Организация Объединенных Наций A/CN.9/WG.IV/WP.120

Генеральная Ассамблея

Distr.: Limited
27 July 2012
Russian
Original: English

Комиссия Организации Объединенных Наций по праву международной торговли
Рабочая группа IV (Электронная торговля)
Сорок шестая сессия
Вена, 29 октября – 2 ноября 2012 года

Обзор вопросов управления идентификационными данными

Справочный документ, представленный Целевой группой по правовым аспектам управления идентификационными данными Американской ассоциации адвокатов

Записка Секретариата

В рамках подготовки к сорок шестой сессии Рабочей группы IV (Электронная торговля) Целевая группа по правовым аспектам управления идентификационными данными Американской ассоциации адвокатов представила Секретариату прилагаемый документ.

Документ, содержащийся в приложении, воспроизводится в той форме, в которой он был получен Секретариатом.

V.12-55148 (R) 270812 030912

I. Введение

1. В 2011 году ОЭСР в своем докладе отметила, что "управление использованием цифровых идентификационных данных имеет основополагающее значение для дальнейшего развития экономики на базе Интернета"[1]. В этом состоит основное требование для всех основных видов электронной торговли.

2. Настоящий документ представляет собой обзор вопросов управления идентификационными данными, его роли в электронной торговле, смежных правовых вопросов и соответствующих юридических препятствий[2]. Он основан на результатах текущей работы Объединенной целевой группы Американской ассоциации адвокатов (ААА) по правовым аспектам управления идентификационными данными[3] и представляется в качестве справки для ознакомления Рабочей группы с соответствующими вопросами[4].

3. На своей сорок четвертой сессии в 2011 году Комиссия согласилась вновь созвать Рабочую группу IV (Электронная торговля) для проведения работы в области электронных передаваемых записей[5]. В то же время Комиссия согласилась дополнительно рассмотреть на одной из будущих сессий вопрос о распространении мандата Рабочей группы IV на другие темы, рассмотренные в документах A/CN.9/728 и Add.1 в качестве отдельных (с точки зрения их возможной взаимосвязи с электронными передаваемыми записями)[6]. К числу этих тем относятся управление идентификационными данными, механизмы единого окна и платежи с помощью мобильных устройств[7].

4. Как отмечается ниже (пункты 6-7), управление идентификационными данными является главным необходимым элементом каждой из тем, рассмотренных Комиссией на ее сорок четвертой сессии (электронные

---

[1] OECD (2011) “Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy — Guidance for Government Policy Makers,” *OECD Digital Economy Papers*, No. 196, OECD Publishing, at p. 3; размещено по адресу www.oecd-ilibrary.org/science-and-technology/digital-identity-management-for-natural-persons_5kg1zqsm3pns-en.

[2] Настоящий документ посвящен коммерческим системам управления идентификационными данными в контексте деловой деятельности, включая сделки между коммерческими структурами (КС-КС), между коммерческими структурами и государством (КС-Г) и между коммерческими структурами и потребителями (КС-П).

[3] Целевая группа по правовым аспектам управления идентификационными данными Комитета по правовым вопросам киберпространства Секции торгового права Американской ассоциации адвокатов; http://apps.americanbar.org/dch/committee.cfm?com=CL320041. Мнения, изложенные в настоящем документе, не были одобрены Палатой делегатов или Советом управляющих Американской ассоциации адвокатов и, соответственно, их нельзя рассматривать как отражающие политические взгляды ААА.

[4] С дополнительными материалами можно ознакомиться также по адресу www.uncitral.org/uncitral/en/commission/colloquia/electronic-commerce-2010.html, где размещена информация о работе коллоквиума ЮНСИТРАЛ по электронной торговле, проведенного 14-16 февраля 2011 года в Нью-Йорке.

[5] *Официальные отчеты Генеральной Ассамблеи, шестьдесят шестая сессия, Дополнение № 17* (A/66/17), пункт 250.

[6] Там же, пункт 251.

[7] Там же, пункты 241-249.

передаваемые записи, механизмы единого окна и платежи с помощью мобильных устройств). В этой связи он будет иметь важное значение для текущей работы Рабочей группы по электронным передаваемым записям, а также для любой будущей работы по другим темам.

5. Важнейшая роль управления идентификационными данными в содействии развитию надежной электронной торговли широко признана. Многие межправительственные группы, государство, частные международные группы и коммерческие структуры активно изучают вопросы управления идентификационными данными и имеющиеся в этой области возможности, разрабатывая технические стандарты и деловые процедуры, а также изыскивая пути реализации жизнеспособных систем идентификации. В порядке примера можно отметить:

a) активную работу межправительственных групп по вопросам и стандартам управления идентификационными данными, в том числе Организацию экономического сотрудничества и развития (ОЭСР)[8], Международную организацию по стандартизации (МОС)[9] и Международный союз электросвязи (МСЭ)[10];

b) проведенное ОЭСР обследование[11], в рамках которого выявлено 18 стран – членов ОЭСР, активно проводящих в жизнь национальные стратегии в области управления идентификационными данными (Австралия, Австрия, Германия, Дания, Испания, Италия, Канада, Люксембург, Нидерланды, Новая Зеландия, Португалия, Республика Корея, Словения, Соединенные Штаты Америки, Турция, Чили, Швеция и Япония)[12]. Такие стратегии также активно реализуются в ряде других стран, таких как Индия, Нигерия и Эстония;

c) несколько региональных проектов по управлению идентификационными данными, осуществляемые в настоящее время в Европейском союзе, в том числе проект PrimeLife (проект в рамках Седьмой рамочной программы Европейской комиссии)[13], Глобальная сеть индивидуальных идентификационных данных – меры поддержки (GINI-SA)[14], STORK (в целях создания европейской платформы оперативной совместимости электронных идентификационных данных)[15] и Европейское агентство сетевой и информационной безопасности (ENISA)[16];

d) работа частных организаций по разработке стандартов и политики в области идентификационных данных на международном уровне, в том числе

---

[8] www.oecd.org/document/38/0,3746,en_2649_34255_49319782_1_1_1_1,00.html.

[9] www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306.

[10] www.itu.int/ITU-T/studygroups/com17/fgidm.

[11] Bernat, L. (2011), “National Strategies and Policies for Digital Identity Management in OECD Countries”, OECD Digital Economy Papers, No. 177, OECD Publishing. doi: 10.1787/5kgdzvn5rfs2-en; at www.oecd-ilibrary.org/content/workingpaper/5kgdzvn5rfs2-en.

[12] Ibid., at pp. 28-35 – список ссылок на национальные документы.

[13] www.primelife.eu.

[14] www.gini-sa.eu.

[15] https://www.eid-stork.eu.

[16] www.enisa.europa.eu.

