

ООО «ЭластикХостинг»

Зарегистрированный хостинг-провайдер и аккредитованный регистратор доменных имён. Компания подключилась к ЕСИА и уже некоторое время успешно работает через эту систему.

Подключение было осуществлено на основании
Правил прохождения идентификации и (или) аутентификации лицами, обратившимися к провайдеру хостинга в целях получения вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети «Интернет», утверждённые постановлением Правительства Российской Федерации от 29.11.2023 № 2011.

В работе используется механизм получения scope-параметров для верификации пользователей и подтверждения данных клиентов через ЕСИА.
Состав данных ЕСИА для провайдеров хостинга:

- openid
- fullname
- birthdate
- birthplace
- addresses
- id_doc
- mobile
- email

Эти параметры используются в scope OAuth2-запроса к ЕСИА.

Преимущества использования ЕСИА для хостинг провайдерови регистраторов доменных имен

1. Законная идентификация клиентов

Исключает фиктивные аккаунты клиентов

2. Снижение рисков мошенничества

Снижает риски регистрации доменов на подставных лиц

3. Автоматизация и достоверность данных

Система автоматически получает верифицированные ФИО, паспортные данные, адрес, телефон и email

4. Упрощение регистрации

Пользователь регистрирует домен в один клик, без загрузки сканов документов

5. Снижение операционных затрат

Исключается ручная проверка документов и их хранение

6. Юридическая защита

В спорных ситуациях регистратор имеет подтверждение идентификации клиента из официального источника

Изменения требований подключения к ЕСИА

С 2025 года вступили в силу новый регламент взаимодействия с Единой системой идентификации и аутентификации (ЕСИА) (версия 2.47) и методические рекомендации (версия 3.48). Эти документы вводят ряд новых требований по безопасности для инфраструктуры и ПО. Новые требования обязательны для всех новых подключений с 2025 года, а для уже работающих с ЕСИА организаций — с конца 2026 года.

Обновление требований к интеграции с ЕСИА характеризуется двумя системными тенденциями.

В актуальной версии методических рекомендаций по работе с ЕСИА значительно расширены разделы, посвященные безопасности сервисов, использующих протоколы OAuth 2.0 и OpenID Connect.
Основные направления усиления защиты:

- Обязательное применение сертифицированных средств криптографической защиты информации (СКЗИ)
- Ужесточение требований к защите серверной части информационных систем
- Контроль защищенности каналов передачи данных между участниками взаимодействия
- Повышение требований к архитектуре типовых решений для интеграции

Фактически это означает, что простая интеграция через веб-интерфейсы или базовые API без создания защищенной инфраструктуры (VPN, СКЗИ) становится невозможной.



НЕМНОГО ТЕОРИИ

Что такое OAuth 2.0 и OpenID Connect:

OAuth 2.0 и OpenID Connect — это два взаимосвязанных протокола, которые используются для **авторизации и аутентификации пользователей** в современных веб-сервисах. Именно на их основе работает вход через **ЕСИА (Госуслуги).**

OAuth 2.0 (Open Authorization) — это протокол **авторизации**, который позволяет одному сервису получить доступ к данным пользователя из другого сервиса **без передачи пароля.**

OpenID Connect (OIDC) — это протокол **аутентификации**, построенный поверх OAuth 2.0.
OpenID Connect позволяет системе получить **подтвержденные данные пользователя.**

СКЗИ (средства криптографической защиты информации) — это программные или аппаратные средства, которые используются для защиты данных с помощью криптографии.

Их основная задача — обеспечить:

- **Конфиденциальность данных (**чтобы их не могли прочитать посторонние)
- **Целостность информации** (чтобы данные нельзя было изменить незаметно)
- **Подтверждение подлинности отправителя**
- **Создание и проверку электронной подписи**

СКЗИ — это **специальные криптографические инструменты**, которые шифруют данные и позволяют подтверждать, кто именно отправил информацию.



