ПРОЕКТ

Единая система идентификации и аутентификации (ЕСИА)

Схемы использования ЕСИА в органах исполнительной власти

Содержание

1 ОБЩИЕ СВЕДЕНИЯ О ЕСИА

1.1 Цели создания ЕСИА

а) Обеспечить идентификацию / аутентификацию пользователей при доступе к ресурсам ИЭП.

б) Обеспечить централизованное управление идентификационными данными пользователей и их полномочиями по доступу к ресурсам ИЭП.

1.2 Основные функциональные возможности ЕСИА

Однократная аутентификация пользователей (Single Sign On)

ЕСИА обеспечивает однократную аутентификацию пользователей. Пользователям это даёт следующее преимущество: пройдя процедуру идентификации / аутентификации в ЕСИА, пользователь может в течение одного сеанса работы обращаться к любым ИС, которые подключены к ЕСИА, и при этом не потребуется повторная идентификация / аутентификация.

В общих чертах однократная аутентификация реализована следующим образом: когда пользователь обращается к защищённому ресурсу ИС, ИС направляет в ЕСИА запрос на аутентификацию пользователя. ЕСИА проверяет наличие открытой сессии у пользователя и, если активная сессия отсутствует, проводит аутентификацию пользователя. Затем ЕСИА передаёт в ИС набор утверждений, содержащих идентификационные данные пользователя, информацию о контексте аутентификации и полномочиях пользователя. На основании полученной из ЕСИА информации, ИС принимает решение об авторизации - разрешает или запрещает доступ к ресурсу.

Единый выход пользователей (Single Logout)

ЕСИА поддерживает возможность единого выхода пользователей. Пользователям это даёт следующее преимущество: после завершения сеанса

работы с одной из ИС, подключенной к ЕСИА, происходит завершение сеансов работы со всеми ИС.

Управление идентификационными данными (Identity Management)

ЕСИА обеспечивает регистрацию и управление идентификационными данными пользователей, организаций, информационных систем. ЕСИА предоставляет пользователям возможность самостоятельного изменения своих идентификационных данных в личном кабинете. ЕСИА обеспечивает верификацию (проверку достоверности) идентификационных данных пользователей и организаций с использованием сервисов ОИВ. В настоящее время ЕСИА использует веб-сервис ПФР для проверки соответствия СНИЛС и ФИО, веб-сервис ФНС — для проверки соответствия ИНН и ФИО, ОГРН/ОГРНИП и ФИО, веб-сервисы ФМС для проверки сведений о паспортах граждан РФ и документов, предъявленных при пересечении границы РФ (только для иностранных граждан и лицах без гражданства).

Поддержка различных методов аутентификации

В настоящее время ЕСИА может выполнять аутентификацию пользователей по постоянному паролю и по электронной подписи.

Поддержка различных уровней достоверности идентификации

Уровень достоверности идентификации (англ. «identity assurance level») – степень уверенности в том, что идентифицированный субъект является тем, за кого себя выдаёт. Повышение уровня достоверности идентификации достигается путём *верификации* идентификационных данных и применения более строгих методов *аутентификации*.

В настоящий момент в ЕСИА предлагается использовать 4 уровня достоверности идентификации:

а) Уровень 1 — предназначен для пользователей, личность которых не подтверждена.

б) Уровень 2 — соответствует пользователям, которые подтвердили свою личность с помощью метода, не дающего высокой гарантии достоверности (через отправку регистрируемого почтового

отправления Почтой России), либо соответствует пользователям, которые подтвердили свою личность с помощью метода, обеспечивающего высокую достоверность (личная явка в офис регистрации и предъявление удостоверения личности) и использующие при идентификации и аутентификации менее надежные средства идентификации (например, логин и пароль).

в) Уровень 3 — соответствует пользователям, которые подтвердили свою личность с помощью метода, обеспечивающего высокую достоверность (личная явка в офис регистрации и предъявление удостоверения личности), и использующие при идентификации и аутентификации более надежные средства идентификации (например, электронную подпись).

г) Уровень 4 — соответствует пользователям, к которым предъявляются самые строгие требования по регистрации и идентификации и аутентификации. Например, пользователям с ролью ДЛ ОИВ, регистрация которых выполняется непосредственно в ОИВ.

На рисунке ниже показаны основные требования к уровням достоверности идентификации в ЕСИА.

Рисунок 1 – Требования к уровням достоверности идентификации

1.3 Функциональные возможности ЕСИА для ОИВ

Основные функциональные возможности, предоставляемые ЕСИА для ОИВ:

а) Регистрация ДЛ ОИВ и ИС ОИВ.

б) Управление полномочиями ДЛ ОИВ.

в) Идентификация и аутентификация ДЛ ОИВ и пользователей Интернет при доступе к ресурсам ИС ОИВ.

г) Управление полномочиями ИС ОИВ по доступу к сервисам СМЭВ.

д) Авторизация ИС ОИВ при межведомственном взаимодействии через СМЭВ.

1.3.1 Особенности регистрации в ЕСИА должностных лиц ОИВ

Регистрация ДЛ ОИВ в ЕСИА имеет следующие особенности:

а) В ЕСИА должна быть исключена самостоятельная регистрация пользователей с ролью ДЛ ОИВ - зарегистрировать ДЛ ОИВ может только уполномоченное лицо ОИВ. Таким лицом может быть сотрудник кадрового подразделения или другой человек

(оператор регистрации).

б) Основным идентификатором ДЛ ОИВ является СНИЛС. СНИЛС не изменяется при изменении других идентификационных данных пользователя. Поэтому, например, при смене фамилии учетную запись регистрировать заново не нужно. ДЛ ОИВ должен иметь возможность изменить свои идентификационные данные в личном кабинете ЕСИА и создать запрос на верификацию изменённых данных.

в) Один человек может работать в нескольких ОИВ, поэтому его учетная запись в ЕСИА может быть связана с несколькими ОИВ.

г) Пользователь с ролью ДЛ ОИВ (в отличие от «обычных» пользователей ЕСИА) не должен иметь возможность удалить свою учетную запись из ЕСИА.

д) При увольнении работник ОИВ должен быть лишен в ЕСИА всех полномочий, связанных с ролью ДЛ ОИВ, но его учетная запись ЕСИА не должна удаляться. После увольнения из ОИВ он может продолжать использовать свою учетную запись, например, для получения государственных услуг в электронном виде. По желанию пользователь может инициировать удаление своей учетной записи из ЕСИА, но только если в этот момент он не обладает ролью ДЛ ОИВ.

1.3.2 Роли пользователей в ЕСИА для ОИВ

Должностное лицо ОИВ

Представитель (должностное лицо) ОИВ – это пользователь, учетная запись которого ассоциирована с учетной записью организации, являющейся органом исполнительной власти (ОИВ). Про таких пользователей можно сказать, что они играют *роль* представителей ОИВ в ЕСИА. ОИВ бывают федеральными и региональными. Как и любые организации, ОИВ могут иметь подразделения.

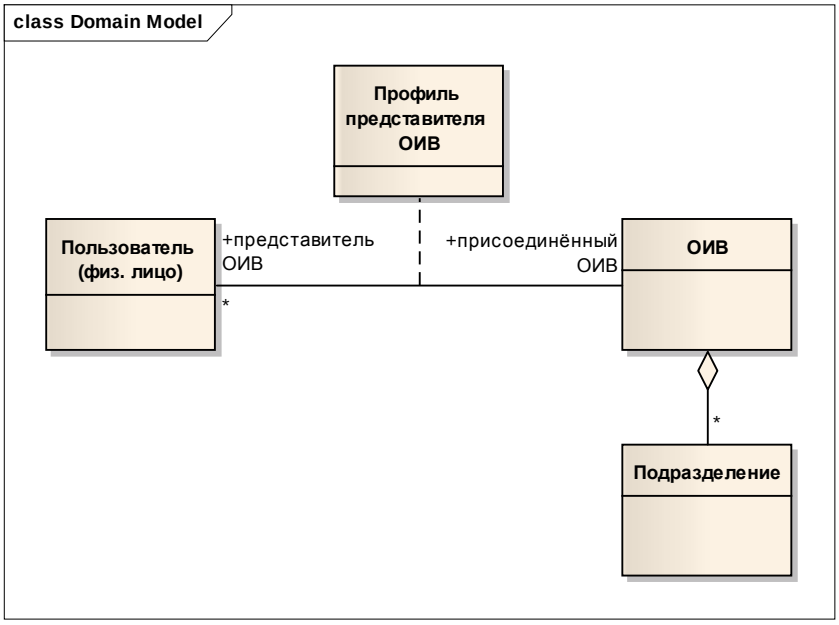

Рисунок 2 – Модель представителя ОИВ в ЕСИА

Представители ОИВ могут иметь полномочия в ИС ОИВ, доверяющих ЕСИА выполнение идентификации и аутентификации пользователей. Поэтому к представителям ОИВ должны предъявляться повышенные требования по подтверждению достоверности идентификационных данных. Регистрацию представителей ОИВ в ЕСИА осуществляют *операторы регистрации*, которые ответственны за проверку предоставленных пользователем данных.

Оператор регистрации ОИВ

Оператор регистрации – это пользователь, который обладает полномочиями по регистрации представителей ОИВ в ЕСИА. Оператор регистрации должен установить личность пользователя и внести данные о пользователе в систему. Оператор регистрации имеет полномочия, позволяющие выполнять следующие функции и операции:

а) управление пользователями ЕСИА:
   1) создание новых пользователей;
   2) назначение и изменение атрибутов пользователя;

б) управление членством пользователей в своей организации/подразделении и нижестоящих по иерархии:
   1) присоединение любых пользователей организации

(предоставление роли представителя ОИВ);

2) назначение и изменение атрибутов профиля пользователя в организации;
3) отсоединение пользователей от организации (отзыв роли представителя ОИВ);

При выполнении операций с учетными записями оператор регистрации заверяет свои действия своей ЭП.

Предоставление полномочий оператора регистрации осуществляет *оператор полномочий*.

При разработке интерфейса взаимодействия операторов регистрации с ЕСИА должны быть учтены следующие ограничения:

а) Операторы регистрации не должны иметь возможность просмотра личной карточки произвольного пользователя ЕСИА.
б) Операторы могут иметь возможность выборки, просмотра и редактирования личных карточек пользователей только в пределах своей организации / подразделения и нижестоящих по иерархии.

Оператор полномочий ОИВ

Оператор полномочий – это пользователь, который может выдавать полномочия по доступу к определённым ресурсам пользователям, входящим в определённую организацию. Для получения полномочий, пользователь должен предоставить оператору полномочий обоснования в соответствии с действующим регламентом.

Оператор полномочий может выполнять следующие операции:

а) предоставление и отзыв полномочий пользователей в своей организации и нижележащих по иерархии.

Оператор полномочий не должен иметь возможность предоставления полномочий самому себе. Предоставление полномочий оператора полномочий осуществляет оператор полномочий вышестоящего ОИВ.

Оператор полномочий при выполнении операций назначения и отзыва полномочий заверяет эти операции своей ЭП.

Для решения задач управления идентификационными данными и полномочиями представителей ОИВ в ЕСИА будет создана иерархическая структура операторов регистрации и операторов полномочий (Рисунок 3). Операторы Минкомсвязи России назначаются в процессе начального конфигурирования ЕСИА. Операторы Минкомсвязи России назначают операторов федеральных и региональных ОИВ самого верхнего уровня (в иерархии ОИВ РФ). Операторы федеральных ОИВ назначают операторов каждого ФОИВ. А они в свою очередь назначают операторов подведомственных им ОИВ. Операторы региональных ОИВ назначают операторов ОИВ в каждом регионе РФ.