Организации по развитию стандартов структурированной информации (OASIS)[17], компании "Открытый обмен идентификационными данными" (OIX)[18], Инициативы "Кантара"[19], Фонда "Открытые идентификаторы"[20], Инициативы tScheme[21], и Общества Интернета[22];

e) создание ряда коммерческих систем идентификации, функционирующих на глобальном уровне в ограниченных областях. К их числу относятся системы, находящиеся под управлением Трансглобальной программы безопасного сотрудничества (ТПБС)[23] и компании "CertiPath"[24] для аэрокосмических и оборонных отраслей, ассоциации "SAFE-BioPharma"[25] для биофармацевтической промышленности, компании "IdenTrust"[26] для финансового сектора, организации "CA/Browser Forum"[27] для сертификации веб-сайтов EV-SSL и Федерации идентификации и сквозной аутентификации (FiXs)[28]. Работа этих групп посвящена, главным образом, разработке технических стандартов и решению вопросов определения деловых процедур, а не правовым вопросам.

II. Как управление идентификационными данными связано с электронной торговлей?

6. Вопрос об управлении идентификационными данными имеет основополагающее значение для большинства электронных торговых сделок и других видов онлайновой деятельности. Важнейшее значение имеет проверка идентификационных данных удаленных сторон, например определение того, кто пытается получить доступ к онлайновой базе конфиденциальных данных, кто пытается произвести онлайновый перевод средств со счета, кто подписал электронный контракт, кто дистанционно санкционировал отправку товара или кто направил сообщение по электронной почте. Хотя участники многих малорискованных онлайновых сделок готовы верить в то, что они имеют дело с конкретным физическим или юридическим лицом, по мере повышения степени конфиденциальности или стоимости той или иной сделки также возрастает и важность обеспечения наличия и надежности достоверной информации для идентификации удаленной стороны в целях принятия заслуживающего доверия решения.

7. Управление идентификационными данными является основным необходимым аспектом электронных подписей для темы электронных

---

[17] www.oasis-open.org/home/index.php.
[18] www.openidentityexchange.com.
[19] http://kantarainitiative.org, раньше известная как Альянс свободы, www.projectliberty.org.
[20] http://openid.net/foundation.
[21] www.tscheme.org.
[22] www.internetsociety.org.
[23] www.tscp.org.
[24] https://www.certipath.com.
[25] www.safe-biopharma.org.
[26] www.identrust.com.
[27] www.cabforum.org.
[28] www.fixs.org.

передаваемых записей и для любой будущей работы по другим темам (механизмы единого окна и платежи при помощи мобильных устройств)[29].

a) Идентификация подписавшего лица является одним из требований создания действительной электронной подписи. Статья 7 Типового закона ЮНСИТРАЛ об электронной торговле (1996 год) и статья 9 Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах (2005 год, Конвенция об электронных сообщениях) требуют в качестве условия действительности электронной подписи, чтобы был "использован какой-либо способ для идентификации" подписавшего лица, который является как надежным, так и соответствующим цели, для которой сообщение данных было подготовлено или передано. Статья 2 Типового закона ЮНСИТРАЛ об электронных подписях требует также наличия в качестве компонента электронной подписи данных, "которые могут быть использованы для идентификации подписавшего".

b) Проверка идентификационных данных является также важнейшим требованием при использовании электронных передаваемых записей, механизмов единого окна и платежей при помощи мобильных устройств. Современное законодательство об использовании электронных передаваемых записей требует идентификации как подписавшего эту запись, так и держателя, имеющего право на ее принудительную реализацию[30]. При использовании механизмов единого окна потребуется идентификация подписавшего таможенные документы, а также представляющего их физического или юридического лица или физического или юридического лица, имеющего право на их принудительную реализацию[31]. Аналогичным образом при использовании платежей с помощью мобильных устройств, как и любых других платежных систем, требуется (для целей санкционирования) идентифицировать лицо, намеревающееся произвести перевод средств[32].

III. Что такое управление идентификационными данными?

8. По своей сути управление идентификационными данными призвано дать ответ на два простых вопроса, которые каждая сторона любой онлайновой сделки задает о другой стороне: "Кто вы?" и "Как вы можете это доказать?". Способность дать надежный и заслуживающий доверия ответ на эти вопросы быстро становится важнейшим требованием для ведения электронной коммерческой деятельности, особенно по мере усложнения характера и повышения значимости и степени конфиденциальности таких сделок. Имея ответы на эти два вопроса, любая сторона онлайновой сделки может решить, стоит ли ей участвовать в такой сделке (например, заключать ли контракт с другой стороной, разрешать ли другой стороне доступ к конфиденциальной базе данных или предоставлять ли другой стороне некоторые другие привилегии или доступ).

---

[29] *Официальные отчеты Генеральной Ассамблеи, шестьдесят шестая сессия, Дополнение № 17* (A/66/17), пункты 241-252.

[30] A/CN.9/WG.IV/WP.115, пункты 24-26 и 45-48.

[31] A/CN.9/728/Add.1, пункты 42 и 45.

[32] См. A/CN.9/728, пункт 52.

9. Любая структура, участвующая в цифровых сделках, может создать собственную систему идентификации и удостоверения подлинности любого из своих деловых партнеров (как это в настоящее время делают многие компании при помощи процедур индивидуальной регистрации, связанных с использованием имен пользователей и паролей), однако это становится все более дорогостоящим и не соответствующим требованиям делом, затрудняющим охват системой все более широкого населения. Кроме того, растущая потребность в межорганизационном сотрудничестве, забота об обеспечении безопасности и трудности управления пользовательскими паролями дают основание полагать, что традиционный подход, связанный с присвоением компанией или продавцом имени пользователя и пароля, утратил свою актуальность.

10. В результате в качестве предпочтительного подхода стали создаваться системы идентификации, в которых ключевую роль играет поставщик идентификационных услуг (или поставщик атрибутов), являющийся третьей стороной. Цель этого подхода заключается в том, чтобы коммерческие компании и государственные учреждения имели возможность проводить электронные сделки с удаленными сторонами, опираясь на идентификационную информацию и процедуры удостоверения подлинности, обеспечиваемые любым из нескольких независимых поставщиков таких услуг, являющихся третьими сторонами. Это часто называется "объединенной" системой идентификации. Иначе говоря, идентификационная информация, проверяемая одной структурой, на согласованной и управляемой основе предоставляется в распоряжение многих сторон в разных системах, которые нуждаются в идентификационной информации для различных целей. Это, например, позволит физическим лицам и коммерческим предприятиям использовать отобранную ими идентификационную информацию для ведения онлайновых операций со многими предприятиями подобно тому, как частное лицо может использовать водительские права для совершения самых различных офлайновых сделок с разными структурами, например покупать алкогольные напитки, получать доступ в зону посадки пассажиров в аэропортах или открывать банковский счет.

