Михаил Якушев

МЕЖДУНАРОДНО-ПОЛИТИЧЕСКИЕ ПРОБЛЕМЫ ИДЕНТИФИКАЦИИ В ИНТЕРНЕТЕ

Вопрос об идентификации пользователей глобальной сети, владельцев сетевых ресурсов (как технических, так и информационных), а также лиц, оказывающих те или иные услуги с использованием интернет-технологий, стал одним из наиболее обсуждаемых представителями государственных органов и экспертным сообществом. Так, в Российской Федерации предложения о законодательном «запрете анонимности» в интернете неоднократно высказывались руководителями правоохранительных ведомств в контексте борьбы с преступностью[1]. Указанная проблема также имеет очевидное международно-политическое измерение в силу трансграничного характера сети интернет, особенностей ее архитектуры и развития.

Глобальная сеть стала значимым фактором социально-экономического развития отдельных государств и за последние годы вошла в число важнейших элементов системы международных отношений. Важно понимать, что интенсивность и эффективность использования современных сетевых технологий на национальном уровне сегодня во многом определяют конкурентоспособность той или иной страны на международных рынках. В то же время стабильность и безопасность инфраструктуры интернета требует согласованных действий всего международного сообщества. В этой связи действительно учащаются случаи, когда выявление (идентификация, локализация) пользователей Сети, владельцев размещенной в ней информации, операторов сетевых услуг становится критически необходимым, например, для пресечения использования тех или иных сетевых ресурсов в противоправных целях.

Нельзя не принимать во внимание и общеизвестный факт, что обеспечение юридической возможности идентификации пользователей интернета никогда не являлось ни целью, ни даже характерной чертой построения, функционирования и развития этой сети. Изначально интернет (точнее компьютерная сеть, впоследствии ставшая тем, что мы сейчас воспринимаем как *глобальный интернет*) предназначался для гарантированной и стабильной работы системы управления стратегическими ядерными силами в условиях ведения активных боевых действий. Вследствие этого интернету были и остаются присущи такие особенности, как устойчивость к внешним воздействиям или способность передавать информацию по различным маршрутам в случае выхода из строя значительного числа каналов связи.

Что же касается реального физического местоположения или юридического обозначения отправителей или адресатов электронных сообщений, то эти факторы практически никак не учитывались при разработке технологических принципов построения интернета как информационной сети. Можно сказать, что интернет *технологически нейтрален* по отношению к своим пользователям и при помощи собственных средств (т. е. стандартов и протоколов, описывающих порядок

информационного обмена) не способен определить, кто именно находится за клавиатурой или манипулятором устройства, подключенного к Сети.

Тем не менее вопрос об идентификации участников правовых отношений, связанных с использованием интернета, на практике весьма важен, даже если не принимать во внимание какие-либо политические обстоятельства или соображения публичного порядка. Объем материальных, в том числе финансовых средств, обращающихся в сфере так называемой *интернет-экономики,* исчисляется уже сотнями миллиардов долларов США в год, поэтому достоверная идентификация участников *интернет-экономики* в самом широком смысле этого понятия весьма важна для обеспечения стабильности гражданского оборота, исключения возможностей совершения хозяйственных правонарушений — и этим, вообще говоря, мало чем отличается от необходимости идентификации лиц, участвующих в *традиционных* видах бизнеса. Однако, как известно, даже в *оффлайновом*, то есть обычном бизнесе, не применяющем наиболее современные средства коммуникации, проблема идентификации продавца, покупателя, коммерческого посредника, организатора расчетных отношений и других контрагентов далеко не всегда решается удовлетворительным образом. Особенно в отношениях, как говорят юристы, «осложненных иностранным элементом», когда, например, хотя бы часть из участников сделки находится по разные стороны государственных границ.

Ситуация приобретает еще большую неоднозначность из-за *трансграничности* интернета, при использовании которого затруднительно определить местоположение контрагента, включая лиц, размещающих информацию либо предлагающих иные информационные услуги. Дополнительную сложность вносит отсутствие согласованных на международном уровне норм и правил, которые закрепляли бы допустимую степень анонимности при использовании интернета.

Иначе говоря, при сложившемся разнообразии подходов национальных законодательных систем к регулированию интернета то, что законно в одних странах, будет однозначно запрещено в других. В качестве нейтрального примера достаточно привести азартные игры и порядок идентификации их участников, в том числе в целях недопущения к ним несовершеннолетних. Фактически в настоящее время в интернете существует только одна глобально общепризнанная процедура идентификации — система WHOIS (о которой речь пойдет позже), однако она действует только применительно к администраторам доменов в системе доменных имен DNS.

Таким образом, правомерно попытаться найти ответы на следующие ключевые вопросы, связанные с идентификацией в интернете:

- можно ли создать универсальную, всеобщую, глобально признанную систему идентификации пользователей интернета, операторов интернет-услуг и владельцев сетевых ресурсов?
- если создание такой системы возможно, то на каких принципах и с использованием каких международно-правовых механизмов? Каковы могут быть цели такой идентификации? Как избежать в процессе ее создания и использования нарушений основных прав человека, в том числе права на неприкосновенность частной жизни?
- если создание системы, упомянутой в предыдущем пункте, невозможно, то по каким основным технологическим, организационным, правовым либо иным причинам? Возможно ли в этом случае создание *частных*, ограниченных по территориальному или функциональному признаку систем идентификации?

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Следует учесть, что многие общеупотребительные в повседневном общении понятия могут иметь несколько иные значения в профессиональных дискуссиях,

а также в текстах юридических, в том числе международно-правовых документов. Употребление словосочетания *идентификация в интернете* также может вызвать неоднозначность.

Так, в *философском* смысле понятие *идентификация* означает «установление тождественности неизвестного объекта известному на основании совпадения признаков», что близко по значению к юридическому термину *опознание*. В информационных же системах под идентификацией обычно понимают существенно более *практический* процесс присвоения как субъектам, так и объектам коммуникации определенных *уникальных идентификаторов* и их сравнение с перечнем присвоенных идентификаторов. Например, оконечные устройства телефонных сетей, то есть собственно телефонные аппараты, идентифицируются в процессе установления телефонных соединений по уникальным абонентским телефонным номерам. Но при этом с технологической точки зрения не происходит идентификации лица — гражданина, который участвует в телефонном разговоре, поскольку для этого недостаточно знать, кому указанный телефонный номер был присвоен в соответствующем договоре об оказании услуг связи. Необходимо каким-то образом удостовериться, что именно лицо, указанное в договоре как абонент, в настоящий момент использует данный телефонный аппарат.