Ключевые сроки перехода на новые требования

Изменения носят не только методический, но и обязательный (нормативный) характер. Для организаций установлены четкие сроки перехода:

1

До 1 сентября 2026
Новые информационные системы могут подключаться к ЕСИА только при условии выполнения обновленных требований, включая соблюдение норм информационной безопасности и использование актуальной архитектуры взаимодействия

2

До 1 января 2027
Организации, уже подключенные к ЕСИА, обязаны привести свои информационные системы в полное соответствие актуальным требованиям по безопасности (в частности, использовать сертифицированные СКЗИ и обеспечить защиту каналов связи).

Это означает необходимость:

- Модернизации инфраструктуры существующих информационных систем;
- Внедрения сертифицированных средств защиты информации;
- Пересмотра архитектуры интеграции с ЕСИА

Важно: Несоблюдение этих требований может привести к блокировке возможности использовать ЕСИА для аутентификации пользователей и, как следствие, к невозможности оказания государственных услуг в электронном виде.

Ужесточение требований к безопасности

(Приложение Д 505-511 страницы Методических рекомендаций по использованию ЕСИА версия 3.48)

В методических рекомендациях по работе с ЕСИА отдельным разделом выделено **Приложение Д**, которое устанавливает требования безопасности для сервисов, реализованных на протоколах OAuth 2.0 и OpenID Connect 1.0. Документ содержит требования к архитектуре, инфраструктуре и защите серверной части.

Ключевые требования:

1. Использование сертифицированных СКЗИ

Информационные системы должны использовать сертифицированные ФСБ России средства криптографической защиты информации (СКЗИ) **класса не ниже КС3** (в соответствии с требованиями к защите информации в ЕСИА)

2. Использование сертифицированных средств электронной подписи (СЭП)

Все операции по подтверждению подлинности сообщений и запросов должны выполняться с использованием сертифицированных СЭП, интегрированных в архитектуру системы

3. Соответствие требованиям инфраструктурной безопасности

В инфраструктуре системы должны использоваться сертифицированные средства защиты информации, включая:

- Межсетевые экраны;
- Системы обнаружения вторжений;
- Антивирусную защиту;
- Системы мониторинга событий безопасности.
- Все средства должны быть сертифицированы ФСТЭК России или ФСБ России.

2. Размещение инфраструктуры

Серверная инфраструктура, взаимодействующая с ЕСИА, должна размещаться на территории Российской Федерации

Порядок действий при подключении

Юридическая подготовка и криптография

ЭТАП 1

Первый этап подключения связан с юридической и криптографической подготовкой организации.

Перед началом интеграции необходимо убедиться, что организация соответствует требованиям для подключения к ЕСИА

После подтверждения соответствия необходимо подготовить инфраструктуру электронной подписи.

Основные действия на этапе подготовки:

1 **Получение квалифицированного сертификата электронной подписи (СЭП)**

Организация должна получить квалифицированный сертификат ключа проверки электронной подписи в аккредитованном удостоверяющем центре. Такой сертификат используется для:

- подписания запросов к ЕСИА;
- подтверждения подлинности информационной системы;
- защищённого обмена данными

Важно: Сертификат должен быть выпущен для использования со средством электронной подписи (СЭП) класса не ниже КС3 и поддерживать алгоритмы ГОСТ (актуальные версии 2012 года). Закрытый ключ сертификата в обязательном порядке хранится на аппаратном носителе — криптографическом токене (например, Рутокен).

2 **Установка средств криптографической защиты информации (СКЗИ)**

Для работы с электронной подписью и криптографией на сервере информационной системы необходимо установить сертифицированное средство криптографической защиты информации (СКЗИ) **класса не ниже КС3**. Наиболее распространённым решением является CryptoPro CSP, поддерживающее российские криптографические алгоритмы ГОСТ.

3 **Планирование аттестационных процедур**

Важно заранее учитывать, что информационная система должна будет пройти **оценку влияния на СКЗИ** (согласно Приказу ФСБ №66*) и **аттестацию по требованиям безопасности информации** силами аккредитованных лабораторий. Это отдельные этапы, которые могут занять несколько месяцев.