11. Для создания объединенной идентификационной системы требуется разработать комплекс технических стандартов и систем[33], порядок и процедуры ведения операций и юридические правила, которые вместе образуют надежную систему для: i) проверки идентификационных данных и отождествления этих идентификационных данных с физическим или юридическим лицом, устройством или цифровым объектом, ii) предоставления этой идентификационной информации стороне, которой она необходима для санкционирования сделки, и iii) сохранения и защиты этой информации в течение всего срока ее действительности. Важнейшим элементом обеспечения функционирования этой системы в коммерческом контексте является требование о наличии надлежащей и, как правило, построенной на договорных началах нормативно-правовой базы, которая определяет права и обязанности сторон, распределяет риски и предусматривает порядок обеспечения

[33] Одним из подходов к созданию системы идентификации является использование инфраструктуры публичных ключей (ИПК). Вместе с тем разрабатываются также и внедряются многие другие технологии и подходы.

исполнения. Такую нормативно-правовую базу часто называют "оперативными правилами" или "структурой доверия".

IV. Основы управления идентификационными данными

12. Хотя термин "управление идентификационными данными" является относительно новым, сама концепция отнюдь не нова. Лежащие в ее основе процедуры давно используются в офлайновой среде. Паспорта, водительские права, а также служебные удостоверения – все это компоненты систем идентификации (т.е. та или иная структура выдает их прошедшим проверку частным лицам, с тем чтобы впоследствии они могли удостоверить свою личность). Процесс идентификации лица и выдачи идентификационного удостоверения может осуществляться стороной, которая сама принимает эти идентификационные удостоверения (как, например, в случае выданного компанией служебного удостоверения), или третьей стороной (как, например, в случае водительских прав или паспорта). Ключевой элемент объединенных систем, предполагающих наличие эмитента, являющегося третьей стороной, заключается в том, что использование этих идентификационных удостоверений не ограничивается сделками со структурами, которые их выдали. Скорее, цель их выдачи и использования предполагает, что они будут приниматься третьими сторонами (например, службой безопасности аэропорта, банком или барменом в случае водительских прав), когда требуется подтверждение определенных идентификационных атрибутов (например, фамилии или возраста).

13. Задача состоит в том, чтобы реализовать аналогичную возможность в онлайновой среде. Речь идет о создании системы защищенных, надежных и пользующихся доверием цифровых идентификационных удостоверений, которые можно использовать в удаленном режиме в разных системах и структурах (т.е. речь идет о создании объединенной системы идентификации). Такая система позволяет субъектам данных использовать те же идентификационные удостоверения для собственной идентификации в целях получения доступа к ресурсам или проведения сделок со многими организациями.

14. Несмотря на существование многих разных подходов к управлению идентификационными данными, по существу оно включает два основных процесса: i) процесс сбора и проверки определенных идентификационных атрибутов лица (или структуры, устройства или цифрового объекта)[34] и выдачи идентификационных удостоверений, отражающих эти атрибуты ("идентификация") и ii) процесс последующей проверки конкретного лица, представляющего такое идентификационное удостоверение и утверждающего, что оно было ранее идентифицировано, на предмет того, что оно действительно является таким лицом ("удостоверение подлинности"). Каждый из таких основных процессов может включать различные подпроцессы в зависимости от характера данных и контекста, в которых эти два процесса

[34] Сбор и проверка идентификационной информации и выдача идентификационных удостоверений могут производиться для физических и юридических лиц, устройств и цифровых объектов. В настоящем документе рассматриваются только системы идентификации физических лиц.

имеют место. После успешного удостоверения подлинности идентификационных атрибутов лица наступает очередь третьего комплекса процессов, называемых "санкционированием", которые задействуются структурой, намеренной воспользоваться идентификационными данными, подлинность которых удостоверена, для определения прав и привилегий, предоставляемых такому лицу (например, заключать ли контракт с таким лицом, предоставить ли такому лицу доступ к базе данных или онлайновому банковскому счету).

A. Идентификация

15. Процесс идентификации призван дать ответ на вопрос: "Кто вы?" Этот процесс осуществляется тем, кто выполняет роль поставщика идентификационных услуг[35], и заключается в установлении соответствия идентификационных атрибутов (таких как фамилия, членский номер, адрес или дата рождения) с тем или иным лицом для идентификации и удостоверения личности этого лица на уровне, достаточном для намеченной цели. Этот процесс, который иногда называют "проверкой идентичности" или "регистрацией", часто является одноразовым действием. Как правило, он включает в себя сбор поставщиком идентификационных услуг информации о лице, подлежащем идентификации (называемом "субъектом"), и часто опирается на самые разные выданные государством документы (например, свидетельство о рождении, карточка социального страхования, водительские права и паспорт), а также на выданные частными структурами идентификационные удостоверения (например, служебный пропуск, мобильная беспроводная SIM-карта и кредитные карты). Хотя такие идентификационные документы и удостоверения были выданы для других целей, их можно часто повторно использовать для облегчения последующего процесса идентификации в новых условиях. Это происходит, например, когда кто-то предъявляет водительские права в целях подтверждения своей личности для получения служебного пропуска.

16. В конце процесса идентификации соответствующие идентификационные атрибуты субъекта получают свое отражение в форме данных в электронном документе, который выдается поставщиком идентификационных услуг и называется идентификационным удостоверением. Идентификационное удостоверение содержит в себе данные (либо ссылки или указания на них), которые используются для проверки подлинности заявленных цифровых идентификационных данных или атрибутов физического или юридического лица или устройства[36]. Идентификационным удостоверением могут быть самые разные носители информации. В материальном мире примерами идентификационного удостоверения являются документ с гербовой печатью, водительское удостоверение, паспорт, читательский билет или служебное удостоверение. В онлайновом мире идентификационным удостоверением могут быть простой идентификатор пользователя или сложный

---

[35] В некоторых случаях, когда для процесса идентификации требуются лишь отдельные атрибуты, эту роль может выполнять так называемый поставщик услуг по атрибуции.

[36] Руководство ОЭСР по электронному удостоверению подлинности (2007 год), стр. 12 оригинального текста: http://www.oecd.org/dataoecd/32/45/38921342.pdf.

зашифрованный цифровой сертификат, которые могут храниться в компьютере, сотовом телефоне, смарт-карте, банкоматовской карте, флэш-накопителе или подобном устройстве.

B. Удостоверение подлинности

17. Когда то или иное лицо представляет идентификационное удостоверение (например, предъявляя водительские права в аэропорту или вводя идентификатор пользователя для получения доступа к корпоративной сети), утверждает, что оно является лицом, идентифицированным в этом удостоверении, и пытается осуществить право или привилегию, предоставляемую такому лицу (например, взойти на борт самолета, получить доступ к корпоративной сети или конфиденциальной базе данных), процесс удостоверения подлинности используется "доверяющей стороной" для определения соответствия действительности утверждений этого лица в отношении своей личности. Иначе говоря, когда то или иное лицо заявляет о том, кем оно является (утверждая, что оно является лицом, идентифицированным в идентификационном удостоверении), процесс удостоверения подлинности призван дать ответ на вопрос: "Да, как вы можете это доказать?". Речь идет об имеющем отношение к конкретной сделке мероприятии, которое заключается в проверке соответствия того или иного лица идентификационному удостоверению для установления того факта, что это лицо, пытающееся участвовать в данной сделке, действительно является тем лицом, которое ранее было идентифицировано в идентификационном удостоверении.