Следовательно, для выявления лица, использующего информационные технологии, необходимо говорить не столько об *идентификации*, сколько об *аутентификации* такого лица. Именно аутентификация позволяет установить соответствие названному им идентификатору. Так, в *оффлайновых* отношениях аутентификация производится по фотографии в предъявляемом документе, а иногда по другим биометрическим признакам, включая дактилоскопическую информацию. Кроме того, нельзя смешивать идентификацию и аутентификацию с *авторизацией* — также производимым в информационной системе процессом проверки и подтверждения прав пользователя на выполнение тех или иных действий. Результат авторизации, производимый интернет-технологиями, как правило, без участия человека, зависит от успешной (т. е. достоверной) аутентификации пользователя.

Таким образом, при собственно *идентификации* пользователь интернета «называет себя» информационной системе, подключенной к Сети, например, путем указания своей учетной записи на том или ином информационном ресурсе. При *аутентификации* устанавливается соответствие лица названному им идентификатору. Такая процедура может осуществляться как путем введения пароля или предъявления сертификата электронной подписи, так и иными способами, в том числе биометрическими методами, например, считыванием дактилоскопической информации пользователя. Наконец, при *авторизации* идентифицируемому лицу предоставляются возможности в соответствии с положенными ему правами либо проверяется наличие таких прав.

Все вышесказанное имеет критически важное значение при расследовании случаев неправомерного использования информационных технологий и для привлечения к ответственности виновных в этом лиц. Поскольку задача настоящей статьи более общего плана, допустимо использовать понятие *идентификация* в расширительном плане, понимая под ней любые способы установления идентичности лица, пользующегося сетью интернет либо оказывающего услуги на основе интернет-технологий.

АНОНИМНОСТЬ В ТЕОРИИ И НА ПРАКТИКЕ

Как уже отмечалось выше, одним из аспектов решения вопросов идентификации в интернете является проблема анонимности, пределов допустимости анонимного поведения и определения случаев, когда анонимность должна или может быть законодательно запрещена. Значительная часть правонарушений в интернете осуществляется с использованием анонимных электронных сообщений либо (что точнее) с использованием *псевдонимов* [nicknames], подлинные имена владель-

цев которых не раскрываются, что позволяет по правовым последствиям приравнивать такие случаи к анонимному поведению.

Основной вопрос, который в этой связи требует юридического ответа и, следовательно, согласования соответствующей правовой позиции на международном уровне, сводится к признанию анонимности (*безымянности*) одним из прав человека, а точнее, существенным элементом права на неприкосновенность частной жизни. Что касается правовых режимов использования анонимности, они могут быть сведены к трем основным вариантам:

- анонимность разрешается (допускается) или подразумевается;
- анонимность предписывается;
- анонимность запрещается (не допускается).

Для иллюстрации приведем следующие примеры:

- анонимность разрешается (допускается) в большинстве повседневных, бытовых ситуаций либо когда речь идет о вопросах морального или медицинского плана — например, при анонимном лечении вредных привычек, либо для обеспечения деятельности отдельных видов юридических лиц, таких как акционерные общества[2];
- анонимность напрямую предписывается законом, когда речь идет об избирательной системе, в соответствии с принципом тайны выборов, о защите персональных данных (обезличивание данных социологических опросов и статистических исследований) и, опять-таки, об отдельных случаях, обусловленных морально-этическими и медицинскими соображениями. Примерами последнего варианта служат тайна усыновления, сохранение анонимности доноров при трансплантологии и суррогатное материнство;
- наконец, в ряде случаев анонимность не допускается. Классическим примером является установление личности преступника, совершившего уголовное правонарушение — ведь привлечь к ответственности можно только лицо, которое надлежащим образом идентифицировано и в отношении которого доказана вина в совершении вменяемого ему деяния. Однако запрет на анонимность существует не только в уголовном праве. Практически повсеместно запрещается анонимное владение недвижимым имуществом, а также источниками повышенной опасности. К последним относятся, например, не только оружие, но и транспортные средства, включая автомобили, — у каждого автомобиля есть собственник, идентифицируемый по регистрационному знаку машины.

Кроме того, следует различать анонимность *относительную* и *абсолютную*, а также анонимность *пассивную* и *активную*. Относительной анонимностью можно считать использование средств идентификации таким образом, что реальное имя известно только одному или нескольким контрагентам, но не известно всем остальным. Классические примеры относительной анонимности: публикация анонимного произведения или произведения под псевдонимом в печатном издании, что, собственно, и породило само понятие *аноним*, *безымянное произведение*; сохранение конфиденциальности сведений о банковских счетах, адвокатская, врачебная и иные виды соответствующих тайн; использование телефонной связи с присвоением пользователям уникальных абонентских номеров и т. д. В случае же абсолютной анонимности, по общему правилу, идентификация лица невозможна либо, что бывает намного чаще, не требуется, поскольку при этом ни у кого не возникает каких-либо юридически значимых прав или обязанностей. В повседневной жизни подавляющее большинство ситуаций не предусматривает представления участников общения друг другу, если это не требуется, скажем, общепринятыми нормами вежливого поведения.

Применительно к интернет-технологиям можно говорить о практически абсолютной степени анонимности при подключении к интернету в местах общего доступа (например, в кафе и ресторанах, аэропортах и тому подобных местах), если при этом не требуется авторизации по уникальному паролю, идентифицируемому именно данного пользователя. Впрочем, в ряде зарубежных стран, включая Китай и Белоруссию, при пользовании подобного рода сервисов как раз обязателен если не предварительный ввод уникального идентификатора с паролем, то предоставление уполномоченному сотруднику документа, удостоверяющего личность пользователя. Еще одним примером анонимного использования интернета является участие в дискуссиях онлайн (в комментариях к блогам, новостным сообщениям и т. д.), при которых не требуется идентификация участника дискуссии. Обычно участник дискуссии в этом случае может зарегистрироваться под любым выбранным им псевдонимом, причем указать при регистрации данные о себе, которые не проверяются владельцем интернет-ресурса.

