УДК 004

А.А. ДОМРАЧЕВ, советник Департамената государственной политики в области создания и развития электронного правительства Минкомсвязи России
В.Б. ИСАКОВ, заведующий кафедрой теории права и сравнительного правоведения Национального исследовательского университета «Высшая школа экономики», заслуженный юрист РФ, д.ю.н., профессор
В.К. САРЬЯН, директор НОЦ ИПТР ФГУП НИИР, акад. НАН РА, д.т.н., профессор
П.С. ПОГЛАЗОВ, техник 1-й категории по ИКТ ФГУП НИИР, студент магистратуры МФТИ

МАССОВАЯ ИНФОРМАЦИОННО-УПРАВЛЕНЧЕСКАЯ СЕТЬ КАК ПРИМЕР ПОСТРОЕНИЯ ДОВЕРЕННОЙ СРЕДЫ

Ключевые слова: доверенная среда; массовая информационно-управленческая сеть; инфокоммуникационные услуги.

Введение

Вопрос доверия является актуальным направлением таких наук, как социология [1], правоведение [2], информационные технологии [3]. В современном обществе благодаря развитию технологий увеличивается количество взаимодействий, причем как «человек – человек», так и «человек – машина», «человек – окружающая среда». Однако человек нуждается в предсказуемости результата при участии во взаимодействиях. Как указывают Earle i Cvetkovich, «мы должны научиться жить так – всегда настороже, балансируя между неопределенностью и изменчивостью ситуации, осознавая это, но не давая себя парализовать жизненным случайностям» [1]. В текущей ситуации «доверие становится основным ресурсом, средством, которое нам это позволяет» [1].

Seligman в [1] определяет доверие так: «Доверие – это определенный вид уверенности в доброй воле другого человека в условиях непрозрачности его намерений и расчетов».

Чтобы создать доверие человека к другим людям и машинам, действия которых человек не может контролировать, необходимо провести специальные мероприятия – создать доверенную среду. Целью данной статьи является обоснование необходимости построения доверенных сред для развития качества взаимодействий человека, а также анализ современных сфер применения доверенных сред.

1. Теоретическое обоснование доверенной среды

Дадим определение доверенной среды в современных условиях: доверенная среда – созданное комплексом технических и организационных мер пространство, которое обеспечивает его участникам предсказуемый результат взаимодействий. При этом степень доверенности среды определяется надежностью контекста в ней.

Рассмотрим модель взаимодействий, представленную на рис. 1.

На протяжении длительного периода развития общества пространство взаимодействий S и связанные с ней параметры n и f были константами. Однако глобализация приводит к изменению количества участников и числа взаимодействий внутри S, а при чрезвычайной ситуации меняются и свойства S – взаимосвязь между параметрами пространства.

Проведем сравнение пространств взаимодействий S_0 и S_1, где S_1 и соответствующие параметры относятся к текущей ситуации, а S_0 со своими параметрами – к доинформационному обществу.

В современном обществе выросло пространство взаимодействия каждого человека – $S_1 >> S_0$. При этом выросло как

Рис. 1. Роль контекста.

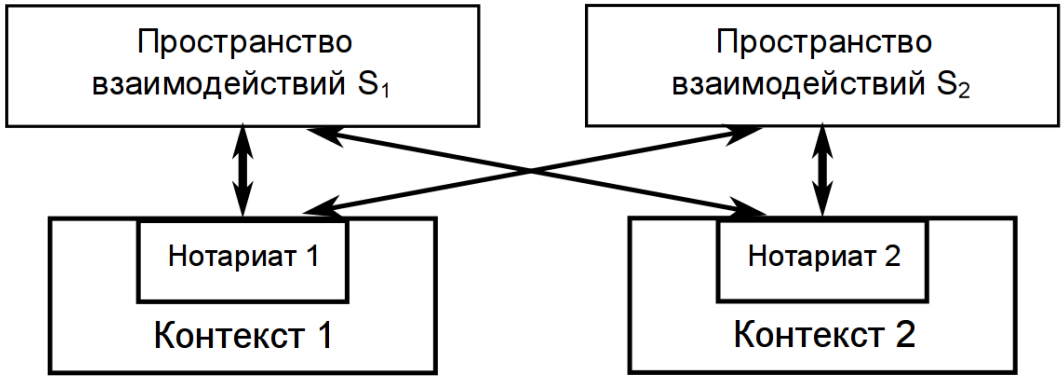

Рис. 2. Связь пространств взаимодействий и их контекстов.

