

Сведения об эксплуатации экземпляра программы

Универсальный выделенный модуль управления персональными данными “Forward PDM”

Forward PDM (Personal Data Management) – Универсальный выделенный модуль управления персональными данными (Personal Data Management) предназначен для изоляции процессов хранения и обработки персональных данных в выделенном защищенном модуле реализующем как установленное законодательством взаимодействие с субъектом персональных данных и оператором, так и процессы обработки персональных данных, логирование производимых с персональными данными операций, а также операции по их отправке в специализированные информационные системы, например в случаях установленных законодательством и проведение верификации путем сравнения с персональными данными, хранящимися в специализированных информационных системах, в том числе государственных.

Модуль позволяет добавить необходимую функциональность к любой информационной системе и организовать работу с персональными данными без передачи их в информационную систему, не предназначенную для работы с персональными данными пользуясь универсальными идентификаторами, не содержащими персональной информации, при этом необходимый доступ к персональным данным осуществляется через предоставление специального интерфейса субъекту персональных данных и оператору.

Использование системы будет максимально полезно для операторов связи и других услуг, служб, осуществляющих обработку персональных данных и т.д., которые хотят получить быструю, надежную и удовлетворяющую требованиям законодательства систему работы с персональными данными. Система поддерживает кластерное масштабирование и может использоваться в распределенных сетях крупных федеральных и региональных компаний, операторов связи и других информационных систем.

Контактная информация: support@fw-t.ru

1 Общая информация

Forward PDM предназначена для централизованного, безопасного управления персональными данными с полным контролем доступа и детальным аудитом всех операций. Она позволяет изолировать хранение и обработку ПДн в выделенном защищенном модуле, предоставляя внешним системам доступ через неперсонифицированные идентификаторы.

Система обеспечивает:

1. Гибкую модель данных – возможность создания произвольных типов документов с произвольными атрибутами и правилами валидации.
2. Детализированное управление доступом – ролевая модель с модификаторами доступа на уровне типов и экземпляров сущностей.
3. Изоляцию хранения и обработки ПДн – персональные данные хранятся в защищенном модуле, внешние системы работают с неперсонифицированными идентификаторами.
4. Аудит операций – неизменяемый журнал аудита действий с ПДн, соответствующий требованиям законодательства.
5. Интеграцию через REST API – унифицированный интерфейс для взаимодействия с внешними системами.
6. Web-интерфейс – функциональность управления системой через браузер.

2 Эксплуатация системы

2.1 Общая концепция работы

Система PDM реализует гибкую модель управления персональными данными, основанную на разделении типов и экземпляров сущностей. Все операции в системе контролируются детализированной системой прав доступа и сопровождаются обязательным аудитом.

2.2 Вебсервисы PDM

PDM предоставляет следующие веб-сервисы (REST API)

2.2.1 REST API для внешних систем

Основной интерфейс взаимодействия, предоставляющий методы для:

- Работы с субъектами ПДн;
- Управления документами и данными документов;
- Загрузки и выгрузки файлов документов;
- Верификации персональных данных;
- Получения журнала аудита (для пользователей, имеющих уполномоченные роли).

2.2.2 Внутренние API для межсервисного взаимодействия

Интерфейсы для взаимодействия сервисов PDM между собой:

- API сервиса PDM для маршрутизации запросов и операций с базой данных;
- API сервиса Auditor Service для записи событий аудита;

2.2.3 Интеграционные API

Интерфейсы для взаимодействия с внешними системами:

- API для интеграции с Keycloak (аутентификация и синхронизация ролей);
- API для работы с объектным хранилищем S3.

2.3 PDM-процесс

Обработка персональных данных в системе PDM осуществляется через выделенный защищенный модуль. Внешние информационные системы не получают прямой доступ к ПДн, а взаимодействуют через универсальный REST API, используя неперсонифицированные идентификаторы.

Работа с ПДн включает следующие процессы:

2.3.1 Настройка модели данных и правил доступа

Перед началом работы с персональными данными необходимо настроить модель данных и правила доступа:

- Создание типов документов – определение структуры документов (паспорт, водительское удостоверение и т.д.)
- Создание типов атрибутов – определение форматов и свойств полей данных (ФИО, номер, серия)
- Определение правил валидации – настройка проверок корректности данных (регулярные выражения, диапазоны, форматы)
- Настройка связей – связывание типов документов с типами атрибутов
- Настройка ролей и модификаторов доступа – определение прав ролей пользователей на работу с сущностями (при этом аутентификация пользователей и привязка к ним ролей осуществляется в Keycloak, а PDM на основе полученных ролей и политик доступа разрешает или запрещает операции с сущностями).