Что же касается понятий *пассивной* и *активной* анонимности, то к первой из них можно отнести все случаи, когда идентифицируемое лицо не называет своего имени, пока его об этом не спрашивают, то есть когда его идентификация не вызывается необходимостью, в том числе не вытекает из каких-либо установленных законодательством предписаний. К *активной* же анонимности относятся ситуации, когда аноним скрывает свое реальное имя даже в случае напрямую обращенного к нему запроса. Наиболее характерным для интернета проявлением анонимности является как раз *пассивная* анонимность.

В большинстве случаев, например, когда пользование Сетью сводится к просмотру интернет-сайтов, идентификации пользователя не требуется. Однако современные интернет-технологии позволяют обеспечивать достаточно высокую степень анонимности и в том случае, когда, с технической точки зрения, пользователь интернет-ресурса *обязан* идентифицировать себя. Так, при обмене сообщениями по электронной почте всегда указывается адрес отправителя, однако при желании отправитель, не желающий быть узнанным, может использовать так называемые *анонимайзеры*, позволяющие создавать временные электронные адреса на любое вымышленное имя и затруднять возможность отследить, через какие почтовые серверы электронное сообщение в реальности прошло, чтобы достигнуть своего адресата. Сходные возможности предоставляют так называемые *прокси-серверы* [proxies][3].

Из вышесказанного легко сделать вывод о том, что *активная* анонимность в *оффлайновом* мире, как, вообще говоря, и стремление добиться некоей стопроцентной абсолютной анонимности, характерны для поведения, скорее характеризуемого как противоправное. В самом деле, для обычного гражданского оборота та или иная степень анонимности допускается, но при необходимости (например, для защиты законных прав третьих лиц) действуют правила раскрытия информации о лицах, выступающих в качестве анонимных, например, в акционерных обществах для этого существуют реестры акционеров. В этих случаях правомерное использование анонимности сочетается с механизмами раскрытия информации в установленных законом случаях. Напротив, при противоправном поведении, например, при совершении уголовно наказуемых проступков, преступник заинтересован в неразглашении информации о себе, чтобы не быть привлеченным к ответственности, то есть стремится к сохранению абсолютной анонимности. В то же время, стремление минимизировать любую возможность идентификации, уничтожение улик характеризует его действия как стремление к активной анонимности.

Подобного рода выводы можно сделать и при анализе вопросов анонимности при использовании интернета. Более того, именно указанные выше факторы и не позволяют поставить знак равенства между понятием *право на анонимность* как одним из компонентов права на неприкосновенность частной жизни и понятием *основные права и свободы человека*[4].

ИДЕНТИФИКАТОРЫ В ИНТЕРНЕТЕ

Несмотря на широкие возможности, которые предоставляют интернет-технологии для использования Сети анонимно или под выбранным самим пользователем псевдонимом, в реальности в интернете существуют самые разнообразные способы идентификации как пользователей тех или иных интернет-ресурсов и их владельцев, так и операторов соответствующих интернет-услуг. По своей архитектуре интернет представляет собой сложную, многоуровневую структуру, на каждом уровне которой мы видим взаимодействие самых различных субъектов, находящихся под различной юрисдикцией.

Так, на самых нижних, так называемых *физическом* и *канальном* уровнях, интернет представляет собой совокупность присоединенных друг к другу и взаимодействующих между собой сетей электросвязи. Каждая из них имеет своего владельца, как правило, оператора связи, имеющего соответствующую лицензию от уполномоченного ведомства страны регистрации данного юридического лица. Сети электросвязи включают каналы связи (оптоволоконные линии связи, спутниковые каналы с наземной и космической инфраструктурой и т. д.), коммутационное серверное оборудование и разнообразные оконечные абонентские устройства. Поскольку все компоненты сетей связи так или иначе являются имущественными объектами, зачастую подлежащими государственной регистрации как недвижимое имущество, идентифицировать владельца того или иного компонента сетевой инфраструктуры не является существенной проблемой.

То же самое можно сказать и об оконечных устройствах, подключаемых к интернету на основании договоров с операторами услуг доступа к Сети. У каждого пользователя такого устройства есть договор с оператором связи с выделением абонентского номера. Например, для пользователей мобильной связи договором выделяется уникальный телефонный номер. В большинстве стран мира, включая Российскую Федерацию, такой договор заключается в письменной форме, с указанием так называемых установочных сведений абонента. В России такими сведениями служат паспортные данные. При необходимости идентификационные сведения из абонентского договора могут быть предоставлены уполномоченным правоохранительным органам в рамках проводимых ими следственно-оперативных мероприятий, а в случае проведения трансграничных расследований в рамках международного сотрудничества, например, по линии Интерпола, в том числе по запросу органов правопорядка зарубежных стран.

На более высоких уровнях архитектурной иерархии Сети, обеспечивающих корректную обработку пересылаемых пакетов информации надлежащим абонентам, применяются идентификаторы подключенных к интернету компьютерных устройств (узлов) в виде набора групп цифр под названием IP-адреса (сетевые адреса)[5]. В настоящий момент используются два вида сетевых адресов, так называемых протоколов 4-й и 6-й версии. При этом второй из них (IPv6) представляет возможность присвоения на несколько порядков большего числа сетевых адресов, чем предыдущий, старый (IPv4). Сетевые адреса распределяются на коммерческой основе пятью региональными сетевыми центрами. Центром, распределяющим адреса для России, является находящаяся в Амстердаме европейская организация RIPE NCC[6]. Получателями сетевых адресов являются уже упомянутые операторы электросвязи, осуществляющие услуги доступа к сети интернет. В принципе, операторы услуг доступа, иногда также именуемые провайдерами [Internet Service Providers], должны в любой момент быть способны определить, кто именно осуществляет ту или иную сетевую активность с использованием установленного сетевого адреса.

