ЕДИНАЯ СИСТЕМА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

Методические рекомендации для государственных и муниципальных органов власти по проведению идентификации пользователей публичных беспроводных сетей Wi-Fi посредством ЕСИА

Версия 1.0

2017

Содержание

1. Назначение документа

Настоящие Методические рекомендации призваны разъяснить государственным и муниципальным органам власти, порядок обеспечения идентификации и аутентификации пользователей публичных беспроводных сетей Wi-Fi посредством механизмов ЕСИА.

Задачи идентификации пользователей с помощью ЕСИА:

- обеспечение предоставления доступа к сети Интернет в местах публичного пользования беспроводными сетями wi-fi в органах государственной и муниципальной власти и соответствие текущему законодательству;
- способствовать повышению доли граждан зарегистрированных в ЕСИА посредством популяризации ЕСИА как единого ключа к получению государственных и муниципальных услуг.

2. Нормативные документы

Настоящий документ разработан в целях реализации и во исполнение следующих нормативно-правовых актов:

- Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

- Государственная программа Российской Федерации «Информационное общество (2011 - 2020 годы)», утвержденная распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р;

- Постановление Правительства от 31 июля 2014 г. N 758 «О внесении изменений в некоторые акты правительства Российской Федерации в связи с принятием Федерального закона «о внесении изменений в федеральный закон «об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей»;

- Постановлением Правительства от 12 августа 2014 г. N 801 «О внесении изменений в некоторые акты правительства Российской Федерации»;

- Регламент информационного взаимодействия Участников с Оператором ЕСИА и Оператором инфраструктуры электронного правительства;

- Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 977 «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»;

- Постановление Правительства Российской Федерации от 25 января 2013 г. № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг»;

- Постановление Правительства Российской Федерации от 10 июля 2013 г. № 584 «Об использовании федеральной государственной информационной системы «Единая система

идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»;

- Положение «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», утверждённое постановлением Правительства Российской Федерации от 8 июня 2011 г. № 451;

- 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», утвержденное приказом Минкомсвязи России от 13 апреля 2012 г. № 107.

3. Термины и определения

ЕСИА	Единая система идентификации и аутентификации
Оператор ЕСИА	Министерство связи и массовых коммуникаций Российской Федерации
Оператор ИС	Организация, осуществляющая регистрацию и управление ИС. В качестве операторов ИС, включенных в регистр информационных систем ЕСИА, могут быть организации, обеспечивающие решение следующих задач: - предоставление государственных и муниципальных услуг; - исполнение государственных и муниципальных функций; - формирование БГИР; - межведомственное электронное взаимодействие; - иные задачи, предусмотренные федеральными законами, актами Президента РФ и актами Правительства РФ
Пользователь ЕСИА	Пользователь информационно-телекоммуникационной сети «Интернет», зарегистрированный в ЕСИА в качестве физического лица
ПЭП	Простая электронная подпись
Регламент	Регламент взаимодействия участников информационного взаимодействия с оператором ЕСИА и оператором инфраструктуры электронного правительства при организации информационно-технологического взаимодействия информационных систем с использованием ЕСИА
Центр обслуживания	Центр обслуживания органа или организации, имеющей право создания (замены) и выдачи ключа ПЭП. В Центре обслуживания специалистами Центра обслуживания осуществляется регистрация и/или подтверждение личности пользователей ЕСИА
Пользователь	Физическое лицо, получающее доступ к информационно-телекоммуникационной сети «Интернет» по технологии Wi-Fi после обязательной идентификации при помощи Системы
Интернет-провайдер	Организация, предоставляющая Клиенту услуги доступа к сети «Интернет»
ПАК	Программно-аппаратный комплекс
OAuth	Открытый протокол авторизации

4. Общее описание

Система авторизации (Далее - Система) предназначена для обеспечения процесса идентификации, авторизации, управления, контроля и учета факта использования гражданами публичных точек беспроводного доступа к сети «Интернет».

В соответствии с постановлением Правительства от 31 июля 2014 г. N 758 «О внесении изменений в некоторые акты правительства Российской Федерации в связи с принятием Федерального закона «о внесении изменений в федеральный закон «об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей» необходимо производить идентификацию пользователей, использующих публичные точки доступа к сети «Интернет». Среди возможных методов идентификации присутствует Единая система идентификации и аутентификации (ЕСИА).