2.3.2 Регистрация субъектов и работа с документами

После настройки модели данных осуществляется работа с персональными данными:

- Регистрация субъекта ПДн – создание записи о физическом лице в системе
- Создание документов – добавление документов, связанных с субъектом
- Заполнение данных документа – внесение персональных данных в соответствии с типом документа
- Загрузка файлов документов – прикрепление сканов/фотографий документов в объектное хранилище

2.3.3 Интеграция с внешними системами

Внешние системы взаимодействуют с PDM через REST API:

- Получение данных – запрос информации о субъектах и документах через неперсонифицированные идентификаторы
- Обновление данных – модификация ПДн с проверкой прав доступа и обязательной фиксацией в журнале аудита

2.3.4 Аудит и мониторинг

Все операции сопровождаются обязательным аудитом:

- Фиксация событий – запись всех действий с ПДн в журнал аудита
- Мониторинг доступа – контроль попыток несанкционированного доступа

2.4 Жизненный цикл данных в PDM

2.4.1 Создание и настройка метаданных

Типы документов и атрибутов

Перед началом работы с персональными данными необходимо настроить структуру данных:

- Тип документа определяет схему документа (например, "Паспорт РФ", "Водительское удостоверение"). Каждый тип документа содержит:

Наименование типа

Схему документа (набор связанных атрибутов)

- Тип атрибута определяет свойства отдельного поля данных (например, "Фамилия", "Номер паспорта", "Дата рождения"). Характеристики типа атрибута:

Наименование

Тип данных (STRING, NUMBER, DATE и т.д.)

Связывание типов документов и атрибутов

Для формирования схемы документа необходимо создать связи между типом документа и типами атрибутов. Каждая связь включает:

- Обязательность: требование обязательного заполнения атрибута;
- Уникальность: требование уникальности значения атрибута в рамках документа.

Примечания:

Настройка не распространяется на другие Типы документов.

Флаг уникальности может быть установлен на несколько атрибутов одновременно. В этом случае система обеспечивает уникальность их совместного значения, в то время как значения каждого атрибута по отдельности могут повторяться. Например: для типа документа «Паспорт» можно установить единый флаг уникальности на атрибуты «Серия» и «Номер». Система не допустит двух паспортов с одинаковой комбинацией *Серия=0302, Номер=123456*, но при этом допускает множество документов с серией 0302 и множество документов с номером 123456.

Правила валидации

Для обеспечения корректности данных система поддерживает правила валидации для контроля целостности данных, правило задается для атрибута в рамках конкретного типа документа:

- Регулярное выражение: проверка соответствия шаблону (регулярное выражение);
- Длина строки: проверка длины строкового значения (равна, не равна, больше, меньше, не меньше, не больше);
- Наличие подстроки: проверка наличия подстроки в значении (искомая подстрока);

- Сравнение с датой: проверка даты относительно фиксированного значения (дата, оператор сравнения);
- Проверка численного значения: проверка числового значения (число, оператор сравнения).

Операторы сравнения (для правил с датами и числами):

- EQ – равно
- NE – не равно
- GT – больше
- LT – меньше
- GE – больше или равно
- LE – меньше или равно

2.4.2 Наполнение сущностей данными

Создание субъекта ПДн

Субъект представляет физическое лицо, чьи персональные данные обрабатываются в системе:

- Идентификатор субъекта – уникальный идентификатор, генерируемый системой;
- Дата регистрации – дата и время создания записи о субъекте;
- Дата последнего обновления – дата и время последнего изменения;
- Дата окончания действия – дата окончания разрешения на обработку ПДн;
- Статус – текущее состояние записи.

Создание документа

Документ связывает субъекта с конкретным набором персональных данных определенного типа:

- Идентификатор документа – уникальный идентификатор, генерируемый системой;
- Идентификатор субъекта – ссылка на субъекта ПДн;
- Идентификатор типа документа – тип создаваемого документа;
- Идентификатор модификатора доступа – правила доступа к документу;
- Дата создания – дата и время создания документа;
- Дата окончания действия – дата окончания действия документа;
- Статус – текущее состояние документа.

