Литература

1. *Chesbrough H.* Open Business Models: How to Thrive in the New Innovation Landscape. Boston: Harvard Business Scholl Press, 2006.
2. *Etzkowitz H.*, *Leydesdorff L.* The dynamics of innovation: from National Systems and «Mode 2» to a Triple Helix of university-industry-government relations, In: Research Policy, 2006. 29 c.
3. *Smirnov A.*, *Levashova T.*, *Shilov N.* Semantic-oriented support of interoperability between production information systems, In: International Journal of Product Development, Inderscience Enterprises Ltd., 2007. V. 4, № 3/4.
4. *Von Hippel E.* Democratizing Innovation. Boston, MA. MIT Press, 2006.
5. *Кашевник А. М.* Автоматизация взаимодействия участников производственной сети на основе технологии управления компетенциями // Автоматизация в промышленности, 2008. № 3.
6. *Смирнов А. В.*, *Левашова Т. В.*, *Пашкин М. П.*, *Шилов Н. Г.* Онтолого-ориентированный многоагентный подход к построению систем интеграции знаний из распределенных источников // Информационные технологии и вычислительные системы, 2002, № 1.

Обеспечение аутентичности взаимодействия в системах поддержки принятия управленческих решений

Р. В. Воронов, О. В. Гусев, В. В. Поляков

Петрозаводский государственный университет

Постоянно возрастающие требования к качеству управленческих решений в условиях жестких ограничений по времени их подготовки и возрастающая сложность администрируемых процессов привели к тому, что в одиночку, без помощи автоматизированных средств обработки информации современному руководителю не обойтись. Поэтому в различных отраслях деятельности, включая региональное управление, значительное внимание уделяется вопросам развития систем поддержки принятия решений (СППР), способных взять на себя подчас наиболее трудоемкую часть работы — математическое обоснование управленческих решений. Такие системы могут иметь значительное число территориально распределенных пользователей, поэтому их целесообразно создавать в виде Web-ресурсов, доступных в сети Интернет, количество пользователей которых практически не ограничено, а поддержка работоспособности и модификация программного обеспечения не требуют больших затрат [1]. Однако при использовании такой технологии могут возникнуть проблемы, связанные с обеспечением безопасности взаимодействия.

Функционирование Web-ресурса, безусловно, должно быть надежно защищено от несанкционированных воздействий, как физических, так и связанных с возможным вмешательством в процессы информационного обмена, что обеспечивается организационными мерами защиты в совокупности с использованием стандартных технических и программных средств. Однако при этом не исключены проблемы, связанные с незаконными действиями пользователей, что требует обеспечения юридически значимых подтверждений корректности выполняемых действий, исключающих возможность фальсификаций [2].

Рассмотрим интересы участников взаимодействия (пользователя и СППР) со стороны каждого из них. Пользователь заинтересован в качественной информационной услуге той СППР, которой он доверяет, предоставленной на основе сформированных им исходных данных с использованной определенной методики. В свою очередь СППР нуждается в защите от злоупотреблений со стороны пользователя предоставляемыми гарантиями правильности решения. Возможность мошенничества здесь обусловливается тем, что пользователь может иметь интересы, выходящие за рамки использования СППР и имеет потенциальный мотив для махинаций с информацией. Назовем некоторые ситуации, связанные с возможными несанкционированными действиями пользователей.

Ситуация 1. Пользователь отправил СППР исходные данные для решения задачи, но сделал это не в установленное время (например, позже крайнего момента принятия решения, что впоследствии повлекло выход параметров объекта управления за пределы допустимых значений и нарушило его нормальное функционирование). Однако позже пользователь может утверждать, что выполнил поиск решения и использовал его своевременно.

Ситуация 2. Пользователь отправил СППР исходные данные для решения задачи и получил ответ, но впоследствии отказался от факта его получения, сославшись на неработоспособность или недоступность СППР.