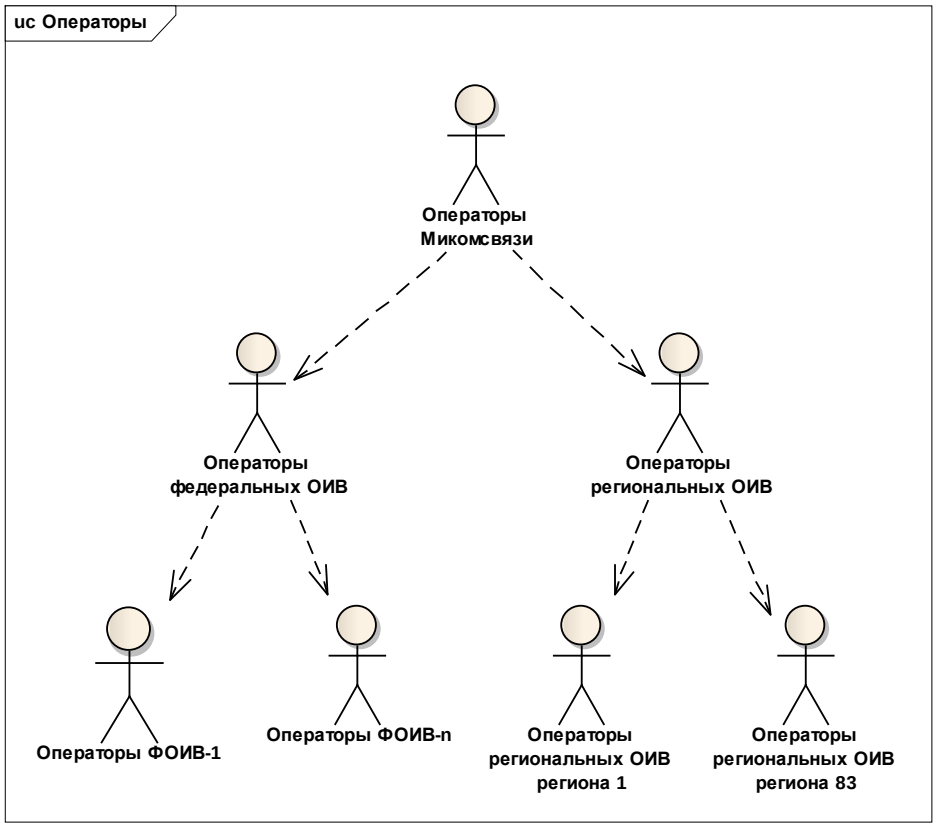

Рисунок 3 – Иерархия операторов

Схема назначения любого нового оператора ОИВ:

а) Оператор регистрации ОИВ регистрирует пользователя с ролью представителя своего или нижестоящего ОИВ;

б) Оператор полномочий ОИВ предоставляет новому пользователю с ролью представителя ОИВ полномочия оператора регистрации или оператора полномочий в своём или нижестоящем ОИВ.

2 СХЕМЫ ИСПОЛЬЗОВАНИЯ ЕСИА ПРИ ДОСТУПЕ ПРЕДСТАВИТЕЛЕЙ ОИВ

ЕСИА участвует в управлении доступом должностных лиц ОИВ к ресурсам информационных систем ОИВ следующим образом:

а) ЕСИА обеспечивает идентификацию и однократную аутентификацию должностных лиц ОИВ и предоставляет информационным системам ОИВ информацию об идентификационных данных и полномочиях должностных лиц ОИВ (п. 2.3);

б) ЕСИА обеспечивает управление идентификационными данными и полномочиями должностных лиц ОИВ на протяжении их жизненного цикла (создание, изменение, удаление данных).

ЕСИА не выполняет авторизацию доступа к информационным системам ОИВ. Решение об авторизации принимает информационная система ОИВ на основании полученной из ЕСИА информации о пользователе, запрашивающем доступ.

Для того чтобы ЕСИА могла обеспечить однократную аутентификацию представителей ОИВ, необходимо следующее:

а) должностные лица ОИВ должны быть зарегистрированы в ЕСИА (п. 2.1);

б) ИС ОИВ должны быть зарегистрированы в ЕСИА и доработаны для взаимодействия с ЕСИА (п. 2.4).

Для того чтобы ЕСИА могла предоставлять информационным системам ОИВ информацию о полномочиях должностных лиц ОИВ:

а) владелец (оператор) ИС ОИВ должен вести в ЕСИА справочник полномочий в привязке к своей ИС (п. 2.5);

б) полномочия должны быть предоставлены должностным лицам ОИВ (п. 2.2).

2.1 Регистрация представителей ОИВ в ЕСИА

Далее рассмотрены следующие варианты регистрации представителей ОИВ в ЕСИА:

а) через графический интерфейс ЕСИА;

б) через веб-сервисы СМЭВ;

в) через систему IdM и веб-сервисы СМЭВ.

2.1.1 Регистрация представителей ОИВ через графический интерфейс ЕСИА

Краткое описание варианта использования: Оператор регистрации[1] вводит данные нового работника в ЕСИА, чтобы создать для него учетную запись с ролью представителя ОИВ[2]. ЕСИА проверяет достоверность идентификационных данных регистрируемого пользователя, вызывая веб-сервисы соответствующих ведомств[3], зарегистрированные в СМЭВ. Если проверки пройдены успешно, ЕСИА создаёт для нового работника ОИВ учетную запись с ролью представителя ОИВ (или изменяет данные пользователя, если он уже был зарегистрирован).

Атрибуты представителя ОИВ:

а) личные данные:

1) СНИЛС – обязательный атрибут; основной идентификатор; выполняется автоматическая верификация в ПФР на соответствие СНИЛС и ФИО;
2) Фамилия – обязательный атрибут;
3) Имя – обязательный атрибут;
4) Отчество – обязательный атрибут (если есть в паспорте);
5) ИНН – необязательный атрибут; если атрибут заполнен, то

[1] Оператором регистрации может быть, например, сотрудник кадрового подразделения ОИВ

[2] Оператор регистрации ответственен за проверку документов регистрируемого пользователя и проверку достоверности вводимой информации.

[3] В настоящее время СИА использует веб-сервис ПФР для проверки соответствия СНИЛС и ФИО; веб-сервис ФНС для проверки соответствия ИНН и ФИО; веб-сервис ФМС для проверки паспортных данных (только для иностранных граждан).

выполняется автоматическая верификация в ФНС на соответствие ИНН и ФИО;

6) удостоверение личности (серия, номер, дата выдачи, кем выдано) – обязательный атрибут[4];

б) информация, характеризующая связь с ОИВ:

1) Идентификатор ОИВ – обязательный атрибут;
2) Подразделение – необязательный атрибут;
3) Должность – необязательный атрибут;
4) Комментарий – необязательный атрибут.

[4] В перспективе возможно внедрение автоматической верификации паспортных данных граждан РФ с использованием веб-сервиса ФМС

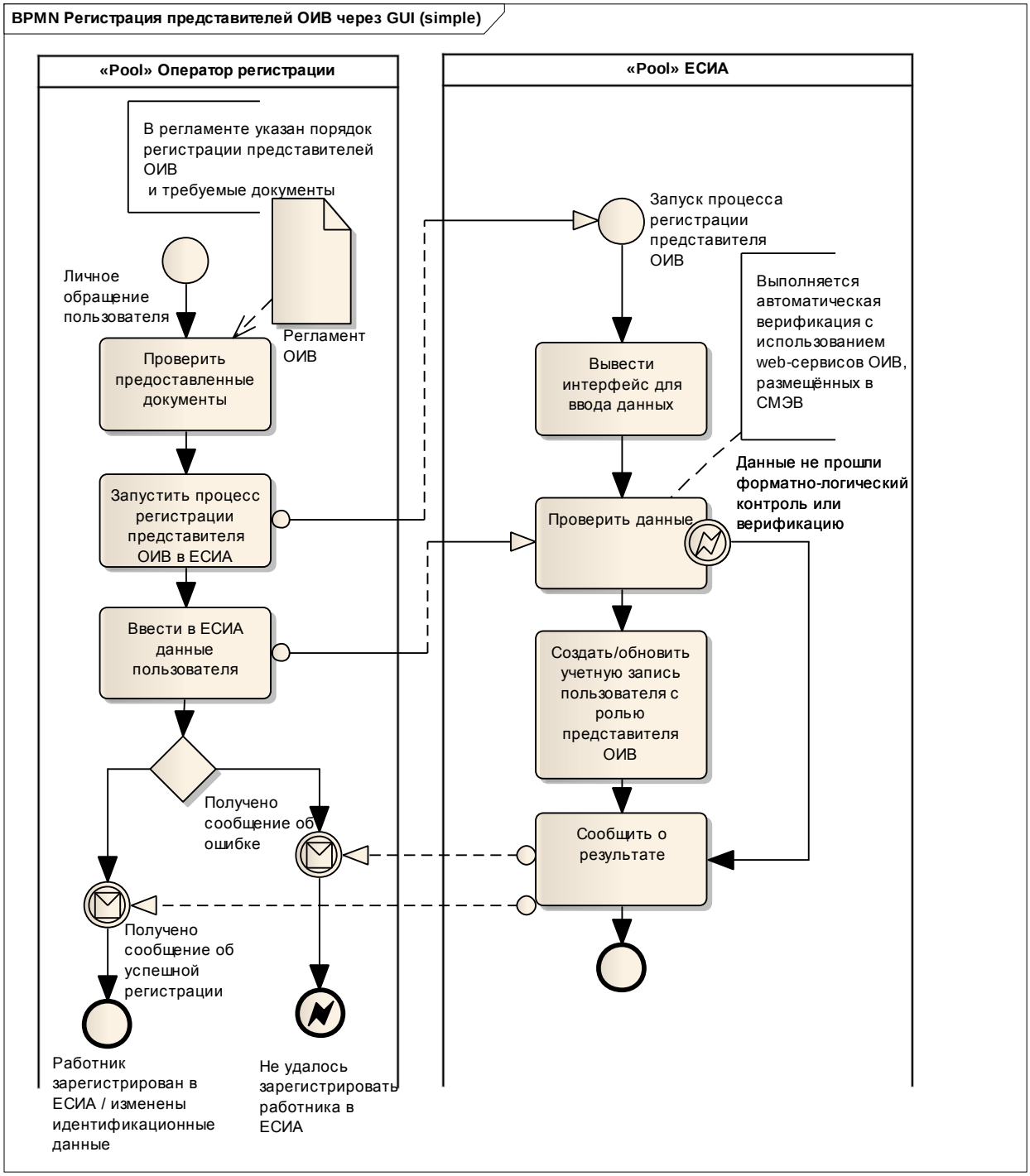

Рисунок 4 – Регистрация / изменение идентификационных данных представителей ОИВ через графический интерфейс ЕСИА (диаграмма процесса)

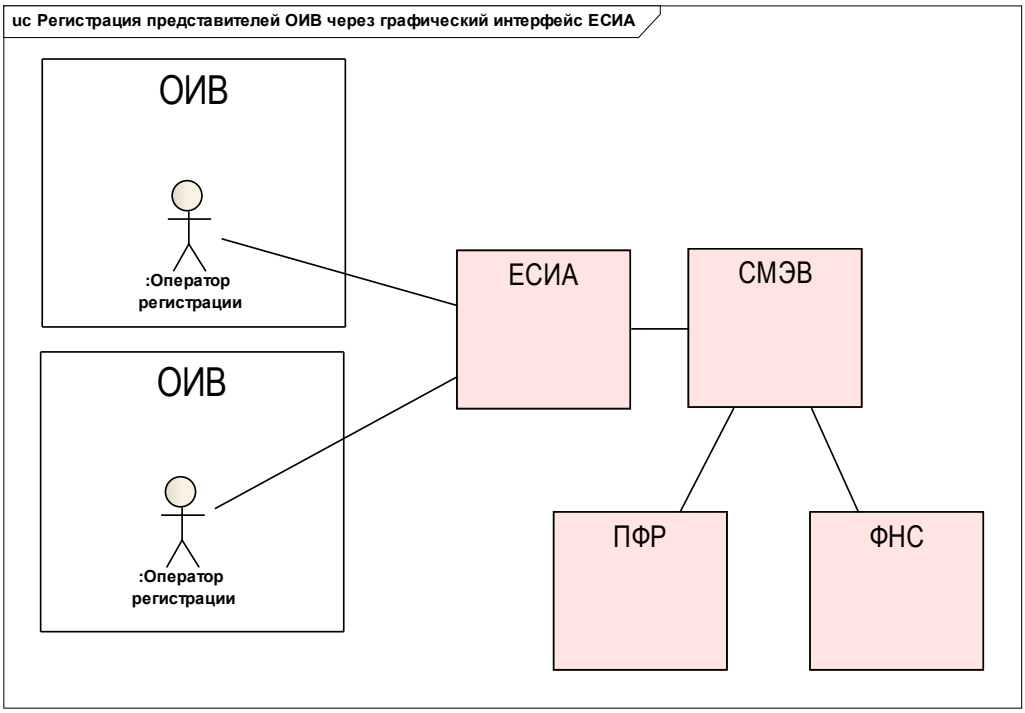

Рисунок 5 - Регистрация / изменение идентификационных данных представителей ОИВ через графический интерфейс ЕСИА (архитектура решения)

Особенности реализации с точки зрения ОИВ: необходимо обязать работника кадрового подразделения или другого работника ОИВ регистрировать учетные записи в ЕСИА.