количество участников $n_1 >> n_0$, так и количество взаимодействий: $f_1 > f_0$. А вот время на проведение одного взаимодействия, тратящееся на анализ контекста, уменьшилось: $t_1 > t_0$.

Контекст $K = D - D_0$ – количество доступных документов для принятия решения минус количество обязательных документов. Однако D прямо зависит от t – чем больше времени мы собираем информацию (документы), тем больше ее становится. В современном мире величина t мала и уменьшается, следовательно, для сохранения нужного размера D и контекста требуются альтернативные способы сбора контекстной информации – специальные нотариаты контекста. Необходимость получения большего коли-

чества контекстной информации требует расширения механизмов ее получения, и одним из важнейших способов станет обмен контекстом между пространствами взаимодействий при помощи их нотариатов (рис. 2).

Может возникнуть вопрос: явление доверия неотрывно связано с деятельностью человека, так почему же необходимость в создании особых доверенных сред появилась только сейчас? Все дело в развитии технологий и возможностей, ими предоставляемых. Например, при единственно возможном в прошлом личном взаимодействии предпринимателей, живущих в одном городе, даже незнакомые друг с другом контрагенты могли, во-первых, получать контекстную информацию о сторонах взаимодействия, прямо или косвенно связанную с их предыдущей деятельностью, а также имели возможность непосредственно контролировать выполнение обязательств. Сегодня, когда количество взаимодействий настолько выросло, что тщательный предварительный анализ каждого из них является невозможным из-за ограничений, в том числе и временных, – сфера взаимодействий мутировала в то, что Ульрих Бек называет «общество риска» [4]. Таким образом, уменьшилась степень доверенности контекста, что современное общество пытается компенсировать при помощи инфокоммуникационных технологий. Необходимо создание механизмов обеспечения дополнительных гарантий, заменяющих использовавшиеся ранее механизмы анализа контекста и контроля.

Ключевая тенденция современной жизни – глобализация – разрушает использовавшуюся ранее связность, делает невозможным полный контроль над контрагентом. Если раньше контекст, в котором находились оба участника локальной сделки, имел механизм обратной связи, удерживающий от нарушений, то теперь без должной организации нарушения не будут замечены теми сторонами, которые могут влиять на виновника.

Примером глобального явления, показывающего важность доверенной среды и вытеснение контекста специальными инфокоммуникационными средствами, является электронный документооборот. В системах электронного документооборота контекст создания традиционных бумажных документов вытесняется различными технологическими решениями, в числе которых – электронная подпись.

2. Обобщение понятия «доверенная среда»

Заметим, что мы расширяем понятие доверенной среды от привычных рамок, связанных с предоставлением инфокоммуникационных услуг по каналам связи [3], до создания среды, предсказуемой для человека, где действия завершаются ожидаемым положительным результатом.

Это обобщение дает возможность построения повсеместной доверенной среды.

Реальным примером формирования глобальной доверенной среды является доверенная среда для оказания инфокоммуникационных услуг на базе массовых информационно-управленческих сетей [5].

Массовые информационно-управленческие сети (МИУС) – описанный в работах [6] и [7] тип сетей. На данный момент одна из таких сетей реализуется в Томской области. Многие важные отличия МИУС уже описаны, например возможность эффективно передавать большие объемы информации широкому кругу пользователей.

Основной задачей МИУС является предоставление массовых инфокоммуникационных (ИК) услуг абонентам. На базе данной системы могут быть оказаны любые ИК-услуги, традиционно оказываемые через персональные компьютеры и мобильные телефоны:

1) доступ абонентов к справочной информации;

2) доступ к информации о деятельности государственных органов и судов;

3) система персональных и групповых сообщений, в том числе электронная почта;

4) прием и обработка запросов поль-

зователей на оказание персональных услуг, в том числе с использованием электронной подписи (ЭП);

5) распространение, заполнение и печать различных документов.