Данные документа

Фактические персональные данные хранятся в БД.

Файлы документа

Метаданные хранятся в БД. Для хранения сканов/фотографий документов используется объектное хранилище S3:

- Идентификатор документа – ссылка на документ;
- Путь к файлу в S3 – путь к файлу в объектном хранилище;
- Идентификатор модификатора доступа – правила доступа к файлу.

2.4.3 Управление доступом

Ролевая модель

Система использует детализированную ролевую модель доступа. Каждый пользователь имеет набор ролей, определяющих его права в системе.

Модификаторы доступа

Глобальные модификаторы определяют права на уровне типов сущностей:

- Право на создание/чтение/обновление/удаление типов сущностей;
- Применяются ко всем экземплярам данного типа.

Локальные модификаторы определяют права на уровне конкретных экземпляров:

- Расширяют права, определенные глобальными модификаторами.

2.4.4 Алгоритм проверки прав доступа

Для операций с типами сущностей:

- Проверяется наличие у пользователя прав в глобальном модификаторе доступа
- При отсутствии прав операция блокируется.

Для операций с экземплярами сущностей:

- Проверяются права в глобальном модификаторе доступа
- При недостаточности прав проверяются права в локальном модификаторе
- Для субъектов проверяются глобальные, а после – локальные модификаторы.

2.4.5 Синхронизация ролей с Keycloak

Архитектура взаимодействия

Keycloak – master-система для хранения ролей и аутентификации пользователей

PDM – использует роли из Keycloak для авторизации операций

Периодическая синхронизация (Keycloak → PDM)

Выполняется автоматически по расписанию (переменная окружения `fixedDelay.rolesync`):

- Роли с атрибутом `pdn_role="true"` импортируются в PDM

- Измененные роли обновляются в PDM
- Удаленные из Keycloak роли удаляются из PDM

Событийная синхронизация (PDM → Keycloak)

Выполняется при операциях управления ролями в PDM:

- Проверка прав пользователя на операцию с ролью
- Выполнение операции в Keycloak (с установкой `pdn_role="true"`)
- При успехе – выполнение операции в PDM

2.4.6 Журнал аудита

Типы событий в журнале аудита:

- Регулярные события – все операции в системе;
- События с нарушениями – операции, завершившиеся из-за нарушения прав доступа;
- События с системными ошибками – внутренние ошибки системы;
- События чтения журнала – факты обращения к журналу аудита.

2.4.7 Статусы сущностей и управление жизненным циклом

Статусы документов и субъектов

- Активный – А – запись активна и доступна для операций;
- Удалённый – D – запись удалена, но сохраняется для историчности;
- К удалению – TD – запись помечена для удаления, обрабатывается как удаленная.

Типы удаления данных

Логическое удаление:

- Запись помечается статусом D или TD;
- Данные сохраняются в базе для обеспечения историчности;
- Невозможно проведение новых операций с записью.

Физическое удаление:

- Полное удаление записи из базы данных;
- Доступно только пользователям с соответствующими правами;
- Применяется в случаях, предусмотренных политикой обработки ПДн.

2.5 Управление настройками и конфигурированием PDM

WEB интерфейс состоит из следующих специализированных справочников (страниц) вида:

Personal Data

Данные ▾

Безопасность ▾

Справочники ▾

Список документов

Поиск по ID

→

Поиск по внешнему

Owner

→

▼

Тип документа

▼

Тип атрибута

Значение атрибута

→

×

ID	Тип документа	Время создания	Время окончания	Статус
152	ОДК	2024-11-25 00:00:00	2500-01-01 00:00:00	A
153	Паспорт	2024-11-25 00:00:00	2500-01-01 00:00:00	A
154	ОДК	2024-05-28 00:00:00	2034-05-28 00:00:00	A
155	ОДК	2024-05-28 00:00:00	2034-05-28 00:00:00	A
158	ОДК	2024-05-28 00:00:00	2034-05-28 00:00:00	A

1

Всего: 5

2.5.1 Валидация

Справочник Правила валидации предназначен для создания и управления условиями проверки корректности данных в документах, обеспечивая соблюдение заданных форматов и ограничений