18. Удостоверение подлинности, как правило, требует наличия элемента, который позволяет ассоциировать данное лицо с идентификационным удостоверением и который обычно называется аутентификатором. Если идентификационным удостоверением являются водительские права или паспорт, то таким аутентификатором будет фотография, при этом ассоциирование обычно осуществляется путем сравнения фотографии в водительском удостоверении или паспорте с самим представившим документ лицом. В случае электронных идентификационных удостоверений аутентификатором обычно является нечто, что данному лицу "известно" (например, секретный пароль или личный идентификационный номер), нечто, чем данное лицо "владеет" (например, частным криптографическим ключом, физическим устройством, таким как смарт-карта, USB, или другим видом маркера) или нечто, что для данного лица "характерно" в физическом плане (например, фотография, отпечаток пальца или другие биометрические данные).

C. Санкционирование

19. После успешного удостоверения подлинности того или иного лица доверяющая сторона может задействовать свой собственный процесс санкционирования для определения того, какие права и привилегии предоставляются такому лицу (например, следует ли разрешать такому лицу доступ к веб-сайту или базе данных или проход в бар или зону вылета авиапассажиров). Этот процесс должен дать ответ на вопрос: "Что вы можете?" Таким образом, удостоверение подлинности идентификационных данных – это

не просто конечный этап сам по себе. Оно часто используется для облегчения принятия доверяющей стороной санкционирующих решений, касающихся, в частности, предоставления прав или привилегий (например, доступа к онлайновой системе информационных ресурсов) или проведения сделки. Например, после удостоверения подлинности идентификационных данных того или иного лица, стремящегося получить доступ к компьютерной сети, владелец системы (т.е. доверяющая сторона) может использовать процесс санкционирования для определения того, какие права следует предоставить такому лицу. Аналогичным образом, после удостоверения подлинности идентификационных данных того или иного лица, стремящего заключить электронную сделку (например, электронный контракт), доверяющая сторона может использовать процесс санкционирования для определения того, следует ли проводить сделку с этим лицом или иным образом отреагировать на сообщение.

D. Объединенная система идентификации

20. При проведении онлайновых сделок идентификация и выдача идентификационных удостоверений традиционно осуществлялись одной и той же стороной, которая предполагала также полагаться на эти идентификационные удостоверения. Например, компания идентифицирует служащего и назначает ему имя пользователя и пароль, с тем чтобы он имел доступ к сети компании. В этом случае компания одновременно выступает и в качестве поставщика идентификационных услуг (поскольку она идентифицировала данное лицо в качестве своего служащего и выдала ему идентификационное удостоверение) и в качестве доверяющей стороны (поскольку для предоставления доступа к своей сети она также принимает это идентификационное удостоверение и доверяет ему).

21. При "объединенной" системе идентификации функции поставщика идентификационных услуг и доверяющей стороны необязательно осуществляются одной и той же структурой. Вместо этого многие не связанные между собой доверяющие стороны могут полагаться на идентификационные удостоверения, выданные любым из нескольких независимых поставщиков идентификационных услуг. В соответствии с такой системой на одно и то же идентификационное удостоверение могут полагаться многие организации, не имеющие прямого отношения к первоначальной выдаче такого удостоверения.

22. Известным офлайновым примером объединенной системы управления идентификационными данными является нынешний порядок выдачи и использования водительских прав. Выданные правительственным учреждением водительские права используются различными не связанными между собой доверяющими сторонами для проверки указанных в них идентификационных атрибутов. Например, они используются службой безопасности аэропорта для проверки фамилии лица, пытающегося пройти в зону вылета авиапассажиров, или барменом для проверки возраста лица, заказавшего алкогольный напиток.

23. Одним из примеров объединенной системы идентификации является система банкоматов. При типичной банкоматовской операции лицо, имеющее счет в банке A, может использовать выданное его банком идентификационное удостоверение (банкоматовскую карту) для получения наличных денег из банкомата, принадлежащего банку B (с которым он не имеет никаких отношений). Для проведения операции банк B, независимо от отсутствия таких отношений, связывается с банком A через банкоматовскую сеть для определения того, действительно ли данное лицо является клиентом банка A, для удостоверения банком A подлинности идентификационных данных данного лица (т.е. правильно ли это лицо ввело пароль) и для получения от банка A определенной идентификационной информации о данном лице (например, информацию о достаточности средств на счете этого лица для покрытия запрашиваемой суммы, а также об остатке на этом счете, с тем чтобы банк B мог распечатать его на квитанции).

IV. Риски, связанные с использованием идентификационной системы

24. Участие в идентификационной системе и доверие к идентификационным данным связаны с рядом потенциальных рисков. К этим рискам относятся:

a) риск, связанный с идентификацией: при использовании любой идентификационной системы важнейшее значение имеет надежность собранной и подтвержденной идентификационной информации о субъектах. Риск, связанный с идентификацией, заключается в недостоверности собранных данных об идентификационных атрибутах, ассоциированных с конкретным субъектом. Этот риск часто зависит от качества офлайновых идентификационных удостоверений, предъявленных субъектом для проверки идентификационных данных;

b) риск, связанный с удостоверением подлинности: идентификация не имеет никакого значения, если доверяющая сторона не имеет возможности удостоверить ее подлинность (т.е. ассоциировать заявленные идентификационные атрибуты с правильным субъектом). Риск, связанный с удостоверением подлинности, включает как риск возможного ненадлежащего удостоверения подлинности правильного субъекта, так и риск неверного указания в результате процесса удостоверения подлинности постороннего субъекта в качестве правильного субъекта;

c) риск, связанный с конфиденциальностью: в случае физических лиц управление идентификационными данными включает сбор и проверку поставщиком идентификационных услуг личной информации о субъекте и предоставление этой информации многим доверяющим сторонам. Кроме того, сделки, связанные с использованием идентификационных данных, могут также облегчать отслеживание деятельности физического лица и тем самым получать дополнительную личную информацию. Риск, связанный с конфиденциальностью, заключается главным образом в несанкционированном или ненадлежащем использовании личной информации о субъекте одной из сторон, имеющей к ней доступ, а также в соблюдении этими сторонами обязательств в отношении обработки и защиты таких данных;

d) риск, связанный с защищенностью данных: при использовании любой идентификационной системы важнейшее значение имеют защита личной информации о физических лицах, а также обеспечение безопасности процессов, необходимых для создания защищенных идентификационных удостоверений, сообщения достоверной идентификационной информации, проверки статуса идентификационных удостоверений, и удостоверение подлинности субъектов. Риск, связанный с обеспечением защищенности, включает риск возможного получения неуполномоченной стороной доступа к личным данным, а также риск дискредитации любого процесса, имеющего решающее значение для общего функционирования идентификационной системы или любых сделок с использованием идентификационных данных физических лиц;