Использование ЭП является современным заменителем контекста, позволяющее получателю документа восстановить условия его подписания.

Построение безопасной инфокоммуникационной среды признается мировым сообществом: министры телекоммуникаций стран АТЭС декларируют своей целью построение безопасной и доверенной инфокоммуникационной среды [8].

Доверенная среда в МИУС характеризуется тремя отличительными особенностями:

1) отсутствует возможность мошенничества с использованием только технических уязвимостей;

2) нарушение обязательств или договоренностей одним из участников данного пространства может быть зафиксировано, потерпевшему будет возмещен ущерб, а нарушитель понесет значительное наказание;

3) в течение всего времени взаимодействия серверу и абонентам доступна контекстная информация об остальных участниках среды, что ведет к контролю и лучшему выполнению обязательств.

В МИУС существует единый поставщик ИК-услуг, что уменьшает риски, связанные с несанкционированным доступом к информации и создает возможность эффективного администрирования ИК-услуг. Указанный результат достигается, прежде всего, путем внедрения в систему промежуточного сервера. Блок-схема МИУС и принцип ее работы приведены в статье [5]. В данной статье мы выделяем только те особенности функционирования МИУС, которые связаны с созданием доверенной среды.

Применение схемы обработки информации в два этапа на промежуточном сервере и пользовательском терминале создает гибкость, благодаря которой возможно выбрать оптимальное соотношение между уровнями безопасности, надежности, комфортности и охвата аудитории ИК-услуги.

Кроме того, само присутствие центра – единого поставщика ИК-услуг позволяет решить важную для взаимодействия пользователей и провайдеров проблему контекста, когда стороны при заключении сделки могут получить дополнительную информацию друг о друге для оценки риска – сервер, через который проходят все сведения об оказанных услугах, может давать свою оценку каждой из сторон, используя накопленные о них данные.

Построение и эксплуатация МИУС должны выполняться организациями, аффилированными с государством (либо уже существующими, либо специально созданными федеральными или муниципальными учреждениями). В таком случае сеть обеспечивает действительно массовый охват всех пользователей, включая малообеспеченные их слои. Государственный надзор за ТВ-каналом данных позволяет ему быть безопасным, а власть, которой наделены государственные органы, позволяет им выступать в роли законно признанного гаранта. Так появляется дополнительный уровень защиты социально незащищенных слоев при пользовании услугами внутри доверенной среды МИУС, когда без дополнительных затрат происходит принуждение к выполнению обязанностей в полном объеме или возложение ответственности.

Данная возможность очень ценна, так как является одним из важнейших инструментов обеспечения предсказуемости взаимодействия. В экономических исследованиях [9] показано, что построение упорядоченной иерархии поддерживающих институтов не всегда позволяет выполнить предназначенную им роль институциональной защиты доверия в денежных системах из-за комплекса проблем, в том числе отсутствия гаранта высшей инстанции, а также сложности и неконтролируемости комплексных систем денежного

обращения. В то же время в доверенной среде, построенной на базе МИУС, можно реализовать такие возможности контроля за честностью абонента, как механизм репутации и создание источников информации, помогающих оценить надежность каждого участника. Эти механизмы, по мнению ученых-экономистов, направляют поведение участников и обеспечивают выполнение финансовых либо иных обязательств.

Для построения механизма репутации в МИУС можно использовать два взаимодополняющих способа: создаваемая всеми участниками МУИС субъективная репутация абонентов и провайдеров услуг (выраженная как численный «уровень доверия» либо как набор отзывов) и механизм экспертиз. Первый способ не является специфическим для МИУС – он широко используется на крупнейших площадках интернет-торговли Amazon и Ebay. Заключается он в том, что после каждой совершенной сделки стороны оценивают качество взаимодействия (например, посредством анкетирования): со стороны абонента это оценка качества услуг провайдера, со стороны провайдера – оценка платежеспособности клиента и способности адекватно воспользоваться предоставленной услугой, не предъявляя к провайдеру завышенных требований.