Однако на практике, по крайней мере при использовании устаревающего протокола сетевых адресов версии IPv4, затруднения вносит тот факт, что сетевой адрес присваивается не отдельному абоненту, а целой группе пользователей, например, обслуживаемых в рамках одной организации-клиента. Аналогией служит ситуация, когда при оказании услуг телефонной связи организации выделяется один *прямой*

городской номер, а конкретные сотрудники этой организации имеют возможность выхода на телефонную сеть общего пользования через собственный *местный* номер. Разумеется, и в этом случае имеется принципиальная техническая возможность определить, кто именно использовал данный сетевой адрес в конкретный промежуток времени, например, с какого номера телефона был получен доступ в интернет. Однако в отсутствие законодательных требований об обязательном документировании и последующем хранении подобного рода сведений подобного рода достаточно затратные процедуры не всегда выполняются.

Следующим иерархическим уровнем, позволяющим проводить идентификацию интернет-ресурсов и их пользователей, является система доменных имен DNS [Domain Names System]. Система DNS обеспечивает однозначное преобразование сетевых адресов, представляющих набор труднозапоминаемых цифр, в удобное для восприятия сочетание букв, слов или символов, имеющих то или иное значение в национальных языках (например, *pircenter.org* или *правительство.рф*)[7]. Владельцы и администраторы доменов верхнего уровня, таких как *.com, .uk* или *.рф*, заключают специальные соглашения с американской корпорацией ICANN [Internet Corporation for Assigned Names and Numbers], отвечающей за распределение адресного пространства сети интернет. Сведения о том, кто является администратором (так называемой регистратурой) того или иного домена верхнего уровня находятся в открытом доступе в Сети.

Несколько иной подход действует в отношении доменов наиболее востребованного, второго уровня — для идентификации их владельцев применяется сервис WHOIS[8]. Данный сервис отображает довольно подробную информацию о том, на кого и какой организацией-регистратором зарегистрировано данное доменное имя, на каких интернет-серверах размещены использующие этот домен интернет-сайты, а также контактную информацию администратора доменного имени второго уровня и его организации-регистратора. В последнее время в связи с повсеместным принятием законов о защите персональных данных наблюдается тенденция предоставлять минимум сведений о собственно администраторе домена, ограничиваясь ссылками на контактные данные организации, зарегистрировавшей данное доменное имя. Однако в соответствующих зональных регистрах доменных имен должна храниться достоверная информация о каждом владельце доменов второго уровня, которая может быть раскрыта в установленном национальном законодательстве порядке.

В то же время следует признать, что с увеличением числа используемых доменных имен до нескольких сотен миллионов и, соответственно, увеличением организаций-регистраторов доменных имен до нескольких десятков тысяч по всему миру остро встает задача унификации процедур верификации информации, предоставляемой на ресурсах WHOIS. Противоправное использование интернет-ресурсов, например, создание фишинговых сайтов банков в мошеннических целях, при невозможности достоверно определить организатора противоправных действий и владельца созданных в этой связи интернет-ресурсов, идентифицируемых по доменному имени сайта, предельно затрудняет привлечение к ответственности виновных лиц. Данная проблема является основанием для достаточно жесткой критики *бесконтрольности интернета* со стороны заинтересованных политических кругов. Процедуры WHOIS де-факто являются единственным общепризнанным мировым стандартом идентификации владельцев интернет-ресурсов, и в настоящее время ведется дискуссия о необходимости адаптации этих процедур к последним изменениям в системе DNS. В частности, речь идет о совершенствовании процедур WHOIS в связи с появлением доменных имен на нелатинской графической основе, таких как *.рф*[9].

Наконец, отдельной — и едва ли не самой сложной — проблемой является идентификация непосредственно пользователей каждого интернет-ресурса, будь то интерактивный сервис (например, использование социальных сетей) или *пассивный* просмотр интернет-сайта. Уместно начать с того, что даже широко распространенные программные средства просмотра интернет-страниц — веб-

браузеры, не предназначенные по своей сути для идентификации применяющих их пользователей, обеспечивают сбор достаточно подробных сведений о них. Так, при любом посещении интернет-страницы фиксируется следующая информация (причем этот список не является исчерпывающим):

- сетевой адрес (с указанием доменного имени) просматриваемой страницы;
- сетевой адрес страницы перехода, с которой осуществлен переход по ссылке;
- IP-адрес пользователя, из которого определяется наименование провайдера и страна регистрации;
- часовой пояс, в котором находится пользователь;
- данные о применяемых технологиях (таких как cookies, proxy server, Java);
- характеристики интернет-браузера (тип, язык, встроенные расширения, поддержка приложений) и прочие настройки компьютера, включая разрешение экрана и передаваемые цвета.

Очевидно, что вся эта информация, хотя бы по косвенным признакам, в случае надобности может достаточно сузить возможный круг пользователей при проведении соответствующих расследований.

Помимо встроенных программных средств фиксации сведений о пользователе применяются различные способы идентификации непосредственных пользователей отдельных интернет-ресурсов и интернет-сервисов. Приведем примеры наиболее известных их них.

Наиболее часто встречающимся методом аутентификации в интернете является комбинация *«логин (имя учетной записи) + пароль (уникальный набор символов)»*. Однако достоверная информация о пользователе возможна лишь в корпоративных информационных системах, где условные имена пользователей (учетные записи) создаются строго в соответствии с внутрикорпоративными политиками и вероятность получения учетной записи посторонним по отношению к данной корпоративной системе лицом исчезающе мала. В остальных случаях, как правило, пользователь вправе самостоятельно выбрать наименование своей учетной записи и создать собственный пароль — то есть проверка идентифицирующих его документов не осуществляется.

Указанное обстоятельство представляет собой известную *проблему удостоверяющего центра*. Дело в том, что для достоверной идентификации пользователей разных корпоративных систем требуется посредник, третья сторона, которой могли бы доверять все остальные участники взаимодействия и который хранил бы и при необходимости предоставлял данные о владельцах всех учетных записей взаимодействующих информационных систем. Разумеется, реализация в полном объеме требования к удостоверяющему центру может быть достаточно затратной и не удобной для пользователей вследствие громоздкости процедур верификации. Например, такой процедурой может быть личный визит в офис удостоверяющего центра с предъявлением соответствующих документов.

