Crosstech Endpoint Device Management

Руководство администратора

CEDM Release 8.0.0

АННОТАЦИЯ

Данный документ представляет собой руководство администратора для работы с Системой Crosstech Endpoint Device Management (далее CEDM или Система).

Руководство содержит сведения, необходимые пользователям для настройки работы Системы, состоящей из следующих компонентов:

- подсистемы аутентификации и авторизации (далее – ПАА);
- системы управления рабочими станциями (далее – СУРС).

СОДЕРЖАНИЕ

1. ТЕРМИНЫ И СОКРАЩЕНИЯ....8
2. СВЕДЕНИЯ О КОМПЛЕКСЕ, ТЕХНИЧЕСКИЕ И ПРОГРАММНЫЕ СРЕДСТВА, ОБЕСПЕЧИВАЮЩИЕ ВЫПОЛНЕНИЕ ФУНКЦИЙ ПРОГРАММЫ....11
2.1. Общие сведения о Системе....11
2.1.1. Назначение подсистемы аутентификации и авторизации....11
2.1.2. Назначение Системы управления рабочими станциями....12
2.2. Структура Системы CEDM....12
2.2.1. Описание компонентов....13
2.2.1.1. ws-web-proxy....13
2.2.1.2. frontend....13
2.2.1.3. ws-web-backend....13
2.2.1.4. agent-proxy-service....13
2.2.1.5. ms-agent-manager....14
2.2.1.6. ms-certificate-manager....14
2.2.1.7. agent-task-runner-service....15
2.2.1.8. ms-app-registry....15
2.2.1.9. ms-file-storage....15
2.2.1.10. ms-agent-builder....16
2.2.1.11. Nginx....16
2.2.2. Схема сетевого взаимодействия....17
2.2.3. Алгоритмы взаимодействия компонентов Системы CEDM при выполнение различных задач....20
2.2.3.1. Регистрация агентов в системе CEDM....20
2.2.3.2. Аутентификации агентов....20
2.2.3.3. Взаимодействие агента и сервера....20
2.2.3.4. Получение данных об отключении агента....21
2.2.3.5. Выполнение задач агента....21
2.3. Сведения о технических и программных средствах, необходимых для функционирования Системы....22
2.3.1. Требования к аппаратному обеспечению....23
2.3.2. Дополнительные рекомендации к выбору аппаратного обеспечения....25
2.3.3. Требования к выделенным ресурсам для работы продукта (агентов)....26

3. ПОДГОТОВКА К УСТАНОВКЕ СИСТЕМЫ 28
4. УСТАНОВКА СИСТЕМЫ 30
4.1. Установка серверной части Системы 30
4.1.1. Доступ к веб-интерфейсу Системы 34
4.2. Установка агентской части Системы CEDM (Desktop Agent) ... 34
4.2.1. Установка на ОС Astra Linux Special Edition 34
4.2.1.1. Установка из консоли ОС 34
4.2.1.2. Установка из графической оболочки 35
4.2.2. Установка на операционной системе macOS 35
4.2.3. Установка на ОС Альт Рабочая станция 39
4.2.4. Установка на РЕД ОС 39
4.2.4.1. Установка из консоли 39
4.2.4.2. Установка из графической оболочки 39
4.2.5. Установка на ОС Windows (10/11) 40
4.2.5.1. Параметры командной строки для установщика 42
5. ОБНОВЛЕНИЕ И УДАЛЕНИЕ СИСТЕМЫ 43
5.1. Обновление серверной части Системы CEDM 43
5.1.1. Подготовка к обновлению Системы 43
5.1.2. Обновление Системы 44
5.2. Обновление агентов Системы CEDM 45
5.3. Удаление агентов Системы CEDM 45
5.3.1. Удаление на ОС Astra Linux Special Edition 45
5.3.2. Удаление на операционной системе macOS 45
5.3.3. Удаление на ОС Альт Рабочая станция 46
5.3.4. Удаление на РЕД ОС 46
5.3.5. Удаление на ОС Windows (10/11) 46
5.3.5.1. Параметры командной строки деинсталлятора 47
6. ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА СИСТЕМЫ 48
6.1. Настройка раздела «Безопасность» 48
6.2. Создание и настройка ролей 49
6.3. Настройка интеграции с корпоративной службой каталогов 49
6.4. Настройка автоматического назначения доступа 49
6.5. Создание локальных пользователей 49
7. ИНТЕГРАЦИЯ С ДРУГИМИ РЕШЕНИЯМИ 50
7.1. Интеграция CEDM со службой каталогов Active Directory 50
7.1.1. Проверка соединения Системы CEDM с Active Directory 54

7.1.2. Импорт данных пользователей из Active Directory.....55
8. УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ И НАСТРОЙКА ДОСТУПА....56
8.1. Типы администраторов в Системе CEDM.....56
8.1.1. Управление пользователями (Администратор ПАА).....56
8.1.2. Управление ролями (Администратор СУРС).....56
8.2. Виды учетных записей.....57
8.3. Создание, управление и удаление учетных записей пользователей.....57
8.3.1. Создание учетной записи пользователя.....58
8.3.2. Установка временного пароля.....59
8.3.3. Редактирование учетной записи пользователя.....61
8.3.4. Удаление учетной записи пользователя.....61
8.3.5. Настройка доступных IP-адресов.....61
8.3.6. Карточка учетной записи пользователя из Active Directory.....62
8.3.7. Синхронизация списка пользователей.....63
8.4. Настройка доступа (роли и пользователи).....64
8.4.1. Раздел «Роли».....64
8.4.2. Раздел «Пользователи».....68
8.4.3. Раздел «Автоматическое назначение доступа».....70
9. УПРАВЛЕНИЕ ПОДСИСТЕМОЙ ПАА.....74
9.1. Настройка системных параметров ПАА.....74
9.2. Просмотр и редактирование нормативно-справочной информации (НСИ).....76
9.2.1. Справочник «Подсистемы».....76
9.2.2. Справочник «Версии протокола брокера Kafka».....77
9.2.3. Справочники «Должность», «Подразделение», «Юридическое лицо».....77
9.2.4. Справочник «Внешние системы аутентификации».....77
9.2.5. Добавление значений в справочники.....78
10. УПРАВЛЕНИЕ ПОДСИСТЕМОЙ СУРС.....79
10.1. Настройка Системы.....79
10.1.1. Экранная форма «Настройки истории инвентаризации».....79
10.1.2. Экранная форма «Системные параметры».....80
10.1.3. Экранная форма «Расписание запуска задач».....81
10.1.4. Экранная форма «Безопасность».....83

10.1.5. Экранная форма «Настройки агентов» 98
10.1.6. Экранная форма «Электронная почта» 108
11. МОНИТОРИНГ. ЖУРНАЛ СОБЫТИЙ ПАА 110
11.1. Фильтрация событий 110
11.2. Формирование отчета 111
12. МОНИТОРИНГ. ЖУРНАЛ СОБЫТИЙ СУРС 112
12.1. Экранная форма «Общий журнал событий» 112
12.1.1. Фильтрация общего журнала событий 112
12.1.2. Просмотр карточки события 113
12.2. Экранная форма «Журнал сеансов удаленного помощника» 114
12.3. Экранная форма «Очередь команд агентам» 115
12.4. Экранная форма «Журнал ошибок» 116
12.4.1. Фильтрация журнала ошибок 117
12.4.2. Просмотр карточки события 117
12.4.3. Выгрузка ошибки в текстовый файл 118
13. КОМПОНЕНТЫ СИСТЕМЫ 119
13.1. Установщики агентов 119
13.1.1. Вкладка «Установщики агентов» 119
13.1.2. Вкладка «Конфигурации агентов» 120
13.1.3. Добавление нового установщика 121
14. О СИСТЕМЕ 123
15. РЕЗЕРВНОЕ КОПИРОВАНИЕ БД POSTGRESQL И ФХ HDFS 124
15.1. Конфигурация БД по умолчанию 124
15.2. Резервное копирование базы данных 124
15.3. Восстановление базы данных из резервной копии 125
15.4. Конфигурация ФХ HDFS по умолчанию 127
15.5. Резервное копирование ФХ HDFS 127
15.5.1. Способ 1: Архивирование каталога с ФХ 127
15.5.2. Способ 2: Резервное копирование docker volume 129
16. СПРАВОЧНАЯ ИНФОРМАЦИЯ 131
16.1. Журналирование событий компонентов Системы CEDM ..131
16.1.1. Расположение и доступ к журналам компонентов Системы CEDM 131
16.1.2. Журналирование ПАА 134
16.1.3. Журналирование событий СУРС 135
16.2. Метрики для постановки на мониторинг 136

16.2.1. Общие принципы мониторинга.....136
16.2.2. Ключевые метрики для постановки на мониторинг..137
16.2.3. Настройка мониторинга.....139
16.2.4. Действия при срабатывании оповещений.....139
17. ДИАГНОСТИКА И РЕШЕНИЕ ПРОБЛЕМ.....141
17.1. Общие рекомендации по диагностике.....141
17.2. Часто встречающиеся проблемы и их решения.....141
17.2.1. Проблемы с аутентификацией пользователей.....141
17.2.2. Проблемы с производительностью системы.....141
17.2.3. Ошибки при интеграции с внешними системами.....141
17.2.4. Ошибки сервера CORE после перезагрузки сервера или его восстановления из снапшота (Snapshot).....142
18. ОБРАЩЕНИЕ В ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ.....144
18.1. Порядок подачи обращений в службу технической поддержки.....144
18.2. Требования к содержанию обращений.....144

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Определение
Ansible	Ansible – система управления конфигурациями, написанная на языке программирования Python, с использованием декларативного языка разметки для описания конфигураций. Применяется для автоматизации настройки и развертывания программного обеспечения
Active Directory (AD)	Централизованная служба каталогов корпоративного уровня, входящая в состав семейства серверных продуктов Microsoft Windows Server
CORE	Сервер, на котором размещаются основные сервисы CEDM, включая брокер сообщений Kafka
Crosstech Endpoint Device Management (CEDM)	UEM-платформа для централизованного управления жизненным циклом корпоративных конечных устройств. Решение обеспечивает автоматизированную инвентаризацию, непрерывный мониторинг и управление гетерогенным парком оборудования с единой консоли
Fully Qualified Domain Name (FQDN)	Полное доменное имя, которое уникально идентифицирует узел в составе иерархии DNS (Domain Name System). FQDN состоит из следующих компонентов: • имя узла (hostname) – имя компьютера или сервера, например «server1». • имя домена (domain name) – имя домена, к которому принадлежит узел, например «company». • имя верхнего уровня домена (top-level domain), например «com», «org», «ru»
HDFS (Hadoop Distributed File System)	Распределенная файловая система, разработанная для хранения очень больших объемов данных на кластере обычных серверов. HDFS обеспечивает высокую доступность данных за счет их репликации между узлами кластера, а также позволяет эффективно обрабатывать и анализировать большие массивы информации
Lightweight Directory Access Protocol (ldap)	Протокол прикладного уровня для доступа к службам каталогов по сети. LDAP обеспечивает стандартизированный метод для хранения, просмотра и изменения данных в службе каталогов
Автоматизированное рабочее место (АРМ)	Программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида. Объединяет программно-аппаратные средства, обеспечивающие взаимодействие человека с компьютером

Авторизация	Процесс принятия решения о предоставлении доступа пользователю на выполнение операции на основании каких-либо знаний о нем. К этому моменту пользователь уже должен быть идентифицирован и аутентифицирован (подтверждена его идентичность)
Администратор доступа	Администратор подсистемы ПАА, осуществляющий настройку конфигурации Системы CEDM, а также создание, удаление и редактирование профилей пользователей CEDM
Аутентификация	Процедура проверки подлинности пользователя при попытке получить доступ к информационной системе
Задача в Системе CEDM	Действие или последовательность действий, которые инициируются администратором в веб-интерфейсе сервера CEDM и выполняются удаленно на выбранных агентах (АРМ)
Логин пользователя	Уникальный идентификатор учетной записи CEDM, необходимый для авторизации пользователя в системе
НСИ	Нормативно-справочная информация
Подсистема аутентификация и авторизации (ПАА)	Подсистема CEDM, предназначенная для управления конфигурацией и пользователями Системы
Система управления рабочими станциями (СУРС)	Система CEDM, предназначенная для управления удаленными устройствами, проведения инвентаризации, также выполнения задач на устройствах
Пользователь CEDM	Пользователь Системы управления рабочими местами, выполняющий функции в соответствии с назначенной ему ролью
Роль	Перечень функциональных возможностей, доступных пользователю CEDM
Сценарий Ansible	Описание последовательности действий на языке YAML для выполнения какой-либо задачи автоматизации в виде плейбука
Учетная запись (УЗ)	Учетная запись пользователя в CEDM – это набор учетных данных, включая логин и пароль, идентифицирующих конкретного пользователя в системе для предоставления ему соответствующих прав доступа и возможностей управления. Учетные записи в системе CEDM можно разделить на локальные и импортированные из внешних систем аутентификации. Кроме того, УЗ разделяются на администраторов ПАА и пользователей СУРС
Файловая система (ФС)	Метод организации и хранения файлов на носителях информации, таких как жесткие диски и SSD и т. д.

	Определяет способ, которым операционная система управляет, именует, хранит и организует файлы и каталоги

2. СВЕДЕНИЯ О КОМПЛЕКСЕ, ТЕХНИЧЕСКИЕ И ПРОГРАММНЫЕ СРЕДСТВА, ОБЕСПЕЧИВАЮЩИЕ ВЫПОЛНЕНИЕ ФУНКЦИЙ ПРОГРАММЫ

2.1. Общие сведения о Системе

Система предназначена для централизованного мониторинга и управления рабочими станциями и серверами, имеющим доступ к корпоративным и иным критически важным данным. Это позволяет организациям защитить широкий спектр устройств сотрудников, используемых в организации, одновременно управляя всем жизненным циклом устройств, а именно:

- конфигурировать и применять политики информационной безопасности (ИБ);
- централизовано распространять корпоративные приложения и управлять ими;
- проводить контроль доступа, инвентаризацию программного обеспечения (ПО) и аппаратных ресурсов.

