содержащего только профессиональную информацию, другого для узкого круга, для близких, используя самые строгие настройки конфиденциальности. При всей трудоёмкости ведения двух профилей, это в определённой степени может быть компромиссным альтернативным решением. Кстати, к такому подходу иногда прибегают дети, которые хотят скрыть занятия в Сети от родительского ока.

Если кто-то из друзей размещает фотографию, по поводу которой есть возражения, то можно удалить тег, идентифицирующий человека на фотографии, если не удастся убедить разместившего удалить фотографию. Бывают и такие печальные ситуации, когда фамилия и имя человека совпадают с именем преступника или просто правона-

рушителя. Бывает и так, что кто-то намеренно распространяет о человеке негативную ложную информацию. По мнению специалистов в области когнитивистики, большая проблема с развенчанием дезинформации заключается в том, что она продолжает влиять на суждения и выводы даже после опровержения[5]. Именно для таких случаев активный действующий профиль может сыграть добрую службу. Регулярный мониторинг на предмет появления возможного негатива поможет принять защитные меры незамедлительно. Если автор, разместивший негатив, отказывается его удалить, рекомендуется организовать серию положительных материалов, которые сместят появившийся «негатив» на последние страницы поисковой выдачи. По этому поводу существует гиковский анекдот: «Где ты спрятал труп? На третьей странице поисковой выдачи». Иными словами, негатив будет появляться, но на последних страницах результатов поиска и вряд ли будет замечен.

Те, кто не имеет времени заниматься управлением репутацией самостоятельно, могут воспользоваться услугами компаний, специализирующихся на защите сетевых репутаций как физических лиц, так и компаний. При этом услуги оказываются в рамках годовой подписки, и цена колеблется между 400 и 5000 долларов и выше зависимости от начальной ситуации и пожеланий заказчика. Максимальная цена запрашивается в случае, если заказчик имеет негативные материалы о себе, размещённые в Интернете, хочет их закамуфлировать и при этом появляться в верхней части результатов поиска. Меньшая сумма обеспечивает уверенность в том, что потенциальные работодатели и клиенты будут находить тот онлайн-контент, который клиент хочет, чтобы они находили.

Злоумышленник может воспользоваться украденными персональными данными: документами, фамилией-именем, фотографиями жертвы[6].

Украденная информация используется и для подделки банковских карт, и для кражи медицинских страховок и т.д. Такие преступления называются кражей идентичности. Кража идентичности стала самой распространённой разновидностью преступлений, например в Соединённых Штатах за последние несколько лет[7].

Катфишинг в Сети

В последнее время в средствах массовой информации регулярно появляются сообщения о мошенниках, которые, заводя романтические знакомства в Сети, выманивают у жертв деньги и исчезают. Как правило, мошенники для этих целей используют украденные фотографии и вымышленные имена. Такой вид мошенничества по-английски называется romanticscam или catfishing. В русском языке используется транслитерация последнего — катфишинг, а мошенников называют катфишерами. Как избежать обмана, как не попасться на удочку мошенника?

Предлагаемая последовательность действий поможет проверить, действительно ли новый сетевой знакомый или знакомая является тем, за кого себя выдаёт[8].

1. Самое простое действие, с которого можно начать, — это **оценка подлинности фотографии, представленной в профиле нового знакомого.** Для проверки следует пропустить изображение через обратный поиск изображений

---

[5] *John Cook, Stephen Lewandowsky.* Thedebunkinghandbook [Электронный ресурс] / Режим доступа: https://www.skepticalscience.com/Debunking-Handbook-now-freely-available-download.html (дата обращения: 8.12.2017).

[6] *Wynne Davis.* Fake or real? How to selfcheck and get the facts/ Wynne Davis [Электронный ресурс] // NPR, 2016. December, 5. —Режим доступа: https://www.npr.org/sections/alltechconsidered/2016/12/05/503581220/fake-or-real-how-to-self-check-the-news-and-get-the-facts (Дата обращения: 03.11.2017).

