М. В. Ванин, И. А. Трифаленков, В. И. Королев

ЕДИНАЯ СИСТЕМА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ КАК НАЦИОНАЛЬНЫЙ СЕРВИС ИНФРАСТРУКТУРЫ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

Создание электронного правительства — ключевое направление государственной политики в сфере информатизации и информационно-коммуникационных технологий (ИКТ). Одной из фундаментальных задач при создании электронного правительства является задача обеспечения возможности взаимодействия граждан и бизнеса с государственными органами власти всех уровней, взаимодействия между государственными органами и учреждениями путем широкого использования ИКТ. Информационное взаимодействие требует построения системы отношений доступа, обеспечивающей гарантированную авторизацию взаимодействующих субъектов и объектов и подтверждение взаимно однозначного адреса устанавливаемого взаимодействия. Это осуществляется с помощью реализации функций идентификации и аутентификации. С одной стороны, это функции назначения систем обеспечения информационной безопасности (СОИБ), реализующие санкционированный доступ к ресурсам. С другой стороны, в рамках электронного правительства это инфраструктурные функции гарантии образования связных процессов (транзакционных инициатив) взаимодействия субъектов, ресурсов (сервисов) и автоматизированных систем, участвующих в реализации государственных или муниципальных заданий (заказов) и исполнении государственных и муниципальных функций (информационно-технологическое взаимодействие). При этом санкционированный доступ должен предоставляться с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие.

Для решения задачи идентификации и аутентификации в составе инфраструктуры электронного правительства выделена специальная система – ФГИС «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (далее – ЕСИА).

К основным функциям ЕСИА относятся:

1) обеспечение ведения регистров участников информационного взаимодействия, таких как регистры физических и юридических лиц, регистр государственных организаций, регистры должностных лиц и их полномочий, регистр информационных систем;

2) обеспечение идентификации и аутентификации участников информационного взаимодействия при их доступе к ресурсам информационных систем;

3) предоставление информационным системам идентификационных данных (в том числе сведений о полномочиях — в рамках авторизации) участников информационного взаимодействия [1].

Отметим некоторые существенные особенности, связанные с реализацией этих функций.

Идентификационные данные, используемые при реализации функций идентификации, аутентификации и авторизации, являются персональной информацией, накопление, хранение и использование которой должно осуществляться в соответствии с законодательными нормами. Следовательно, системные и технические решения относительно этого специфичного информационного ресурса должны быть сбалансированными и эффективными с позиций правовых норм [2] и операционных характеристик [3].

Масштабируемость системы и интероперабельность процессорных решений по ЕСИА распространяются как по горизонтали взаимодействия (федеральный, региональный или муниципальный уровни), так и по вертикали (межуровневое взаимодействие). Эту особенность необходимо иметь в виду, несмотря на тот факт, что в настоящее время использование ЕСИА на федеральном уровне имеет обязательный характер, а на региональном и муниципальном — рекомендательный [1]. Тем не менее идентификационные данные в механизмах реализации в любом случае должны быть совместимыми.

Исходя из рассмотренных предпосылок формировались подходы к выбору решений при разработке ЕСИА.

При реализации функции *обеспечения ведения регистров* рассматривалось два возможных подхода:

1) использовать уже существующие государственные регистры и выполнять к ним запросы из ЕСИА — практически неприменимый подход, так как существующие регистры органов власти в настоящий момент не обладают полнотой информации, необходимой для обеспечения идентификации субъекта, зачастую содержат противоречивую информацию о субъекте и не всегда предоставляют уникальные идентификаторы записей регистра для возможности их однозначного сопоставления друг с другом при получении информации из различных регистров;

2) создать в составе ЕСИА свои регистры физических лиц, организаций, должностных лиц организаций, информационных систем. Связать эти регистры ЕСИА с наиболее значимыми существующими государственными регистрами, такими как регистры ФНС (реестры ЕГРЮЛ, ЕГРИП, реестр индивидуальных номеров налогоплательщиков), регистры Пенсионного фонда РФ (реестр страховых номеров индивидуальных лицевых счетов граждан РФ — СНИЛС), регистры ФМС (реестр паспортов граждан РФ).