CEDM позволяет управлять конфигурациями устройств с разными типами операционных систем (ОС) и набором установленного ПО из одной консоли. Унифицированный подход дает много преимуществ:

- возможность упрощенного и централизованного управления позволяет снизить объем ручной работы специалистов и сократить расходы на автоматизацию;
- управление устройствами как в локальной сети, так и в сети Интернет;
- быстрое подключение автоматизированного рабочего места к работе вне зависимости от типа платформы;
- контроль использования ПО;
- контроль использования оборудования, подключения внешних накопителей, сетевых адаптеров и др.

2.1.1. Назначение подсистемы аутентификации и авторизации

Подсистема аутентификации и авторизации предназначена для решения следующих задач:

- идентификация, аутентификация и авторизация пользователей;

- управление учетными записями пользователей;
- настройка и добавление подсистем CEDM;
- журналирование событий и формирования отчетов ПАА.

2.1.2. Назначение Системы управления рабочими станциями

Система управления рабочими станциями (СУРС) является ключевым компонентом Системы CEDM и предназначена для:

- проведения инвентаризации программного и аппаратного обеспечения на управляемых устройствах;
- централизованного управления оконечными устройствами;
- выполнения задач на оконечных устройствах, включая установку и удаление программного обеспечения, настройку параметров операционной системы и применение политик безопасности;
- мониторинга состояния оконечных устройств и сбора событий безопасности;
- обеспечения удаленного доступа к рабочим столам управляемых устройств для оказания технической поддержки;
- автоматизации процессов управления жизненным циклом устройств в организации.

2.2. Структура Системы CEDM

Система CEDM имеет микросервисную архитектуру. Логическая схема архитектуры CEDM приведена на рисунке 1.

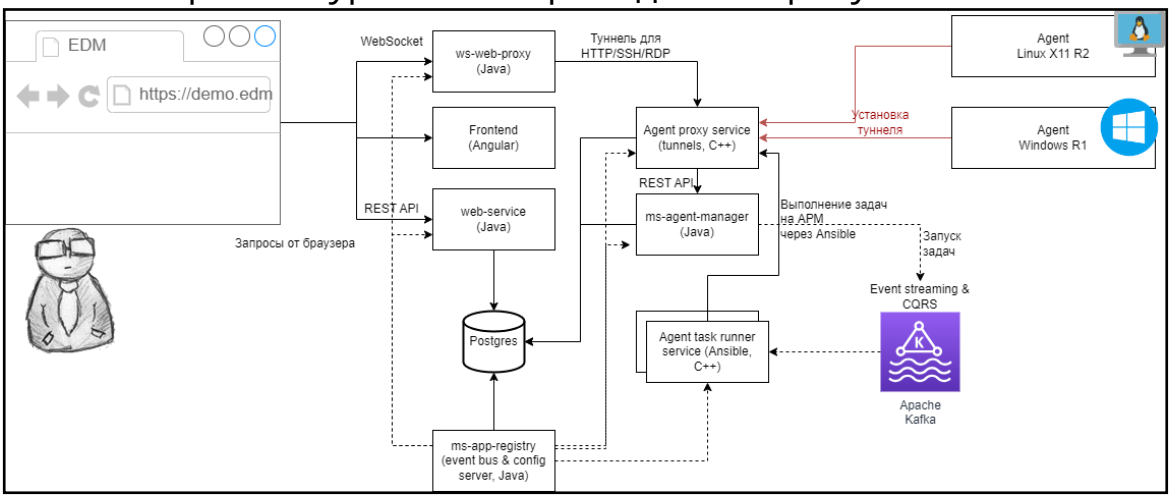

Рисунок 1. Логическая схема архитектуры Системы CEDM

2.2.1. Описание компонентов

Система CEDM состоит из следующих основных модулей:

- ws-web-proxy;
- frontend;
- ws-web-backend;
- agent-proxy-service;
- ms-agent-manager;
- ms-certificate-manager;
- agent-task-runner-service;
- ms-app-registry;
- ms-file-storage;
- ms-agent-builder;
- nginx.

2.2.1.1. ws-web-proxy

Сервис, разработанный на Java и выступающий в роли посредника между веб-интерфейсом администратора и внутренними сервисами системы. Проксирует WebSocket соединения от веб интерфейса к внутренним сервисам системы и обратно.

2.2.1.2. frontend

Сервис на Angular, реализующий пользовательский интерфейс для администрирования и управления системой. Предоставляет веб-интерфейс, с помощью которого администраторы могут настраивать параметры системы, управлять пользователями, контролировать работу различных модулей и сервисов, просматривать журналы событий и статистику. Кроме ого, модуль агрегирует и отображает данные, получаемые от различных сервисов бэкенда.

2.2.1.3. ws-web-backend

Сервис обеспечивает бизнес-логику и API для веб-интерфейса администраторов системы CEDM. Взаимодействует с веб-интерфейсом через ws-web-proxy по протоколу WebSocket. Отвечает за основную функциональность Системы.

2.2.1.4. agent-proxy-service

Сервис обеспечивает взаимодействие серверной части системы CEDM с агентами, развернутыми на удаленных устройствах.

Реализован на языке C++ в виде кластера из нескольких микросервисов. Основные функции:

- аутентификация агентов на устройствах;
- обратное туннелирование канала связи между серверной частью и ОС устройства;
- ретрансляция сеансов подключения по протоколу удаленного рабочего стола;
- прочее взаимодействие с удаленными устройствами.

2.2.1.5. ms-agent-manager

Сервис управления жизненным циклом агентов CEDM, развернутых на удаленных устройствах. Реализован на языке Java. Основные функции:

- регистрация и отслеживание активных агентов;
- проверка подлинности и статуса агентов;
- мониторинг ключевых параметров агентов;
- формирование задач для агентов;

Для передачи данных агентам взаимодействует с agent-proxy-service через шину событий ms-app-registry.

2.2.1.6. ms-certificate-manager

Сервис управления инфраструктурой открытых ключей (PKI) системы CEDM. Реализован на Java в виде микросервиса, работающего в среде Docker. Основные функции:

- генерация и управление жизненным циклом ключей и сертификатов для защищенного взаимодействия между серверными компонентами и агентами;
- реализация модели безопасности на основе цифровых сертификатов;
- управление центром сертификации CEDM;
- отзыв и обновление сертификатов;
- ведение реестра действующих сертификатов.

Сервис взаимодействует с другими компонентами CORE через брокера сообщений Kafka по порту 10134.

2.2.1.7. agent-task-runner-service

Сервис для запуска задач на удаленных устройствах с применением Ansible. Реализован на C++ как кластер микросервисов. Основные функции:

- получение задач на выполнение от ms-agent-manager;
- передача задач агентам через agent-proxy-service;
- запуск задач на агентах с помощью Ansible;
- сбор результатов выполнения задач из консоли агентов;
- возврат результатов задач в ms-agent-manager.

2.2.1.8. ms-app-registry

Сервис для централизованного хранения конфигураций всех микросервисов системы CEDM. Реализован на Java. Основные функции:

- хранение конфигов;
- предоставление API для чтения конфигов другими микросервисами;
- рассылка уведомлений об изменении конфигов (Event bus).

2.2.1.9. ms-file-storage

Сервис предназначен для хранения загружаемых пользователями в систему файлов, которые в дальнейшем могут быть использованы в задачах.

Сервис реализован с использованием распределенной, отказоустойчивой и масштабируемой файловой системы Apache Hadoop Distributed File System (HDFS).

Сервис включает два компонента:

- NameNode – центральный узел, хранящий метаданные файловой системы и информацию о распределении блоков данных между DataNode. Отвечает за обработку операций уровня файлов и каталогов;
- DataNode – вычислительные узлы кластера, на которых непосредственно хранятся блоки данных файлов в репликах согласно заданному коэффициенту репликации.

Адресация файлов реализована через традиционный URL-путь в пространстве имен HDFS.

Доступ к чтению, записи и управлению файлами осуществляется через WebHDFS REST API.

По умолчанию HDFS монтируется по пути /var/lib/docker/volumes/test_CEDM_dfs_data. Пространство распределяется динамически по мере заполнения файлового хранилища и ограничено размером логического раздела операционной системы. Узнать размер, занимаемый файловым хранилищем можно командой:

du -h /var/lib/docker/volumes/test_CEDM_dfs_data

Средствами операционной системы можно смонтировать отдельный диск для файлового хранилища. Также можно выделить заданное пространство из имеющегося диска на этапе установки операционной системы.

2.2.1.10. ms-agent-builder

Сервис, предназначен для автоматизированной сборки установщиков агентов CEDM с параметрами, специфичными для конкретного экземпляра системы. Реализован на Java в виде микросервиса, работающего в среде Docker. Основные функции:

- формирование установочных пакетов агентов CEDM для различных операционных систем с предустановленными параметрами подключения к серверу;
- включение в установочные пакеты необходимых сертификатов и ключей для защищенного взаимодействия;
- конфигурирование параметров агентов в соответствии с политиками безопасности организации;
- сохранение собранных установщиков в файловом хранилище системы для последующего распространения.

Сервис взаимодействует с другими компонентами CORE с помощью брокера сообщений Kafka по порту 10135.

2.2.1.11. Nginx

Веб-сервер и обратный прокси-сервер, обеспечивающий веб-интерфейс системы CEDM и маршрутизацию запросов между

компонентами. Реализован в виде Docker-контейнера. Основные функции:

- обработка HTTP/HTTPS запросов к веб-интерфейсу системы;
- маршрутизация запросов между фронтендом и бэкендом;
- терминация SSL/TLS соединений;
- балансировка нагрузки между компонентами;
- кэширование и выдача статического контента;
- обеспечение отказоустойчивости веб-интерфейса;
- базовая защита от DDoS-атак и других веб-угроз;
- ведение журналов доступа и ошибок.

2.2.2. Схема сетевого взаимодействия

Схема сетевого взаимодействия приведена на рисунке 2. В таблице 1 представлены используемые порты и их назначение.

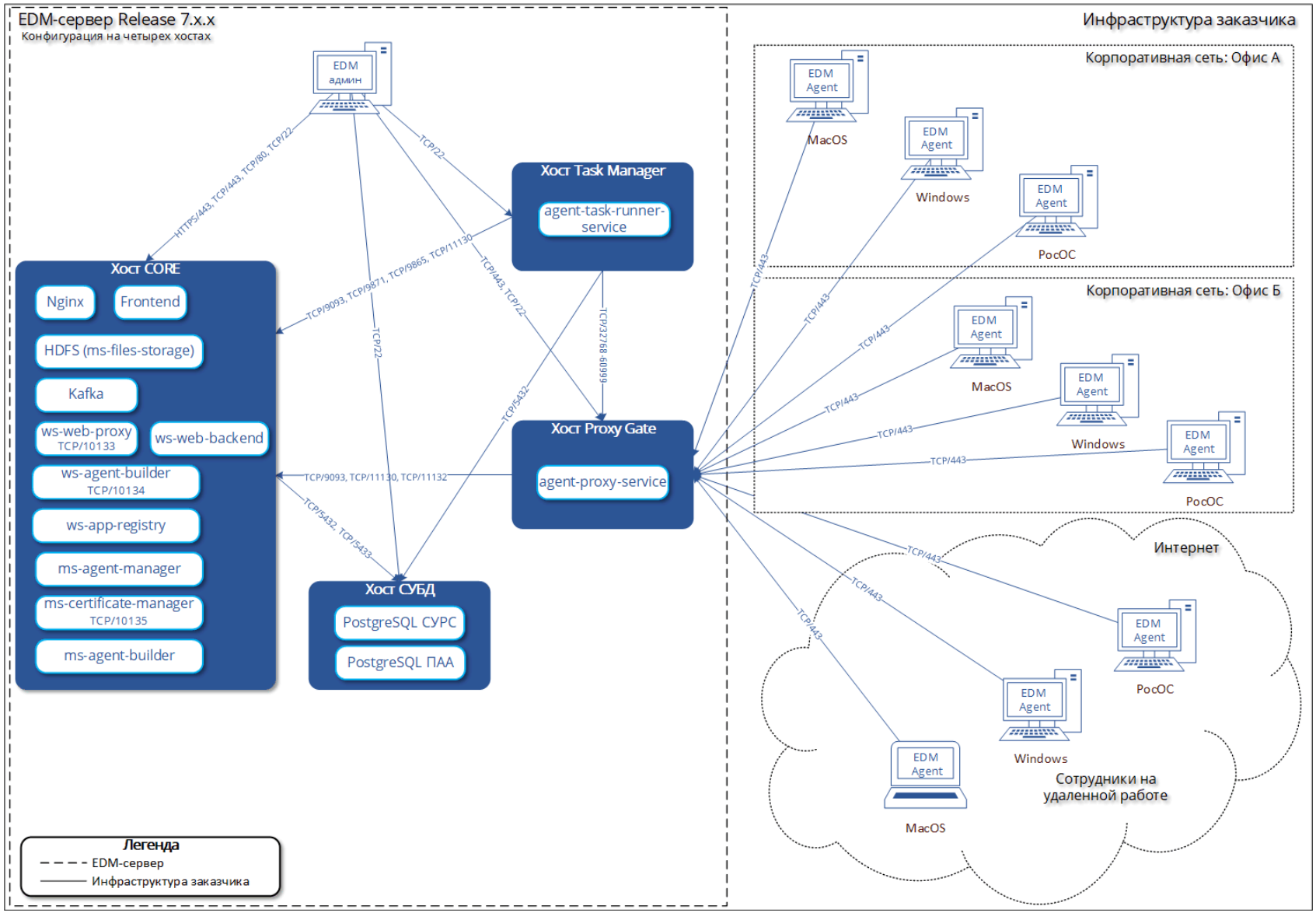

Рисунок 2. Схема сетевого взаимодействия компонентов Системы CEDM

Таблица 1. Сетевое взаимодействие

Источник	Назначение	Протокол / порт	Предназначение
Task Manager agent-task-runner-service	СУБД	TCP / 5432	Загрузка задачи и сохранение результатов ее выполнения
Task Manager agent-task-runner-service	CORE* (Kafka)	TCP / 9093	Получение задач на выполнение, чтение плейбуков Ansible, передача результатов выполнения задач в backend Системы, доступ к файловому хранилищу HDFS
	CORE* (HDFS)	TCP / 9871 TCP / 9865	
	CORE* (Backend)	TCP / 11130	
Task Manager agent-task-runner-service	Proxy Gate agent-proxy-service	TCP / 32768-60999	Туннелирование трафика от агентов на внутренние компоненты Системы
CORE	СУБД CEDM	TCP / 5432	Чтение/запись данных о состоянии компонентов системы
	СУБД ПАА	TCP / 5433	
Proxy Gate agent-proxy-service	CORE* (Kafka)	TCP / 9093	Взаимодействие серверных компонент Системы с агентами.
	CORE* (Backend)	TCP / 11130 TCP / 11132	Запрос аутентификации агента, регистрации агента
CORE	CORE	TCP / 10133	ws-web-proxy
CORE	CORE	TCP / 10134	ms-certificate-manager
CORE	CORE	TCP / 10135	ms-agent-builder
Агент CEDM	Proxy Gate agent-proxy-service	TCP / 443	Регистрация и аутентификация агентов. Получение/передача команд управления и задач между агентами и серверных компонент
Рабочее место администратора	CORE	HTTPS / 443 TCP / 80	веб-интерфейс администратора

Рабочее место администратора	все хосты	TCP / 22	SSH-доступ для администрирования

*CORE – сервер с основными приложениями

2.2.3. Алгоритмы взаимодействия компонентов Системы CEDM при выполнение различных задач

2.2.3.1. Регистрация агентов в системе CEDM

Агент, установленный на клиентской машине и не имеющий учетной записи на сервере, должен пройти процедуру регистрации. Агент отправляет пакет с запросом регистрации, в ответ сервер возвращает пакет с выданными идентификационными данными или ошибку. Агент сохраняет идентификационные данные в консистентном хранилище и использует их при последующих процедурах аутентификации.