e) риск, связанный с ответственностью: при использовании любой системы идентификации неизбежно будут возникать сбои, приводящие к причинению ущерба. Применительно к этому риску участники системы идентификации должны осознавать, что они будут нести ответственность за ущерб, причиненный другим сторонам в результате проблемы, которую они создали или за которую они по закону несут ответственность. Ключевым аспектом риска, связанного с ответственностью, является правовая неопределенность в отношении ответственности, которая возникает в связи с любым конкретным действием или бездействием со стороны участника системы идентификации, особенно участника, который действует в нескольких отраслях и юрисдикциях;

f) риск, связанный с обеспечением исполнения: риск, связанный с обеспечением исполнения, дополняет риск, связанный с ответственностью. Этот риск заключается в том, что один участник будет не в состоянии обеспечить исполнение i) своего права на соблюдение правил другим участником или ii) своего права взыскать ущерб в случае фактического причинения ему вреда, когда другой участник несет за это юридическую "ответственность". Этот риск возникает, когда происходят какие-то сбои и кто-то стремится взыскать убытки. Он также возникает в тех ситуациях, когда проблема еще не стала очевидной, но неисполнение со стороны одного или нескольких участников может подвергнуть угрозе всю систему идентификации. Это особенно важно в системе, объединяющей несколько юрисдикций. В этом случае риск, связанный с обеспечением исполнения, заключается как в способности обнаружить эту проблему, так и в способности потребовать от конкретного участника выполнить свои обязанности или выйти из системы;

g) риск, связанный с соблюдением нормативных положений: во многих случаях участие в системе идентификации затрагивает вопросы соблюдения нормативных положений одним или несколькими участниками (т.е. соответствует ли поведение конкретного участника применимому внутреннему законодательству). В других случаях участие в системе идентификации само по себе обусловлено стремлением выполнить юридические требования, предъявляемые к участнику. Например, финансовое учреждение может участвовать в системе и полагаться на идентификационные удостоверения в целях исполнения своих юридических обязанностей надлежащим образом удостоверять подлинность физических лиц, получивших

онлайновый допуск к банковским счетам и платежным механизмам. В таких случаях риск, связанный с соблюдением, заключается, главным образом, в том, осуществляется ли такое участие с соблюдением установленных юридических обязанностей.

25. Как и в любой системе, вышеуказанные риски зависят от используемых технологий, реализации различных процессов и соблюдения или несоблюдения обязательств самими участниками (и возможного влияния внешних сторон). Создание надежной системы идентификации потребует принятия мер по уменьшению этих рисков, т.е. таких мер, которые обеспечат доверие участников к используемым технологиям (которые функционируют надлежащим образом), реализованным процессам (которые дают достоверные результаты) и другим участникам (которые будут надлежащим образом исполнять свои обязательства).

V. Обеспечение функциональности и уменьшение рисков: оперативные правила

26. Обеспечение функционирования объединенной системы идентификации в онлайновой среде и уменьшение вышеуказанных рисков потребуют не только внедрения соответствующих технологий, но и соблюдения всеми участниками (например, субъектами, поставщиками идентификационных услуг и доверяющими сторонами) общего свода технических стандартов, оперативных требований и юридических норм. Коммерческие системы идентификации, как правило, стремятся достичь этой цели путем разработки соответствующих "оперативных правил" (иногда называемых структурой доверия), соблюдать которые участники обязаны на договорной основе.

27. Оперативные правила системы идентификации состоят из двух общих категорий компонентов: i) деловые и технические оперативные правила и спецификации, необходимые для обеспечения функциональности системы и доверия к ней, и ii) договорные юридические правила, которые, помимо применимого законодательства и нормативных положений, определяют права и юридические обязанности сторон, участвующих в системе идентификации, и, в необходимых случаях, способствуют обеспечению исполнения.

a) Деловые и технические оперативные правила устанавливают требования, необходимые для надлежащего функционирования системы идентификации, определяют роль и оперативную ответственность участников и обеспечивают надлежащие гарантии достоверности, целостности, конфиденциальности и защищенности процессов и данных (чтобы обеспечить желание различных сторон участвовать и чтобы это вызывало доверие). Во многих случаях такие правила основаны на существующих стандартах.

b) Договорные юридические правила содержатся в заключенных между двумя или несколькими участниками соглашениях, которые определяют и регулируют юридические права, обязанности и ответственность участников в отношении конкретной системы идентификации, конкретизируют правовые риски, принимаемые на себя участниками системы идентификации (например, в связи с предоставлением гарантий, ответственностью за убытки и рисками, которым подвергаются их личные данные), и предусматривают средства

правовой защиты в случае возникновения споров между сторонами, включая механизмы урегулирования споров и обеспечения исполнения решений, права, касающиеся расторжения соглашений, а также размеры компенсации ущерба, штрафные санкции и другие формы ответственности. Они также придают деловым и техническим оперативным правилам юридически обязательный характер и исковую силу в отношении участников.

28. Само собой разумеется, что деловые и технические оперативные правила и договорные юридические правила учитывают и, как правило, построены со ссылкой на другие существующие обязанности и обязательства, вытекающие из законодательных и нормативных положений, которые применяются к сторонам. Оба компонента оперативных правил системы идентификации (т.е. как деловые и технические оперативные правила, так и юридические правила) регулируются существующими законодательными и нормативными положениями, которые применяются в юрисдикции(ях), где данная система идентификации будет функционировать или использоваться.

29. Оперативные правила системы идентификации весьма похожи на оперативные правила, используемые в системах кредитных карт или системах электронных платежей, которые должны иметь возможность обслуживать многих участников в различных юрисдикциях в соответствии с общим набором правил. Например, оперативные правила использования кредитных карт регулируют деятельность эмитентов, процессинговых центров, торговых подразделений доверяющей стороны и действия индивидуальных держателей карт, а также определяют спецификации и правила, применимые к участникам онлайновых кредитных операций и последующего процессинга[37]. Аналогичным образом, оперативные правила системы электронных переводов средств регулируют ответственность всех банков, участвующих в платежном процессе, а также, в меньшей степени, ответственность клиентов или других плательщиков и правила, применимые к участникам во всех случаях, когда электронные переводы средств (например, переводы SWIFT) используются для облегчения платежей при проведении онлайновых сделок[38].

---

[37] Оперативные правила использования кредитных карт включают спецификации и правила для эмитентов кредитных карт (например, the Visa International Operating Regulations at http://usa.visa.com/merchants/operations/op_regulations.html and the Payment Card Industry Data Security Standards — PCIDSS at https://www.pcisecuritystandards.org/security_standards/index.php), которые имеют обязательную силу для процессинговых банков и торговых компаний, а также контракты между эмитентами кредитных карт и процессинговыми банками, контракты между процессинговыми банками и торговыми компаниями и контракты между процессинговыми банками и держателями карт. Эти правила дополняются законодательными и нормативными положениями, которые регулируют процессинг кредитных карт в каждой соответствующей юрисдикции.