Добавить новый

Список правил валидации

ID	Описание	Тип	Правило	Флаг
52	4 цифры	Регулярное выражение	^\d{4}\$	
53	6 цифр	Регулярное выражение	^\d{6}\$	
54		Длина строки	1	Больше или равно
55	0 или 1	Регулярное выражение	^[01]\$	

1

Всего: 4

Интерфейсы Добавления, Обновления и Удаления Правил валидации доступны при наличии соответствующих Глобальных прав доступа

Правило валидации

Описание правила валидации *

Тип правила валидации *

Правило валидации

Флаг сравнения правила валидации

Создать

Отменить

2.5.2 Типы документа

GRID-справочник по всем полям Типа документа. Наполняется в случае наличия соответствующего Глобального модификатора доступа.

Добавить новый

Список типов документов

ID	Имя	Псевдоним
102	ОДК	ОДК
103	Паспорт	passport
104	тест	test

1 Всего: 3

Интерфейсы Добавления, Обновления и Удаления Типов документа доступны при наличии соответствующих Глобальных прав доступа.

Тип документа

Имя типа документа *

Псевдоним (alias) типа документа *

Атрибуты документа

+ Добавить

Создать

Заккрыть

2.5.3 Типы атрибутов

GRID-справочник по всем полям Типа атрибута. Наполняется в случае наличия соответствующего Глобального модификатора доступа.

[Добавить новый](#)

Список типов атрибутов

ID	Имя	Тип
52	Серия	Строка
53	Номер	Строка
54	Орган выдавший документ	Строка
55	Дата выдачи документа	Дата/Время
56	Код подразделения, выдавший документ	Строка
57	Дата начала действия документа	Дата/Время
58	Дата окончания действия документа	Дата/Время
59	Имя	Строка
60	Отчество	Строка
61	Фамилия	Строка

1 2 3 > >> Всего: 25

Интерфейсы Добавления, Обновления и Удаления Типов атрибута доступны при наличии соответствующих Глобальных прав доступа.

Тип атрибута

Имя типа атрибута *

Тип данных *

[Создать](#)[Отменить](#)

2.5.4 Связь Типа документа и Типа атрибута

GRID-справочник по всем полям Связи Типа документа и Типа атрибута + существующие Правила валидации. Наполняется в случае наличия соответствующего Глобального модификатора доступа для Связи и Глобального модификатора доступа для Правил валидации.

[Добавить новый](#)

Список связей между документами, атрибутами и правилами валидации

ID	Тип документа	Тип атрибута	Правила валидации	Обязательная связь	Часть составного ключа
102	Паспорт	Серия	• 4 цифры	☒	☒
103	Паспорт	Номер	• 6 цифр	☒	☒
104	Паспорт	Орган выдавший документ		☒	☐
105	Паспорт	Дата выдачи документа		☒	☐
106	Паспорт	Код подразделения, выдавший документ		☒	☐
107	Паспорт	Дата начала действия документа		☐	☐
108	Паспорт	Дата окончания действия документа		☐	☐
109	ОДК	Имя		☒	☒
110	ОДК	Отчество		☐	☒
111	ОДК	Фамилия		☒	☒

Интерфейсы Добавления, Обновления и Удаления Связи доступны при наличии соответствующих Глобальных прав доступа.

Связь между документом, атрибутами и правилами валидации

Тип документа *

Тип атрибута *

Правила валидации

[52] 4 цифры
[53] 6 цифр
[54]
[55] 0 или 1

Обязательная связь

☐

Часть составного ключа

☐

Создать

Отменить

В интерфейсе Добавления / Обновления Связи должен содержаться интерфейс Добавления / Обновления Правил валидации.

Интерфейс Добавления / Обновления Правила валидации содержит параметры, актуальные для Правил валидации.

2.5.5 Роли

GRID-справочник по всем полям Ролей. Наполняется в случае наличия соответствующего Глобального модификатора доступа.