В определенной степени проблема удостоверяющих центров решена в Российской Федерации с принятием в 2011 г. федерального закона «Об электронной подписи»[10], который заменил устаревшие нормативные акты и легитимировал использование в России сразу нескольких видов электронных подписей. Данные подписи предназначены как для подтверждения неизменности электронного подписания после его подписания отправителем, так и для установления личности самого отправителя. Самый защищенный вид электронной подписи, так называемая электронно-цифровая подпись с квалифицированным сертификатом, как раз и предназначен для достоверной идентификации любого пользователя онлайн

сервисов. Однако такая подпись отличается максимальным неудобством в использовании, поскольку процедура ее получения весьма напоминает процедуру заверения у нотариуса собственноручной подписи на бумажном документе. Еще одной проблемой для таких подписей является признание квалифицированных сертификатов за рубежом. Алгоритмы шифрования информации, подтверждающей сведения сертификата, и сам статус российских удостоверяющих центров для зарубежных контрагентов могут и не признаваться надлежащими автоматически, поскольку в мире существует несколько самостоятельных *систем доверия* применительно к электронным подписям.

Более удобны для пользователей, но и более затратны, с материальной точки зрения, аппаратно-программные средства типа электронных карточек доступа, иных средств условного доступа, *электронных паспортов*[11]. Для считывания информации с таких карточек могут потребоваться дополнительные устройства, однако по мере развития технологий способы использования подобных карточек становятся все более удобными. Недостатком указанного метода, помимо относительной дороговизны, является необходимость постоянно иметь карточку условного доступа при себе. Однако, если такая карточка к тому же выполняет функцию обычного удостоверяющего документа типа внутреннего паспорта или водительского удостоверения, данное неудобство скорее становится достоинством. Неоспоримыми преимуществами являются как удобство применения, так и возможность записи на электронную карточку дополнительной информации, позволяющей превратить ее в универсальное средство доступа практически к любому интернет-ресурсу. При этом, что немаловажно, исчезает необходимость запоминания многочисленных паролей и имен учетных записей. Кроме того, такая функция позволяет использовать *электронный паспорт* в трансграничных отношениях, поскольку записанная на нем информация, фактически представляющая собой разновидность электронной подписи, будет соответствовать требованиям максимального числа *систем доверия*.

Также достаточно удобным, а в ряде случаев единственно возможным средством идентификации являются *уникальные цифровые идентификаторы*: номера банковских карточек, номера социального и пенсионного страхования, индивидуальные номера налогоплательщика. Однако следует помнить, что сам по себе ввод такого номера по запросу информационной системы является не средством идентификации, а лишь средством авторизации. Ту же самую идентификационную информацию может ввести лицо, случайным или неправомерным образом получившее доступ к таким идентификаторам, например, получив физический доступ к чужой кредитной карточке. В этом случае указанное лицо будет успешно авторизовано в информационной системе по чужим идентификационным данным.

Отмеченная проблема отсутствует в случае использования так называемых биометрических средств идентификации, Примерами таких средств являются оцифрованная фотография лица, дактилоскопическая карта, эталонная запись голоса пользователя, сканирование радужной оболочки глаза. Степень достоверности идентификации при использовании биометрических средств сегодня намного выше, чем даже пять-семь лет назад, но она все равно не является стопроцентной. Коэффициент ошибок, при которых может быть проведена ошибочная идентификация постороннего человека, либо, наоборот, отказано в авторизации надлежащему пользователю, достаточно велик.

Недостатками биометрических методов идентификации, с одной стороны, является относительная дороговизна необходимой для идентификации аппаратуры. С другой стороны, биометрическую идентификационную информацию почти невозможно изменить, что весьма неудобно по сравнению, например, с паролями. Эта проблема становится особо актуальной в тех случаях, когда идентификационная информация неправомерным образом стала известна третьим лицам и для защиты информационной системы необходимо ее заменить. Кроме того, биометрические сведения во многих странах мира, в том числе в Российской Федерации, рассматриваются как *особая категория* специальных данных. Такие данные

по законодательству подлежат сбору и обработке с определенными ограничениями, обусловленными необходимостью соблюдения прав человека на неприкосновенность частной жизни. Еще более жесткие ограничения чаще всего накладываются на трансграничную передачу биометрических данных. Эти вопросы, как минимум, требуют согласования на уровне дву- или многосторонних межправительственных соглашений.

Развитие интернет-технологий позволило начать использоваться такой способ идентификации, как верифицируемые электронные почтовые адреса. Речь идет об адресах электронной почты, которые принадлежат определенным компаниям (корпоративная электронная почта) или государственным органам и которые предоставляются сотрудникам таких организаций либо лицам, обращающимся за государственными услугами. Как правило, при назначении корпоративного сетевого адреса происходит предварительная верификация пользователя, которому назначается почтовый адрес, а сам такой почтовый адрес содержит фамилию и (или) имя соответствующего пользования. Иначе говоря, маловероятно появление в домене, обозначающего администрацию президента США *.whitehouse.gov*, почтового адреса *barack.obama@whitehouse.gov*, принадлежащего сотруднику по имени Джон Смит. Таким образом, вероятность того, что почтовый адрес вида *(name)@ (corporation domain)* принадлежит именно сотруднику данной организации с указанным в адресе именем, намного выше, чем при использовании любых иных, в том числе бесплатных, почтовых сервисов.

Однако, к сожалению, те же интернет-технологии позволяют имитировать отправку электронного сообщения с иного почтового адреса, что обесценивает возможности верификации отправителя без использования методов, аналогичных средствам электронно-цифровой подписи, или защищенных каналов связи. Впрочем, на корпоративном уровне использование этих средств намного менее обременительно для пользователей и в целом может осуществляться с приемлемым уровнем общих затрат. Проблема остается в признании трансграничных транзакций: необходимо понять, каким способом российский пользователь может убедиться, что домен *.whitehouse.gov* на самом деле имеет отношение к администрации президента США.