Особенности реализации с точки зрения ЕСИА: необходимо разработать графический интерфейс для регистрации представителей ОИВ.

2.1.2 Регистрация представителей ОИВ через веб-сервисы СМЭВ

Краткое описание варианта использования: Сотрудник кадрового подразделения ввёл данные нового работника в кадровую информационную систему (или изменил данные существующего работника). Кадровая информационная система предоставляет в ЕСИА данные о работнике. Для этого кадровая информационная система вызывает веб-сервис регистрации пользователей ЕСИА, зарегистрированный в СМЭВ. ЕСИА проверяет достоверность идентификационных данных регистрируемого пользователя, вызывая веб-сервисы соответствующих ведомств, зарегистрированные в

СМЭВ. Если проверки пройдены успешно, ЕСИА создаёт для нового работника ОИВ учетную запись с ролью представителя ОИВ (или изменяет данные зарегистрированного пользователя).

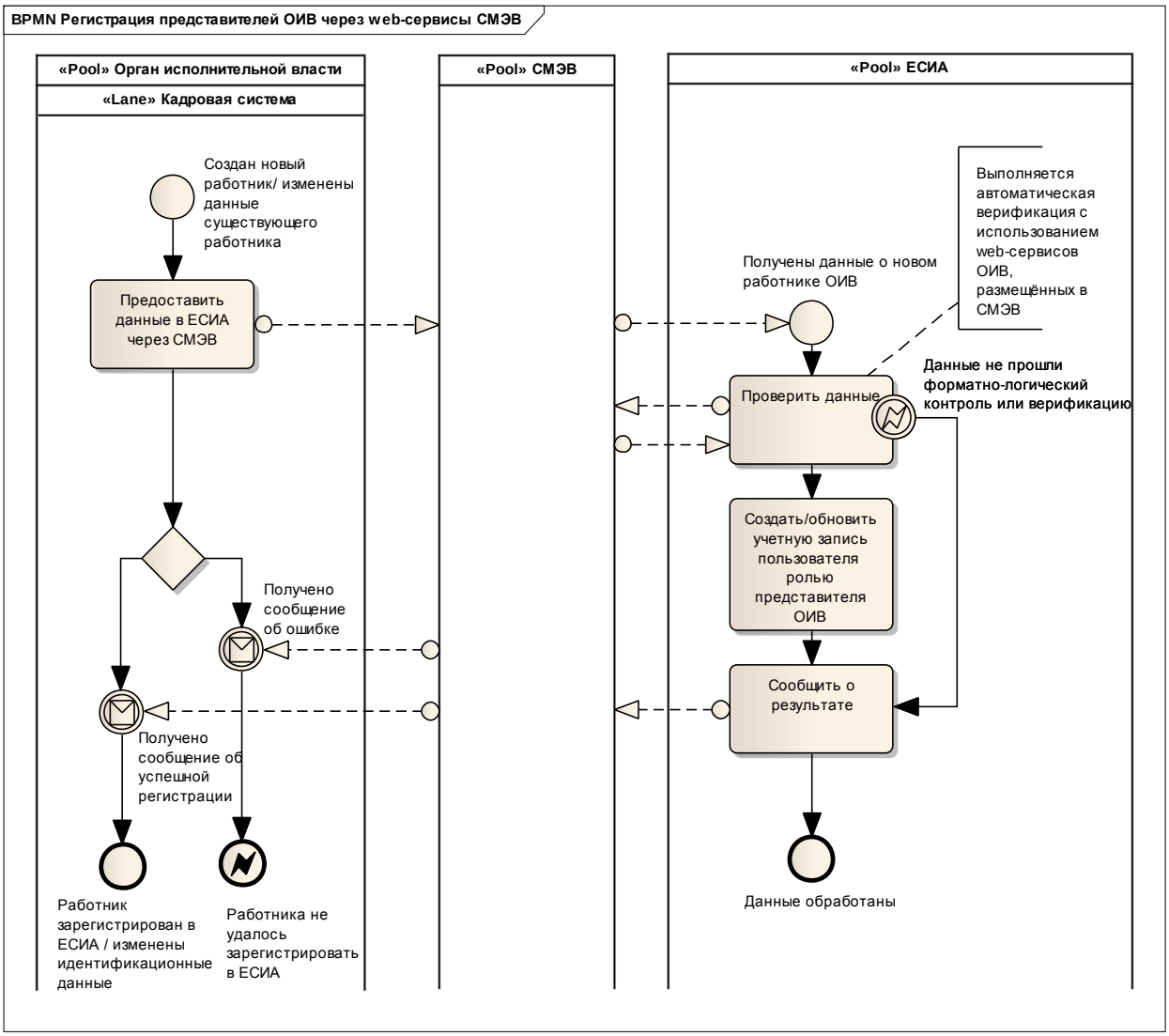

Рисунок 6 – Регистрация / изменение идентификационных данных представителей ОИВ через веб-сервисы СМЭВ (диаграмма процесса)

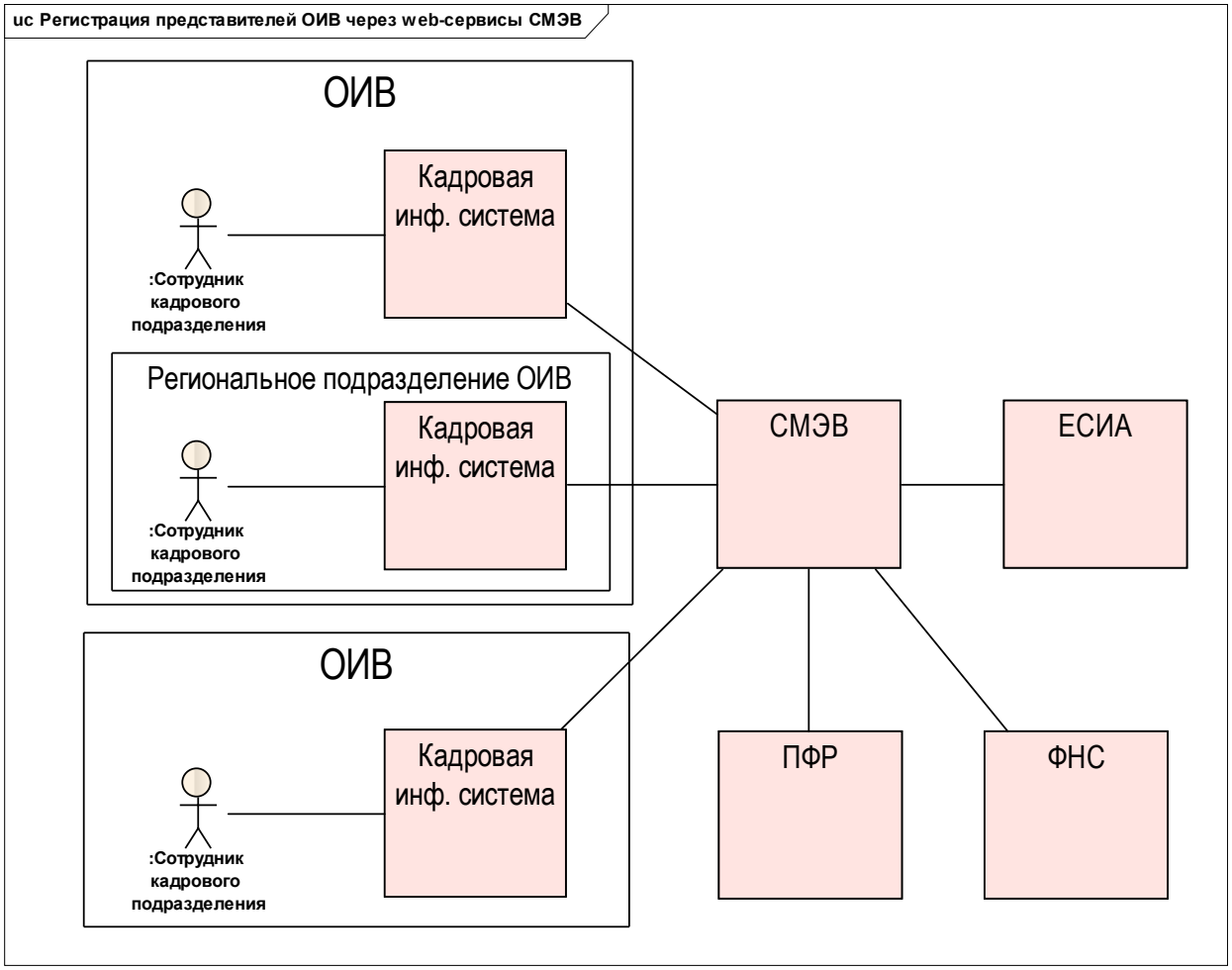

Рисунок 7 – Регистрация / изменение идентификационных данных представителей ОИВ через веб-сервисы СМЭВ (архитектура решения)

Особенности реализации с точки зрения ОИВ: необходимо доработать кадровую систему.

Особенности реализации с точки зрения ЕСИА: необходимо разработать для СМЭВ веб-сервис для регистрации пользователей.

2.1.3 Регистрация представителей ОИВ через систему IdM[5] и веб-сервисы СМЭВ

Краткое описание варианта использования: Сотрудник кадрового подразделения ввёл данные нового работника в кадровую информационную систему. Кадровая информационная система предоставляет в IdM-систему ОИВ данные о новом работнике. IdM-система предоставляет в ЕСИА

[5] Система IdM – класс информационных систем, предназначенных для централизованного управления идентификационными данными и полномочиями пользователей в масштабах организации

данные о новом работнике. Для этого IdM-система вызывает веб-сервис регистрации пользователей ЕСИА, зарегистрированный в СМЭВ. ЕСИА создаёт для нового работника ОИВ учетную запись с ролью представителя ОИВ.