Был выбран второй подход. Ввод и актуализация информации обеспечиваются субъектами, владеющими наиболее актуальной информацией и мотивированными в поддержании информации о себе в актуальном виде, а именно участниками информационного взаимодействия.

Заинтересованные в использовании сервисов электронного правительства лица регистрируют в регистрах ЕСИА свои учетные записи, учетные записи организаций и их информационных систем. В процессе регистрации вводимые данные подвергаются проверке по существующим государственным регистрам (для исключения возможности создания в ЕСИА записей о не существующих в реальности субъектах, а также для подтверждения правомочности действий субъектов, которые определены при регистрации ими организаций и информационных систем).

При регистрации в ЕСИА физических лиц (прежде всего, граждан РФ) используется процедура подтверждения учетной записи, в процессе которой осуществляющее регистрацию лицо подвергается проверке на то, что именно оно является законным владельцем своей учетной записи. В настоящий момент предусмотрено два способа подтверждения учетной записи:

1) получение кода активации учетной записи лично в руки в центре регистрации (отделения Почты России, центры регистрации ОАО «Ростелеком», иные уполномоченные организации);

2) подтверждение учетной записи с помощью квалифицированной электронной подписи, установленной с использованием средства электронной подписи, содержащего квалифицированный сертификат ключа проверки подписи, выпущенный аккредитованным удостоверяющим центром.

При регистрации организаций и информационных систем выполняется проверка факта, что записи об этих сущностях регистрируются в ЕСИА субъектами, имеющими подтвержденные полномочия. Первичные полномочия субъектов на действия от имени организации подтверждаются благодаря проверке прав субъектов через ЕГРЮЛ. Далее ЕСИА предоставляет механизмы присоединения должностных лиц организаций и делегирования им полномочий на действия от имени организаций и принадлежащих организации информационных систем.

При реализации функции обеспечения идентификации и аутентификации участников информационного взаимодействия в ЕСИА в качестве основы решения по взаимодействию информационных систем и ЕСИА были выбраны распространенные в мире стандарты и технологии взаимодействия, широко поддержанные производителями прикладного программного обеспечения и программного обеспечения промежуточного уровня. Данные стандарты и технологии относятся к области, называемой федеративным управлением идентификационными данными (в зарубежных материалах используется термин Federated Identity Management). Следование этим стандартам и технологиям позволило обеспечить высокую интероперабельность ЕСИА. В свою очередь, стандартизация взаимодействия информационных систем с ЕСИА была достигнута через публикацию Минкомсвязи России документа «Методические рекомендации по использованию ЕСИА» [4]. В соответствии с этим документом в основе взаимодействия систем и ЕСИА лежат стандарт SAML 2.0 и ряд его базовых профилей и рекомендаций. Применение SAML 2.0 позволяет обеспечить интеграцию многих информационных систем через их настройку или с помощью ограниченных по сложности доработок, в основу которых положено использование готовых программных компонентов с открытым исходным кодом, доступных для широкого перечня программных платформ и обеспечивающих реализацию взаимодействия через SAML 2.0.

ЕСИА обеспечивает расширение поддерживаемого ею перечня механизмов аутентификации. В настоящий момент ЕСИА поддерживает возможность аутентификации пользователей с использованием следующих методов:

1) аутентификация с использованием логина/пароля;

2) аутентификация с использованием отправляемых по SMS кодов подтверждения (разновидность one-time password аутентификации);

3) аутентификация с использованием квалифицированной электронной подписи.