Для обеспечения соответствия законодательству и удобству использования беспроводной публичной сети «Интернет» Система должна обладать рядом базовых функций.

Основные функции:

1. Инструментарий сбора статистики авторизации (идентификационных данных пользователя, время доступа и объем услуг — для исполнения требований законодательства).
2. Интеграция ИС с ЕСИА.
3. Создание и регистрация точки доступа в Системе.
4. Активация/деактивация точек доступа.
5. Настройка конфигурации точки доступа.
6. Создание объекта (группы точек доступа с едиными настройками).
7. Тестирование точек доступа на доступность соединения.
8. Создание новой учетной записи пользователей Системы.
9. Назначение прав доступа пользователям Системы.

Дополнительные возможности:

1. Настройка дизайна страницы авторизации для объекта.
2. Инструментарий аналитики.
3. Возможность отображения информационных сообщений на экране входа.
4. Электронная очередь для МФЦ (когда посетитель может на экране входа заказать электронный талон на получение услуги создания/подтверждения учетной записи в ЕСИА).
5. Кроссавторизация пользователей между точками (сохранение сессии авторизации, при переходе пользователя, например, из одного МФЦ в другое, в пределах допустимого времени жизни сессии авторизации).

4.1 Типовая архитектура системы авторизации

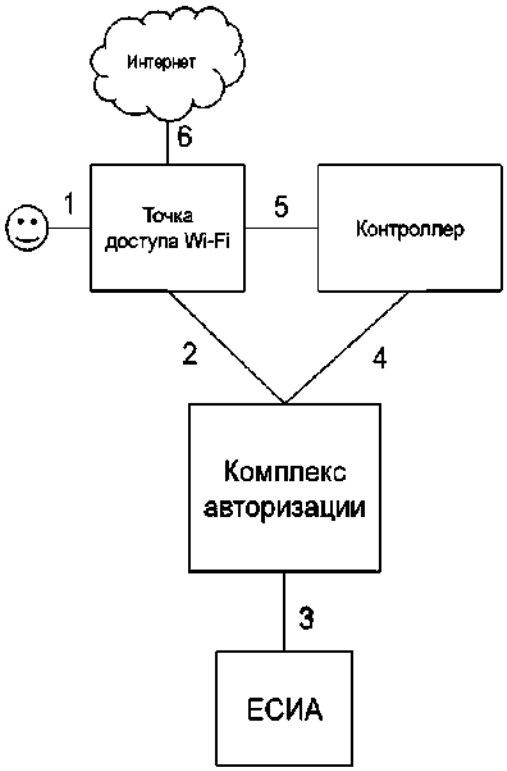


Рисунок 1

На рисунке 1. изображено схематическое представление архитектуры комплекса авторизации с помощью ЕСИА.

Сценарий работы:

1. Пользователь подключается к Wi-Fi.
2. Точка обращается к комплексу авторизации, который инициирует процесс входа через Госуслуги (ЕСИА).
3. Пользователь авторизуется через ЕСИА.
4. Комплекс авторизации сообщает Контроллеру, что авторизация прошла успешно и можно предоставить доступ к сети «Интернет».
5. Контроллер разрешает данному пользователю доступ к сети «Интернет» на данной точке.
6. Точка предоставляет пользователю доступ к сети «Интернет».

Пользователь, с помощью своего устройства, подключается к публичной WiFi-сети. Точка доступа с помощью параметров устройства определяет имеется ли устройство в базе данных комплекса авторизации или нет, определяет доступный тайм аут (время жизни сессии авторизации - время которое пользователь может не авторизоваться повторно) если устройство уже имеется в базе и тайм аут не истек, то происходит мгновенная авторизация и может быть предоставлен

доступ к сети «Интернет». В случае первичного подключения к точке доступа, доступ к сети «Интернет» до момента авторизации через ЕСИА не предоставляется.

Контроллер в данной схеме выдает точке права доступа к сети «Интернет» на основании полученных от комплекса авторизации команд.

4.2 Типовые схемы подключения

1) Типовая схема подключения с использованием шлюза ЕСИА

Шлюз ЕСИА выступает внешней по отношению к системе идентификации системой и позволяет подключаться к ЕСИА другие информационные системы и является центральным звеном авторизации в сети органа власти.