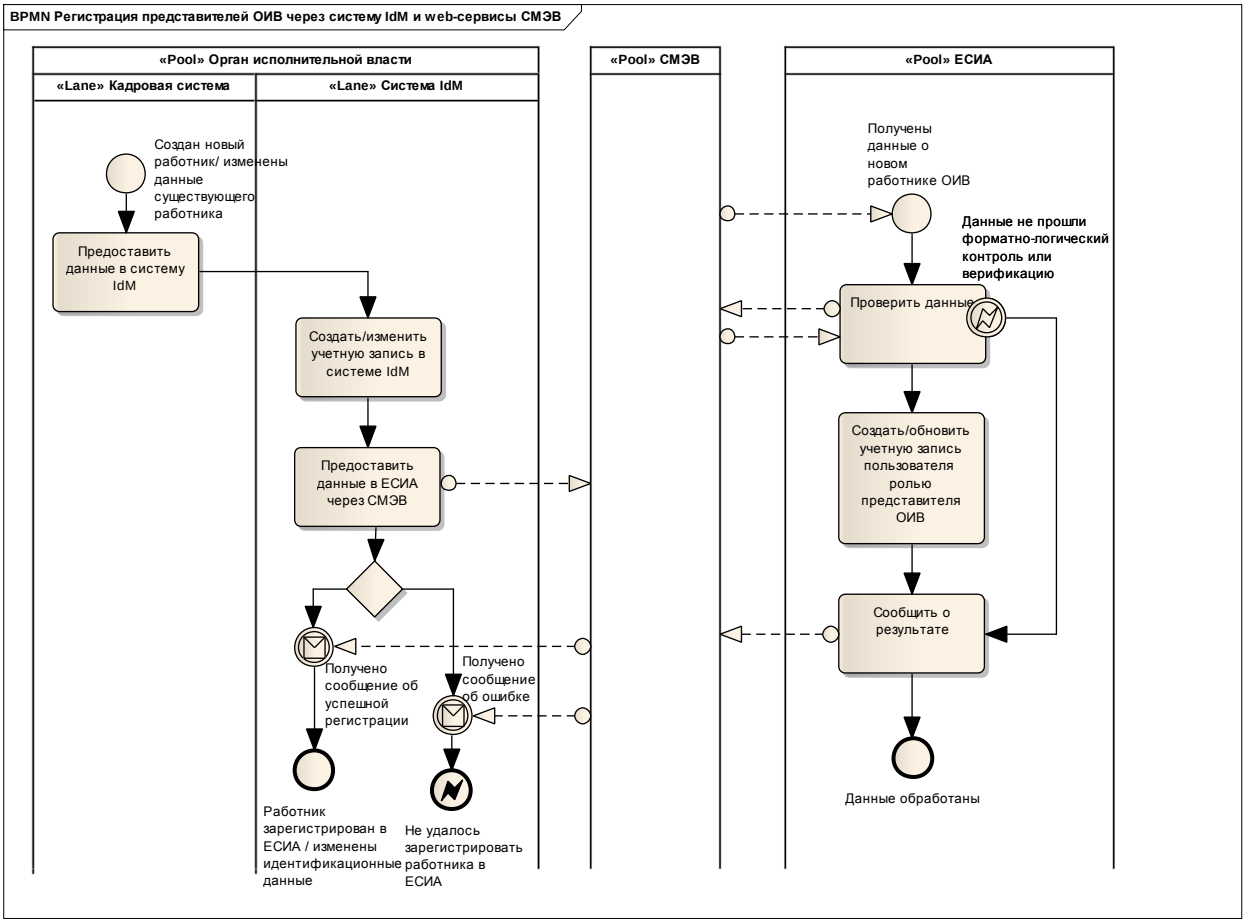

Рисунок 8 – Регистрация / изменение идентификационных данных представителей ОИВ через систему IdM и веб-сервисы СМЭВ (диаграмма процесса)

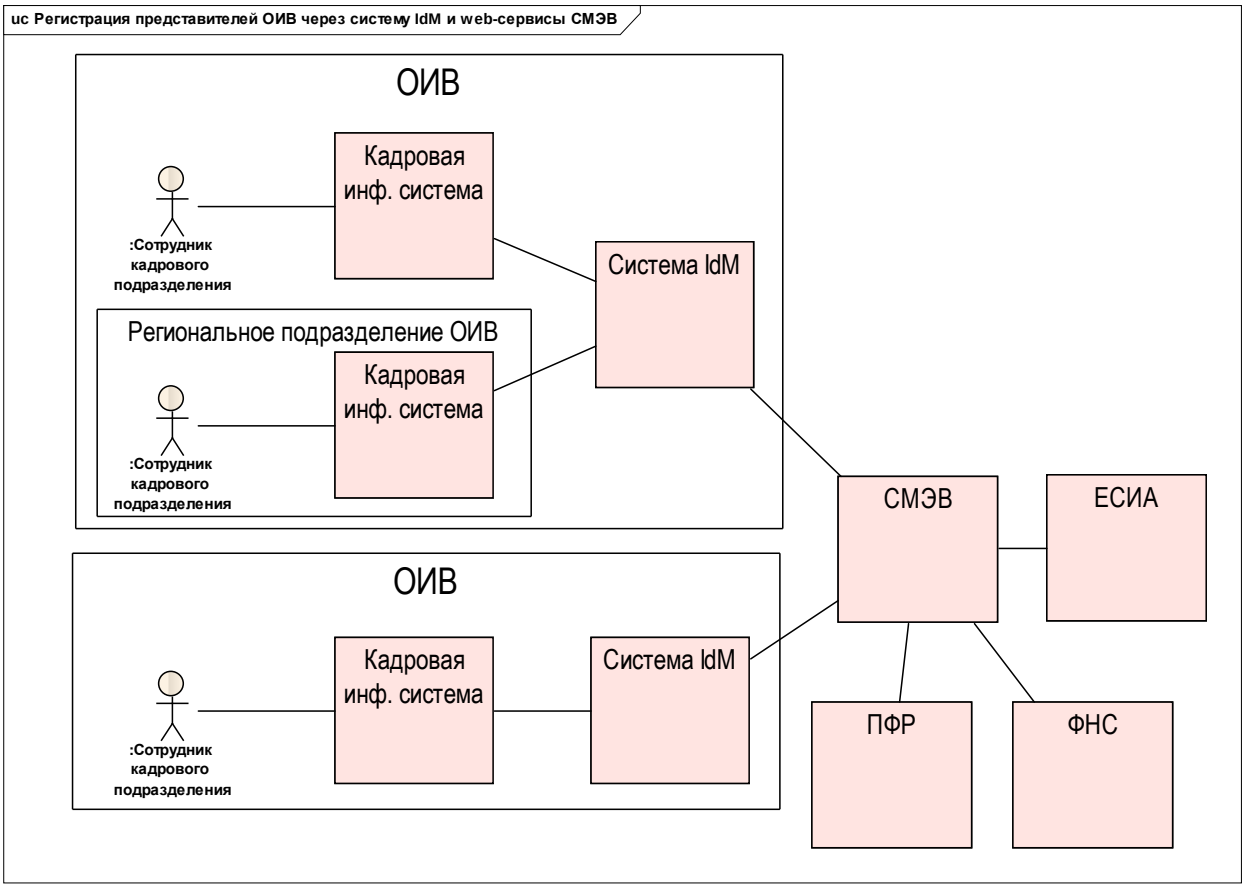

Рисунок 9 - Регистрация / изменение идентификационных данных представителей ОИВ через систему IdM и веб-сервисы СМЭВ (архитектура решения)

Особенности реализации с точки зрения ОИВ: необходимо внедрить систему IdM и интегрировать IdM с кадровой системой и со СМЭВ.

Особенности реализации с точки зрения ЕСИА: необходимо разработать для СМЭВ веб-сервис для регистрации пользователей.

2.2 Предоставление/отзыв полномочий представителям ОИВ в ЕСИА

2.2.1 Предоставление / отзыв полномочий представителям ОИВ через графический интерфейс ЕСИА

Краткое описание варианта использования: Оператор полномочий получил обоснования необходимости предоставления полномочий одному из

работников ОИВ[6]. Оператор полномочий предоставляет полномочия работнику ОИВ, используя графический интерфейс ЕСИА.

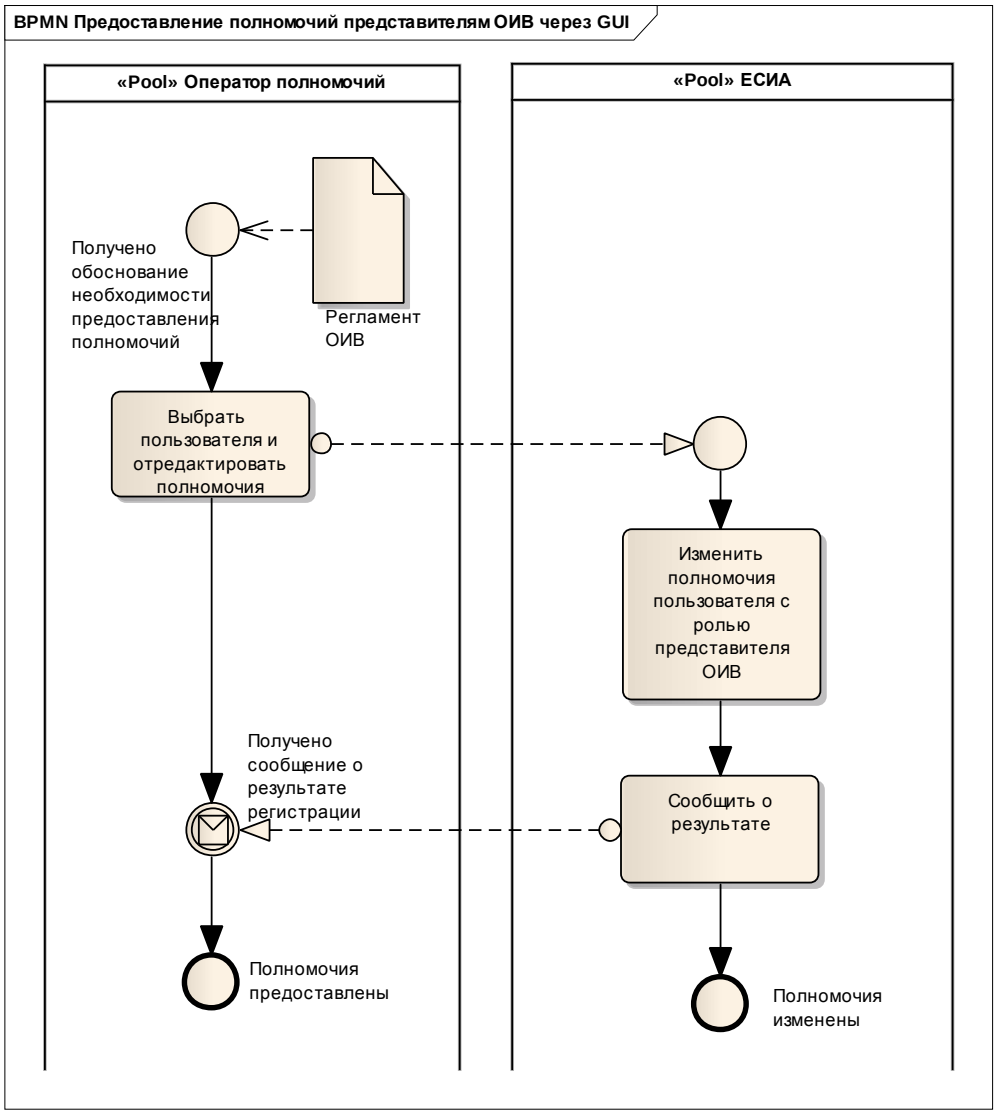

Рисунок 10 - Предоставление / отзыв полномочий представителям ОИВ через графический интерфейс ЕСИА (диаграмма процесса)[7]

[6] Требования к обоснованию необходимости предоставления полномочий должны быть определены в регламенте ОИВ