Ситуация 3. Отправив СППР некорректные исходные данные, получив решение и реализовав его с неудовлетворительным результатом, пользователь утверждает, что оно было рассчитано на основе иных исходных данных.

Ситуация 4. Получив решение, пользователь не следует полученным рекомендациям, но в случае неудовлетворительного результата подменяет решение и утверждает впоследствии, что именно такое решение было получено от СППР в ответ на предоставленные им исходные данные.

Ситуация 5. Пользователь отправляет СППР несколько различных наборов исходных данных для решения задачи и, получив ответы для каждого набора, может реализовать один из них, сославшись впоследствии на другой.

Для исключения описанных ситуаций СППР должна сохранять (по крайней мере, в течение определенного времени) поступающие запросы в виде, позволяющем установить их авторство, время поступления и исключающем возможность фальсификации запросов на стороне СППР. Пользователь, в свою очередь, также должен получать решения в форме, позволяющей установить их принадлежность СППР и исключающей возможность фальсификации с его стороны. Более того, желательно, чтобы на основе сведений, переданных СППР пользователю, было возможным

разрешение если не всех, то большинства из названных выше проблем. Обеспечить все это позволит только выбор такого способа взаимодействия пользователей с СППР — протокола взаимодействия, который обеспечит аутентичность взаимодействующих сторон, а также подтверждение целостности и авторства передаваемых сообщений.

Заметим, что большинство протоколов строится на принуждении последовательного совершения исполнителями зависимых действий для достижения конечного результата. По отношению к СППР, функционирующей по формальному алгоритму, это не составляет проблемы. Однако у пользователя отсутствуют явные стимулы для подтверждения получения ответа, так как в момент, когда пользователь должен направить подтверждение получения ответа, информационная услуга уже предоставлена. Поэтому здесь требуется использование иных рычагов воздействия, например, путем введения ограничений на использование СППР в дальнейшем — тогда нежелание пользователя предоставить подтверждение получения ответа приведет в дальнейшем к отказу в обслуживании его запросов.

Предлагаемый протокол предполагает использование методов асимметричной криптографии и технологии цифровых сертификатов [3, 4], в соответствии с которой для каждого пользователя создается пара ключей — открытый $K_{П}^{O}$ и тайный $K_{П}^{T}$, первый из которых регистрируется на имя пользователя одним из центров сертификации. В результате пользователь приобретает цифровой сертификат, включающий ключ $K_{П}^{O}$, сведения о владельце сертификата и все эти сведения, зашифрованные на тайном ключе центра сертификации. При направлении такого сертификата СППР, последняя, используя открытый ключ центра сертификации, получает возможность убедиться, что полученное сообщение действительно послано владельцем сертификата.

У СППР также имеется пара ключей $K_{С}^{O}$ и $K_{С}^{T}$, и она также получает цифровой сертификат.

Открытые ключи $K_{П}^{O}$ и $K_{С}^{O}$ доступны всем, тайные хранятся, соответственно, у владельцев и никому кроме них не известны.

Протокол, который должен реализовываться при каждом обращении к СППР, состоит из следующих шагов.

Шаг 1. Пользователь формирует запрос к СППР, включающий исходные данные и идентификатор запроса (например, порядковый номер), к которым добавлена временная метка. Запрос подписывается на ключе пользователя $K_{П}^{T}$ и вместе с его сертификатом отправляется СППР.

Шаг 2. СППР, получив запрос, фиксирует время получения, проверяет достоверность сертификата, с помощью открытого ключа $K_{П}^{O}$, извлекаемого из сертификата, проверяет подлинность цифровой подпи-

си, удостоверяясь одновременно в целостности и авторстве сообщения. В случае недостоверности сертификата, недопустимых значений даты и времени или нарушения формата запроса, его обработка прекращается с уведомлением легального пользователя.

Шаг 3. СППР сохраняет запрос в базе данных, выполняет решение задачи, на основе которого формируется сообщение-ответ, включающее результаты решения, время поступления запроса к СППР и сам запрос, включая цифровую подпись.