2.2.3.2. Аутентификации агентов

Агент присылает серверу пакет с идентификационной информацией, сервер возвращает пакет с кодом успешной или неудачной аутентификации. В случае неудачной аутентификации сервер разрывает соединение, агент сообщает об ошибке пользователю (если запущена UI часть агента) и не повторяет попыток соединения до следующей перезагрузки ОС. Если агент прислал тип канала, отличный от управления, то после успешной аутентификации канал переводится в указанный режим (например, обратного туннелирования).

2.2.3.3. Взаимодействие агента и сервера

Агент CEDM на удаленном устройстве устанавливает соединение с сервером по протоколу TCP, создавая двухсторонний канал управления. Сервер ждет от агента пакет с регистрацией, либо аутентификацией. После успешной процедуры регистрации или аутентификации сервер и агент переходят в режим ожидания команд или данных. Взаимодействие по каналу управления производится пакетами в формате JSON. Пакет в JSON завершается специальной последовательностью символов, означающей конец передачи пакета.

2.2.3.4. Получение данных об отключении агента

При нормальном завершении сеанса оконечного устройства agent-proxy-service обнаруживает отключение агента и высылает сообщение в брокер сообщений Kafka. Далее сообщение передается в ms-agent-manager, и, после его обработки, в web-интерфейсе обновляется иконка состояния связи. Среднее время реакции web-интерфейса на отключение оконечного устройства до двух секунд. Максимальное – десять секунд.

2.2.3.5. Выполнение задач агента

В базе данных создается задание на выполнение сценария на удаленном устройстве.

Сервис ms-agent-manager отправляет команды через шину событий ms-app-registry сервису туннелирования ms-agent-proxy-service на создание/удаление туннеля с протоколом SSH для Ansible. Команда на создание туннеля отправляется при получении информации из базы данных о наличии задач в статусе ожидания выполнения и удаленное устройство подключено к серверу.

Сервис agent-proxy-service отправляет на агента команду CREATE_CHANNEL по каналу управления, агент устанавливает новое TCP соединение с agent-proxy-service с указанным типом туннеля.

Сервис ms-agent-manager принимает пакеты от сервиса туннелирования, в частности информацию об успешном поднятии туннеля.

Сервис agent-task-runner-service после создания SSH-туннеля получает из базы данных задание на выполнение сценария, загружает архив с плейбуком. Файл из файлового хранилища, сохраняется на локальный диск. В БД помечается задание, как принятое на исполнение. Запускается Ansible, в параметры передаются путь к плейбуку и файлу. Результат выполнения плейбука сохраняется в БД, а также передается через системе обработки потоковых данных и событий Kafka в ws-web-proxy для вывода на веб-странице через WebSocket. После завершения задачи меняется статус ее статус в БД, SSH -туннель разрывается.

2.3. Сведения о технических и программных средствах, необходимых для функционирования Системы

Общие рекомендации и положения по установке и настройке Системы:

- компоненты CEDM могут быть развернуты на нескольких серверах в зависимости от количества рабочих станций в организации;
- Система поддерживает развертывание как на физических серверах, так и в виртуальных средах. При использовании виртуальных сред необходимо обеспечить выделение достаточных ресурсов для виртуальных машин;
- все серверы CEDM должны иметь стабильное сетевое подключение. Рекомендуется использовать статические IP-адреса для серверов CEDM;
- рекомендуется использовать высокопроизводительные системы хранения данных на основе SSD-накопителей, особенно для серверов баз данных. Для повышения отказоустойчивости рекомендуется использовать RAID-массивы;
- все серверы должны быть защищены современными средствами информационной безопасности, включая антивирусное ПО и межсетевые экраны. Рекомендуется регулярное обновление операционной системы и установка обновлений безопасности;
- рекомендуется выполнять регулярное резервное копирование всех компонентов CEDM, особенно для баз данных и конфигурационных файлов;
- рекомендуется развернуть систему мониторинга и сбора логов для отслеживания производительности и доступности всех компонентов CEDM.

Установка серверной части Системы CEDM должна осуществляться на серверы, функционирующие под управлением операционной системы РЕД ОС версии 7.3.5 (конфигурация «Сервер минимальный»).

Установка агентской части Системы CEDM (Desktop Agent) должна осуществляться на автоматизированные рабочие места

(АРМ), функционирующие под управлением одной из следующих операционных систем:

- Альт Рабочая станция версии 10 и выше;
- Astra Linux Special Edition версии 1.8 (64 бит), сертификат соответствия № 2557 (выдан ФСТЭК России 27 января 2012 г.);
- РЕД ОС версии 7.3 (64 бит), сертификат соответствия № 4060 (выдан ФСТЭК России 12 января 2019 г.);
- Microsoft Windows 10 (64 бит);
- Microsoft Windows 11 (64 бит);
- macOS Monterey версии 12 и выше.

Веб-интерфейс Системы CEDM поддерживает работу с браузерами, которые работают на основе проекта с открытым кодом Chromium, начиная с версии 120 и выше, с браузером Mozilla Firefox, начиная с версии 121.0.1 и выше, а также с браузером о Apple Safari версии 14 и выше.

Для эксплуатации и эффективного применения Системы необходимо использовать лицензионное системное программное обеспечение.

2.3.1. Требования к аппаратному обеспечению

В таблице 2. представлены рекомендации по выбору конфигурации системы CEDM и выделению аппаратных ресурсов в зависимости от количества управляемых устройств и предполагаемой нагрузки.

Таблица 2. Рекомендации по выбору конфигурации Системы

кол-во АРМ, шт	Кол-во серверов	Сервисы	Ресурсы на один сервер		
			ОЗУ, Гб	кол-во ядер CPU, шт	свободное место на диске, Гб
до 750	1	Основные сервисы (CORE), файловое хранилище HDFS* и Kafka	16	4	64 – на системном разделе ОС 64 – на логическом разделе для ФХ HDFS
	1	СУБД для СУРС и ПАА	16	4	32
	1	Сервис agent-proxy-service	2	2	16
	1	Сервис agent-task-runner-service	4	2	32
от 750 до 1500	1	Основные сервисы (CORE), файловое хранилище HDFS и Kafka	32	8	64 – на системном разделе ОС 240 – на логическом разделе для ФХ HDFS
	1	СУБД для СУРС и ПАА	32	8	64 (SSD)
	1	agent-proxy-service	4	4	16
	1	agent-task-runner-service	8	4	64
от 1500 до 3000	1	Основные сервисы (CORE), файловое хранилище HDFS и Kafka	32	16	64 – на системном разделе ОС 64 – на логическом разделе для ФХ HDFS
	1	СУБД для СУРС и ПАА	64	16	64 (SSD)
	1	agent-proxy-service	4	4	64
	1	agent-task-runner-service	16	8	100
от 3000 до 5000	1	Основные сервисы (CORE)	32	16	100
	1	Файловое хранилище HDFS namenode	2	2	20
	1	Файловое хранилище HDFS datanode*	2	2	100
	1	Kafka	4	2	100
	1	СУБД для СУРС и ПАА	64	16	100 (SSD)
	1	agent-proxy-service	5	4	16
	1	agent-task-runner-service	16	8	100
от 5000 до 8000	1	Основные сервисы (CORE)	32	16	100
	1	Файловое хранилище HDFS namenode	4	4	20
	1	Файловое хранилище HDFS datanode*	4	4	100
	1	Kafka	6	4	100
	1	СУБД для СУРС и ПАА	96	24	100 (SSD)
	2	agent-proxy-service	4	2	16
	2	agent-task-runner-service	4	2	100
от 8000 до 12000	1	Основные сервисы (CORE)	44	22	100
	1	Файловое хранилище HDFS namenode	6	6	20
	1	Файловое хранилище HDFS datanode*	6	6	100

	1	Kafka	8	6	100
	1	СУБД для СУРС и ПАА	128	36	100 (SSD)
	2	agent-proxy-service	4	2	16
	2	agent-task-runner-service	4	2	100
от 12000 до 16000	1	Основные сервисы (CORE)	64	32	100
	1	Файловое хранилище HDFS namenode	8	8	20
	1	Файловое хранилище HDFS datanode	8	8	1024
	1	Kafka	12	8	100
	1	СУБД для СУРС и ПАА	196	54	100 (SSD)
	3	agent-proxy-service	4	2	16
	3	agent-task-runner-service	4	2	100
от 16000 до 25000	2	Основные сервисы (CORE)	32	16	100
	2	Кластер файлового хранилища HDFS namenode	2	2	20
	2	Кластер файлового хранилища HDFS datanode	2	2	100
	2	Kafka	4	2	100
	2	СУБД для СУРС и ПАА**	64	16	100 (SSD)
	от 3 до 5	agent-proxy-service***	4	2	16
	от 3 до 5	agent-task-runner****	4	4	100
от 25000 до 35000	3	Основные сервисы (CORE)	32	16	100
	3	Кластер файлового хранилища HDFS namenode	2	2	20
	3	Кластер файлового хранилища HDFS datanode	2	2	100
	3	Kafka	4	2	100
	2	СУБД для СУРС и ПАА**	64	16	100 (SSD)
	от 5 до 7	agent-proxy-service***	4	2	16
	от 5 до 7	agent-task-runner****	4	4	100

2.3.2. Дополнительные рекомендации к выбору аппаратного обеспечения

Размер дискового пространство, необходимый для файлового хранилища HDFS и резервных копий Системы, зависит от индивидуальных потребностей Заказчика.

Сервера баз данных рекомендуется использовать в конфигурации Master-Standby. Standby работает в режиме горячего резерва и поддерживает актуальную копию данных через потоковую репликацию. Кроме того, Standby-сервер может использоваться для операций чтения, снижая нагрузку на Master-сервер.

Дисковый ввод-вывод является основным узким местом для производительности базы данных при использовании CEDM,

поэтому настоятельно рекомендуется оптимизировать дисковый ввод-вывод.

Сервис agent-proxy-service при масштабировании рекомендуется добавлять из расчета один сервер на 5000 устройств. Расчет оперативной памяти для agent-proxy-service рекомендуется производить исходя из размера буфера на прием данных от одного агента (по умолчанию в Системе установлен размер буфера равный 1Мб).

Сервис agent-task-runner при масштабировании рекомендуется добавлять из расчета один сервер на 5000 устройств. Расчет ядер CPU рекомендуется производить исходя из желаемого количества одновременно выполняемых задач в Системе. Одна задача – одно ядро CPU. Расчет свободного места на диске производить в зависимости от объема файлов, участвующих в выполнении задач. Сервис использует кеш для одинаковых файлов.

Между всеми компонентами системы требуется обеспечить высокоскоростное соединение (10 Гбит/с).

Расчет ширины канала связи для работы «удаленной помощи» (RDP) производится исходя из планируемого объема использования данного функционала. В максимальном качестве требуется 17 Мбит на одно соединение. Получаем, что для 500 одновременно работающих сеансов удаленной помощи потребуется пропускная способность сервера с сервисом agent-proxy-service в 8500 Мбит.

Сервера из каждой группы желательно физически распределять, чтобы исключить риск потери работоспособности.

2.3.3. Требования к выделенным ресурсам для работы продукта (агентов)

В таблице 3 представлены минимальные рекомендованные требования к выделенным ресурсам для работы продукта (агентов).

Таблица 3. Минимальные рекомендованные требования

Элемент	Параметр
Операционная система	Требуется наличие одной из ОС, указанных в подразделе 3.3 настоящего документа
Браузер	Требуется наличие одного из браузеров, указанных в подразделе 3.3 настоящего документа
Процессор	Не менее 1 ГГц

Элемент	Параметр
Оперативная память	Не менее 1 Гб
Дисковое пространство	Для установки программы – 50 Мб. Для работы агента требуется от 500 Мб до 2 Гб в зависимости от режима работы агента и настроек политики сбора событий

3. ПОДГОТОВКА К УСТАНОВКЕ СИСТЕМЫ

Перед развертыванием Системы CEDM необходимо выполнить следующие действия:

- выбрать конфигурацию Системы и количество хостов, на которых она будет развернута, в зависимости от числа управляемых устройств и предполагаемой;
- убедиться, что выполняются требования к аппаратному и программному обеспечению серверов, выделенных для развертывания Системы;
- убедиться, что открыты сетевые порты для взаимодействия компонентов CEDM;
- для корректной работы защищенного соединения необходимо подготовить SSL-сертификат и закрытый ключ для веб-сервера nginx;
- задать имена хостов. Например:

```bash
hostname edm-core
hostname edm-db
hostname edm-proxy
hostname edm-task-runner
```

На всех хостах требуется создать технологическую учетную запись (ТУЗ). Важно, чтобы и учетная запись пользователя (и пароль от УЗ) совпадали на всех хостах.