Personal Data

Данные ▾

Безопасность ▾

Справочники ▾

Добавить

Список ролей

ID	Имя	Описание
52	ACCESS_MODIFIER_CREATOR	
53	ACCESS_MODIFIER_DELETER	
54	ACCESS_MODIFIER_READER	
55	ACCESS_MODIFIER_UPDATOR	
56	ATTRIBUTE_INST_CREATOR	
57	ATTRIBUTE_INST_DELETER	
58	ATTRIBUTE_INST_READER	
59	ATTRIBUTE_INST_UPDATOR	
60	ATTRIBUTE_TYPE_CREATOR	
61	ATTRIBUTE_TYPE_DELETER	
62	ATTRIBUTE_TYPE_READER	
63	ATTRIBUTE_TYPE_UPDATOR	

Интерфейсы Добавления, Обновления и Удаления Роли доступны при наличии соответствующих Глобальных прав доступа.

2.5.6 Модификаторы доступа

GRID-справочник по всем полям Модификаторов доступа. Наполняется в случае наличия соответствующего Глобального модификатора доступа.

Список глобальных модификаторов доступа

ID	Тип модификатора	Роли
52	Документ	- Create: [77] DOCUMENT_INST_CREATOR - Read: [79] DOCUMENT_INST_READER - Update: [80] DOCUMENT_INST_UPDATOR - Delete: [78] DOCUMENT_INST_DELETER
53	Аттрибут	- Create: [56] ATTRIBUTE_INST_CREATOR - Read: [58] ATTRIBUTE_INST_READER - Update: [59] ATTRIBUTE_INST_UPDATOR - Delete: [57] ATTRIBUTE_INST_DELETER
54	Данные документа	- Create: [69] DOCUMENT_DATA_CREATOR - Read: [71] DOCUMENT_DATA_READER - Update: [72] DOCUMENT_DATA_UPDATOR - Delete: [70] DOCUMENT_DATA_DELETER
55	Файл документа	- Create: [73] DOCUMENT_FILE_CREATOR - Read: [75] DOCUMENT_FILE_READER - Update: [76] DOCUMENT_FILE_UPDATOR - Delete: [74] DOCUMENT_FILE_DELETER

Интерфейсы Добавления, Обновления и Удаления Модификатора доступа доступны при наличии соответствующих Глобальных прав доступа.

2.5.7 Субъекты

GRID-справочник по всем полям Субъектов. Наполняется в случае наличия соответствующего Глобального модификатора доступа + При соответствии Локальных модификаторов доступа.

Добавить

Список субъектов

Поиск по ID	Q	→	Поиск по вне	Owner	Q	→
ID	Время регистрации	Время окончания	Статус	Документы		

Интерфейсы Добавления, Обновления и Удаления Субъекта доступны при наличии соответствующих Глобальных прав доступа.

Субъект

Время регистрации *

ДД.ММ.ГГГГ --:--



Время

окончания *

ДД.ММ.ГГГГ



Статус *

Активный

Внешние идентификаторы

Добавить

Создать модификатор доступа ▾

Создать

Отменить

2.5.8 Документы

GRID-справочник по всем полям Документов. Наполняется в случае наличия соответствующего Глобального модификатора доступа + При соответствии Локальных модификаторов доступа.

Список документов

Поиск по ID



Поиск по внеi

Owner



Тип документа



Тип атрибута

Значение атрибута



ID	Тип документа	Время создания	Время окончания	Статус
152	ОДК	2024-11-25 00:00:00	2500-01-01 00:00:00	A
153	Паспорт	2024-11-25 00:00:00	2500-01-01 00:00:00	A
154	ОДК	2024-05-28 00:00:00	2034-05-28 00:00:00	A
155	ОДК	2024-05-28 00:00:00	2034-05-28 00:00:00	A
158	ОДК	2024-05-28 00:00:00	2034-05-28 00:00:00	A

1

Всего: 5

Интерфейсы Добавления, Обновления и Удаления Документа доступны при наличии соответствующих Глобальных прав доступа.

Данные документа

GRID-справочник по всем полям Данных документа. Наполняется в случае наличия соответствующего Глобального модификатора доступа + при соответствии Локальных модификаторов доступа Документа + данных документа + атрибутов документа (некоторые поля будут принимать значение null).

Personal Data Данные ▾ Безопасность ▾ Справочники ▾

Документ [152]

ID субъекта
152

Тип документа * [102] ОДК	Время создания * 25.11.2024 00:00 📅	Время окончания * 01.01.2500 📅	Статус * Активный
-------------------------------------	---	--	-----------------------------

Внешние идентификаторы Добавить

Создать модификатор доступа ▾

Добавить данные документа

Интерфейсы Добавления, Обновления и Удаления Данных документа доступны при наличии соответствующих Глобальных прав доступа + Локальных прав доступа.