[38] Оперативные правила электронных переводов средств включают спецификации и правила для операций по электронному переводу средств (например, the Operating Rules and Guidelines of U.S.-based NACHA – The Electronic Payments Association, http://www.nacha.org/), которые имеют обязательную силу для процессинговых банков и торговых компаний, а также контракты между торговыми компаниями и индивидуальными плательщиками. Они дополняются законодательными и нормативными положениями, регулирующими электронные переводы средств, такими как (в США) Закон об электронных переводах средств и Постановление E.

30. Несмотря на общее признание необходимости разработки для систем идентификации оперативных правил, содержащих соответствующие юридические правила, для практического решения этого вопроса еще предстоит сделать многое. Необходимо определить и решить многочисленные правовые проблемы и преодолеть связанные с ними препятствия.

VI. Законодательство, регулирующее функционирование систем идентификации

31. В большинстве правовых систем существует множество действующих законов и подзаконных актов, которые будут оказывать серьезное регламентирующее воздействие (и которые могут вводить ограничения, предъявлять требования о соблюдении и/или устанавливать риски ответственности) на участие в системе идентификации. Кроме того, различия в законах в разных юрисдикциях, если рассматривать их в призме глобального характера Интернета, являют весьма разнородную картину правового регулирования, что само по себе может затруднить разработку стройной правовой структуры. Некоторые из этих законов и подзаконных актов конкретно затрагивают деятельность, связанную с идентификационными данными. Вместе с тем большинство из них были разработаны в контексте, не имеющем никакого отношения к управлению идентификационными данными (например, законодательство о гражданско-правовых деликтах, законодательство о договорных отношениях и законодательство о гарантиях), но тем не менее они могут оказывать существенное воздействие, причем нередко так, как этого нельзя было предвидеть во время их первоначального принятия.

32. К системам идентификации (или их участникам) применяются, в частности, следующие категории законодательства:

a) законодательство, регулирующее достоверность идентификационной информации: задача системы идентификации заключается в сборе и проверке поставщиками идентификационных услуг или поставщиками атрибутов информации о субъектах и сообщении определенной части этой информации доверяющим сторонам. Это часто происходит в ситуациях, когда достоверность и/или надежность этой информации имеет важное значение. В этой связи при оценке прав, обязанностей и ответственности участников систем идентификации важную роль будут играть законы, касающиеся представления ложной и недостоверной информации, будь то намеренно или по небрежности. Основными из них являются законы о гражданских деликтах, регулирующие неумышленное введение в заблуждение, одобрение по небрежности и клевету, а также законы о гарантиях, законы о хищении идентификационных данных и законы, регулирующие недобросовестную и вводящую в заблуждение деловую практику;

b) законодательство, регулирующее конфиденциальность идентификационной информации: по своему характеру управление идентификационными данными включает сбор (поставщиком идентификационных услуг или его агентами) и раскрытие (доверяющей

стороне) личной информации о субъекте[39]. В этой связи на управление идентификационными данными серьезное влияние будут оказывать законы о защите данных, законы об обеспечении конфиденциальности и другие законы и подзаконные акты, регулирующие сбор, использование, обработку, передачу и хранение личных данных. Хотя многие из таких законов были разработаны до появления цифровых систем идентификации и поэтому в них не предусматривались конкретные процессы или потенциальный вред, который такие системы могут причинить, они тем не менее оказывают прямое воздействие на такую деятельность;

c) законодательство, регулирующее сбор идентификационной информации: помимо законов об обеспечении конфиденциальности и защиты данных, на компании, создающие информационные продукты и оказывающие услуги, основанные на массивах данных публичного сектора, оказывают воздействие законы, регулирующие повторное использование информации публичного сектора. Эти законы могут создавать правовые ограничения для широкого использования данных, имеющихся у публичных органов, в контексте оказания идентификационных услуг[40];

d) законодательство, регулирующее защищенность идентификационной информации и процессов: многие законы обязывают компании обеспечивать защищенность личной информации (которая по-разному трактуется в разных юрисдикциях и в конкретных законах в данном секторе) и других данных, находящихся в их владении. Помимо законов и подзаконных актов, обязывающих принимать меры безопасности для защиты данных, во многих юрисдикциях приняты также законы и подзаконные акты, обязывающие информировать затронутых лиц о случаях нарушения защищенности личной информации;

e) законодательство, касающееся обязанности идентифицировать: многие законы и подзаконные акты требуют идентификацию в качестве составного элемента, особенно в электронной среде. Например, в Конвенции об электронных сообщениях содержится прямое требование об идентификации в качестве компонента юридически обязательной электронной подписи. В конкретном плане, когда законодательство требует, чтобы сообщения или договоры были подписаны стороной, то Конвенция об электронных сообщениях предусматривает, что требование о подписи считается выполненным, если использован какой-либо способ для идентификации этой стороны и указаны намерения этой стороны в отношении информации, содержащейся в электронном сообщении[41];

f) законы, касающиеся обязанности удостоверять подлинность: ряд законов регулирует один или несколько элементов удостоверения подлинности. Одни законы обязывают компании удостоверять подлинность лиц, с которыми

---

[39] За исключением случаев, когда субъектом не является физическое лицо – например, когда субъектом являются корпорация, устройство, прикладное программное обеспечение и т.д.

[40] См. в целом Global Networking of Individuals (GINI), Legal provisions for Deploying INDI Services (October 5, 2011) at Section 5, размещены по адресу www.gini-sa.eu/images/stories/2011.11.06_GINI_D3.1_Legal%20Provisions%20for%20Deploying%20INDI%20Services_FINAL.pdf.

[41] Конвенция об электронных сообщениях, статья 9(3).

они имеют дело в удаленном режиме, а другие регулируют аспекты процесса удостоверения подлинности. Одним значимым примером являются требования органов США, регулирующих банковскую деятельность, об удостоверении подлинности при осуществлении онлайновых банковских операций. Так, финансовые учреждения, предлагающие своим клиентам онлайновые продукты и услуги, обязаны "использовать эффективные методы для удостоверения подлинности идентификационных данных клиентов, использующих такие продукты и услуги"[42]. В других странах, например в Сингапуре, также приняты аналогичные требования[43];

g) законодательство, конкретно регулирующее функционирование системы идентификации: в некоторых юрисдикциях приняты законы, прямо регулирующие некоторые аспекты управления идентификационными данными. Одним из примеров является директива ЕС об электронных подписях[44], которая предписывает государствам-членам регулировать сбор личных данных о субъектах определенными поставщиками идентификационных услуг (называемыми поставщиками сертификационных услуг) и регулирует порядок выдачи идентификационных удостоверений[45]. Аналогичным образом, в Типовом законе ЮНСИТРАЛ об электронных подписях (статьи 8-12) сформулированы правила выдачи и использования идентификационных удостоверений, необходимых для создания определенных электронных подписей.