В настоящем руководстве для примера используется ТУЗ ansible:

```bash
sudo -i
useradd -c "Ansible User" -G wheel ansible
```

1) На всех хостах в файле /etc/sudoers найти строку, указанную ниже, раскомментировать ее или добавить, если она отсутствует:

```
%wheel ALL=(ALL)       NOPASSWD: ALL
```

Для этого можно использовать встроенный текстовый редактор Nano:

```bash
nano   etc/sudoers
```

2) На всех хостах задать пароль для ТУЗ ansible, выполнив команду:

```
bash
passwd ansible
```

4. УСТАНОВКА СИСТЕМЫ

4.1. Установка серверной части Системы

Установочный пакет Системы CEDM позволяет выполнить установку как один сервер, так и выполнить установку в режиме горизонтального масштабирования.

Для установки серверной части Системы CEDM требуется перейти в каталог с дистрибутивами и в консоли РЕД ОС выполнить последовательность действий и команд, приведенных ниже:

1) Архив с дистрибутивом edm_server_install_x.x.x.tar.gz (x.x.x – версия Системы) поместить в каталог /root на одном из хостов.
2) Разархивировать его, выполнив команду:

```
bash
tar xzvf edm_server_install_x.x.x.tar.gz
```

3) Для корректной работы системы внешней аутентификации пользователей по протоколу LDAPS в каталог /root/ansible-edm/roles/deploy_app/files/ldaps поместить корневой сертификат и переименовать его в «ca.crt».
4) Для корректной работы веб-интерфейса Системы в каталог /root/ansible-edm/roles/deploy_app/files/ssl/ поместить файлы SSL-сертификата и закрытого ключа к нему с именами nginx.crt и nginx.key соответственно.
5) Зайти в каталог /ansible-edm и запустить установку командой:

```
bash
cd ./ansible-edm
./install_edm main
```

6) Указать количество серверов в конфигурации.
7) Указать через пробел имя хоста и его IP-адрес. Например:

Примечание: под именем хоста понимается DNS-суффикс, который будет добавлен к именам хостов, на которых развертывается Система. Например, edm01.test, где edm01 – имя хоста (hostname), a test – DNS-суффикс (DNS suffix).

```
bash
edm01 192.168.10.1
```

Примечание: IP-адреса хостов можно узнать, введя в терминале команду:

```
bash
```

```
ip a
```

Имена хостов можно узнать, введя в терминале команду:

```
bash
hostname
```

8) В случае корректного ввода IP-адреса на экран будет выведено построчно имя хоста, его IP-адрес и запрошено подтверждение пользователя (консоль принимает ответы в виде: Y y Yes yes Д д Да да / N n No no Н н Нет нет).
9) Указать имя учетной записи пользователя, из-под которого будет производиться установка системы CEDM.

Далее необходимо выбрать на какой сервер будет установлен тот или иной компонент Системы в зависимости от количества серверов, указанных при выполнении пункта 6 данного перечня.

На экране появится меню, где стрелочками и последующим нажатием клавиши «Enter» можно произвести выбор. Например:

```
bash
>edm01
edm02
edm03
edm04
```

10) Выбрать сервер для установки приложений (CORE).
11) Выбрать сервер для установки брокера сообщений Kafka.
12) Выбрать сервер для установки основной базы данных.
13) Выбрать сервер для установки базы данных ПАА.

Примечание: пункты 14-16 данного перечня выполняются при установке Системы в режиме горизонтального масштабирования.

14) Указать количество серверов для установки сервиса agent-proxy.
15) Выбрать сервер для установки сервиса agent-proxy.
16) Указать необходимость установки HAProxy в качестве балансировщика нагрузки. Если выбран ответ «Да», то в далее требуется указать на какой сервер будет установлен HAProxy.
17) Выбрать сервер для установки agent-taskrunner.

Ниже представлены примеры рекомендованного распределения компонентов Системы по серверам при разных конфигурациях:

- для конфигурации из четырех серверов:
  - edm01: Приложения (CORE) и Kafka;
  - edm02: основная БД, БД ПАА;
  - edm03: сервис edm-proxy.service;
  - edm04: сервис agent-taskrunner.
- для конфигурации из двух серверов:
  - edm01: Приложения (CORE) и kafka;
  - edm02: основная БД, БД ПАА, сервисы edm-proxy и edm-task-runner.

18) Настроить основную базу данных CEDM. Для этого по запросу установщика выполнить следующие шаги:
    - ввести допустимое название для основной базы данных CEDM. Например:

```
bash
edm_db
```

    - указать порт, на котором будет работать основная БД. По умолчанию предлагается порт 5432;
    - задать имя администратора PostgreSQL основной БД CEDM;
    - задать пароль администратора PostgreSQL CEDM;

Примечание: введенные символы не будут отображаться на экране.

- задать имя администратора БД CEDM;
- задать пароль администратора БД CEDM;
- задать имя пользователя БД CEDM;
- задать пароль пользователя БД CEDM.

19) Настроить базу данных ПАА. Для этого по запросу установщика выполнить следующие шаги:
    - ввести название для БД ПАА. Например:

```
bash
paa_db
```

    - указать порт, на котором будет работать БД ПАА. По умолчанию предлагается порт 5433
    - задать имя администратора PostgreSQL БД ПАА;
    - задать пароль администратора PostgreSQL БД ПАА

- задать имя администратора БД ПАА;
- задать пароль администратора БД ПАА;
- задать имя пользователя БД ПАА;
- задать пароль пользователя БД ПАА.

20) Настроить хранилище Ansible vault, который используется для хранения паролей пользователей баз данных. Доступ к хранилищу осуществляется с помощью файла с кодовым словом (секретом шифрования).

Для настройки хранилища необходимо создать файл с секретом для хранилища Ansible:

- ввести секрет (произвольную строку символов), который будет использоваться для дешифрования хранилища Ansible с паролями;

Примечание: введенные символы не будут отображаться на экране.

- указать полный путь к файлу с секретом.

Примечание: если указать только имя файла, то файл будет создан в текущем рабочем каталоге /root/ansible-edm. Полный путь необходимо указывать с именем файла включительно: /root/ansible-edm/vault_secret.

- задать пароль для сервисной учетной записи (суперадминистратор СУРС CEDM) edm;
- задать пароль для сервисной учетной записи (суперадминистратор ПАА CEDM) auth;
- задать имя вашего домена Системы EDM (адрес web-интерфейса Системы CEDM). Например:

```bash
edm-test.ru
```

Примечание: обратите внимание, что в настоящем руководстве адрес веб-интерфейса CEDM «edm-test.ru» задан в качестве примера.

- ввести пароль по для учетной записи пользователя.

После выполнения всех вышеперечисленных шагов запускается скрипт установки Системы CEDM необходимо дождаться завершения работы скрипта и убедится в отсутствии ошибок.

После выполненных действий Система CEDM считается установленной и готовой к работе.

4.1.1. Доступ к веб-интерфейсу Системы

При наличии DNS-сервера для доступа к веб-интерфейсу Системы необходимо создать на нем две CNAME записи:

```
<edm_web>.domain.local
auth.<edm_web>.domain.local
```

где <edm_web>.domain.local – FQDN хоста, на котором развернуты основные приложения Системы CEDM (CORE). Например:

```
edm-core.test,
auth.edm-core.test
```

При отсутствии DNS-сервера на рабочем месте, с которого будет осуществляться вход в веб-интерфейс Системы, необходимо добавить в файл HOSTS следующие строки:

```
XXX.XXX.XXX.XXX edm-test.ru
XXX.XXX.XXX.XXX auth.edm-test.ru
```

где XXX.XXX.XXX.XXX – IP-адрес хоста, на котором развернуты основные приложения Системы CEDM (CORE), edm-test.ru – адрес веб-интерфейса Системы CEDM.

4.2. Установка агентской части Системы CEDM (Desktop Agent)

Примечание: работа с агентами на ОС Windows ведется от имени учетной записи System. Для ос семейства Linux и macOS при установке агента будет автоматически создана технологическая учетная запись (service account), от имени которой в дальнейшем будет запускаться сервис.

Установка агентской части Системы CEDM (Desktop Agent) выполняется из установщика, собранного на сервере CEDM. Все настройки, необходимые для подключения оконечного устройства к серверу, включены в установщик.

4.2.1. Установка на ОС Astra Linux Special Edition

4.2.1.1. Установка из консоли ОС

Для установки из консоли ОС необходимо выполнить следующие действия:

1) Скопировать собранный на CEDM-сервере deb-пакет Агента в каталог файловой системы, в который будет производиться установка. В текущем руководстве для примера использован каталог /opt.
2) Перейти в каталог /opt, выполнив команду:

```
sh
ls /opt
```

3) Выполнить установку командой:

```
sh
sudo dpkg -i <имя_файла_установщика>.deb
```

4.2.1.2. Установка из графической оболочки

Для установки из графической оболочки необходимо выполнить следующие действия:

1) Скопировать собранный на EDM-сервере deb-пакет Агента в каталог файловой системы, в который будет производиться установка.
2) Открыть файл установки двойным нажатием.
3) В появившемся диалоговом окне нажать «Установить пакет».
4) В окне «Требуется аутентификация» ввести свой пароль.
5) Нажать кнопку «Применить».

4.2.2. Установка на операционной системе macOS

Для установки CEDM Desktop Agent необходимо выполнить следующие шаги:

1) Запустить установщик EDM Desktop Agent.

После запуска файла установки может появиться предупреждение безопасности macOS (рисунок 3).

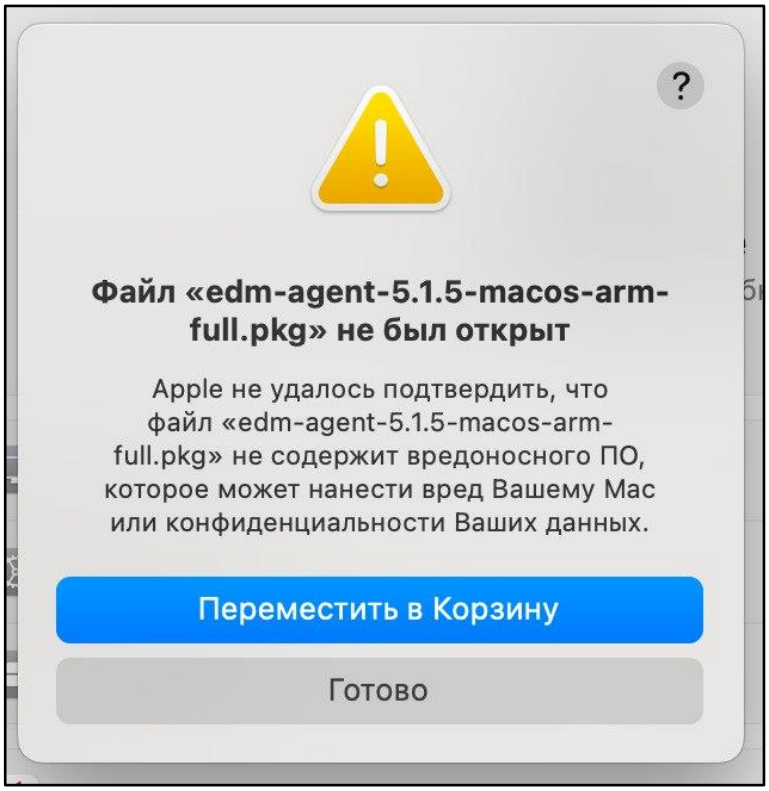

Рисунок 3. Предупреждение безопасности MacOS

Данное окно является стандартным предупреждение данной операционной системы для приложений, которые были загружены не из App Store или от неидентифицированных разработчиков.

2) Разрешить установку из непроверенного источника.

Если будет получено предупреждение о безопасности, то необходимо:

- открыть «Системные настройки»;
- перейти в раздел «Конфиденциальность и безопасность» (рисунок 4);
- в нижней части окна найти сообщение: «Файл «имя_файла_установщика.pkg» заблокирован для защиты Вашего Mac»;
- нажать кнопку «Все равно открыть» справа от этого сообщения.

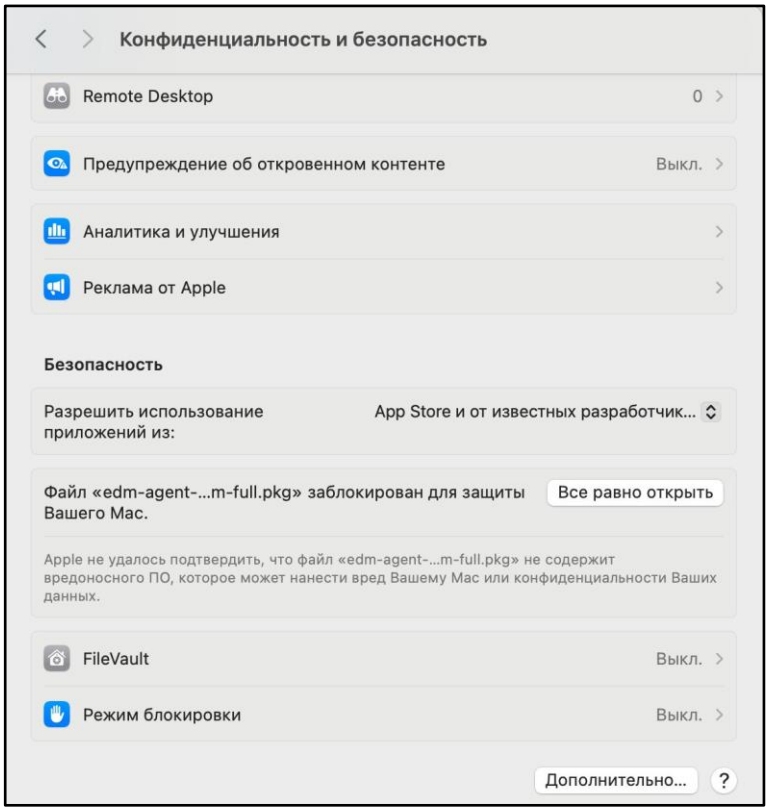

Рисунок 4. Подтверждение открытия

3) В появившемся окне мастера установки нажать «Продолжить» (рисунок 5).