Возвращаемый от ЕСИА в информационную систему набор идентификационных данных определяется зарегистрированными в ЕСИА настройками информационной системы. Каждой системе доступно только определенное для нее разрешенное подмножество атрибутов. В настоящий момент ЕСИА обеспечивает ведение более двух десятков атрибутов идентификационных данных пользователя. Набор ведущихся в регистрах ЕСИА атрибутов со временем расширяется.

Уже сейчас ЕСИА обеспечивает идентификацию и аутентификацию пользователей при доступе ко всем системам инфраструктуры электронного правительства, к Единому порталу государственных и муниципальных услуг (функций), большинству региональных порталов государственных услуг, к информационным системам национальной облачной платформы (www.o7.com) и к ряду специализированных порталов органов власти. Фактически ЕСИА уже является национальным сервисом инфраструктуры электронного правительства.

ЕСИА — важный компонент обеспечения информационной безопасности систем электронного правительства. Одновременно, учитывая характер решаемых задач и ответственность по защите информации в сформированных в ЕСИА регистрах, безусловным приоритетом выступает обеспечение информационной безопасности самой ЕСИА.

Применение ЕСИА в информационных системах в качестве ключевого элемента систем контроля доступа требует переосмысления устоявшихся и отраженных в нормативных документах РФ по информационной безопасности подходов к защите информации, и это в настоящий момент является открытой задачей, требующей решения.

ЕСИА можно рассматривать как пример облачного сервиса с присущими облачным вычислениям особенностями в части обеспечения информационной безопасности, такими как:

1) потеря владельцем информационной системы, использующей ЕСИА, абсолютного контроля над обеспечением информационной безопасности, так как одна из ключевых задач информационной безопасности — идентификация и аутентификация пользователя — теперь обеспечивается внешней системой (ЕСИА), находящейся в ведении оператора ЕСИА (Минкомсвязь России);

2) совместное использование сервиса идентификации пользователей ЕСИА множеством информационных систем;

3) размытие периметра безопасности информационной системы — теперь необходимо предоставить доступ пользователям информационной системы также и к ЕСИА для прохождения ими идентификации и аутентификации. Соответственно, нет возможности с помощью изоляции вычислительной сети или межсетевого экранирования полностью отсечь информационную систему от внешних нарушителей. Необходим будет, как минимум, доступ к сервисам идентификации и аутентификации ЕСИА.

Внедрение и дальнейшее развитие ЕСИА как национального инфраструктурного сервиса выгодно гражданам, операторам информационных систем и государству. Единая система идентификации и аутентификации позволяет:

1) *гражданам* использовать единые механизмы доступа к широкому перечню электронных сервисов и услуг, а также потенциально позволяет им контролировать распространение их персональных данных;

2) *операторам информационных систем* сосредоточиться на развитии основных функций их систем и использовать готовые механизмы обеспечения доступа пользователей на основе широкой базы зарегистрированных пользователей ЕСИА. Если владельцы информационных систем используют данные о пользователях только в целях обеспечения их доступа, то для владельцев также упрощается задача обеспечения защиты информационных систем персональных данных (ИСПДн), так как фактически хранение и обработка персональных данных теперь выполняются в системе ЕСИА и оператору системы остается обеспечить безопасность данных только при передаче и обработке;

3) *государству* оптимизировать затраты на создание информационных систем через повторное использование в каждой из них уже разработанных в ЕСИА механизмов обеспечения доступа пользователей, а также открывает новые возможности к обеспечению межведомственного взаимодействия.

СПИСОК ЛИТЕРАТУРЫ:

1. Требования к федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме». Постановление Правительства РФ от 28 ноября 2011 г. № 977.

2. Закон РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Положение о федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме». Приказ Министерства связи и массовых коммуникаций Российской Федерации от 13 апреля 2012 г. № 107.

4. Методические рекомендации по использованию Единой системы идентификации и аутентификации. URL: http//minsvyaz.ru/Metodicheskie_rekomendatsii_ESIA.pdf (дата обращения: 02.04.2013).