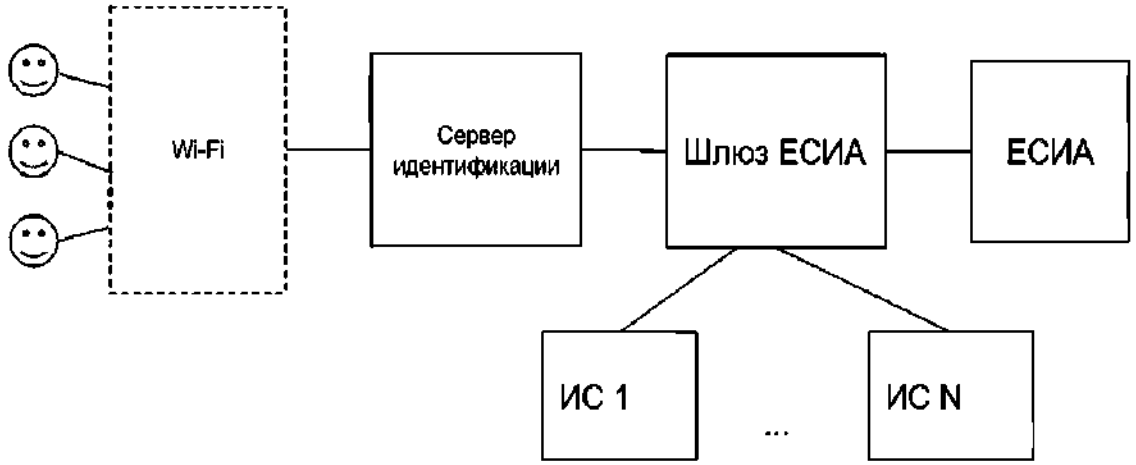


Рисунок 2

2) Типовая схема подключения с использованием встроенного модуля работы с ЕСИА

При данной схеме подключения в система идентификации интегрируется с ЕСИА напрямую

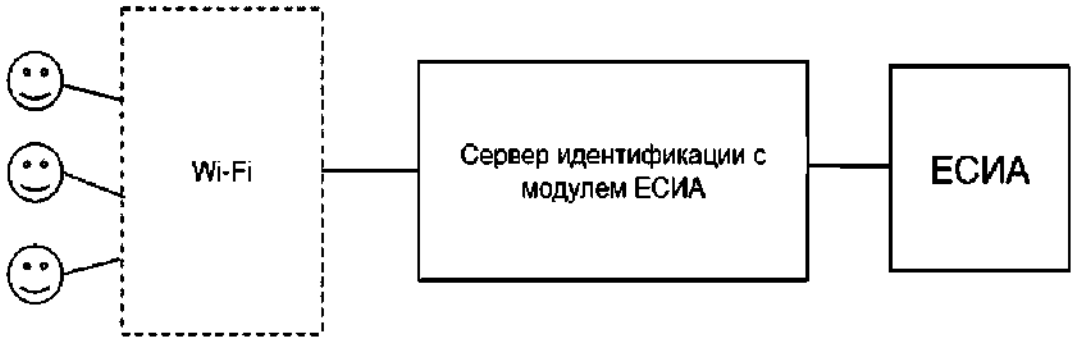


Рисунок 3

4.3 Рекомендации по программному обеспечению

На текущий момент распространены два формата поставки программного обеспечения для идентификации:

a) “Коробочное” программное обеспечение. Приобретается специализированное ПО, обеспечивающее идентификацию на точках доступа. В этом случае нужно обеспечивать и поддерживать инфраструктуру, где будет функционировать данное решение, но при этом не лимитируется количество подключаемых точек доступа. Данный вариант допустим в случаях, когда число точек больше 30-40 штук и если неудобна модель с абонентской платой за каждую точку.

b) “Облачный сервис” - в этом случае оплата производится за каждую подключенную точку за период (месяц/год), но все вопросы обеспечения функционирования на себя берет оператор системы. Такой подход удобен в случае небольшого количества точек на сети (до 20-30 шт.).