H. Проблемы и правовые препятствия

33. Указанные выше, а также другие действующие законы и подзаконные акты создают ряд основных проблем, затрудняющих разработку и функционирование частных идентификационных систем. К этим проблемам относятся следующие:

a) в законодательстве не прописаны вопросы, касающиеся управления идентификационными данными: многие новые вопросы, связанные с процессами управления идентификационными данными, просто не рассматриваются в существующем законодательстве. Большинство существующих законов, которые применяются в этом контексте, не были сформулированы с учетом возможного появления цифровых систем идентификации и поэтому часто неадекватным или ненадлежащим образом рассматривают или регулируют идентификационную деятельность. Например, существующее законодательство, как правило, обходит молчанием вопрос об обязанности удостоверителя подлинности проявлять бдительность при оценке подлинности идентификационных документов или вопрос об объеме любого

---

[42] Федеральный совет по надзору за финансовыми учреждениями ("ФСНФУ"), "Authentication in an Internet Banking Environment", October 12, 2005, at p. 1; см. www.ffiec.gov/pdf/authentication_guidance.pdf.

[43] Валютное управление Сингапура, циркуляр № SRD TR 02/2005, 25 ноября 2005 года.

[44] Директива 1999/93/ЕС от 13 декабря 1999 года о применяемых Сообществом рамках в отношении электронных подписей ("Директива ЕС об электронных подписях"), статьи 6-8 и приложения I и II, см. http://europa.eu/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf.

[45] Директива ЕС об электронных подписях, статья 8.

обязательства поставщика идентификационных услуг по раскрытию информации, которую он несет перед субъектом данных;

b) правовая неопределенность/двусмысленность: существующие законы и подзаконные акты могут регулировать определенные вопросы управления идентификационными данными, однако применимость этих законов часто носит неясный или двусмысленный характер, в результате чего для участников системы идентификации создается ситуация серьезной правовой неопределенности, которая может замедлить темпы экономического роста, инноваций и инвестиций. Поэтому даже там, где действующее законодательство применяется к управлению идентификационными данными, порядок его применения к тому или иному конкретному вопросу или предложенный в системе идентификации подход могут быть неясны. Это особенно справедливо в отношении законов, касающихся конкретной технологии. Такая ситуация может ограничивать способность сторон проводить операции по идентификации для оценки рисков, которые они берут на себя в этой связи, и управления этими рисками;

c) вопросы конфиденциальности: по своему характеру управление идентификационными данными включает сбор поставщиком идентификационных услуг определенной личной информации о субъекте и ее раскрытие доверяющей стороне. Для участия в системе идентификации субъекты должны раскрывать личную информацию и таким образом подвергать себя риску несанкционированного или ненадлежащего использования такой информации. Кроме того, поскольку субъекты взаимодействуют со многими доверяющими сторонами, требуемое сообщение или проверка их информации поставщиком идентификационных услуг позволяет прослеживать деятельность каждого субъекта, вызывая обеспокоенность в отношении сбора и использования такой информации о сделках. Таким образом, обеспечение конфиденциальности имеет важнейшее значение для любой системы идентификации. Достижение этой цели может быть связано с решением следующих вопросов: i) какую информацию может собирать поставщик идентификационных услуг?; ii) в каком объеме информация может раскрываться доверяющим сторонам?; iii) в каких пределах субъект может регулировать раскрытие информации?; iv) какие меры безопасности должны принимать стороны при обращении с данными?; и v) какие ограничения накладываются на использование информации поставщиком идентификационных услуг и доверяющими сторонами? Эти вопросы часто регулируются существующим законодательством, которое может быть также дополнено договорными оперативными правилами;

d) вопросы ответственности: важнейший правовой вопрос, волнующий участников любой системы идентификации, заключается в определении того, кто будет нести ответственность, связанную с любым риском (см. пункт 24 выше). Для выявления, определения и уточнения источника и объема такой потенциальной ответственности выдвинуто множество теоретических концепций в области статутного права, общего права и договорного права[46].

---

[46] См. *Certification Authority Liability Analysis* (проведенное для Американской ассоциации банкиров исследование, в котором рассматриваются потенциальные риски

Однако эти правовые риски часто плохо определены и лишены необходимой ясности. Обеспокоенность в связи с неясностью вопроса об ответственности является основным препятствием на пути принятия частным сектором согласованных решений в области использования идентификационных данных. Решение вопросов ответственности при помощи оперативных правил или других форм соглашений между участниками часто является наилучшим подходом, поскольку он позволяет "адаптировать" контракт к конкретным потребностям для обеспечения надлежащего распределения рисков, которое в каждом конкретном случае будет разным;

e) юрисдикционные различия и коллизии: существует ряд ключевых вопросов, по которым применение к управлению идентификационными данными существующих законов и подзаконных актов имеет существенные отличия в разных юрисдикциях. Чаще всего речь идет о законах, регулирующих ответственность участников, и о законах о защите данных, регулирующих конфиденциальность личной информации. Кроме того, в некоторых случаях дополнительные препятствия для трансграничного функционирования систем идентификации создает регулирование или лицензирование деятельности в рамках системы идентификации. Таким образом, в тех случаях когда системы идентификации функционируют в рамках нескольких юрисдикций, проблемы разработки надлежащих оперативных правил усугубляются тем фактом, что существующие законы и подзаконные акты отличаются друг от друга (нередко весьма значительно) в разных юрисдикциях;

f) необходимость правовой совместимости: использование систем идентификации часто осложняется тем фактом, что в разных юрисдикциях применимые законы могут отличаться друг от друга. В отсутствие единообразных законов, регулирующих функционирование систем идентификации, часто предпринимаются попытки решить эту проблему путем разработки оперативных правил, обеспечивающих правовую совместимость всей системы в целом. Различие в законах и подзаконных актах в разных юрисдикциях затрудняет разработку таких оперативных правил и других договоров, необходимых для придания деятельности участников системы более единообразного характера в рамках всей онлайновой системы;

g) ограничения возможности изменять законодательство на договорной основе: некоторые существующие законы и подзаконные акты можно изменять на договорной основе. Например, многие законы содержат принципы договорного или торгового права, которые только устанавливают "правила по умолчанию", применяемые в отсутствие явного выбора сторон, но позволяющие изменять эти правила по соглашению сторон сделки. В таких случаях участники системы идентификации вправе изменять правила по умолчанию и заполнять пробелы, используя соответствующие договорные оперативные правила. Однако в других случаях императивные нормы закона не могут изменяться простым соглашением сторон, поскольку они служат общественным интересам, таким как защита прав потребителей или третьих сторон.

ответственности поставщика идентификационных услуг, действующего в качестве сертифицирующего органа), см. http://64.78.35.30/article/ca-liability-analysis.pdf.