Интерфейсы Обновления и Удаления доступны при наличии соответствующих Локальных прав доступа.

Интерфейс Обновления Данных документа содержит все Атрибуты документа, доступные для ЧТЕНИЯ. При этом Атрибуты документа, чьи Модификаторы доступа запрещают редактирование – заблокированы (readonly).

Файлы документа

GRID-справочник по всем полям Файлов документа. Наполняется в случае наличия соответствующего Глобального модификатора доступа + При соответствии Локальных модификаторов доступа Документа + Файлов документа.

Создать модификатор доступа ▾

Добавить данные документа

Файлы документа

Добавить новый файл

Выберите файл

Файл не выбран

Загрузить

Очистить

Обновить

Отменить

При этом поле с Файлом документа поддерживает возможность скачивания исходного Файла.

Интерфейсы Добавления, Обновления и Удаления Данных документа доступны при наличии соответствующих Глобальных прав доступа + Локальных прав доступа.

2.6 Управление доступом и безопасностью

2.6.1 Ролевая модель и модификаторы доступа

PDM реализует детализированную ролевую модель доступа с использованием модификаторов доступа:

- Глобальные модификаторы доступа – определяют права ролей на действия с типами сущностей;
- Локальные модификаторы доступа – определяют права ролей на действия с конкретными экземплярами сущностей.

2.6.2 Порядок проверки прав доступа

При выполнении операции система проверяет права доступа в следующем порядке:

- Для операций с типами сущностей проверяются только глобальные модификаторы доступа;
- Для операций с экземплярами сущностей:

Сначала проверяются глобальные модификаторы доступа;

Если прав недостаточно, проверяются локальные модификаторы доступа.

2.6.3 Синхронизация ролей с Keycloak

PDM интегрирован с Keycloak для аутентификации пользователей. Синхронизация ролей осуществляется в двух направлениях:

1. Периодическая синхронизация (Keycloak → PDM) – автоматическая синхронизация ролей по расписанию:

- Роли с атрибутом `pdn_role="true"` импортируются в PDM;
 - Изменения ролей в Keycloak отражаются в PDM;
 - Роли, удаленные из Keycloak, удаляются из PDM.
2. Событийная синхронизация (PDM → Keycloak) – синхронизация при операциях с ролями в PDM:
- Перед созданием, обновлением или удалением роли в PDM проверяются права пользователя;
 - Операция сначала выполняется в Keycloak, затем в PDM;
 - Созданным ролям в Keycloak присваивается атрибут `pdn_role="true"`.

2.6.4 Инициализация системы

При первом запуске системы выполняется автоматическая инициализация:

- Импорт ролей из Keycloak – загрузка ролей с атрибутом `pdn_role="true"`;
- Создание начальных модификаторов доступа – формирование глобальных модификаторов доступа на основе атрибутов ролей;
- Настройка параметров ролей – для корректной работы ролей должны быть заполнены атрибуты:

ActionType – тип действия (CREATE, READ, READ_ANONYMOUS, UPDATE, DELETE);

MasterType – тип сущности, к которой относится модификатор доступа.

2.7 Операционные процедуры

2.7.1 Работа с типами документов и атрибутами

Создание нового типа документа

- Проверка глобального права пользователя на создание типов документов
- Проверка уникальности имени типа документа
- Создание типа документа с указанными параметрами
- Фиксация события в журнале аудита

Создание нового типа атрибута

- Проверка глобального права пользователя на создание типов атрибутов
- Проверка уникальности имени типа атрибута
- Создание типа атрибута с указанными параметрами
- Фиксация события в журнале аудита

Создание связи между типом документа и типом атрибута

- Проверка глобального права пользователя на создание связей
- Проверка существования типа документа и типа атрибута

- Проверка отсутствия связи между указанными типом документа и типом атрибута
- Создание связи с указанием флагов обязательности и уникальности
- Фиксация события в журнале аудита

Создание правила валидации

- Проверка глобального права пользователя на создание правил валидации
- Проверка существования связи между типом документа и типом атрибута
- Проверка корректности параметров правила валидации
- Создание правила валидации
- Фиксация события в журнале аудита