Но второй способ создания репутации – механизм экспертиз – невозможно повсеместно использовать на открытых для всех желающих площадках торговли, в то время как в доверенной среде на базе МИУС он может быть использован для любых случаев. Механизм экспертиз заключается в том, что в случае возникновения конфликтной ситуации между провайдером и абонентом центр МИУС назначает эксперта, который выносит независимое решение о виновнике конфликта. Полученное решение влияет не только на разрешение ситуации, по поводу которой оно было принято, но может сказаться и на дальнейших сделках виновника, поскольку отражается на его репутации. В МИУС механизм экспертиз может быть удобно построен благодаря участию государственных органов – в пользу какой бы из сторон ни было вынесено решение, оно будет признано легитимным.

Кроме механизма репутации, в МИУС также удобно строить базы данных о провайдерах и абонентах. Например, возможна оценка платежеспособности клиента по среднему чеку в интернет-магазине, либо раскрытие информации о доходах провайдера услуги. Раскрытие этой информации не является принудительным, однако может быть осуществлено для обеспечения доверия контрагента.

У МИУС как платформы для реализации доверенной среды есть важное преимущество – репутационная информация может быть моментально одновременно разослана благодаря циркулярно-распределительному характеру доставки информации. При этом, разумеется, не должно нарушаться действующее законодательство, в том числе Федеральный закон «О персональных данных» [10].

3. Доверенная среда в трансграничном пространстве взаимодействия

Как было показано выше, МИУС обладают рядом свойств, которые позволяют строить на их основе доверенные среды, причем доверенные не только в узком смысле, подразумевающем техническую защищенность, а в широком, включающем также предсказуемость и надежность взаимодействий между провайдерами и абонентами. Для этого средствами МИУС могут быть реализованы механизмы репутации, в том числе с задействованием экспертов, а также информационные базы, позволяющие контролировать поведение контрагента и создающие контекст, учитывающийся при взаимодействии.

Также доверенная среда реализуется в трансграничном пространстве взаимодействия – при совершении юридических сделок агентов из разных стран. В то время как безбумажное (построенное на циф-

ровой подписи) взаимодействие успешно реализуется во многих странах и имеет полный юридический вес, взаимодействия между странами (в первую очередь электронная коммерция) зачастую не защищены, так как ни одна из стран не имеет возможностей контроля над компанией из другой страны. Но данная задача успешно решается на пространстве стран – участников СНГ. Их дальнейшая экономическая интеграция требует постановки вопроса об обеспечении трансграничного юридически значимого электронного информационного обмена и предоставления электронных услуг на межгосударственном уровне [11].

Решением возникающих вопросов является реализация трансграничного юридически значимого документооборота на базе МИУС, что позволяет обеспечивать взаимодействие не только разных стран, но и регионов внутри одной страны, расширяя тем самым контекст каждого из них.

Интернет предоставляет уже сегодня технологическую возможность получения жителями государств СНГ на условиях удаленного доступа качественных деловых, медицинских и образовательных услуг, которые локализованы в ряде центров, как правило, в столицах ведущих государств, располагающих достаточным количеством квалифицированных специалистов и передовыми технологиями.

Трансграничное пространство доверия может создаваться на однодоменной или многодоменной основе в зависимости от использования единого криптографического алгоритма электронной подписи или совокупности национальных криптографических алгоритмов электронной подписи в соответствии с внутренним законодательством каждой из входящих в пространство стран [11].

Основная тенденция, сопровождающая процессы перевода документов и услуг в электронный вид, сводится к решению главной задачи – созданию доверенной инфраструктуры, включающей доверенные сервисы, которые могли использоваться в автоматизированных системах, реализующих те или иные бизнес-процессы [12].

Еще одна сфера для реализации повсеместной доверенной среды – обеспечение безопасности людей при чрезвычайной ситуации. В современной сложной для всеобъемлющего восприятия техногенной среде человеку уже бывает непросто ориентироваться, а в случае катастрофы эта задача многократно усложняется, и неверные действия (особенно в первые минуты [13]) ведут к человеческим жертвам.

4. Доверенная среда для обеспечения безопасности человека

Применение современных информационно-коммуникационных технологий (ИКТ) способно повысить безопасность людей во время чрезвычайных ситуаций. ФГУП НИИР была предложена система обеспечения индивидуальной безопасности населения в случае возникновения чрезвычайных ситуаций (СБЧС), работающая непосредственно с индивидуальными пользователями посредством их мобильных телефонов.