[7] *Shin L.* Someone had taken over my life: an identity theft victim's story / L. Shin [Электронный ресурс] // Forbes, 2014. November, 18. Режим доступа: http://www.forbes.com/sites/laurashin/2014/11/18/someone-had-taken-over-my-life-an-identity-theft-victims-story/#1b40bcce9787 (Дата обращения: 05.11.2017).

[8] *John Cook, Stephen Lewandowsky.* Thedebunkinghandbook [Электронный ресурс] / Режим доступа: https://www.skepticalscience.com/Debunking-Handbook-now-freely-available-download.html (дата обращения: 8.12.2017).

Google и посмотреть, появится ли изображение ещё где-нибудь. Для обратного поиска изображений можно также использовать сайт TinEye. Если изображение связано с разными именами или профилями, вполне вероятно, что аккаунт мошеннический.

2. Критический анализ краткой информации о владельце аккаунта. Катфишинговые аккаунты часто используют специфические биографические компоненты. Некоторые аспекты, которые должны вызвать настороженность:

• Статус «овдовёл» или «разведена». Очевидно, что не все овдовевшие или разведённые люди — катфишеры, но этот статус в сочетании с другими особенностями может быть признаком фальшивого аккаунта.

• Работа, которая имеет исключительный статус, требующий постоянных поездок и / или периодов без связи (например, военный, инженер, нефтяник), что помогает мошеннику оправдываться за то, что долгое время был не доступен для связи.

• Информация «О себе» содержит романтические клише, такие, например, как «ищет любовь» или заявления, которые могут стереотипно укрепить впечатление, например, «богобоязненный», присутствуют орфографические ошибки в названии предполагаемой «альма-матер».

3. Анализ имени тоже может послужить подсказкой относительно легитимности профиля:

• Многие мошенники, похоже, выбирают своё из списка популярных имён. Если поискать имя обладателя профиля на Facebook, и всплывёт множество других профилей с тем же именем и аналогичными профессиями, профиль следует изучить более внимательно.

• Можно «погуглить» имя профиля. У большинства людей есть по крайней мере какой-то цифровой след в эти дни. Можно ли найти человека? То, что удаётся найти, совпадает ли с тем, что говорится?

4. Исследование профиля. Некоторые другие элементы профиля для анализа:

• Количество друзей: сколько у человека друзей? Взаимодействуют ли его друзья между собой?

• Типы друзей: часто список друзей мошенника состоит в основном из людей противоположного пола.

• Возраст профиля: профиль совершенно новый или есть история загрузок фото, обновления статуса, сообщения от других? Кроме того, следует обратить внимание, что сообщения профиля можно пометить задним числом, чтобы создать впечатление, будто профиль имеет более длинную историю, чем на самом деле. Тем не менее, год создания профиля (Facebook) подделать невозможно.

• Общие друзья. Следует отметить, что небольшое число общих друзей не обязательно гарантия легитимности: мошенники иногда просятся в друзья друзей, чтобы сделать профиль более правдоподобным. Если общих друзей немного, то можно связаться с ними, чтобы выяснить, действительно ли они знают этого человека. Иногда бывает, что человека принимают в «друзья» на основе или фальшивого профиля, или просто по ошибке.

• Религиозная принадлежность: Мошенники часто представляются, как очень религиозные люди и иногда используют писание или религиозный язык, чтобы казаться более надёжным или манипулировать жертвами через общие системы верований.

5. Наблюдение за поведением. Мошенники часто следуют предсказуемым моделям поведения, имеющим общие признаки, на которые следует обратить внимание:

• Быстрый перенос общения в личную переписку: электронная почта, смс или

другой сервис мгновенного обмена сообщениями. Это делается для того, что, если Сеть идентифицирует исходный профиль как поддельный и удалит его из социальной сети, мошенник не потеряет непосредственного контакта с потенциальной жертвой.

● Стремление к быстрому созданию обязательств: мошенники развивают онлайновые отношения очень быстро и зачастую могут заговорить о любви или браке всего лишь через несколько дней общения; это способствует формированию у жертвы привязанности и чувства ответственности, что впоследствии поможет обратиться к жертве за помощью.