4.3.1 Типовые рекомендации по функциональности программного обеспечения идентификации:

- возможность предоставления доступа к сети «Интернет» в сетях ОГВ или ОМСУ с использованием пунктов коллективного доступа после проведения идентификации пользователей через ЕСИА;
- возможность предоставления доступа к сети «Интернет» в сетях ОГВ или ОМСУ только абонентам, имеющим подтвержденную учетную запись ЕСИА;
- ведение списка сетевых идентификаторов устройства для пропуска в сеть «Интернет» без повторной авторизации;
- система регистрации статистики посещений с возможностью получения отчета об использовании доступа по заданному интервалу времени и сетевому идентификатору пользователя;
- хранение сведений о пользователях (фамилия, имя, отчество (при наличии), реквизиты основного документа, удостоверяющего личность), которым были оказаны универсальные услуги связи по передаче данных и предоставлению доступа к сети «Интернет» с использованием пунктов коллективного доступа, а также об объеме и времени оказания им услуг связи в течении 6 месяцев;
- возможность выгрузки отчётов о пользователях (фамилия, имя, отчество (при наличии), реквизиты основного документа, удостоверяющего личность), которым были оказаны универсальные услуги связи по передаче данных и предоставлению доступа к сети «Интернет» с использованием пунктов коллективного доступа;
- возможность настройки внешнего вида экрана входа;
- функционал работы с точками (создание, настройка, включение, выключение, удаление, редактирование);
- кроссавторизация пользователей — если пользователь уже проходил авторизацию на одной из точек сети, подключенных к Системе, то на другой точке Система его “помнит” и не требует снова проходить процесс авторизации.

4.3.2 Рекомендации по Личному кабинету Администратора Системы

Кабинет администратора предоставляет следующие возможности;

- добавление и изменение параметров подключения точек доступа;
- управление объектами на которых установлены точки (создание, удаление);
- просмотр сводной информации по объектам и в разрезе каждого объекта (отчетность);
- управление точками доступа (добавление устройств и редактирование параметров);
- редактирование дизайна страницы авторизации с возможностью предпросмотра на экранах мобильных телефонов, планшетов, ПК;
- управление информационными сообщениями и графиком их показа на странице авторизации с возможностью предпросмотра на экранах мобильных телефонов, планшетов, ПК;
- формирование статистической отчетности с информацией о том, какие пользователи, с каких устройств, когда авторизовывались и сколько они были в сети, а также необходимые идентификационные данные.

4.3.3 Рекомендации по процессу предоставления доступа к сети «Интернет»

При регистрации нового пользователя в сети ОГВ или ОМСУ и первой попытке использования Интернет ресурсов в браузере, Система осуществляет перенаправление на страницу авторизации.

Далее пользователь нажимает кнопку «Войти через Госуслуги» после чего он будет направлен на страницу ввода логина и пароля ЕСИА - Рисунок 4.