Наконец, все более широкое распространение получают способы установления личности пользователей, основанные на иных, специфических видах сетевых идентификаторов. Так, для регистрации учетной записи в некоторых социальных сетях требуется указать номер мобильного телефона, который, в свою очередь, по правилам оказания услуг мобильной связи, может быть предоставлен только абоненту сотового оператора при предъявлении таким абонентом надлежащих идентифицирующих его документов. Может быть и так, что для регистрации в социальной сети и не требуется предоставления какой-либо информации, позволяющей достоверно идентифицировать нового пользования. Однако для последующей активации отдельных сервисов такой сети все же придется указать номер телефона, по которому должно прийти сообщение с кодом активации. Кроме того, для некоторых учетных записей допускается так называемый *верифицированный* или *официальный* статус, для получение которого необходимо предъявить дополнительные документы и/или выполнить ряд дополнительных действий[12].

В свою очередь, учетные записи в социальных сетях и сервисах сами могут служить удобным способом идентификации. Например, название (адрес) пользователя в одной социальной сети может автоматически служить способом авторизации того же пользователя во множестве других, не связанных с такой социальной сетью, сетевых сервисов. Указанные способы идентификации получили название *Open ID* («открытый идентификатор») или «технологии единого входа». Об их популярности может свидетельствовать хотя бы тот факт, что при использовании вебкамер на выборах Президента Российской Федерации для регистрации заинтересованных лиц использовалась именно такая технология[13]. К числу недостатков указанного способа можно отнести разве что возможность несанкционированного доступа сразу ко всем сервисам, в которых зарегистрирован пользователь *пер-*

вичной социальной сети, в случае потери или перехвата его первоначальных идентификационных данных.

Вышесказанное подводит нас к выводу, что применяемые способы идентификации пользователей и владельцев интернет-ресурсов достаточно разнообразны и зависят как от характера собственно сетевого ресурса и политики его владельца, так и от объема прав, предоставляемых пользователю. Безусловно, свою роль играет и трансграничный характер Сети. В частности, для признания надлежащим в одной стране зарубежного идентификатора по технологии единого входа, например, учетной записи в социальной сети *Facebook*, нужна, как минимум, достаточная степень доверия к процедурам идентификации пользователей в данной сети. А в возможной перспективе может потребоваться заключение соответствующего межправительственного соглашения по данному вопросу.

НАЦИОНАЛЬНЫЕ СИСТЕМЫ ИДЕНТИФИКАЦИИ

Наибольшую степень достоверности идентификационных сведений, позволяющую безоговорочно доверять средствам идентификации конкретного пользователя или владельца конкретного интернет-ресурса, могут предоставить различные комбинации применяемых технологий. Однако у всех таких способов есть общий недостаток в виде необходимости привязки существенной части идентифицирующих признаков к программным или организационным средствам, строго регулируемым нормами национального законодательства или не регулируемым вообще, в зависимости от того, о каком государстве идет речь. Так, комбинация *предоставление сведений о себе заявителем + уникальный пароль + указание номера мобильного телефона для последующей авторизации в социальной сети*, вообще говоря, обеспечивает максимальную достоверность при указании телефонного номера *только* в той стране, где возможен доступ к установочной информации о владельце такого номера.

Различные способы подразумеваемой идентификации (например, признание пользователя *другом* иными пользователями социальной сети), дополнительный верифицируемый статус учетных записей, использование технологий единого входа и другие моменты ставят вопрос о надежности оператора социальной сети как посредника в идентификации ее пользователей. Проблема становится особо актуальной, когда владелец такой сети находится под юрисдикцией одного государства, а вопросы об идентификации его клиентов возникают в другом. Еще один способ идентификации, при котором в дополнение к предоставляемым сведениям требуется предоставить сканированные копии подтверждающих их бумажных документов, с одной стороны, не исключает возможности фальсификаций, а с другой — наталкивается на сложности трансграничной передачи указанных персональных данных.

Наконец, применяемый в России способ идентификации пользователей Портала государственных услуг[14], при котором пароль доступа высылался по указанному заявителем адресу обычной, не электронной почтой (на что могли уходить несколько дней или даже недель), вряд ли сможет когда-либо получить международное признание в онлайновых транзакциях. Впрочем, то же можно сказать и об эстонских ID-картах, поскольку записанная на них информация в полном объеме может быть считана и достоверна оценена только на территории Эстонской Республики.

Таким образом, встает задача не только создания общенациональных систем идентификации пользователей и владельцев интернет-ресурсов, но и сопряжения таких систем между собой для обеспечения среды доверия, среды достоверного обмена идентификационной информацией в интернете.

В России указанная проблема находится на начальном этапе ее решения. Задачи общенациональной идентификации в интернете не сформулированы, если не считать отдельных заявлений руководителей правоохранительных органов. Также

отсутствует законодательное регулирование данного вопроса. К примеру, порядок использования Портала государственных услуг или вебкамер в избирательном процессе был установлен распорядительными, а не нормативно-правовыми актами. По сути, единственным формально регламентированным, но применяемым относительно редко способом идентификации в РФ является технология электронной подписи.

Более системно указанные задачи решаются в Китайской Народной Республике[15]. Так, операторы доступа к сети интернет обязаны иметь лицензию Министерства промышленности и информатизации Китая, при этом доступ к точкам трансграничного обмена трафиком имеют лишь девять таких операторов. Все интернет-пользователи на территории КНР подлежат идентификации по паспорту или заменяющему его документу при заключении договора об оказании услуг доступа к интернету, при этом каждому пользователю предоставляется уникальный идентификатор. Администраторами доменных имен могут быть только юридические лица, имеющие лицензию на право торговой деятельности на территории КНР, или зарегистрированные средства массовой информации.

Наконец, операторами контент-услуг (т. е. распространителями информации) на территории Китая могут быть только лица, являющиеся администраторами доменных имен либо имеющие договоры с операторами доступа. При этом распространение информации возможно только при наличии договора с правообладателями. Разумеется, при такой подробной регламентации на каждом этапе получения (предоставления) интернет-услуг проводится надлежащая идентификация пользователей и операторов сетевых ресурсов. Однако при этом не предоставляется открытого доступа онлайн к информации о реестре операторов или пользователей, вследствие чего китайская система интернет-идентификации *автоматически* не может быть полезной для зарубежных правоохранительных органов. Для проведения межправительственных процедур взаимодействия таких органов требуется оформление письменных запросов.