● Отказ в использовании видеосвязи: мошенники зачастую предпочитают пользоваться только текстовой или голосовой связью, оправдывая отсутствие альтернативных возможностей, например, использования Skype, ненадёжной связью. Если же всё-таки сеанс связи состоится, изображение может быть очень низкого качества, а артикуляции не совпадать со звуком. Это будет объяснено плохой связью, а видео может быть скопировано из Youtube. По этой же причине может быть сокращена и продолжительность видеообщения.

● Мошенники нередко договариваются с жертвой о встрече, но эти планы никогда не реализуются по той или иной причине. В последний момент всегда возникает некоторое непреодолимое препятствие.

● Чрезвычайные ситуации. После того как мошенник «зацепил» жертву, он приступает к отработке «чрезвычайной ситуации». Это может быть болезнь, потеря работы, необходимость по какой-либо причине срочной смены места пребывания.

● Просьба о деньгах: это очевидный признак того, что новый знакомый — мошенник. Просьба может принимать различные формы, главное — обустроить перевод денег таким образом, чтобы в результате получателя невозможно было выявить, например, просьба об отправке денег через WesternUnion. Иногда жертву могут попросить перевести деньги «третьему лицу».

6. Запрос на подтверждение идентификации. Если всё же остаются некоторые сомнения, что человек на той стороне провода — мошенник, можно прибегнуть к той или иной форме подтверждения:

● Паспорт: в качестве документа, удостоверяющего личность, мошенник может предоставить паспорт, изготовленный с помощью фотошопа. Если паспорт покажется сомнительным, можно поискать в Интернете, как выглядят реальные паспорта из разных стран. Сравнить, например, насколько фото на паспорте соответствует требованиям страны: размер / форма.

● В случае, если всё же удастся организовать видеообщение в режиме реального времени, можно попросить «знакомого» выполнить действия, например, показать газету с датой того дня, хлопнуть в ладоши.

И главное, о чём не следует забывать, — это здравый смысл. Если профиль выглядит чрезвычайно привлекательным, слишком хорошим, чтобы быть правдой, то весьма вероятно, что действует профессиональный мошенник.

Что делать, если всё же возникла уверенность, что это мошенник?

7. После того как **возникла уверенность, что общение происходит с катфишером**, следует предпринять несколько шагов:
● Проинформировать службу социальной сети.
● Исключить катфишера из списка друзей.
● Предупредить друзей.

Разговор о краже идентичности вывел на другую проблему, когда жертвами становятся не только обманутые люди, но и те, чьими данными, в частности фотографиями, мошенники пользуются для создания ложных профилей

в социальных сетях. Поэтому, размещая фотографии, следует хорошо подумать, так ли необходимо их размещать. А размещаемые фото снабжать «водяными знаками»(watermarks), фиксирующими принадлежность фотографии.

Очевидно, что существование в современном цифровом мире требует от пользователя владения дополнительным комплексом знаний и умений для создания и мониторинга собственной цифровой идентичности, отличающихся от существующих в оффлайновом мире. Предложенный перечень рекомендаций поможет минимизировать риски, связанные с пребыванием в Сети. Это и сознательное формирование «цифровых следов», особенно их активной части, и мониторинг сетевой идентичности, и профилактические меры, которые не позволят стать жертвой «романтического» сетевого знакомства. И хотя новая среда, новый стиль общения во многом формируют и современный лексикон, все советы можно описать русскими пословицами: «Береги платье снову, а честь — смолоду» и «Что написано пером — не вырубишь топором». **НО**

Socialization Of The Individual In The World Wide Web

D.A. Bogdanova, senior researcher, Institute of Cybernetics and educational Informatics of the Federal research center «Informatics and management» Russian Academy of Sciences, candidate of pedagogical Sciences

Abstract. *Special features of life online that distinguish them from offline existence rules are considered. Recommendationsfor the network reputation building, monitoring and management are provided, as well as steps for the prevention of catfishing, a type of network fraud.*

Keywords: *Internet safety, digital footprints, digital reputation management, identity theft, network fraud, romance scam, catfishing, social network autentification, misinformation debunking.*