[7] На этой и последующих диаграммах процессов рассмотрены только успешные сценарии развития процесса. Это сделано умышленно, чтобы излишне не перегружать диаграммы

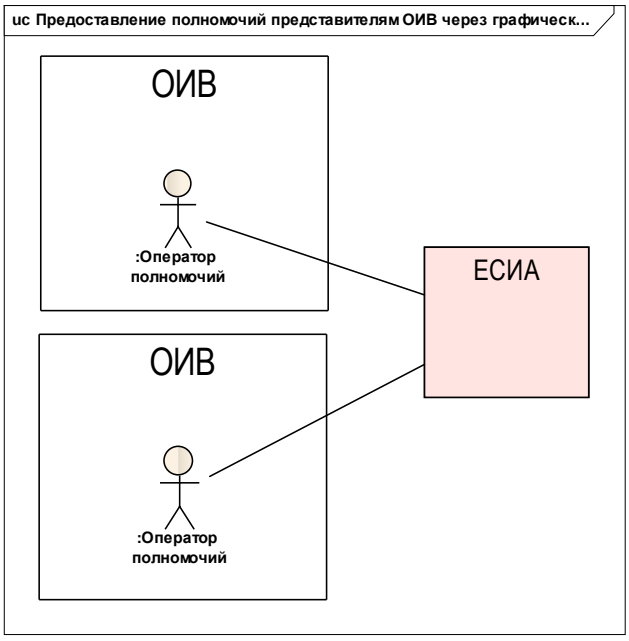

Рисунок 11 - Предоставление / отзыв полномочий представителям ОИВ через графический интерфейс ЕСИА (архитектура решения)

2.2.2 Предоставление / отзыв полномочий представителям ОИВ через систему IdM и веб-сервисы СМЭВ

Краткое описание варианта использования: В системе IdM произошло назначение и/или согласование полномочий работника ОИВ по доступу к информационным ресурсам[8]. IdM-система передаёт в ЕСИА данные о полномочиях работника ОИВ. Для этого IdM-система вызывает веб-сервис управления полномочиями пользователей ЕСИА, зарегистрированный в СМЭВ. ЕСИА предоставляет полномочия соответствующему пользователю с ролью представителя ОИВ.

[8] Процессы предоставления прав доступа проектируются для каждого ОИВ при внедрении им системы IdM

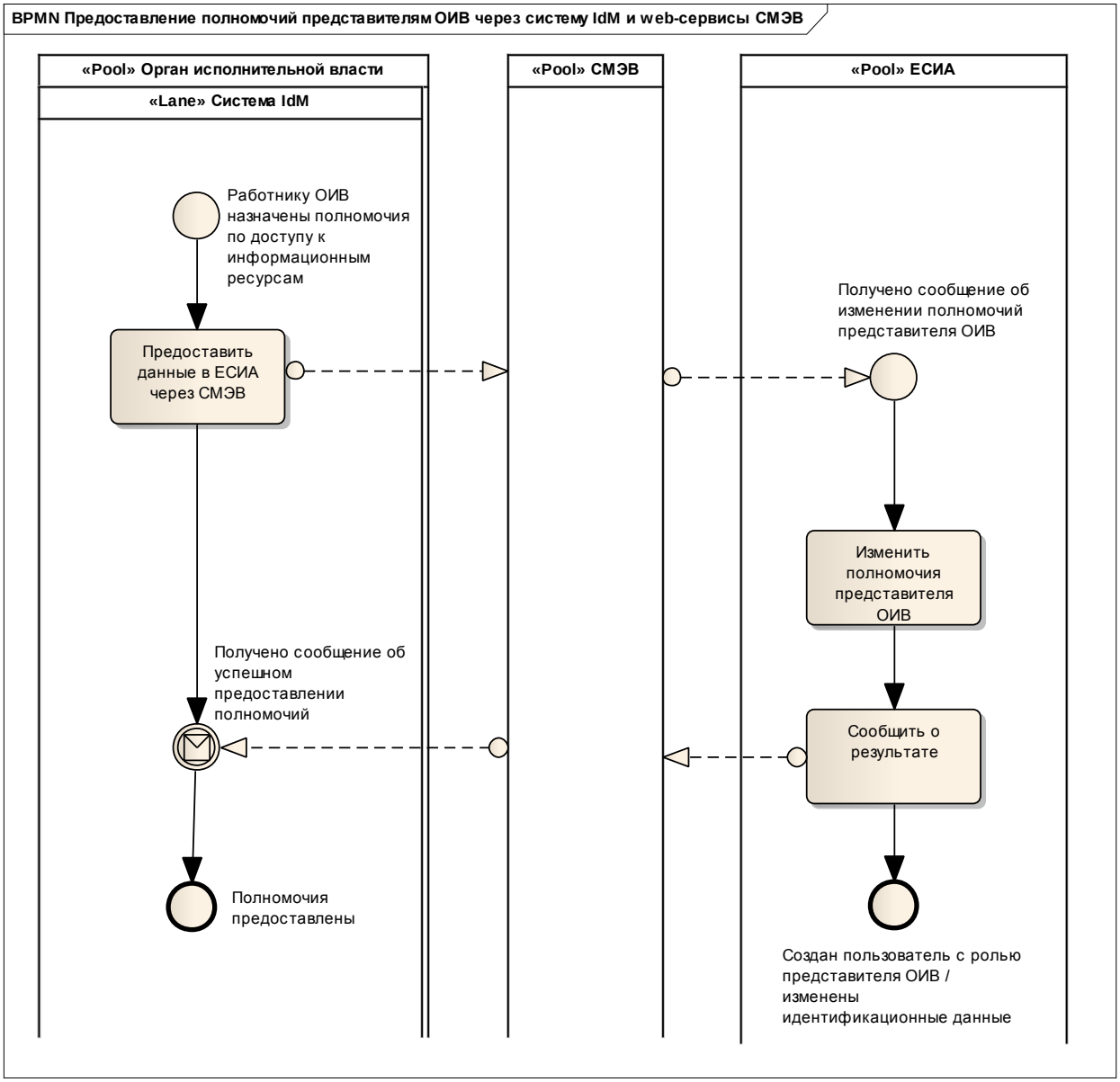

Рисунок 12 – Предоставление полномочий представителям ОИВ через систему IdM и веб-сервисы СМЭВ

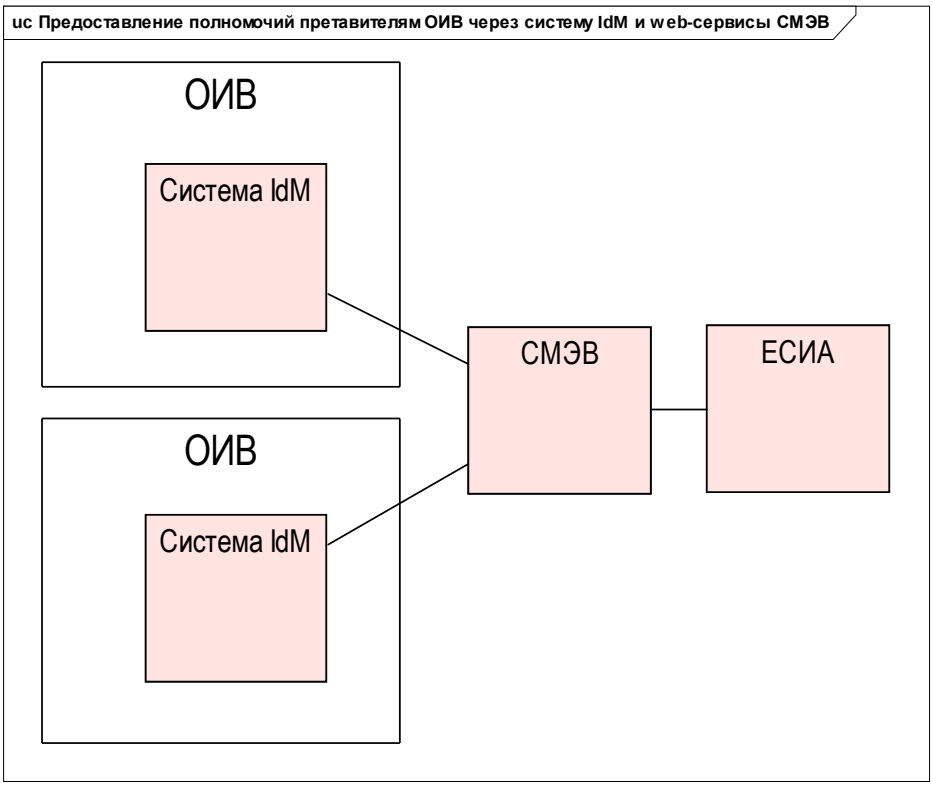

Рисунок 13 - Предоставление / отзыв полномочий представителям ОИВ через систему IdM и веб-сервисы СМЭВ (архитектура решения)

2.3 Идентификация / аутентификация представителей ОИВ в ЕСИА

Краткое описание варианта использования: Должностное лицо ОИВ запрашивает доступ к защищённому ресурсу ИС ОИВ. ИС ОИВ запрашивает в ЕСИА информацию о должностном лице ОИВ и принимает решение о предоставлении доступа.

Основной сценарий:

а) Должностное лицо ОИВ запрашивает доступ к защищённому ресурсу ИС ОИВ.

б) ИС ОИВ направляет в ЕСИА запрос на аутентификацию.

в) ЕСИА проверяет наличие у должностного лица ОИВ открытой сессии и, если активная сессия отсутствует, проводит его аутентификацию. Для этого ЕСИА направляет пользователя на свою страницу аутентификации.

г) ЕСИА передаёт в ИС ОИВ набор утверждений, содержащих идентификационные данные пользователя, информацию о контексте аутентификации и полномочиях пользователя.

д) На основании полученной из ЕСИА информации, ИС принимает решение об авторизации — разрешает или запрещает доступ к ресурсу

Примечания:

а) В соответствии с описанным выше сценарием может осуществляться идентификация / аутентификация как внешних, так и внутренних пользователей (по отношению к ОИВ, владеющему ИС).

б) Внешние пользователи, не имеющие учетных записей в самой ИС, могут быть аутентифицированы только через ЕСИА (в соответствии с описанным выше сценарием).

в) Аутентификацию внутренних пользователей можно выполнять как с использованием ЕСИА, так и с использованием уже внедрённых в ИС механизмов аутентификации пользователей. Два механизма аутентификации могут работать одновременно. Выбор приоритетного механизма аутентификации внутренних пользователей осуществляется на усмотрение владельца ИС.

г) В результате авторизации пользователь получает доступ к ресурсам ИС в соответствии с назначенными ему полномочиями.