Противоположная картина складывалась до недавнего времени в Соединенных Штатах, где формально отсутствовали какие-либо нормативные требования к системе идентификации в интернете. В этой связи представляет особый интерес инициатива президента США Барака Обамы в области Национальной стратегии доверительной идентификации в киберпространстве от 2011 г. [National Strategy for Trusted Identities in Cyberspace][16]. В документе ставится задача повышения надежности идентификационных данных и степени защиты информации, которая позволяет установить реальную личность пользователя. Вследствие разнообразия видов и большого числа учетных записей (паролей, других средств авторизации) предложено создание трехуровневой *Экосистемы идентичности* [Identity Ecosystem][17].

При этом предлагается добровольный принцип участия в *Экосистеме идентичности* и допускается как возможность информационного обмена без полной идентификации его участников, так и использование самых различных сетевых средств идентификации и корреляция их с данными, накапливаемых вне сети (в оффлайне). Сама по себе Национальная стратегия подробно не рассматривает вопросов сопряжения американской *Экосистемы идентичности* с зарубежными аналогами, предполагая, что именно американские предложения станут де-факто стандартом на международном уровне.

Вопросы идентификации в интернете частично затрагиваются и в российском проекте концепции Конвенции об обеспечении международной информационной безопасности (2011 г.)[18]. В качестве дополнительных факторов, усиливающих опасность угроз информационной безопасности, в документе указывается «неопределенность в идентификации источника враждебных действий, особенно с учетом возрастающей активности отдельных лиц, групп и организаций». Также в этом списке фигурируют «различия в национальных законодательствах».

Концепция Конвенции предлагает государствам-участникам «стремиться к гармонизации национальных законодательств, при этом различия в них не должны создавать барьеры на пути формирования надежной и безопасной информационной среды». Также фиксируется принцип ответственности каждого государства-участника «за собственное информационное пространство, в том числе и за его безопасность и содержание размещаемой в нем информации». В частности, в целях организации уголовного процесса государства-участники должны принимать «законодательные и иные меры, необходимые для того, чтобы гарантировать оперативное предоставление компетентным органам государства-участника или лицу, назначенному этими органами, достаточного количества данных о потоках информации, которые позволят идентифицировать поставщиков услуг и путь, которым передавалось конкретное сообщение в информационном пространстве».

Исходя из практики создания и функционирования национальных систем идентификации и решений, предлагаемых на международном уровне, можно говорить о складывающемся консенсусе по поводу того, в каких случаях в интернете не должна предоставляться бесконтрольная анонимность и, напротив, должна проводиться идентификация пользователей, операторов, владельцев ресурсов (источников информации и соответствующих угроз):

- совершение противоправных действий (мошенничества, кражи идентичности и других преступлений);
- распространение незаконной информации (антиобщественного характера, не предназначенной для детской аудитории и т. п.) либо вредоносных программных средств;
- террористические угрозы (воздействие на общественное мнение, создание паники, распространение слухов и другие действия террористической направленности);
- незаконное получение информации, представляющей объекты интеллектуальной собственности;
- необходимость прекращения прав третьих лиц. Подразумевается, что защищать необходимо не только права анонимных пользователей, но и в равной степени законные права любых третьих лиц.

Разумеется, при этом требуется соблюдать принцип соразмерности ограничения прав, гарантированных основными, в том числе международными, правовыми актами. Кроме того, при любых обстоятельствах пользователь интернета имеет право знать и должен быть уведомлен о том, какие права он имеет, какие обязательства при использовании сетевых ресурсов несет и какие ограничения и при каких обстоятельствах могут у него возникнуть. Вся информация подобного рода, как правило, описывается в соответствующих пользовательских соглашениях каждого интернет-ресурса.

ВЫВОДЫ И РЕКОМЕНДАЦИИ

1. Простых и быстрых решений проблем, возникающих в связи с необходимостью идентификации в интернете, на данный момент не просматривается ни на национальном, ни, тем более, на международном уровне.
2. В силу разнообразия используемых в разных странах и в различных ситуациях мер идентификации, аутентификации и авторизации любые решения, принимаемые на локальном или национальном уровне, могут быть эффективны *только* на территории данной страны. Попытки распространить такие решения на иные сферы применения чреваты конфликтами, в том числе на межгосударственном уровне. Кроме того, такие решения могут быть в принципе неэффективными, а нарушение принципа технологической нейтральности интернета способно привести к реальной

сегментации Сети и отразиться на стабильности ее развития в соответствующих сегментах.

3. Введение каких-либо общеобязательных мер всеобщей идентификации, например, по образцу Китая, может быть оправдано только при заранее обозначенной цели, соразмерной объему и обременительности предлагаемых мер. Без комплексного подхода, в том числе в отношении ограничения доступа к информации, признаваемой антиобщественной, такие меры будут либо бесполезны, либо легко обходимы.

4. Право на анонимность является составным элементом законного права на неприкосновенность частной жизни и в этом качестве должно безусловно признаваться и уважаться. Однако абсолютное право на анонимность невозможно. Можно лишь говорить о допустимой степени относительности такого права, поскольку *абсолютная анонимность = абсолютный криминал*. Следовательно, ограничения права на анонимность должны быть соразмерны, установлены национальным законом и соответствовать общепризнанным принципам международного права.

5. Не могут и не должны ограничиваться в *онлайне* права и свободы, гарантированные для *оффлайна*. Следовательно, случаи и порядок идентификации пользователей, операторов и владельцев сетевых ресурсов не должны в правовом смысле отличаться от случаев и порядка идентификации лиц, не использующих интернет. В противном случае пользователи и операторы интернета будут явным образом дискриминированы.

6. Российским органам власти следовало бы отказаться от идеи введения обязательной идентификации в интернете, что бы под такой идентификацией ни подразумевалось. Необходимо определить цели *реально необходимой* идентификации и сфер применения, в которых подобная идентификация целесообразна. Необходим и диалог между заинтересованными органами власти, организациями интернет-бизнеса, экспертным сообществом и представителями гражданского общества по техническим и правовым мерам, отвечающим заявленным государством целям идентификации.