34. В результате существующие законы могут создавать препятствия для принятия эффективных, совместимых и заслуживающих доверия систем идентификации, которые могут функционировать в трансграничном режиме. Основным методом решения этих правовых проблем и уменьшения неопределенности для участников является разработка договорных оперативных правил. Это также облегчает экспериментирование с разными системами и разными подходами, по мере того как сам рынок решает вопросы управления идентификационными данными.

35. Все участники объединенной системы идентификации заинтересованы в заблаговременном справедливом распределении рисков ответственности, сопряженных с участием в процессе, а также в максимально возможном уменьшении этих рисков. В отсутствие решения вопроса о том, как распределять ответственность или кто находится в наилучшем положении для несения рисков, основным препятствием для реализации заслуживающей доверия системы идентификации является существующая правовая неопределенность. Поскольку процессы управления идентификационными данными используются для все более крупных сделок и поскольку риски для сторон соответственно увеличиваются, выгоды для всех сторон, связанные с применением надлежащих оперативных правил для заблаговременного учета этих рисков, а также уменьшением этих рисков (по мере возможности) путем требования о соблюдении конкретных обязательств каждым участником, являются весьма существенными.

36. Создание частных, трансграничных и совместимых систем идентификации для проведения деловых операций – это задача, которую еще предстоит решить. Подобно системам кредитных карт и электронных платежей, оперативные правила для систем идентификации, видимо, будут носить договорный характер, особенно в той степени, в какой они предназначены для использования в масштабах Интернета в рамках многих юрисдикций. В этой связи, возможно, целесообразно рассмотреть законодательство, призванное устранить имеющиеся препятствия для функционирования таких систем (а не регулировать их).

* * *

ОПРЕДЕЛЕНИЯ

[*ПРИМЕЧАНИЕ: настоящие определения носят общий характер и приводятся исключительно в порядке оказания помощи в понимании вышеприведенного текста*]

Атрибут: указанное качество или характеристика, присущая или приписываемая объекту, такие как фамилия, адрес, возраст, пол, должность, оклад, чистая стоимость активов, номер водительских прав, номер карточки социального страхования и т.д. (для физического лица), марка и модель, серийный номер, местоположение, мощность и т.д. (для устройства) и т.д. Синонимы: атрибут идентичности.

Поставщик атрибутов: структура, которая действует в качестве авторитетного источника одного или нескольких атрибутов идентификационных данных

субъекта и отвечает за процессы, связанные со сбором и поддержанием таких атрибутов. Поставщик атрибутов подтверждает достоверность и подлинность заявленных атрибутов в ответ на запросы о проверке атрибутов от поставщиков идентификационных услуг и доверяющих сторон. Примерами поставщиков атрибутов являются, в частности, государственный регистр правовых титулов, национальное кредитное бюро или коммерческая маркетинговая база данных.

Удостоверение подлинности: процесс проверки заявленных идентификационных данных субъекта путем подтверждения их соответствия с идентификационным удостоверением. Например, ввод пароля, который ассоциируется с именем пользователя, считается удостоверением того, что пользователь является лицом, которому это имя пользователя было присвоено. Аналогичным образом, сравнение лица, предъявившего паспорт, с фотографией в этом паспорте удостоверяет или подтверждает, что он/она является лицом, указанным в этом паспорте.

Аутентификатор: нечто, используемое для проверки связи между субъектом и идентификационным удостоверением; обычно объект, единица информации или определенная характеристика владельца, которая используется для увязки лица с идентификационным удостоверением. Например, функции пароля как аутентификатора идентификатора пользователя, функции фотографии как аутентификатора для паспорта или водительских прав.

Санкционирование: процесс предоставления прав и привилегий прошедшим удостоверение подлинности субъектам на основе критериев, определяемых доверяющей стороной; предназначено для контроля доступа к информации или ресурсам, с тем чтобы только лица, специально уполномоченные на использование таких ресурсов, имели доступ к ним.

Идентификационное удостоверение: данные, представляемые в качестве доказательства заявленных идентификационных данных субъекта. Примерами бумажных идентификационных удостоверений являются, в частности, паспорта, свидетельства о рождении, водительские права и служебные удостоверения. Примерами цифровых идентификационных удостоверений являются, в частности, имена пользователя, смарт-карты и цифровые сертификаты.

Объединенная система идентификации: система идентификации, в которой субъект может использовать идентификационное удостоверение, выданное любым из нескольких поставщиков идентификационных услуг для удостоверения своей подлинности перед многими не связанными между собой доверяющими сторонами в разных системах.

Идентификация: процесс сбора, проверки и установления действительности достаточной атрибутивной информации о конкретном субъекте для определения и подтверждения его идентификационных данных в конкретном контексте (синонимы: регистрация; проверка идентичности).

Идентификационные данные: информация о конкретном субъекте в форме одного или нескольких атрибутов, позволяющих субъекту быть в достаточной степени отличимым в определенном контексте. Набор атрибутов лица, которые позволяют этому лицу отличаться от других лиц в конкретном контексте.

Управление идентификационными данными: процессы, функции и возможности для сбора, проверки, увязки и сообщения доверяющей стороне идентификационной информации о субъекте, с тем чтобы доверяющая сторона могла проверить соответствие такой идентификационной информации с конкретным субъектом.

Поставщик идентификационных услуг: структура, ответственная за идентификацию физических и юридических лиц, устройств и/или цифровых объектов, выдачу соответствующих идентификационных удостоверений и сохранение и управление такой идентификационной информации в интересах субъектов (синонимы: поставщик услуг по идентификационным удостоверениям (ПУИУ); сертифицирующий орган (СО); поставщик атрибутов (когда предоставляются ограниченные атрибутивные данные)).

Система идентификации: онлайновая система для управления идентификационными данными, которая регулируется набором оперативных правил и в которой физические лица, организации, службы и устройства могут доверять друг другу, поскольку авторитетные источники устанавливают и удостоверяют подлинность их идентификационных данных.

Оперативные правила: деловые процессы, технические спецификации и договорные юридические правила, которые регулируют функционирование конкретной системы идентификации. Как правило, они разрабатываются частным сектором (например, оператором системы идентификации) и являются обязательными и имеющими исковую систему для участников на основе договора (синонимы: структура доверия; системные правила; общие оперативные правила; оперативные положения).

Доверяющая сторона: физическое или юридическое лицо, которое полагается на идентификационное удостоверение или подтверждение идентификационных данных для принятия решения о том, какие действия следует предпринять в данном прикладном контексте, например, решения о проведении сделки или предоставлении доступа к информации или системе (синоним: поставщик услуг).

Субъект: физическое или юридическое лицо, устройство или цифровой объект, которые идентифицируются в конкретном идентификационном удостоверении и подлинность которых может быть удостоверена поставщиком идентификационных услуг (синонимы: субъект данных; пользователь).