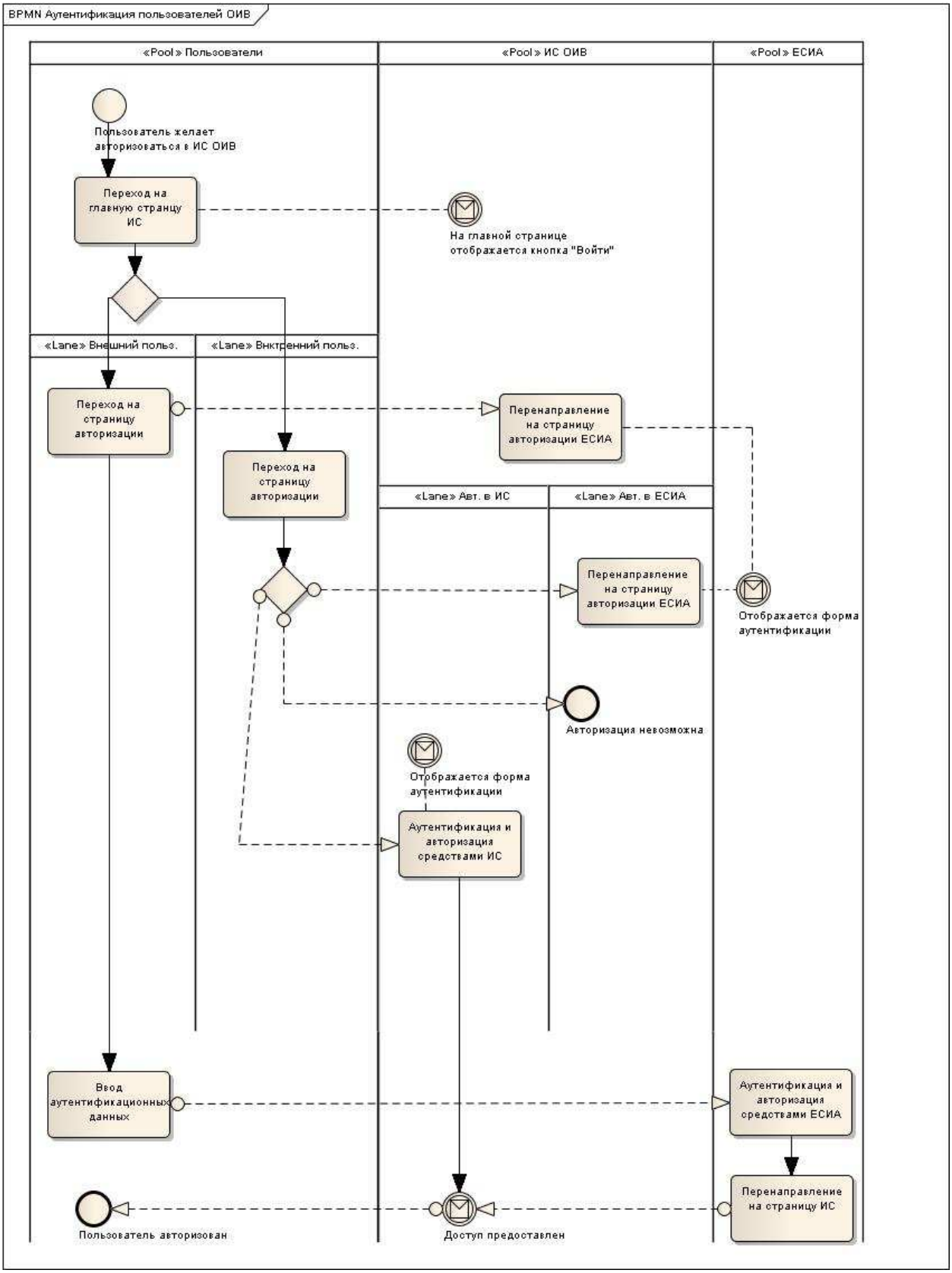

Рисунок 14 – Идентификация / аутентификация пользователей в ЕСИА

2.4 Регистрация информационной системы, использующей ЕСИА для идентификации / аутентификации пользователей

Краткое описание варианта использования: Владелец ИС через технологический портал ЕСИА обращается к оператору ЕСИА для регистрации ИС и ее метаданных. Оператор ЕСИА в установленные регламентом сроки регистрирует ИС в системе НСИ и метаданные ИС в системе ЕСИА.

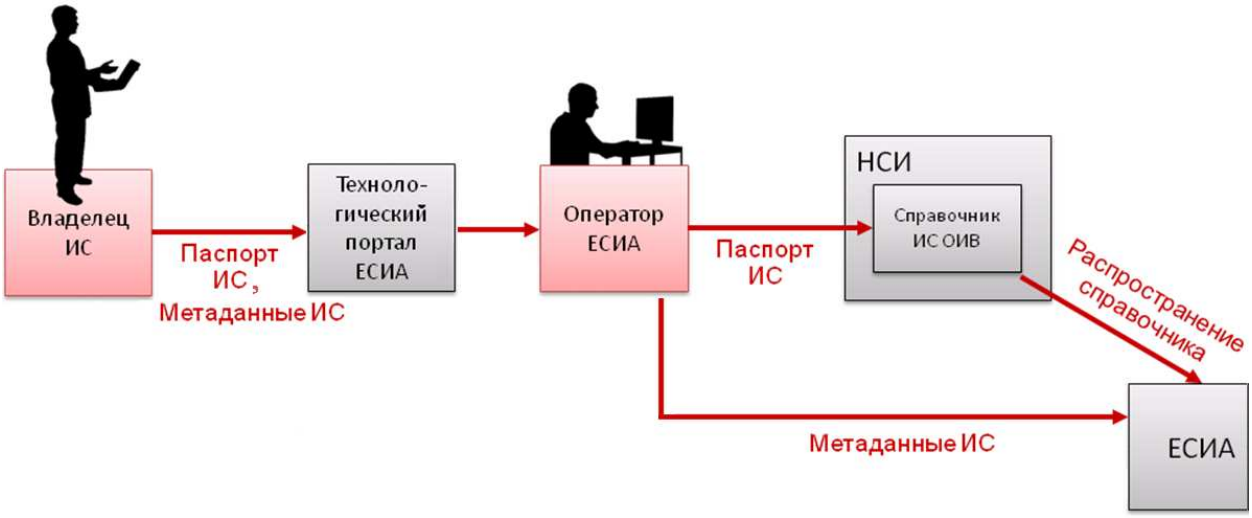

Рисунок 15 – Регистрация информационной системы, использующей ЕСИА для идентификации/аутентификации пользователей

Основной сценарий:

а) Владелец ИС хочет настроить аутентификацию пользователей своей системы через ЕСИА.

б) Владелец ИС дорабатывает свою ИС[9].

в) Владелец ИС обращается к оператору ЕСИА и передаёт ему через технологический портал ЕСИА паспорт ИС и метаданные ИС.

г) Оператор ЕСИА в установленные регламентом сроки вносит данные об ИС в справочник ИС, расположенный в системе НСИ.

д) Данные из справочника ИС ОИВ распространяются в ЕСИА.

[9] Необходимые доработки рассмотрены в «Руководстве разработчика по интеграции внешней ИС с СИА ИЭП»

е) Оператор ЕСИА после успешной регистрации ИС в системе НСИ регистрирует метаданные ИС (в том числе сертификат ЭП ИС) в системе ЕСИА.

Примечания:

а) Справочник ИС ОИВ должен содержать следующую информацию:

- краткое наименование ИС;
- полное наименование ИС;
- владелец ИС (наименование ОИВ);
- контактные данные ответственного лица.

2.5 Ведение справочника полномочий ИС ОИВ

Краткое описание варианта использования: Владелец ИС ведёт справочник полномочий ИС через технологический портал ЕСИА.

Основной сценарий:

а) Владелец ИС хочет, чтобы разные категории пользователей получали разные права доступа к ресурсам его ИС.

б) Владелец ИС обращается к оператору ЕСИА и передаёт ему через технологический портал ЕСИА справочник полномочий своей ИС.

в) Оператор ЕСИА через технологический портал ЕСИА подтверждает изменение справочника полномочий ИС (добавляет или удаляет полномочия)

г) Владелец ИС изменяет механизм авторизации в своей ИС так, чтобы ИС принимала решение об авторизации на основании информации о полномочиях, полученной из ЕСИА.

Примечания:

а) После добавления нового полномочия в справочник полномочий, оператор полномочий ЕСИА сможет предоставить это полномочие должностному лицу ОИВ.

3 СХЕМА ИСПОЛЬЗОВАНИЯ ЕСИА ПРИ ДОСТУПЕ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ

ЕСИА участвует в управлении доступом пользователей Интернет к ресурсам информационных систем ОИВ (например, веб-порталам ОИВ) следующим образом:

а) ЕСИА обеспечивает идентификацию и однократную аутентификацию пользователей и предоставляет информационным системам ОИВ информацию об идентификационных данных пользователей (п. 3.2);

б) ЕСИА обеспечивает управление идентификационными данными пользователей.

ЕСИА позволяет пользователям Интернет использовать один пароль для доступа ко всем веб-порталам ОИВ, подключенным к ЕСИА, и проходить процедуру аутентификации только один раз на протяжении одного сеанса работы в Интернет. Для того чтобы ЕСИА могла выполнять однократную аутентификацию пользователей Интернет, необходимо следующее:

а) пользователи должны быть зарегистрированы в ЕСИА (п. 3.1);

б) ИС ОИВ должны быть зарегистрированы в ЕСИА (п. 2.4).

3.1 Регистрация пользователей Интернет в ЕСИА

Краткое описание варианта использования: Пользователь Интернет регистрируется в ЕСИА, чтобы получить возможность доступа к персональным сервисам на веб-порталах ОИВ.

Основной сценарий:

а) Пользователь заходит на главную страницу веб-портала ИС ОИВ и нажимает кнопку регистрации.

б) ИС ОИВ перенаправляет пользователя в ЕСИА.

в) Пользователь заполняет форму регистрации.

г) ЕСИА осуществляет проверку введенных данных, после чего создает учетную запись.

3.2 Идентификация / аутентификация пользователей Интернет в ЕСИА

Идентификация и аутентификация для пользователей Интернет осуществляется так же, как и для должностных лиц ОИВ (см. пункт 2.3).

4 СХЕМА ИСПОЛЬЗОВАНИЯ ЕСИА ПРИ МЕЖВЕДОМСТВЕННОМ ВЗАИМОДЕЙСТВИИ

ЕСИА участвует в межведомственном взаимодействии ИС ОИВ через СМЭВ следующим образом: ЕСИА предоставляет в СМЭВ информацию об идентификационных данных и полномочиях ИС ОИВ, вызывающих сервисы СМЭВ (п. 4.4). Для того чтобы ЕСИА могла предоставлять эту информацию, ИС ОИВ должны быть предварительно зарегистрированы в ЕСИА (п. 4.1.1) и им должны быть предоставлены полномочия по доступу к сервисам СМЭВ (п. 4.3). Кроме этого в ЕСИА и СМЭВ должен вестись справочник полномочий по доступу к сервисам СМЭВ (п. 4.2).

4.1 Регистрация информационных систем ОИВ, осуществляющих межведомственное взаимодействие через СМЭВ

4.1.1 Регистрация информационной системы, использующей сервисы СМЭВ

Краткое описание варианта использования: Владелец ИС обращается к оператору СМЭВ. Оператор СМЭВ регистрирует ИС, её сертификат и полномочия по доступу к СМЭВ.

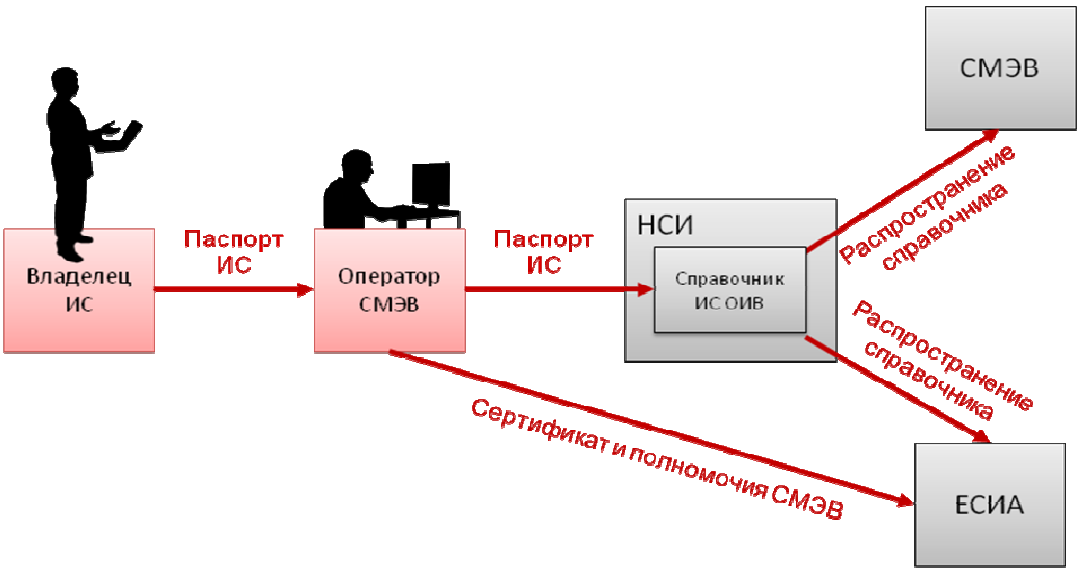

Рисунок 16 - Регистрация информационной системы, вызывающей сервисы СМЭВ

Основной сценарий:

а) Владелец ИС хочет, чтобы его система могла использовать электронный сервис СМЭВ. Он получает в доверенном (аккредитованном) УЦ сертификат ЭП для своей ИС. Затем он обращается к оператору СМЭВ и передаёт ему паспорт ИС и сертификат ЭП для информационной системы.