Используется приложение для мобильного телефона, которое работает в фоновом режиме, обеспечивая обмен данными с СБЧС, независимо от того, где на объекте находится пользователь. Данный процесс невидим для пользователя, и приложение активируется только в режиме тревоги. СБЧС не только посылает оповещения, но также передает пользователю информацию о самом коротком и безопасном пути из здания с учетом текущего местонахождения пользователя. Пользователь получает как аудио-, так и видеосообщения.

После активации приложения и отправки первоначального оповещения СБЧС непрерывно взаимодействует с пользователем, отслеживая изменения чрезвычайной ситуации и процесс эвакуации из здания, при необходимости от-

правляя пользователю дополнительную информацию.

СБЧС повышает безопасность, побуждая пользователя сосредоточиться на эвакуации. Приложение блокирует все другие функции мобильного телефона, поэтому обычными каналами связи пользоваться невозможно. Кроме того, выключая лишние функции, приложение экономит энергию аккумулятора.

Как мы видим, СБЧС реализует идею доверенной среды для взаимодействия «человек – окружающая среда». С внедрением СБЧС человек получает гарантию предсказуемости своего нахождения в зданиях и объектах, подверженных опасности, сколь большим бы ни было их число. Пользователю не приходится самостоятельно заботиться о каждом посещенном им здании, проверяя систему защиты и проверяя план эвакуации – заранее разработанные схемы активируются в тот момент, когда они нужны, и дают пользователю возможность эвакуации, делая тем самым его взаимодействие с окружающей средой предсказуемым.

Заключение

Как мы видим, создание универсальной доверенной среды, заменяющей привычный для современного общества риск, вызванный количеством взаимодействий и отсутствием их контекста, на предсказуемость результата взаимодействия, является важной задачей. Все направления по созданию доверенных сред растут и активно поддерживаются мировым сообществом [8].

ЛИТЕРАТУРА

1. **Штомпка П.** Доверие – основа общества // М.: Логос. 2012.
2. **Кокотов А.Н.** Доверие. Недоверие. Право // М.: Юристъ. 2004.
3. **URL:** http://www.itsec.ru/newstext.php?news_id=76906
4. **Бек У.** Общество Риска. На пути к другому модерну. М.: Прогресс-Традиция, 2000.
5. **Назаренко А.П., Сарьян В.К., Сущенко Н.А., Хижниченко А.Е., Ткаченко Д.А.** Современные решения в области конвергенции телевидения и сетей передачи данных // Труды НИИР. 2012. № 4.
6. **Issues affecting the evaluation** of the beneficial effect of new technologies and ways to solve these issues, 23rd European Regional Conference of the International Telecommunication Society / International Telecommunications Society. Vienna. Juli, 2012.
7. **Бутенко В.В., Назаренко А.П., Сарьян В.К., Сущенко Н.А.** К вопросу определения социо-экономического полезного эффекта от внедрения новых инфокоммуникационных технологий // Труды НИИР. 2012. № 2. С. 3–10.
8. **Saint Petersburg Declaration** – Building Confidence and Security in the Use of ICT to Promote Economic Growth and Prosperity. 2012. URL: http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2012_tel.aspx
9. **Ляско А.** Роль институтов доверия и контроля в неформальных денежных трансакциях // Вопросы экономики. 2012. № 6.
10. **Федеральный закон** от 27 июля 2006 г. № 152-ФЗ (в ред. от 25 июля 2011 г.) «О персональных данных» // Собрание законодательства Российской Федерации. 31 июля 2006. № 31 (ч. 1). Ст. 3451.
11. **URL:** http://www.rcc.org.ru/index.php?option=com_content&view=article&id=872:2011-12-23-&catid=109:2008-10-03-08-29-33&Itemid=1516
12. **URL:** http://www.rcc.org.ru/userdocs/docs/Sravnitelniy_analiz.pdf
13. **Бутенко В.В., Назаренко А.П., Сарьян В.К., Сущенко Н.А., Лутохин А.С.** Обеспечение личной безопасности в чрезвычайных ситуациях // Новости МСЭ. 2012. № 3.