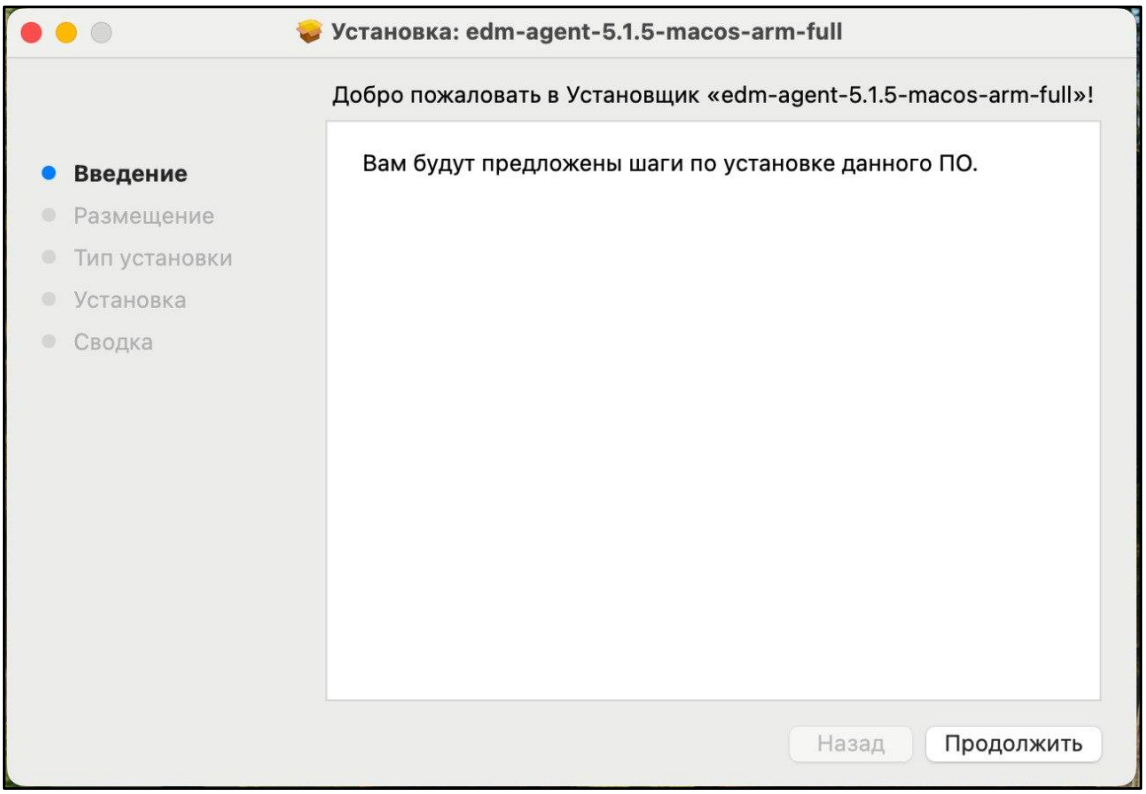

Рисунок 5. Мастер установки – Введение

4) На шаге «Тип установки» нажать «Установить» (рисунок 6).

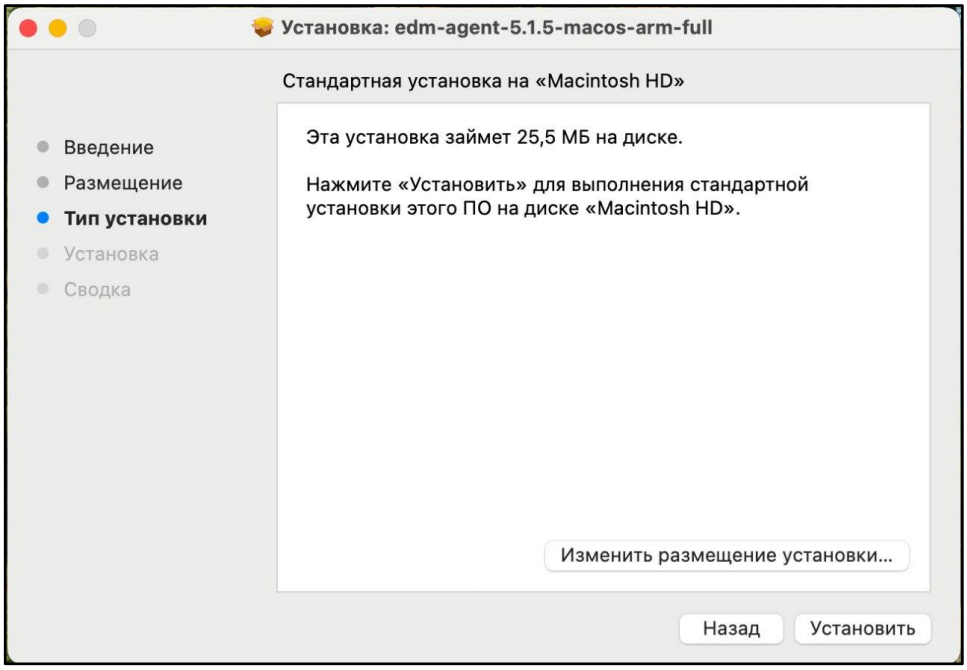

Рисунок 6. Мастер установки – Тип установки

5) После успешной установки появится сообщение «Установка прошла успешно» (рисунок 7).

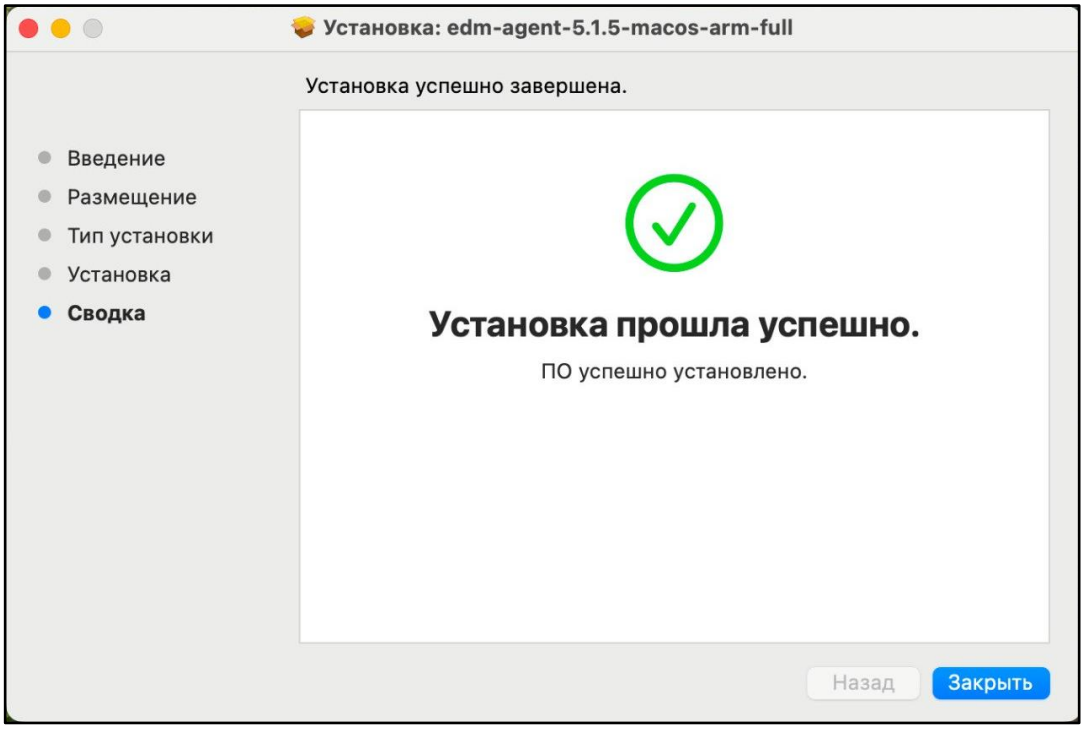

Рисунок 7. Мастер установки – Успешная установка

6) Закрыть мастер установки.

7) Для выполнения задач на MacOS необходимо установить интегрированную среду разработки xCode. Для этого необходимо запустить терминал и выполнить команду:

```
xcode-select --install
```

4.2.3. Установка на ОС Альт Рабочая станция

Для установки CEDM Desktop Agent необходимо выполнить следующие шаги:

1) Скопировать RPM-пакет агента в каталог файловой системы, в который будет производиться установка. В текущем руководстве для примера использован каталог /opt).
2) Перейти в каталог /opt, выполнив команду:

```
sh
ls /opt
```

3) Выполнить установку командой:

```
sh
sudo apt-get install <имя_файла_установщика>.rpm
```

4.2.4. Установка на РЕД ОС

4.2.4.1. Установка из консоли

Для установки CEDM Desktop Agent необходимо выполнить следующие шаги:

1) Скопировать RPM-пакет агента в каталог файловой системы, в который будет производиться установка. В Руководстве для примера использован каталог /opt).
2) Перейти в каталог /opt, выполнив команду:

```
sh
ls /opt
```

3) Выполнить установку командой:

```
sh
sudo dnf install <имя_файла_установщика>.rpm
```

4.2.4.2. Установка из графической оболочки

Для установки из графической оболочки необходимо выполнить следующие действия:

1) Скопировать собранный на CEDM-сервере rpm-пакет агента в каталог файловой системы, в который будет производиться установка.
2) Открыть файл установки двойным нажатием. Запустится стандартный интерфейс управления программами и диалоговое окно аутентификации.
3) Ввести свой пароль и нажать «Аутентификация» (рисунок 8). Запустится процесс установки.
4) В окне «Результат транзакции» нажать «Хорошо».
5) Закрыть окно управления программами.

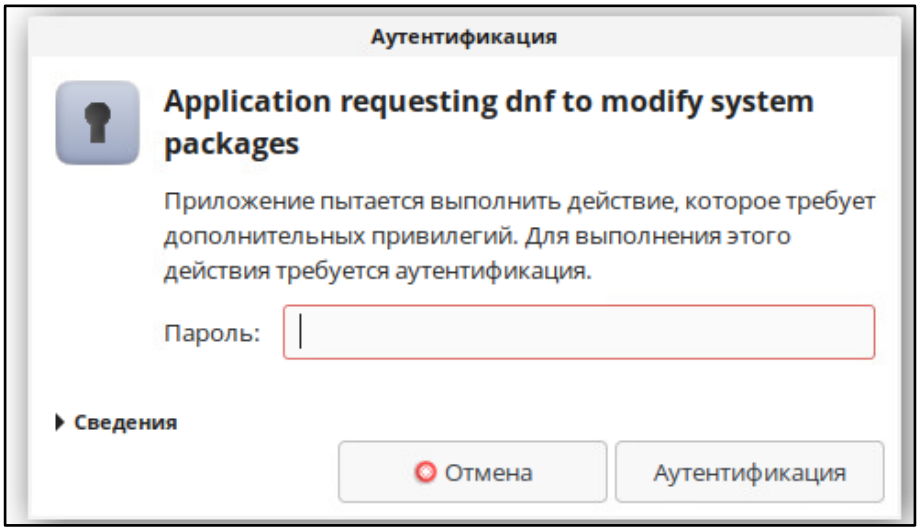

Рисунок 8. Установка EDM-агента из графической оболочки

4.2.5. Установка на ОС Windows (10/11)

Для установки CEDM Desktop Agent необходимо выполнить следующие шаги:

1) Запустить установщик CEDM Desktop Agent. В появившимся диалоговом окне нажать «Далее» (рисунок 9).

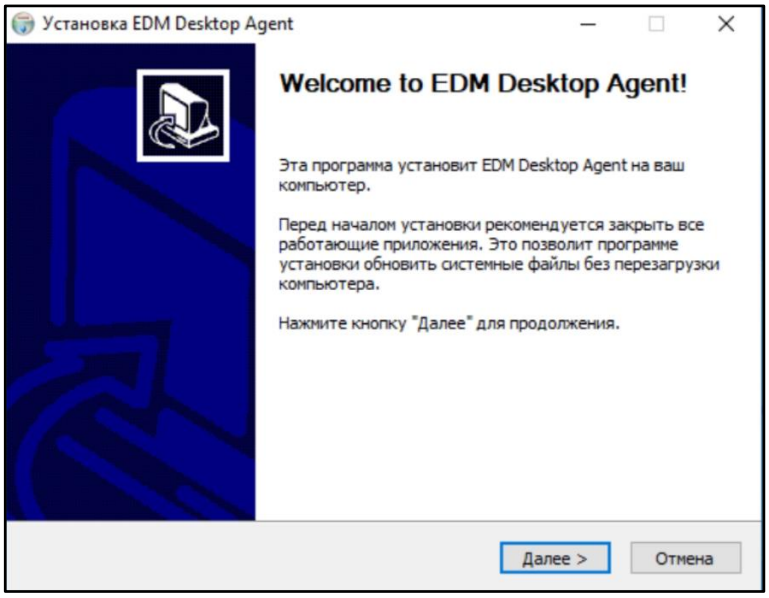

Рисунок 9. Мастер установки EDM Desktop Agent

2) Выбрать папку для установки. Нажать «Далее» (рисунок 10).

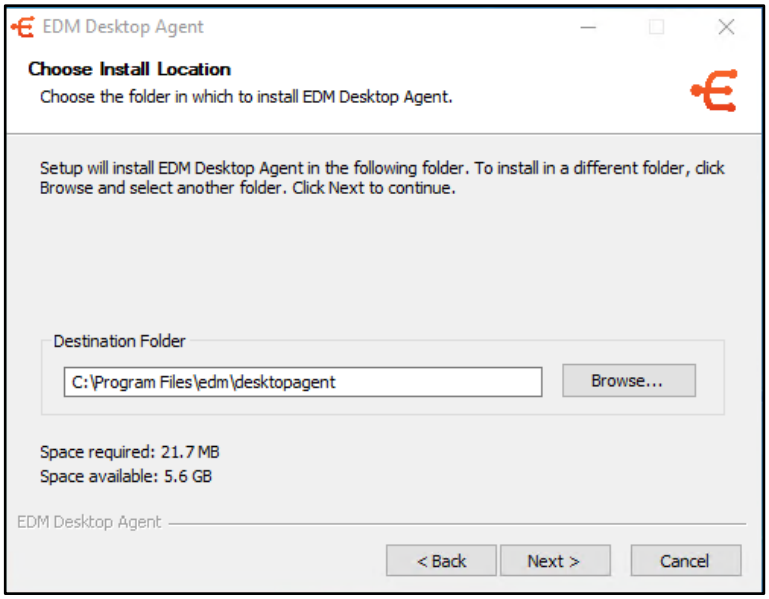

Рисунок 10. Выбор папки установки

3) Выбрать папку для размещения ярлыков в меню «Пуск». Нажать «Install», после чего мастер выполнит установку программы.
4) После корректной установки отобразится окно завершения мастера (рисунок 11). Нажать «Готово».