б) Оператор СМЭВ вносит данные об ИС (и её владельце) в справочник ИС, расположенный в системе НСИ.

в) Данные из справочника ИС распространяются в ЕСИА и СМЭВ.

г) Оператор СМЭВ регистрирует в ЕСИА сертификат ИС и назначает полномочия по доступу к сервисам СМЭВ.

4.1.2 Регистрация информационной системы, предоставляющей сервисы в СМЭВ

Краткое описание варианта использования: Владелец ИС обращается к оператору СМЭВ. Оператор СМЭВ регистрирует ИС, электронные сервисы, а также осуществляет настройку прав доступа к электронным сервисам для различных полномочий СМЭВ.

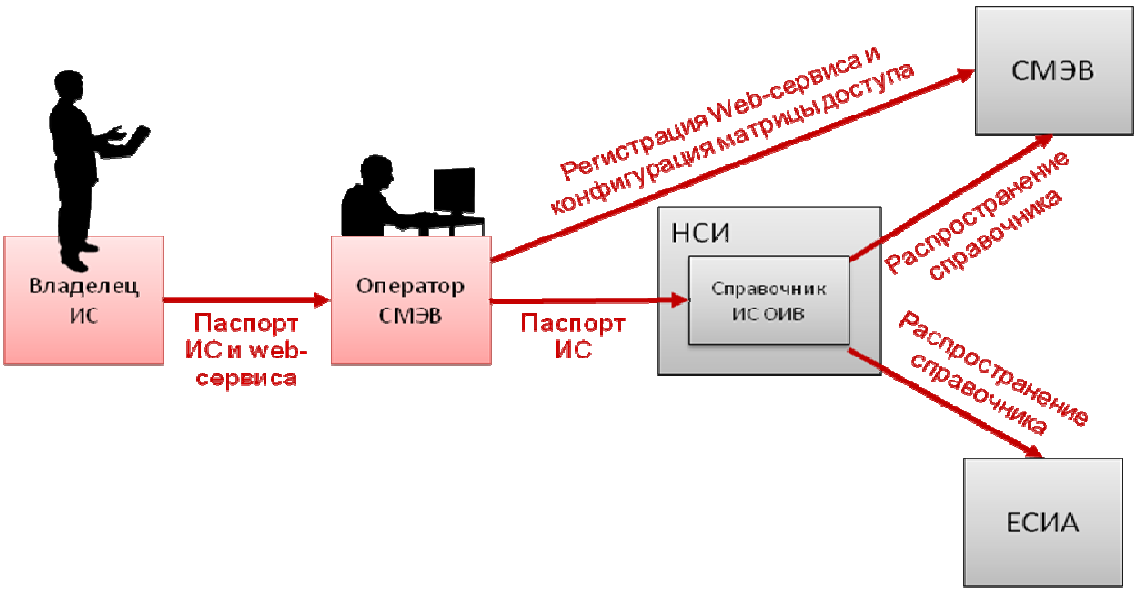

Рисунок 17 – Регистрация информационной системы, предоставляющей сервисы на СМЭВ

Основной сценарий:

а) Владелец ИС хочет разместить в СМЭВ электронный сервис своей системы. Он обращается к оператору СМЭВ и передаёт ему паспорт ИС и электронного сервиса.

б) Оператор СМЭВ вносит данные об ИС в справочник ИС, расположенный в системе НСИ.

в) Данные из справочника ИС распространяются в СМЭВ и ЕСИА.

г) Оператор СМЭВ регистрирует в СМЭВ электронный сервис и настраивает матрицу доступа, в которой указывает, какие полномочия должны иметь другие ИС для получения доступа к новому электронному сервису.

4.2 Ведение справочника полномочий СМЭВ

Краткое описание варианта использования: Оператор СМЭВ пополняет справочник полномочий СМЭВ.

Основной сценарий:

а) Оператор СМЭВ решил, что с использованием действующего справочника полномочий СМЭВ стало невозможно настроить

политику доступа, отвечающую потребностям ОИВ.

б) Оператор СМЭВ регистрирует новое полномочие по доступу к СМЭВ в справочнике полномочий ЕСИА.

в) Оператор СМЭВ регистрирует новое полномочие по доступу к СМЭВ в справочнике полномочий СМЭВ.

г) Оператор СМЭВ настраивает в СМЭВ матрицу доступа, в которой указано соответствие полномочий и объектов доступа (веб-сервисов, зарегистрированных в СМЭВ).

Примечания:

а) После выполнения описанного выше сценария, оператор СМЭВ сможет предоставить новое полномочие информационной системе ОИВ, зарегистрированной в ЕСИА.

б) Справочник может иметь иерархическую структуру, например:

- Базовое полномочие

- - Базовое полномочие федеральной системы

- - Базовое полномочие региональной системы

- - - Базовое полномочие доступа к сервисам ФНС

в) При ведении справочника полномочий оператор СМЭВ должен стремиться минимизировать количество полномочий.

4.3 Предоставление информационным системам ОИВ полномочий по доступу к сервисам СМЭВ

Краткое описание варианта использования: Оператор СМЭВ получил обоснования необходимости предоставления полномочий информационной системе ОИВ[10]. Оператор СМЭВ входит в ЕСИА (с ролью оператора полномочий) и предоставляет информационной системе полномочия, используя графический интерфейс ЕСИА.

[10] Требования к обоснованию необходимости предоставления полномочий должны быть определены в регламенте

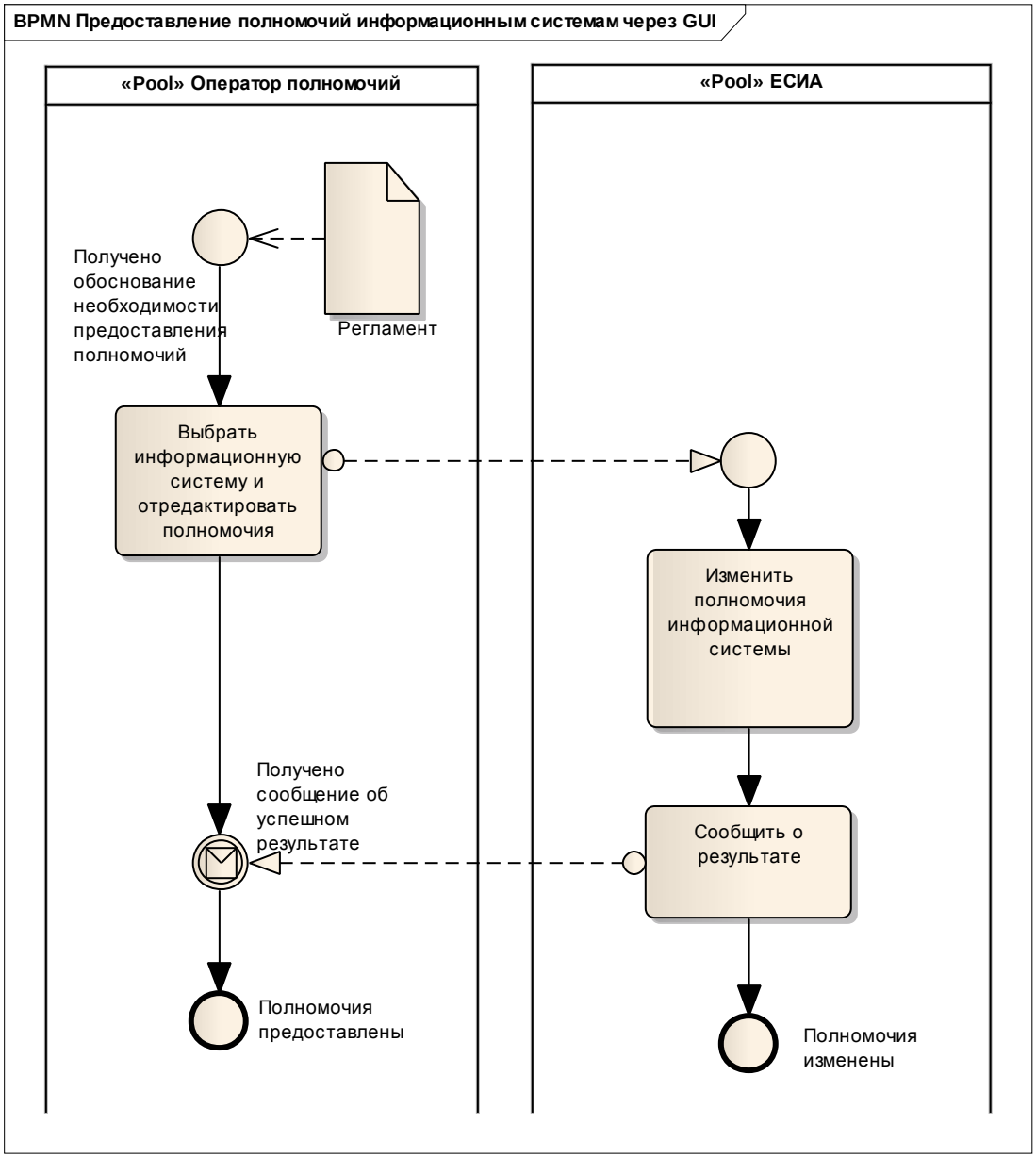

Рисунок 18 – Предоставление полномочий информационным системам ОИВ

4.4 Авторизация информационных систем при межведомственном взаимодействии

Краткое описание варианта использования: ИС ОИВ передаёт через СМЭВ сообщение для другой ИС ОИВ. СМЭВ запрашивает в ЕСИА идентификационные данные и полномочия ИС ОИВ, инициировавшей межведомственное взаимодействие.