Шаг 4. Сообщение-ответ подписывается на ключе СППР K_C^T и отправляется пользователю вместе с сертификатом СППР и требованием подтвердить получение сообщения-ответа. Одновременно устанавливается запрет на работу пользователя до поступления подтверждения о получении им сообщения-ответа.

Шаг 5. Пользователь, получив сообщение-ответ, проверяет достоверность сертификата СППР, с помощью открытого ключа K_C^O проверяет подлинность цифровой подписи, одновременно проверяя целостность сообщения-ответа и авторство СППР.

Шаг 6. Пользователь посылает подписанное на ключе $K_П^T$ подтверждение получения сообщения-ответа, включающее сообщение-ответ и, возможно, свое решение о его использовании (принято к реализации, отклонено, отложено и др.).

Шаг 7. СППР фиксирует факт поступления подтверждения (и, если требуется, разрешает дальнейшую работу данного пользователя).

Применение описанного протокола позволяет решить следующие проблемы.

1. Наличие в запросе цифрового сертификата пользователя позволяет СППР удостовериться в том, что запрос направлен от имени легального пользователя.
2. Подписание пользователем запроса на ключе $K_П^T$ позволяет СППР удостовериться в его целостности и в том, что он прислан именно тем легальным пользователем, чей сертификат предъявлен, и, кроме того, не позволяет пользователю отказаться от факта направления запроса, а СППР не дает возможности изменить содержание запроса.
3. После отправки сообщения-ответа СППР не может отказаться от факта получения запроса и результатов решения, так как никто кроме СППР не владеет ключом K_C^T и не может сформировать цифровую подпись сообщения-ответа.
4. Пользователь не может фальсифицировать сообщение-ответ, поскольку не владеет ключом K_C^T.

5. Если пользователь заявит, что решение задачи велось несоответствующим образом, то, используя сообщение-ответ, поступивший к пользователю, возможно повторное выполнение решения с теми же исходными данными, позволяющее подтвердить (или опровергнуть), что расчет проводился на основе установленной методики.
6. Если пользователь не пошлет СППР необходимое подтверждение о получении сообщения-ответа, то в дальнейшем ему будет отказано в использовании СППР.

Предлагаемый способ взаимодействия поначалу представляется непривычным и тяжеловесным. Однако, в отличие от многих «одноразовых» решений, требующих для своей работы создания параллельных систем защиты, протокол позволяет использовать уже существующую инфраструктуру открытых ключей с сертифицирующим центром, что позволит внести минимальные коррективы в устоявшиеся процедуры взаимодействия и создаст минимальные неудобства для пользователя. В качестве выигрыша пользователь получает юридически значимые гарантии правильности предоставленных ему данных и отсутствие возможности различных злоупотреблений, что позволит повысить степень доверия к подобным системам и применять их при подготовке решений любого уровня ответственности и масштаба.

Литература

1. *Поляков В. В.* Интерактивная система моделирования на основе Web-сервиса / В. В. Поляков, Ю. А. Сидорова // Материалы научно-метод. конф. «Университеты в образовательном пространстве региона: опыт, традиции, инновации». Петрозаводск, 2007. Петрозаводск: Изд-во ПетрГУ, 2007. С. 107–109.
2. *Поляков В. В.* Об одном аспекте взаимодействия с корпоративными сетевыми сервисами, предназначенными для поддержки принятия решений // Труды ПетрГУ. Сер. «Прикладная математика и информатика». Вып. 12. Петрозаводск: Изд-во ПетрГУ, 2007. С. 19–25.
3. *Романец Ю. В.*, *Тимофеев П. А.*, *Шаньгин В. Ф.*. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. 2-е изд., перераб. и доп. М.: Радио и связь, 2001. 376 с.
4. *Горбатов В. С.* Основы технологии PKI. М.: Горячая линия — Телеком, 2004. 248 с.