*Приказ ФСБ РФ от 9 февраля 2005 г. N 66
"Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)"
С изменениями и дополнениями от: 12 апреля 2010 г.

ЭТАП 2 — РЕГИСТРАЦИЯ НА ТЕХНОЛОГИЧЕСКОМ ПОРТАЛЕ

Следующий этап — регистрация информационной системы на Технологическом портале ЕСИА.

Этот портал используется для управления параметрами интеграции и регистрации систем, которые взаимодействуют с ЕСИА.

Основные действия на этапе подготовки:

1 **Создание учетной записи организации**

Организация должна создать учётную запись на технологическом портале и подтвердить полномочия администратора системы.

2 **Регистрация информационной системы**

После регистрации организации добавляется запись информационной системы (ИС).

При этом необходимо указать ключевые параметры:

- **мнемоника системы** — уникальный идентификатор ИС;
- **алгоритм подписи** — используется алгоритм ГОСТ;
- **URL системы** — точный адрес приложения, которое инициирует авторизацию через ЕСИА.
- **области доступа (scope)** — перечень запрашиваемых данных пользователя.

Важно: Указанный URL должен **полностью совпадать** со значением параметра redirect_uri, используемого в запросах авторизации (включая протокол http/https, домен, порт и путь).

* **Redirect URI** (перенаправление URI, URL ответа) — это **URL-адрес, на который пользователь перенаправляется после успешной авторизации** в процессе аутентификации.

3 **Загрузка сертификата организации**

На портал необходимо загрузить публичный сертификат электронной подписи, полученный в удостоверяющем центре. Этот сертификат будет использоваться ЕСИА для проверки подписанных запросов от информационной системы.

ЭТАП 3 — ТЕХНИЧЕСКАЯ НАСТРОЙКА СЕРВЕРА (КРИПТОГРАФИЯ)

После регистрации информационной системы необходимо настроить криптографическую инфраструктуру сервера.

Основные действия на этапе подготовки:

1 **Установка закрытых ключей**

Закрытые ключи и сертификаты должны быть установлены в хранилище криптографического провайдера (СКЗИ). Это обеспечивает возможность:

- подписывать запросы к ЕСИА;
- шифровать передаваемые данные;
- подтверждать подлинность информационной системы.

2 **Импорт сертификатов ЕСИА**

Для проверки ответов, получаемых от ЕСИА, необходимо импортировать **публичные сертификаты головного удостоверяющего центра (ГУЦ),** которыми подписаны ответы от системы Госуслуг.

Как правило, корневые и промежуточные сертификаты распространяются в виде архива esia.zip, доступного на портале Госуслуг (или на Технологическом портале).

После установки сертификаты используются для:

- проверки цифровой подписи ответов ЕСИА;
- валидации маркеров доступа (access_token, id_token);
- обеспечения доверенного обмена данными.

3 **Проверка криптографической инфраструктуры**

Перед началом разработки необходимо проверить:

- корректность установки криптографического провайдера;
- доступность контейнеров с закрытыми ключами;
- возможность выполнения операций подписи.

ЭТАП 4 — НАСТРОЙКА СЕТИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

После настройки криптографии необходимо обеспечить сетевую и программную интеграцию системы с ЕСИА.

Основные действия на этапе подготовки:

1 **Доступ к инфраструктуре ЕСИА**

Сервер информационной системы должен иметь сетевой доступ к сервисам ЕСИА.

В**ажно учитывать, что доступ к продуктивной среде ЕСИА разрешён только с российских IP-адресов.**

2 **Настройка межсетевых экранов**

На межсетевых экранах и сетевом оборудовании необходимо добавить домены ЕСИА в список разрешённых ресурсов ("белые списки"):

- esia.gosuslugi.ru — для промышленной среды;
- esia-portal1.test.gosuslugi.ru — для тестовой среды.

Это необходимо для обеспечения стабильного соединения между информационной системой и инфраструктурой ЕСИА.