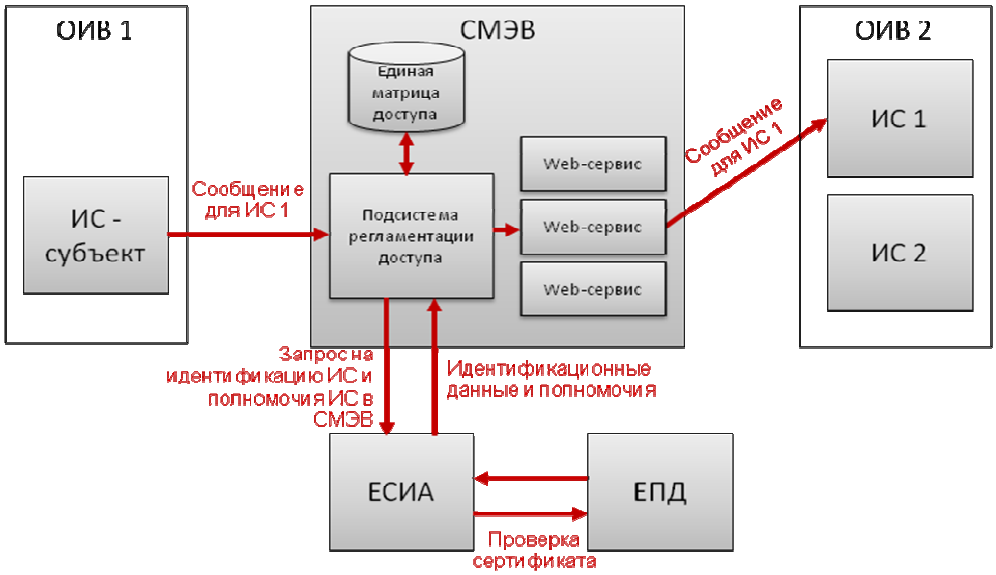

Рисунок 19 - Авторизация информационных систем при межведомственном взаимодействии

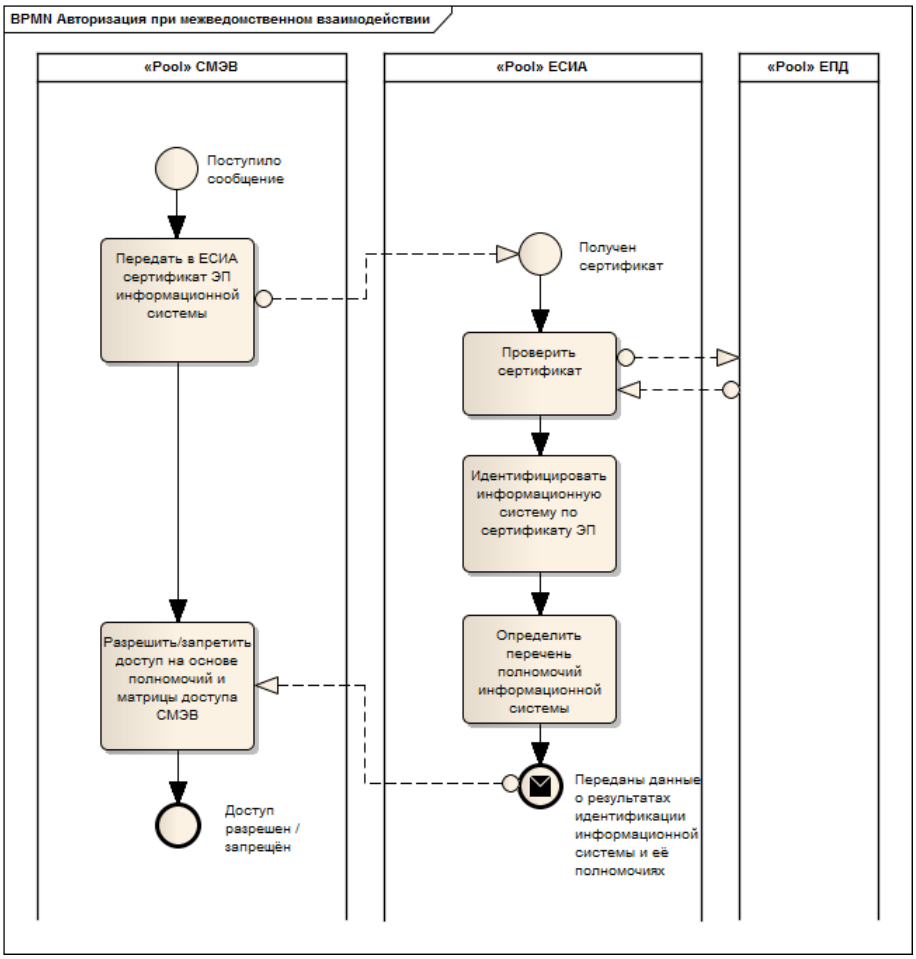

Рисунок 20 – Авторизация информационных систем при межведомственном взаимодействии

Основной сценарий:

а) Информационная система инициировала передачу через СМЭВ сообщения. Сообщение соответствует методическим рекомендациям СМЭВ и содержит электронную подпись информационной системы, инициировавшей отправку сообщения через СМЭВ.

б) СМЭВ осуществляет проверку поступившего сообщения. Для целей авторизации межведомственного взаимодействия передает запрос, содержащий сертификат информационной системы (отправителя сообщения) в ЕСИА.

в) Система ЕСИА взаимодействует с информационной системой сервисов ЕПД для проверки действительности сертификата информационной системы. Затем, с помощью сертификата, выполняет идентификацию информационной системы. Результаты идентификации информационной системы ЕСИА передает в СМЭВ. Вместе с результатами идентификации в СМЭВ также передаются данные о полномочиях информационной системы.

г) СМЭВ на основе полученной от ЕСИА информации с результатами идентификации осуществляет контроль доступа с использованием матриц доступа, задающих набор информационных систем, сервисов и операций, доступных для использования при наличии тех или иных полномочий информационных систем.

5 РАЗЛИЧИЯ МЕЖДУ ТЕХНОЛОГИЧЕСКИМИ ПОРТАЛАМИ ЕСИА И СМЭВ

Из бизнес-сценариев, рассмотренных в главах 2.4, 2.5, 4.1, 4.2, 4.3, следуют следующие варианты использования технологических порталов ЕСИА и СМЭВ и системы НСИ:

а) Оператор СМЭВ использует технологический портал СМЭВ для:
   1) регистрации и настройки сервисов СМЭВ;
   2) настройки Единой матрицы доступа, в которой определено, какие полномочия должны иметь другие ИС для получения доступа к сервису.

б) Оператор СМЭВ использует технологический портал ЕСИА для:
   1) ведения справочника полномочий по доступу к сервисам СМЭВ;
   2) регистрации сертификата ЭП ИС участника взаимодействия, вызывающей сервисы СМЭВ;
   3) предоставления ИС участника взаимодействия полномочий по доступу к сервисам СМЭВ.

в) Оператор ИС, который хочет использовать ЕСИА для идентификации и аутентификации пользователей, использует технологический портал ЕСИА для:
   1) подачи заявки на регистрацию ИС и ее метаданных (в том числе сертификата ЭП) в системе ЕСИА;
   2) ведения справочника полномочий по доступу к своей ИС.

г) Операторы СМЭВ используют систему НСИ для регистрации в справочнике ИС участников взаимодействия базовой информации об ИС, взаимодействующих через СМЭВ.

д) Операторы ЕСИА используют систему НСИ для регистрации в справочнике ИС ОИВ базовой информации об ИС, использующих ЕСИА для идентификации и аутентификации пользователей.

6 РЕКОМЕНДАЦИИ ДЛЯ ВЛАДЕЛЬЦЕВ ИС ОИВ

6.1 Рекомендации по регистрации должностных лиц ОИВ в ЕСИА

У каждого ведомства должна быть возможность самостоятельно принять решение по вопросу, каких работников нужно регистрировать в ЕСИА в обязательном порядке. В первую очередь в ЕСИА рекомендуется зарегистрировать следующие категории работников ОИВ:

а) должностные лица ОИВ, которые потенциально являются пользователями ИС других ведомств;

б) должностные лица ОИВ, которые для выполнения своей деятельности используют СМЭВ или ИС, подключенные к СМЭВ;

в) владельцы ИС ОИВ, которые хотят интегрировать свою ИС с ЕСИА, чтобы использовать ЕСИА для идентификации / аутентификации пользователей;

г) должностные лица ОИВ, которые станут операторами ЕСИА (будут регистрировать других должностных лиц в ЕСИА, предоставлять полномочия).

6.2 Рекомендации по авторизации доступа пользователей, которые прошли аутентификацию в ЕСИА

За разработку и настройку механизма авторизации и политик доступа к ресурсам ИС отвечает владелец ИС. ЕСИА только предоставляет в ИС информацию о пользователе, которая включает:

а) идентификатор пользователя;

б) значения определенных атрибутов учетной записи пользователя;

в) способ аутентификации пользователя;

г) уровень достоверности идентификации пользователя;

д) полномочия пользователя в ИС.

Далее рассмотрены рекомендации по авторизации доступа к некоторым категориям ресурсов (Таблица 1)

Таблица 1 – Требования к авторизации доступа к различным типам ресурсов

№ п.п.	Описание доступа	Требования к пользователю
1	Использование пользователем Интернет публичного сервиса с возможностью персонализированных запросов (форум, социальная сеть и т.п.). Достаточно различать пользователей по псевдонимам и не требуется сложное подтверждение личности	Пользователь прошел аутентификацию в ЕСИА, допустим 1-ый уровень достоверности идентификации.
2	Получение гражданином РФ, иностранным гражданином, лицом без гражданства государственных услуг в электронном виде. Необходимо подтверждение личности.	Пользователь прошел аутентификацию в ЕСИА, уровень достоверности идентификации не менее 2.
3	Получение гражданином РФ государственных услуг в электронном виде, регламент предоставления которых требует строгую аутентификацию заявителя. Необходимо подтверждение личности.	Пользователь прошел аутентификацию в ЕСИА, 3-ий уровень достоверности идентификации.
4	Доступ должностного лица ОИВ к информации ограниченного доступа, обрабатываемой в ИС ОИВ. Необходимо подтверждение личности и прав доступа к ресурсу.	Пользователь прошел аутентификацию в ЕСИА, уровень достоверности идентификации не менее 4, пользователю

		предоставлены полномочия на доступ к запрашиваемому ресурсу.

6.3 Рекомендации по регистрации в ИС ОИВ пользователей, которые прошли аутентификацию в ЕСИА

ЕСИА является инструментом, который позволяет предоставить работникам одного ОИВ авторизованный доступ к ресурсам ИС другого ОИВ. Когда пользователь обращается к защищённому ресурсу ИС, ИС направляет пользователя для аутентификации в ЕСИА. ЕСИА передаёт в ИС данные о пользователе. ИС принимает решение об авторизации — разрешает или запрещает доступ к ресурсу.

Когда ИС ОИВ авторизует доступ нового пользователя, который прошел аутентификацию в ЕСИА, она может регистрировать или не регистрировать этого пользователя в своём хранилище учетных записей пользователей. Для ИС ОИВ возможны следующие варианты:

а) ИС ОИВ может вообще не регистрировать у себя пользователей и принимать решение об авторизации пользователя каждый раз заново на основании данных о пользователе, полученных от ЕСИА.

б) ИС ОИВ может зарегистрировать пользователя при первом входе на основе данных, полученных от ЕСИА, а при последующих обращениях пользователя, если приходящие от ЕСИА данные изменились, вносить изменения в своё хранилище данных о пользователях.

в) ИС ОИВ может попросить пользователя ввести дополнительные данные, если данных, полученных от ЕСИА, недостаточно, а потом

предоставить пользователю или оператору ИС возможность редактировать данные пользователя в самой ИС.

6.4 Рекомендации по выбору механизма аутентификации в ИС ОИВ

Работники ОИВ (внутренние пользователи) могут входить в ИС своего ОИВ как через существующие механизмы аутентификации, так и через ЕСИА. Выбор приоритетного механизма должен осуществляться на усмотрение ОИВ.

Для обеспечения доступа внешних пользователей (например, работников других ОИВ, аудиторов, подрядчиков и т.п.) следует использовать ЕСИА.

6.5 Некоторые ограничения по использованию ЕСИА

а) ЕСИА предназначена для идентификации / аутентификации пользователей, которые пытаются получить доступ к закрытым ресурсам ИС, имеющих веб-интерфейс. **Если веб-портал не предусматривает закрытой части, то ЕСИА использовать не нужно**.

б) ЕСИА не выполняет проверку ЭП в документах. Для проверки ЭП документов необходимо использовать собственные механизмы ИС или использовать сервисы информационной системы ЕПД.