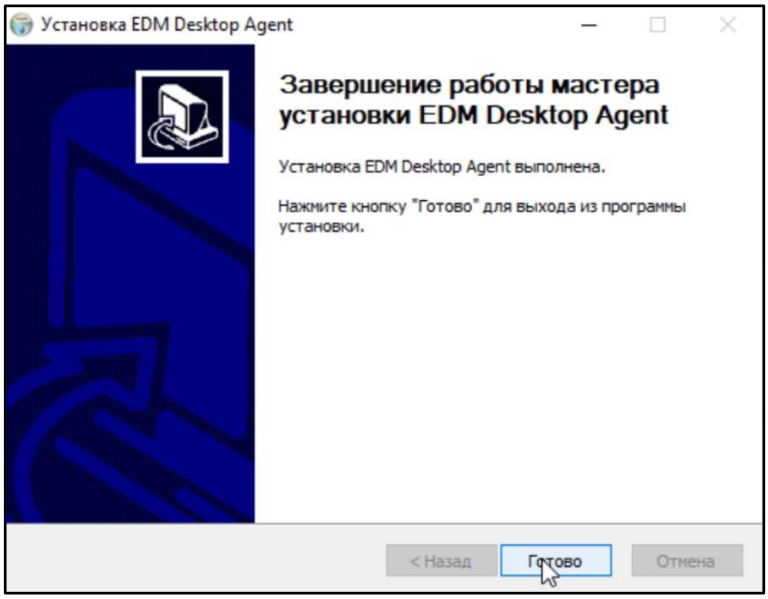

Рисунок 11. Завершение установки

4.2.5.1. Параметры командной строки для установщика

Ниже представлены возможные командной строки для установщика:

- /S – задать тихий режим установки. Например:

```
<имя_файла_установщика>.exe /S
```

- /D – указать полный путь установки. Полный путь для установки. Должен быть последним в командной строке, его не следует помещать в кавычки, даже если в нём присутствуют пробелы. Например:

```
<имя_файла_установщика>.exe /D=C:\Program files\edm\desktopagent
```

5. ОБНОВЛЕНИЕ И УДАЛЕНИЕ СИСТЕМЫ

5.1. Обновление серверной части Системы CEDM

Примечания:

1) Обновление серверной части CEDM на версию 8.0.0. возможно только с версии 7.2. Если установлена более ранняя версия, то рекомендуется установка с нуля на чистые хосты.
2) Рекомендуется выполнить снимки хостов (Snapshot), на которых развернута Система CEDM.
3) Если планируется обновление Системы в режиме горизонтального масштабирования, то необходимо предварительно на всех дополнительных хостах выполнить действия, указанные в разделе 3 настоящего руководства.

5.1.1. Подготовка к обновлению Системы

Перед обновлением Системы требуется выполнить резервное копирование конфигураций, а также очистить старые файлы установки. Для этого необходимо:

1) На сервере CORE выполнить последовательно следующие команды для создания резервных копий критически важных файлов:

```bash
cd /root
mkdir -p ~/edm_backup
cp -rf ~/ansible-edm/inventories ~/edm_backup/
cp -rf ~/ansible-edm/roles/deploy_app/files ~/edm_backup/
```

2) Если имеется файл с секретом для ansible vault, находящийся в каталоге ansible-edm, то его необходимо скопировать в каталог edm_backup:

```bash
cp -r ~/ansible-edm/vaultfile ~/edm_backup/
```

где vaultfile – имя файла с секретом для ansible vault.

3) Удалить старые каталоги установки, выполнив команду:

```bash
rm -rf ~/{ansible-edm,deploy-edm}
```

5.1.2. Обновление Системы

Для обновления Системы необходимо выполнить следующие действия:

1) Распаковать архив обновления. Для этого требуется скопировать архив с новой версией системы (например, edm_server_install_x.x.x.tar.gz, где x.x.x – версия системы) в каталог с установленным CEDM и распаковать его следующей командой:

```
bash
tar xzvf edm_server_install_ x.x.x.tar.gz
```

2) Скопировать ранее сохраненные файлы конфигураций в новый каталог установки:

```
bash
cp -rf ~/edm_backup/inventories ~/ansible-edm
cp -rf ~/edm_backup/files/ ~/ansible-edm/roles/deploy_app/
```

3) Если при подготовке к обновлению (см. пункт 5.1.1 данного руководства) была сделана резервная копия файла с секретом для ansible vault, то необходимо вернуть данный файл в каталог ~/ansible-edm, выполнив команду:

```
bash
mv -f ~/edm_backup/vaultfile ~/ansible-edm
```

где vaultfile – имя файла с секретом для ansible vault.

4) Перейти в каталог ansible-edm:

```
bash
cd ~/ansible-edm
```

5) Перейти в каталог ansible-edm и произвести настройку ssh-доступа к edm-серверам к по публичному ключу, выполнив команду:

```
bash
./update_edm set_ssh_pub_key_access
```

По запросу Системы ввести пароль от технологической учетной записи ansible, созданной подготовке к установке Системы (см. раздел 3 настоящего руководства).

6) Запустить скрипт обновления:

```
bash
./update_edm main
```

7) Подтвердить текущий домен Системы CEDM или изменить его в случае необходимости.

Примечание: консоль принимает ответы в виде: Y y Yes yes Д д Да да / N n No no Н н Нет нет.

8) Подтвердить установку обновления.
9) Указать необходимость установки edm-proxy в режиме горизонтального масштабирования. Если указать «Нет», то далее будет выполнено автоматическое обновление Системы. Если выбран ответ «Да», то необходимо перейти к выполнению пунктов 7-10 данного перечня.
10) Указать необходимость установки HAProxy в качестве балансировщика нагрузки. Если выбран ответ «Да», то в далее требуется указать необходимость конфигурирования hosts для HAProxy.
11) Указать необходимость конфигурирования hosts для режима горизонтального масштабирования.
12) Указать количество серверов, на которые будет производиться установка.
13) Указать через пробел имя хоста и его IP-адрес.

После выполненных действий начнется процесс обновления Системы.

5.2. Обновление агентов Системы CEDM

После обновления серверной части для обеспечения корректной работы Системы рекомендуется также обновить агенты до последней актуальной версии.

5.3. Удаление агентов Системы CEDM

5.3.1. Удаление на ОС Astra Linux Special Edition

Для удаления пакета агента необходимо из консоли ОС выполнить следующую команду:

```
sh
sudo dpkg -r edm-desktopagent
```

5.3.2. Удаление на операционной системе macOS

Для удаления пакета агента необходимо выполнить следующие действия:

1) Остановить службу «edm.desktopagent».
2) Удалить каталог программы. Путь по умолчанию: /opt/edm/desktopagent/

5.3.3. Удаление на ОС Альт Рабочая станция

Для удаления пакета агента необходимо из консоли ОС выполнить следующую команду:

```
sh
sudo apt-get remove <имя_файла_установщика>.rpm
```

5.3.4. Удаление на РЕД ОС

Для удаления пакета агента необходимо из консоли ОС выполнить одну из следующих команд:

- выполнить команду удаления, передав в качестве аргумента имя файла установщика:

```
sh
sudo dnf remove <имя_файла_установщика>
```

- выполнить команду удаления, передав в качестве аргумента имя пакета:

```
sh
sudo dnf remove edm-desktopagent
```

5.3.5. Удаление на ОС Windows (10/11)

Для удаления агента необходимо выполнить следующие действия:

1) Запустить мастер удаления CEDM Desktop Agent с помощью средства «Установка и удаление программ» в Windows или непосредственно из директории с установленной программой (рисунок 12).

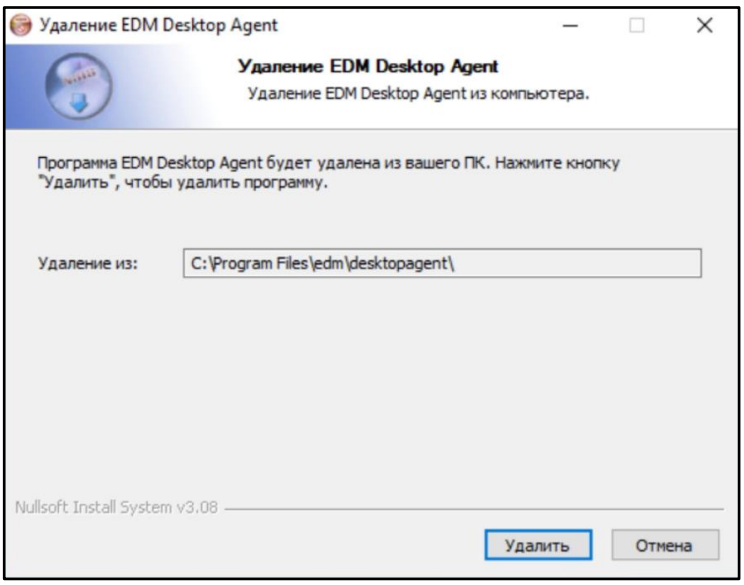

Рисунок 12. Мастер удаления CEDM Desktop Agent

2) Нажать кнопку «Удалить».
3) После успешного удаления программы закрыть мастер (рисунок 13).

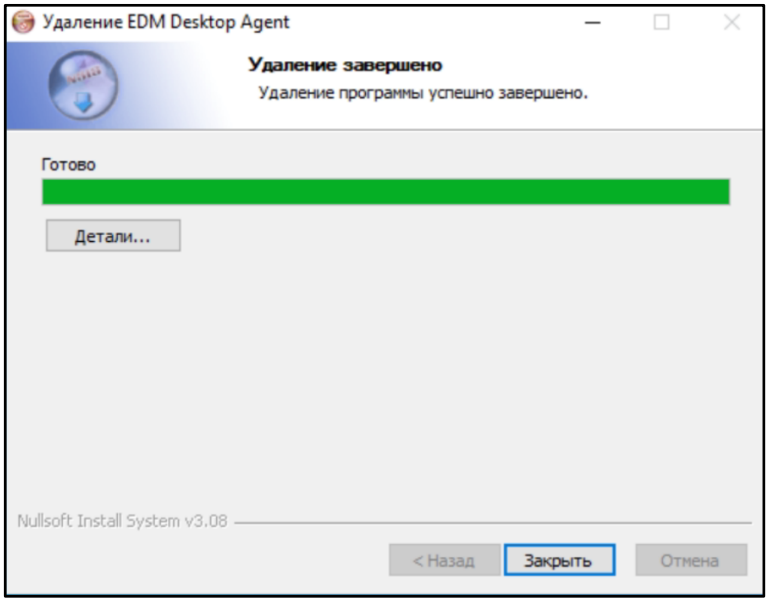

Рисунок 13. Успешное удаление CEDM Desktop Agent

5.3.5.1. Параметры командной строки деинсталлятора

Ниже представлены возможные командной строки для деинсталлятора:

- /S – задать тихий режим удаления. Например:

```
uninstaller.exe /S
```

- _? – задать директорию с установленной программой. Например:

```
uninstaller.exe _?=C:\Program files\edm\desktopagent
```

6. ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА СИСТЕМЫ

Для использования функциональных возможностей CEDM после установки должна быть выполнена настройка параметров Системы.

Настройка параметров комплекса осуществляется в веб-интерфейсе Системы, для запуска которого необходимо:

1) Запустить браузер на АРМ администратора.

2) Ввести в адресной строке браузера адрес веб-интерфейса Системы CEDM и авторизоваться (см. пункт 5.1.1 настоящего руководства).

После успешного входа можно перейти к настройке параметров Системы, согласно представленному ниже описанию.

6.1. Настройка раздела «Безопасность»

В первую очередь необходимо добавить и настроить и настройка сертификаты и параметры безопасности, которые будут встроены в установщики агентов.

Примечание: требуется наличие корневого сертификата и наличие серверного сертификата (при необходимости допускается использовать корпоративные сертификаты, а серверный сертификат может быть сгенерирован Системой).

Для настройки модели безопасности на основе сертификатов необходимо выполнить следующие действия:

1) Загрузить корневой сертификат.
2) Настроить серверные ключи.
3) Выполнить конфигурацию параметров сертификатов.
4) Включить выбранную модель безопасности.
5) Включить секрет сервера.
6) Определить секрета сервера.

После выполненных действий необходимо выполнить проверку сетевых параметров агентов в СУРС:

Примечание: адрес сервера для подключения агентов должен быть установлен автоматически при установке Системы.

1) В разделе «Администрирование» → «Настройки системы» → «Настройки агентов» проверить параметр «Адрес сервера» (см. пункт 11.1.5 настоящего руководства).

2) В разделе «Администрирование» → «Компоненты системы» → «Установщики агентов» → «Конфигурации агентов» проверить поле «Адрес сервера» и указать URL сервера (см. пункт 14.1.2 настоящего руководства).
3) Проверить параметры сертификата.
4) Установить уровень журналирования.

6.2. Создание и настройка ролей

Необходимо произвести настройку системы управления доступом. Для этого требуется в СУРС перейти в раздел «Администрирование» → «Настройка доступа» → «Роли», где создать и настроить роли.

6.3. Настройка интеграции с корпоративной службой каталогов

Необходимо импортировать учетные записи из корпоративной службы каталогов.

Подробная информация о создании подключения к внешней системе аутентификации и импорте пользователей представлена в подразделе 8.1 настоящего руководства.

6.4. Настройка автоматического назначения доступа

Для назначения ролей и групп для пользователей из AD необходимо в СУРС перейти в раздел «Настройка доступа» → «Автоматическое назначение доступа» для каждой роли создать и настроить правило автоматического назначение доступа (см. пункт 9.4.3 настоящего руководства).