2.7.2 Работа с субъектами и документами

Создание субъекта ПДн

- Проверка глобального права пользователя на создание субъектов
- Создание записи субъекта с метainформацией
- Фиксация события в журнале аудита

Создание документа

- Проверка глобального права пользователя на создание документов
- Проверка существования субъекта и типа документа
- Создание документа с метainформацией
- Фиксация события в журнале аудита

Заполнение данных документа

- Проверка глобального права пользователя на создание данных документа
- Проверка существования документа
- Проверка права пользователя на обновление документа
- Проверка модификаторов доступа для данных документа и атрибутов
- Проверка глобального права на создание новых ролей (при наличии новых ролей в модификаторах)
- Создание данных документа
- Фиксация события в журнале аудита

Загрузка файла документа

- Проверка глобального права пользователя на создание файлов документов
- Проверка существования документа
- Проверка права пользователя на обновление документа
- Генерация предварительно подписанного URL для загрузки в S3

- Загрузка файла в объектное хранилище
- Создание записи о файле в базе данных
- Фиксация события в журнале аудита

2.7.3 Управление доступом

- **Назначение ролей пользователям**
- Назначение ролей пользователям осуществляется в Keycloak
- Роли должны иметь атрибут `pdn_role="true"` для синхронизации с PDM
- Синхронизация ролей выполняется автоматически по расписанию

Создание модификатора доступа

- Проверка глобального права пользователя на создание модификаторов доступа
- Создание модификатора доступа с указанием:
 Типа сущности
 Идентификатора сущности (для локальных модификаторов)
 Наборов ролей для каждого типа действия
- Фиксация события в журнале аудита

Примечание: Глобальные модификаторы доступа создаются при первоначальной инициализации системы и доступны для редактирования (удаление невозможно). Локальные модификаторы создаются вместе с сущностью или добавляются в процессе её обновления, при этом операции с ними требуют одновременного наличия прав: на управление модификаторами доступа и на изменение целевой сущности.

Изменение модификатора доступа

- Проверка глобального права пользователя на обновление модификаторов доступа
- Проверка существования модификатора доступа
- Обновление параметров модификатора доступа
- Фиксация события в журнале аудита

2.7.4 Работа с журналом аудита

Просмотр журнала аудита

- Проверка права пользователя на чтение журнала аудита
- Фильтрация записей по параметрам:
 Тип события
 Период времени
 Пользователь
 Сущность

2.7.5 Мониторинг и обслуживание

Мониторинг состояния системы

PDM предоставляет метрики для мониторинга через Prometheus и визуализации в Grafana.

Резервное копирование

Рекомендуется регулярное резервное копирование:

- Базы данных – основная БД и БД аудита
- Объектного хранилища – файлы документов в S3
- Конфигураций – конфигурационные файлы и настройки Kubernetes

Восстановление после сбоев

Процедура восстановления системы:

- Восстановление баз данных из резервных копий
- Восстановление файлов документов из объектного хранилища
- Проверка целостности данных после восстановления
- Верификация работы системы.

2.8 Особенности работы системы

2.8.1 Транзакционность операций

Все операции, затрагивающие несколько сущностей, выполняются в рамках транзакций:

- Атомарность изменений;
- Откат при ошибках;
- Согласованность данных.

2.8.2 Блокировка операций при недоступности аудита

В случае недоступности сервиса аудита:

- Document Manager блокирует операции с ПДн;
- Система ожидает восстановления доступности аудита.

2.8.3 Масштабируемость и производительность

Система поддерживает:

- Горизонтальное масштабирование сервисов;
- Кэширование для повышения производительности;
- Балансировку нагрузки между экземплярами сервисов.

2.9 Рекомендации по эксплуатации

2.9.1 Производительность

Масштабирование – горизонтальное масштабирование сервисов в Kubernetes.

2.9.2 Безопасность

Регулярное обновление – своевременное обновление компонентов системы и исправлений безопасности.

Мониторинг безопасности – регулярный анализ журналов аудита на предмет подозрительной активности.

Проверка доступа – регулярный аудит прав доступа пользователей.

2.9.3 Соответствие законодательству

Соблюдение сроков хранения – контроль сроков хранения персональных данных.

Реализация прав субъектов – обеспечение возможности субъектов осуществлять свои права на доступ, исправление и удаление ПДн.