7. Используя опыт работы в интернете российских и зарубежных компаний, признать возможным использование различных способов и методов идентификации и начать работу по легализации в России технологий единого входа, подобных Open ID. При необходимости возможно подключение к этой технологии государственных и муниципальных органов. Правоохранительным органам, причем не только российским, следует уделить особое внимание тактике и методике использования систем авторизации во взаимодействии с операторами соответствующих сетевых сервисов.

8. Российские государственные органы совместно с компаниями IT-сектора могли бы провести комплексные НИОКР по внедрению в нашей стране зарекомендовавших себя и перспективных способов идентификации, которые доказали высокую эффективность в отдельных, критически важных сферах применения. К числу подобных мер можно отнести распространение среди населения программно-аппаратных средств электронной подписи, развитие технологий единого входа, развитие биометрических средств идентификации, создание верифицируемых средств создания электронных почтовых адресов и использования защищенных каналов обмена электронными документами с этих адресов без предоставления и использования средств электронной подписи пользователями.

9. В повестку дня международных форумов с участием Российской Федерации должны быть внесены вопросы создания *Международной экосисте-*

мы идентификации в интернете. Такая экосистема должна обеспечивать взаимное признание различных видов идентификаторов (пользователей интернета, операторов интернет-услуг, владельцев интернет-ресурсов) независимо от их местонахождения. Для этого, в частности, требуется заинтересованное изучение американской Национальной стратегии по доверительной идентификации в интернете в целях допустимости ее положений на практике в российских и иных реалиях использования интернета. Рассмотрение такого практического для всех стран мира вопроса, как идентификация в интернете, особенно в деполитизированном и *неконфронтационном* формате, способно благоприятно воздействовать на обеспечение международного мира и безопасности применительно к развитию интернета.

Примечания

[1] Полицейское управление «К» предложило запретить анонимные выступления в интернете. *Российская газета: Федеральный выпуск.* 2011, 8 декабря. № 5652 (276), http://www.rg.ru/2011/12/08/moshkov.html (последнее посещение — 31 августа 2012 г.).

[2] В ряде европейских языков акционерные общества как раз и называются анонимными, поскольку для их деятельности не требуется раскрытие имени акционеров. Так, по-французски акционерное общество звучит как *societ'e anonyme*.

[3] Подробнее см., например: Часто задаваемые вопросы о proxy (proxy FAQ). *CIT Forum*. http://citforum.ru/internet/webservers/proxy_faq (последнее посещение — 31 августа 2012 г.).

[4] О *праве на анонимность* см. подробнее:

The right to anonymity on Internet and legal implications. *Security Affairs.* 2012, June 14, http://securityaffairs.co/wordpress/6452/intelligence/the-right-to-anonymity-on-internet-and-legal-implications.html (последнее посещение — 31 августа 2012 г.).

Gapper G. It is right to curtail web anonymity. *Financial Times.* 2011, August 31, http://www.ft.com/cms/s/0/f3637672-d31e-11e0-9ba8-00144feab49a.html#axzz259kp6VPc (последнее посещение — 31 августа 2012 г.).

Якушев М. Анонимность в интернете и право на неприкосновенность частной жизни. Координационный центр Национального домена сети интернет, http://cctld.ru/files/ppt.pptx (последнее посещение — 31 августа 2012 г.).

[5] Более подробно см. статью в этом номере *Индекса Безопасности*: Якушев М. Интернет-2012 и международная политика. *Индекс Безопасности*. 2013. Весна. №1 (104). С. 36.

[6] RIPE NCC. RIPE Network Coordination Centre, http://www.ripe.net (последнее посещение — 31 августа 2012 г.).

[7] Более подробно см. статью в этом номере *Индекса Безопасности*: Якушев М. Интернет-2012 и международная политика. С. 36–38.

[8] От английского WHO IS (it) дословно КТО (есть) ЭТО.

[9] Подробнее см.: WHOIS Policy Review Team Draft Report. Internet Corporation for Assigned Names and Numbers. 2012, March 18, http://www.icann.org/en/news/public-comment/whois-rt-draft-final-report-05dec11-en.htm (последнее посещение — 31 августа 2012 г.).

[10] Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ (принят Государственной Думой Федерального собрания Российской Федерации 25.03.2011).

[11] Например, ID-карты, широко применяющиеся в Эстонии.

Подробнее см., например: Цифровое подписывание. ID. Удостоверение личности нового поколения. 2012, 10 мая, http://www.id.ee/?id=11080&&langchange=1 (последнее посещение — 31 августа 2012 г.).

[12] См., например: Страница председателя правительства Российской Федерации Дмитрия Анатольевича Медведева. Facebook, http://www.facebook.com/Dmitry.Medvedev (последнее посещение — 31 августа 2012 г.).

[13] Доступ к архиву видеотрансляции выборов Президента Российской Федерации. Электронное правительство. Госуслуги,

http://epgu.gosuslugi.ru/pgu/service/-10000000413_418.html#_description (последнее посещение — 31 августа 2012 г.).

[14] Электронное правительство. Госуслуги, http://epgu.gosuslugi.ru (последнее посещение — 31 августа 2012 г.).

[15] Более подробно см., например: Цензура Интернета в Китае. Ваш личный Интернет. 2005, 16 июня, http://www.content-filtering.ru/allinet/regulinet/regulinet_249.html (последнее посещение — 31 августа 2012 г.).

Также см. статью в этом номере *Индекса Безопасности*: Ибрагимова Г. Стратегия КНР в области управления интернетом и обеспечения информационной безопасности. С. 169–184.

[16] National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy. 2011. May,

http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (последнее посещение — 31 августа 2012 г.).

[17] Более подробно об *Экосистеме идентичности* см. статью в этом номере *Индекса Безопасности*: Демидов О. Социальные сетевые сервисы в контексте национальной и международно безопасности. *Индекс Безопасности*. 2013. Весна. №1 (104). С. 81–83.

[18] Более подробно о концепции Конвенции см. статью в этом номере *Индекса Безопасности*: Демидов О. Международное регулирование информационной безопасности и национальные интересы России. *Индекс Безопасности*. 2013. Весна. №1 (104). С. 99.