6.5. Создание локальных пользователей

Последним этапом настройки является добавление локальных пользователей Системы. Для этого необходимо в подсистеме ПАА перейти в раздел «Пользователи», где требуется создать локальных пользователей Системы.

7. ИНТЕГРАЦИЯ С ДРУГИМИ РЕШЕНИЯМИ

7.1. Интеграция CEDM со службой каталогов Active Directory

Интеграция CEDM с со службой каталогов Active Directory предназначена для импорта доменных учетных записей пользователей в Систему и использовании корпоративных политик безопасности внутри CEDM, в частности требования к сложности паролей, частоте их смены, блокировке учетных записей и т. д.

Для корректной интеграции Системы со службой каталогов по протоколу LDAPS необходим корневой сертификат. Если при развертывании системы корневой сертификат добавлен не был, то его необходимо разместить в каталоге:

/opt/ws-auth/ca

где, ca – имя файла с сертификатом. И установить права доступа:

chmod 664 /opt/ws-auth/ca

Примечание: корневой сертификат должен быть в кодировке base64.

Настройка подключения CEDM к службе каталогов Active Directory осуществляется администратором доступа в подсистеме аутентификации и авторизации.

Для настройки подключения CEDM к службе каталогов Active Directory необходимо выполнить следующие действия:

- войти в ПАА с использованием учетной записи администратора доступа;
- в разделе НСИ открыть справочник «Внешние системы аутентификации» (рисунок 14).

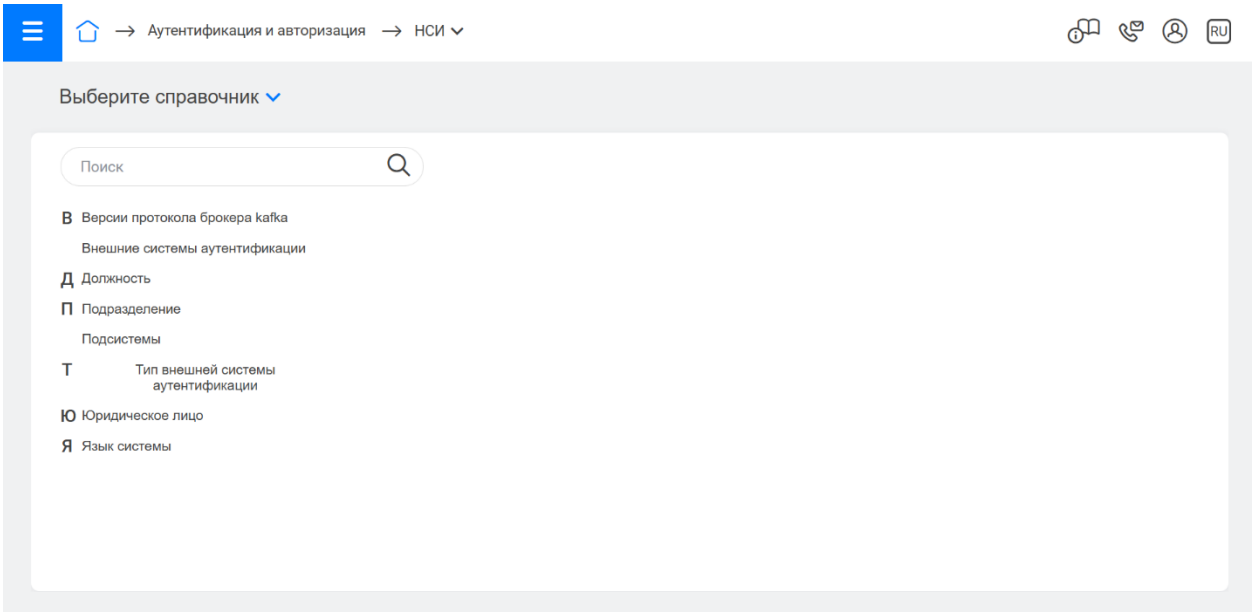

Рисунок 14. Экранная форма «НСИ». «Внешние системы аутентификации»

Для добавления внешней системы аутентификации необходимо нажать **+** в верхнем правом углу экранной формы справочника. Откроется карточка с параметрами подключения к внешней системе аутентификации:

- тип системы аутентификации – необходимо выбрать «Active Directory» из раскрывающегося списка;
- код – уникальный идентификатор подключения к внешней системе аутентификации в Системе. Можно использовать только латинские буквы верхнего регистра, например, «AD_MAIN»;
- Наименование – понятное название подключения к внешней системе аутентификации для удобства администрирования, например «Подключение к основному домену AD»;
- Активна – переключатель, определяющий активно ли текущее подключение к внешней системе аутентификации. Только при активном состоянии система будет запрашивать данные из службы каталогов AD;
- Домен – имя домена AD, к которому требуется подключение в формате «domain.ru»;
- URL – адрес подключения к серверу AD в одном из двух форматов:

– в виде полного URL сервера AD:

ldap://<hostname>.<domain_name>:<порт>

например:

ldap://ad_main.domain.ru:389

– в виде IP-адреса сервера AD:

ldap://<xxx.xxx.xxx.xxx>:<порт>

например:

ldap://192.168.10.200:389

где, 389 – порт протокола LDAP, используемый по умолчанию.
Возможно подключение к серверу AD по протоколу LDAPS:

ldaps://<hostname>.<domain_name>:<порт>

или

ldaps://<xxx.xxx.xxx.xxx>:<порт>

например:

ldaps://ad_main.domain.ru:636

или

ldaps://192.168.10.200:636

где, 636 – порт протокола LDAPS, используемый по умолчанию.

- Логин и Пароль – учетные данные пользователя AD с правами на чтение списка пользователей в службе каталогов;

- База поиска пользователей (baseDN) – путь в структуре каталогов AD, из которого будут извлекаться пользователи. Указывается без пробелов. Например:

OU=subunit11,OU=unit1,DC=domain,DC=ru

где:

  - OU (Organizational Unit) – организационное подразделение в дереве каталога AD для логической группировки объектов (пользователей и групп);
  - DC (Domain Component) – компоненты полного доменного имени (FQDN);
- Фильтр – фильтр учетных записей пользователей по атрибутам для импорта в Систему CEDM. Указывается без пробелов. Например:

(&(objectcategory=person)(objectclass=user)
(|(memberof=CN=group1,OU=subunit111,DC=domain,DC=ru)
(memberof=CN=group2,OU=subunit112,DC=domain,DC=ru))

где:

  - (&(objectcategory=person)(objectclass=user) – обязательная часть строки фильтра;
  - CN (Common Name) – имя группы;
  - *&* и | – логические операторы. Указываются слева от логических условий (&(условие1)(условие2)).

В данном примере в систему CEDM будут импортированы учетные записи пользователей, которые являются членами групп group1 или group2, входящих в организационные подразделения subunit111 и subunit112 соответственно. В свою очередь организационные подразделения subunit111 и subunit112 входят в subunit11.
Поле LDAP для уникального логина – атрибут учетной записи пользователя AD, который будет использоваться как логин при входе в систему. По умолчанию используется атрибут «sAMAccountName»;
Группа LDAP для назначения администратором доступа – группа AD пользователи, входящую в которую, станут администраторами ПАА и получат доступ к подсистеме ПАА. Например, group1. Остальные импортированные пользователи получат доступ к подсистемам,

указанным в поле «Доступные подсистемы».

- Доступные подсистемы – перечень подсистем, к которым будет предоставлен доступ импортированным из AD пользователям, не входящим в группу администраторов;
- Телефон СТП и Email СТП – контактные данные техподдержки по вопросам интеграции в AD.

Пример заполненной карточки «Внешние системы аутентификации» приведен на рисунке 15.

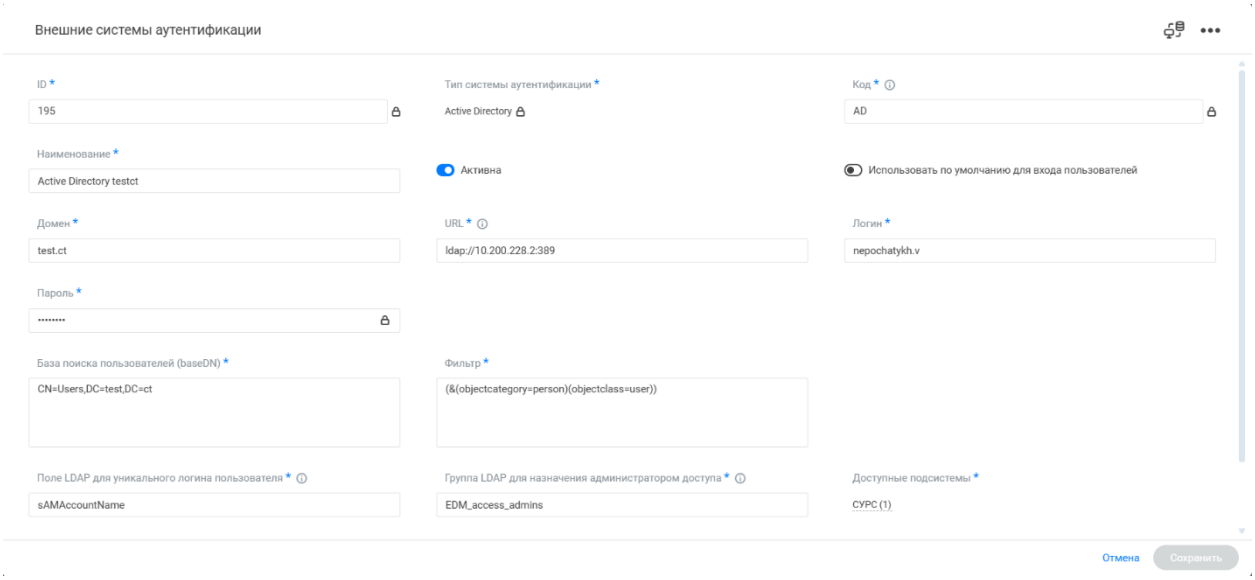

Рисунок 15. Карточка «Внешние системы аутентификации»

После внесения всех данных нажать кнопку «Сохранить», запись с внешней системой аутентификации появится в справочнике.

7.1.1. Проверка соединения Системы CEDM с Active Directory

Для проверки соединения Системы CEDM со службой каталогов в карточке «Внешние системы аутентификации» нажать (см. рисунок 4). Если соединение установлено, Система отобразит сообщение «Соединение установлено успешно». Если CEDM не удалось подключится, отобразится сообщение «Ошибка проверки соединения. Детальная информация в разделе «Мониторинг»».

События и ошибки подключения к службе каталогов Active Directory и импорта учетных данных пользователей отображается в журнале событий ПАА. Для просмотра ошибок, возникших в ходе проверки, выполнить следующие действия:

- перейти в раздел мониторинг и в журнале событий открыть событие с типом «Тест соединения с внешней системой аутентификации»;
- в карточке события раскрыть раздел «Ошибки».

7.1.2. Импорт данных пользователей из Active Directory

Запрос учетных записей пользователей осуществляется раз в 10 минут. Дата и время последнего запроса пользователей отображается в карточке внешней системы аутентификации. Импортированные учетные записи пользователей отображаются в разделе «Пользователи» с постфиксом <ad>, например konovalov.a<ad> (рисунок 16).

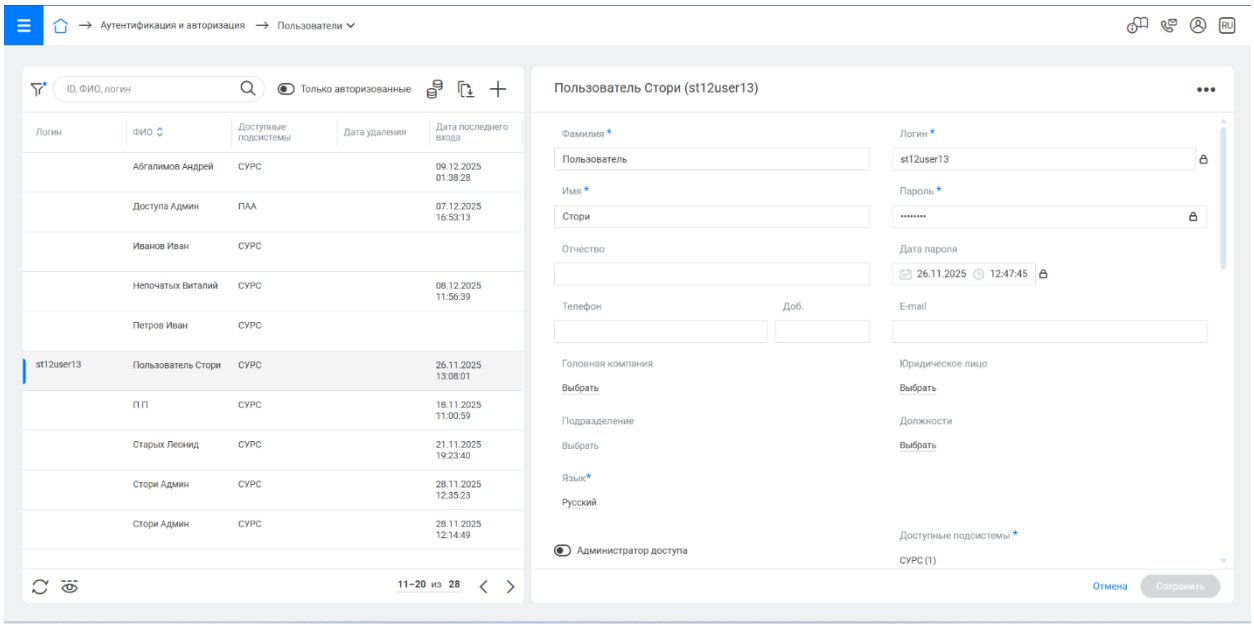

Рисунок 16. Экранная форма «Пользователи». Карточка УЗ пользователя, импортированного из AD

8. УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ И НАСТРОЙКА ДОСТУПА

Система CEDM использует гибкую ролевую модель для управления доступом пользователей к функциональности платформы. Управление учетными записями пользователей и ролями распределено между подсистемами ПАА и СУРС.

8.1. Типы администраторов в Системе CEDM

Администратор доступа (Администратор ПАА):

- управляет учетными записями пользователей (создание, редактирование, удаление);
- настраивает ограничения доступа по IP-адресам для пользователей;
- управляет интеграцией с внешними системами аутентификации.