3 **Настройка параметров интеграции**

В конфигурации приложения необходимо указать параметры интеграции:

- мнемонику информационной системы;
- пути к сертификатам электронной подписи (или идентификаторы контейнеров в СКЗИ);
- адреса сервисов ЕСИА (endpoint авторизации и получения токенов);
- области доступа (scope), запрашиваемые у пользователя.

ЭТАП 5 — ТЕСТИРОВАНИЕ ИНТЕГРАЦИИ

Перед подключением к продуктивной среде ЕСИА обязательным является тестирование интеграции.

Для этого используется **тестовая среда ЕСИА.** Пример адреса тестового портала: esia-portal1.test.gosuslugi.ru

На этапе тестирования необходимо проверить ключевые сценарии взаимодействия:

- авторизация пользователя через ЕСИА;
- получение маркера доступа (access_token);
- получение данных профиля пользователя (через REST API или СМЭВ в зависимости от типа системы);
- корректность обработки ошибок.

Тестирование позволяет выявить ошибки интеграции до перехода на промышленную эксплуатацию.





Ввод системы в эксплуатацию

После успешного завершения тестирования организация может перейти к подключению к продуктивной среде ЕСИА.

Основные действия:

- Подготовка и подача заявки на подключение к продуктивной среде через Технологический портал
- Проверка корректности работы интеграции со стороны Минцифры (при необходимости)
- Подтверждение выполнения требований информационной безопасности (включая аттестацию системы и оценку влияния на СКЗИ)
- Получение доступа к продуктивным сервисам ЕСИА

После этого информационная система может использовать ЕСИА как механизм идентификации и аутентификации пользователей.

Важно: Процедуры аттестации и оценки влияния на СКЗИ могут занимать несколько месяцев, поэтому их планирование должно начинаться параллельно с технической настройкой системы.



Самостоятельная интеграция или использование готовых решений

Подключение информационной системы к ЕСИА может быть выполнено собственными силами, однако успешная реализация требует высокой технической компетенции в следующих областях:

- реализация протоколов OAuth 2.0 и OpenID Connect;
- российская криптография (алгоритмы ГОСТ);
- работа со средствами криптографической защиты информации (СКЗИ) класса КС3 и выше;
- администрирование серверной инфраструктуры и сертификатов;

Наиболее распространённые проблемы интеграции:

- несоответствие параметра redirect_uri зарегистрированному URL системы;
- ошибки формирования цифровой подписи запроса;
- неправильная установка сертификатов или использование несертифицированных СКЗИ;
- несовпадение параметров scope

В связи с высокой сложностью и ответственностью многие компании выбирают модель технологического аутсорсинга или используют готовые интеграционные решения.
Важно: применение готового решения не освобождает организацию от обязанности по аттестации системы и оценке влияния на СКЗИ — эти процедуры проводятся в инфраструктуре заказчика.



Ориентировочные сроки проекта

4–12 недель

При наличии готовой аттестованной инфраструктуры и сертифицированных СКЗИ

6–9 месяцев

Если требуется полный цикл: проектирование, закупка СКЗИ, аттестация, оценка влияния на СКЗИ (согласно Приказу ФСБ №66)

Основные этапы проекта:

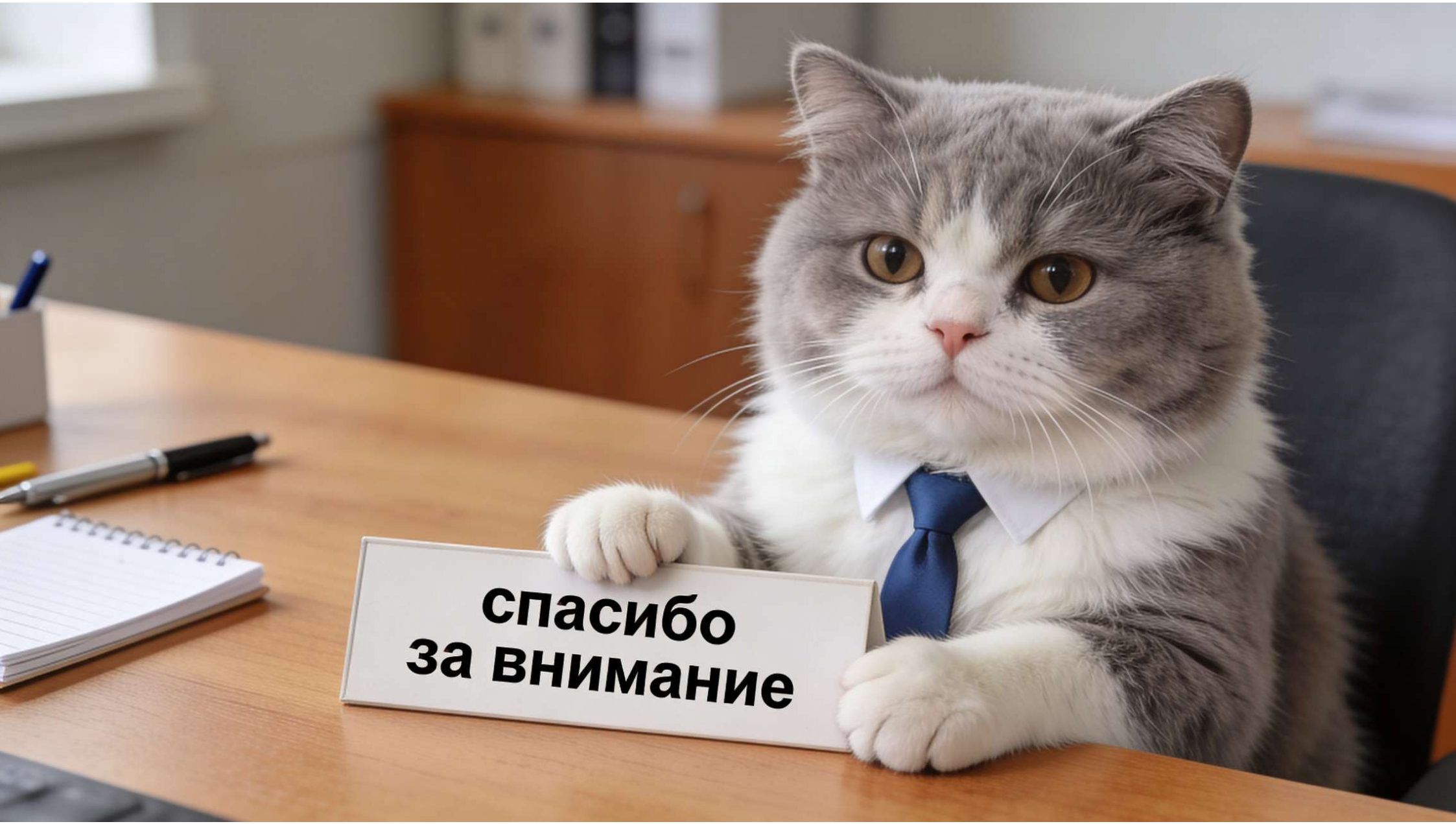
1. Получение сертификатов электронной подписи (СЭП).
2. Установка сертифицированных СКЗИ класса КС3.
3. Регистрация информационной системы на Технологическом портале.
4. Настройка криптографической инфраструктуры.
5. Тестирование в тестовой среде ЕСИА.
6. Получение доступа к продуктивной среде.

На данный момент на рынке есть готовые решения, сертифицированные Минцифрами для интеграции с ЕСИА.

Но ценник высоченный и не все компании могут это себе позволить.

Мы предлагаем рассмотреть возможность «ресселинга» доступа к ЕСИА на базе решения Эластикхостинга.

Описание решения и его детальную конфигурацию мы собираемся представить на рассмотрение в соответствующие ведомства на согласования в самое ближайшее время.


спасибо
за внимание