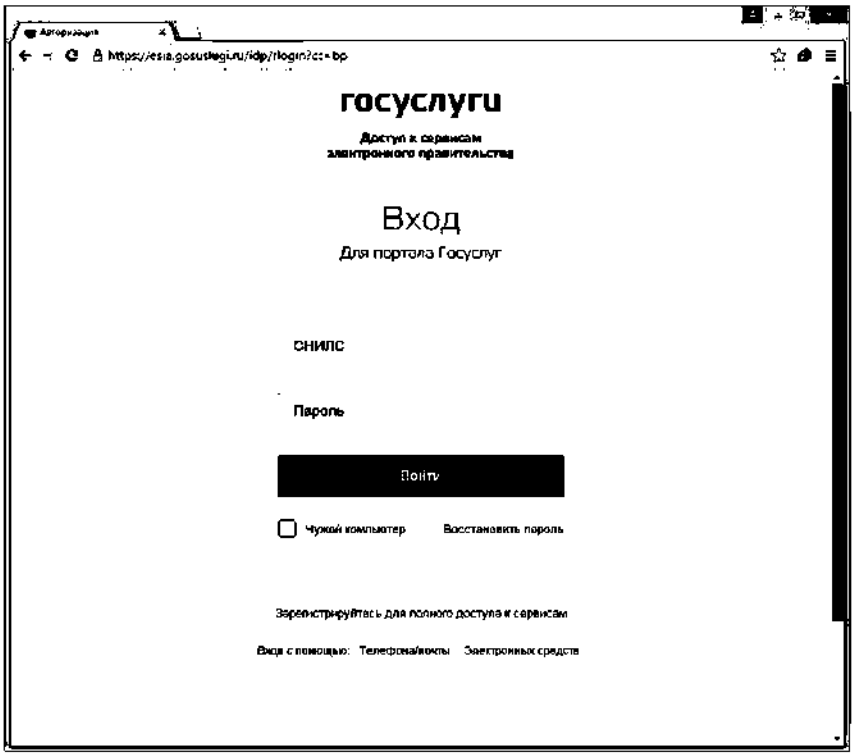


Рисунок 4. Страница авторизации ЕСИА

После успешной авторизации и проверки, что учётная запись ЕСИА является подтверждённой, пользователю будет предоставлен доступ к сети «Интернет».

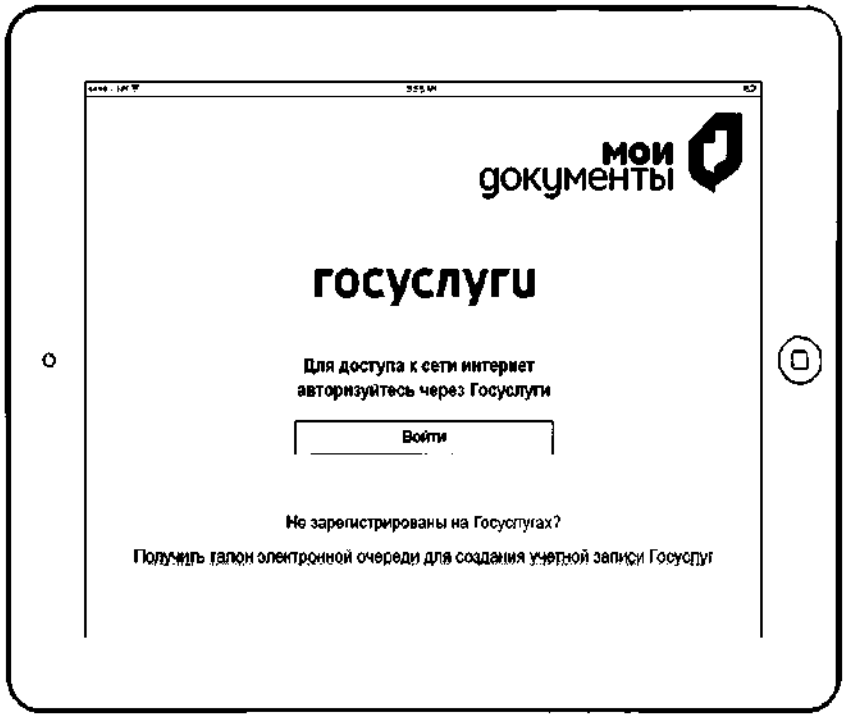
При этом идентификационные данные пользователя сохраняются в Системе.

По завершению сеанса Система сохраняет информацию об объеме и времени оказания услуг связи пользователю.

4.3.4 Рекомендации к интерфейсу экрана идентификации

Рекомендуемое расположение элементов экранных форм для смартфонов и планшетов указано ниже. При оформлении экранных форм рекомендуется стилистическое оформление из брендбука Госуслуг.


госуслуги
Для доступа к сети интернет
авторизуйтесь через Госуслуги
Войти
Не зарегистрированы на Госуслугах?
Ближайший центр регистрации


мои
документы
госуслуги
Для доступа к сети интернет
авторизуйтесь через Госуслуги
Войти
Не зарегистрированы на Госуслугах?
Получить талон электронной очереди для создания учетной записи Госуслуг

4.4 Этапы организации подключения

Общие шаги по организации идентификации посредством ЕСИА при организации беспроводного коллективного доступа к сети «Интернет»:

1. Определиться с количеством и географической распределенностью точек доступа (физических роутеров), на которых предполагается организовать коллективные пункты доступа к сети «Интернет».
2. Определить, будут ли для этого использоваться уже имеющиеся устройства, или предполагается закупать новые. Решение о использовании текущего или закупке нового оборудование принимается на основании требований к аппаратному обеспечению беспроводных устройств. При этом следует учитывать, что не все типы роутеров поддерживают функцию внешней авторизации (Captive portal). Также, разнотипное оборудование порождает большое число ошибок авторизации, при этом как правило стоимость обслуживания существенно вырастает.
3. Определится с типовой схемой подключения в зависимости от варианта интеграции с ЕСИА.
4. Сформировать требования к ПО или услуге в виде технического задания. Целесообразно консультироваться для составления ТЗ с представителями организаций, предоставляющих схожие услуги или ПО, по запросам в поисковых системах словосочетаний, например: “ЕСИА Wi-Fi”, “Wi-Fi Госуслуги”.
5. Выполнить регламентные процедуры подключения к ЕСИА, согласно методическим рекомендациям, раздел 4.6.
6. Разместить конкурс/аукцион по закупке ПО или услуг.
7. Развернуть систему или подключить сервис, настроить соединение с интернетом беспроводной сети доступа.

4.4.1 Общие рекомендации при выборе ПО/услуг:

При выборе программного обеспечения необходимо ориентироваться на ПО, входящее в реестр Минсвязи РФ в соответствии со статьей 12.1 Федерального закона «Об информации, информационных технологиях и о защите информации» в целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из Российской Федерации, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки.

При выборе облачного решения рекомендуется включить в состав технического задания требование наличие у оператора облачного сервиса соглашения об уровне обслуживания (SLA) которое определяет набор гарантируемых параметров качества Сервиса и устанавливает для них соответствующие гарантируемые пороговые значения, условия, дающие право органу власти на получение перерасчёта, а также описывает процедуры, связанные с устранением неисправностей, проведением плановых и неотложных ремонтных работ и сервисной поддержкой.

Идентификация пользователей публичных беспроводных точек доступа к сети «Интернет» может осуществляться как самим ОГВ или ОМСУ путем приобретения соответствующего ПО или услуг, так и посредством заказа таких услуг у оператора связи.

4.5 Рекомендации по аппаратному обеспечению

4.5.1 Рекомендации по аппаратным средствам

Для ПАК с коробочном исполнении работоспособность Системы авторизации может быть обеспечена на оборудовании, с характеристиками эквивалентными или выше следующих: процессор - 1 процессор, 2 ядра 2.53 GHz, ОЗУ 4Gb, HDD 80 Gb,из расчета ~ 10000 авторизаций в день.

4.5.2 Рекомендации по каналам связи

Подключение ПАК авторизации к сети с пропускной способностью канала не менее 2 Мбит/с.

4.6 Требования к информационной безопасности

Подсистема обеспечения информационной безопасности должна обеспечивать уровень защиты по классу информационных систем персональных данных К1, в соответствии с Приказом ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» и требованиями Постановления Правительства Российской Федерации от 01 ноября 2012 года №1119.

4.7 Рекомендации по процедуре подключения Системы к Единой системе идентификации и аутентификации

Система должна соответствовать актуальному на момент заключения контракта регламенту информационного взаимодействия Участников с Оператором ЕСИА и Оператором инфраструктуры электронного правительства и методическим рекомендациям по использованию Единой системы идентификации и аутентификации.

http://minsvyaz.ru/ru/documents/4244/

http://minsvyaz.ru/ru/documents/4243/

Система должна быть интегрирована с ЕСИА посредством протокола OAuth 2.0 и, в соответствии с положениями Правительства от 31 июля 2014 г. N 758 и от 12 августа 2014 г. N 801, получать из ЕСИА и хранить, следующие данные: ФИО, серию и номер документа удостоверяющего личность абонента, а также степень достоверности учетной записи (простая, стандартная, подтвержденная).

4.8 Рекомендации по документированию

По результатам Поставки Исполнитель должен предоставить комплект документов, необходимых для эксплуатации Системы и отразить её текущее состояние.

Комплект документов, разрабатывается на русском языке и в минимальной поставке должно состоять:

Для программного продукта идентификации

№ п.п.	Наименование документа
1.	Спецификация на программный продукт
2.	Руководство администратора
3	Программа и методика испытания системы
4.	Лицензионное соглашение (договор)

Для услуг облачного сервиса идентификации

№ п.п.	Наименование документа
1.	Спецификация на сервис идентификации
2.	Руководство администратора
3	Программа и методика испытания системы
4.	Соглашение об уровне обслуживания (SLA)
5.	Лицензионное соглашение (договор)