Администратор СУРС:

- создает и управляет ролями пользователей;
- назначает роли пользователям;
- определяет права доступа для каждой роли.

8.1.1. Управление пользователями (Администратор ПАА)

Администраторы доступа выполняют следующие функции в подсистеме ПАА:

- создание новых учетных записей пользователей;
- редактирование существующих учетных записей;
- удаление учетных записей;
- настройка разрешенных IP-адресов для входа в систему;
- настройка интеграции с внешними системами аутентификации.

8.1.2. Управление ролями (Администратор СУРС)

Администраторы СУРС управляют ролями через интерфейс СУРС, где они могут:

- создавать новые роли;
- редактировать существующие роли;
- назначать пользователям соответствующие роли;

- настраивать права доступа для ролей, включая доступ к отдельным экранам, карточкам и группам устройств;
- настраивать возможности удаленного подключения к оконечным устройствам.

8.2. Виды учетных записей

В Системе CEDM существуют два основных вида учетных записей:

- локальные учетные записи, созданные непосредственно в ПАА CEDM;
- учетные записи, импортированные из внешних систем аутентификации, в частности из Active Directory (см. раздел 5).

Подробные инструкции по созданию и управлению учетными записями пользователей, а также по настройке ролей приведены в следующих разделах.

8.3. Создание, управление и удаление учетных записей пользователей

Создание, управление и удаление учетных записей пользователей Системы CEDM осуществляется администратором доступа в разделе «Пользователи» подсистемы ПАА. Экранная форма «Пользователи» приведена на рисунке 17.

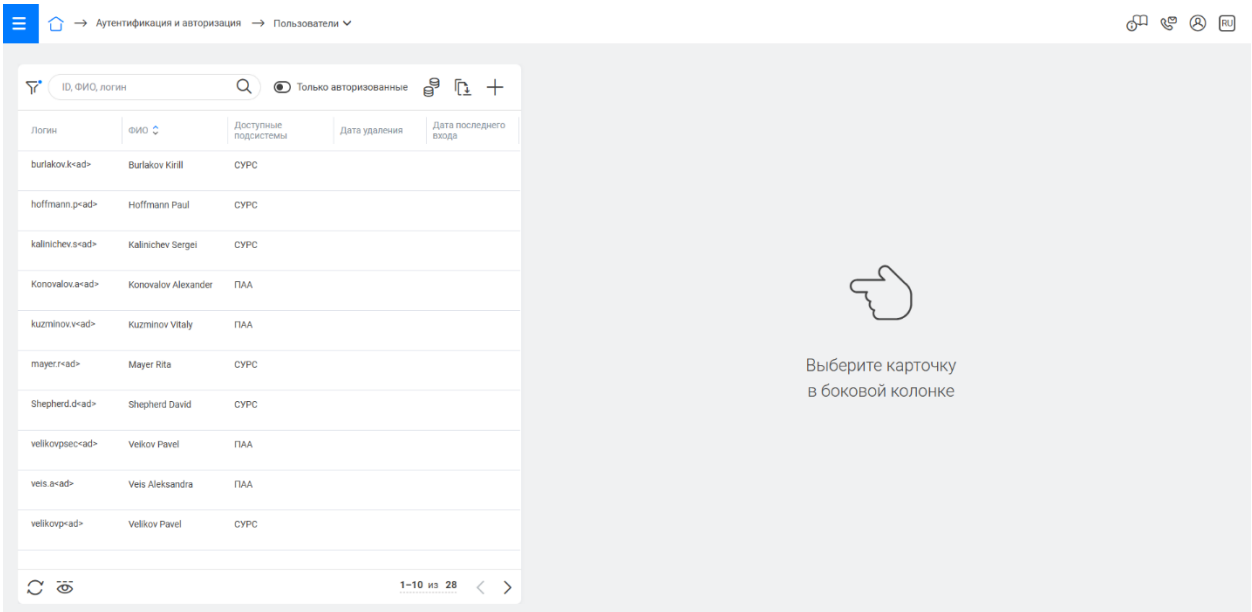

Рисунок 17. Экранная форма пользователи

В правой верхней части экранной формы находятся элементы управления списком пользователей:

- – фильтрация по любым свойствам учетной записи пользователя;
- – поиск пользователя по Ф. И. О. или логину;
- переключатель «Только активные» для отображения пользователей, которые в данный момент времени авторизованы в системе;
- – синхронизация списка пользователей;
- – выгрузка отчета со списком пользователей в формате csv;
- – создание нового пользователя.

8.3.1. Создание учетной записи пользователя

Для создания учетной записи пользователя необходимо нажать +. В правой части экрана откроется карточка для ввода данных пользователя (рисунок 18).

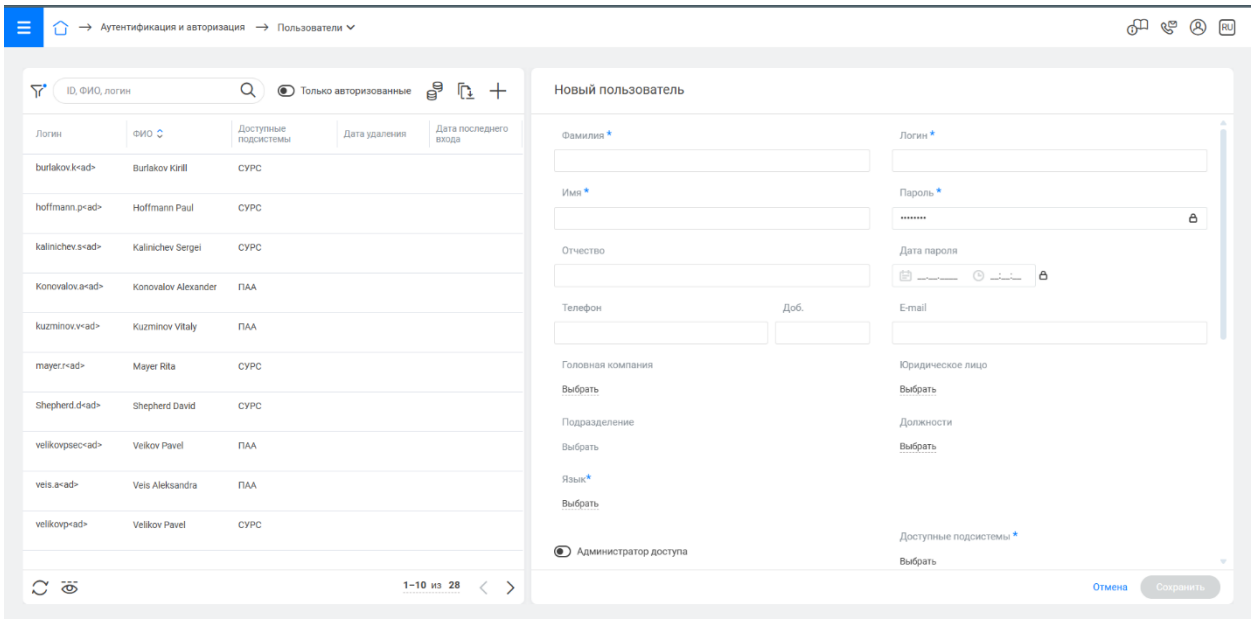

Рисунок 18. Экранная форма «Пользователи» → «Новый пользователь»

Для создания учетной записи пользователя необходимо заполнить поля с символом * и задать следующие параметры учетной записи:

- «Администратор доступа» – создание учетной записи администратора ПАА;

- «Доступные подсистемы» – создание учетной записи пользователя Платформы CEDM с доступом к выбранным подсистемам.

Параметры учетной записи «Администратор доступа» и «Доступные подсистемы» взаимоисключающие.

Доступные значения для полей «Головная компания», «Подразделение», «Юридическое лицо» и «Должности» задаются в разделе «НСИ» (см. раздел 7.2.3).

Поля со знаком заполняются Системой автоматически.

После заполнения полей нажать кнопку «Сохранить». Учетная запись пользователя появится в левой части экрана (рисунок 19).

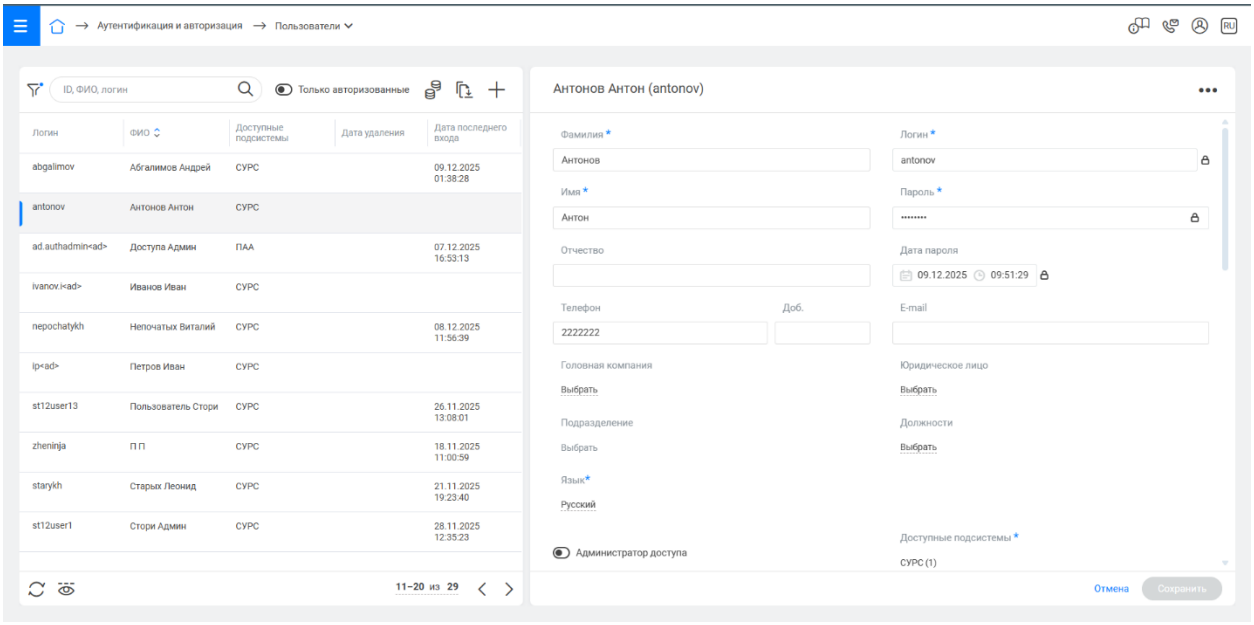

Рисунок 19. Учетная запись пользователя и ее параметры

8.3.2. Установка временного пароля

Для доступа пользователя к системе необходимо задать временный пароль его учетной записи. Для этого необходимо в левой части в экранной формы «Пользователи» выбрать нужную запись, в правой части нажать ••• и выбрать «Задать временный пароль» (рисунок 20).

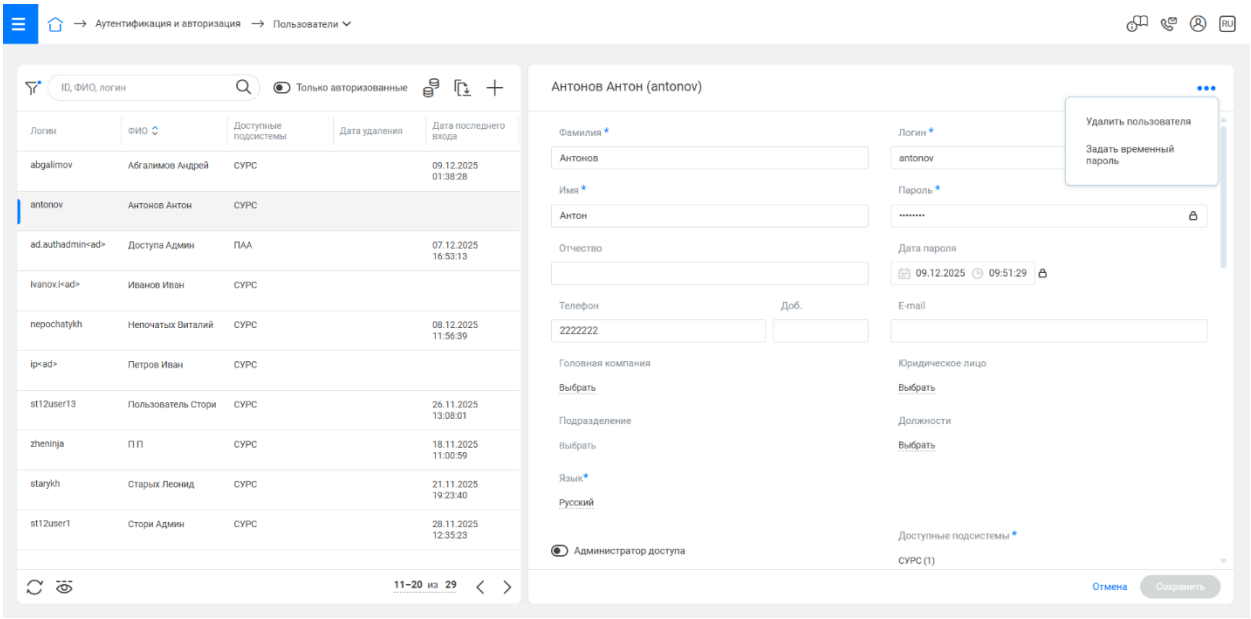

Рисунок 20. Задание временного пароля

Появится диалоговое окно, в котором необходимо ввести пароль и нажать «Применить» (рисунок 21).

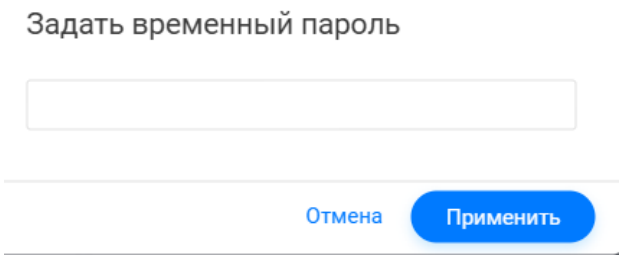

Рисунок 21. Диалоговое окно ввода временного пароля

Если пароль не соответствует требованиям безопасности появится предупреждение (рисунок 22).

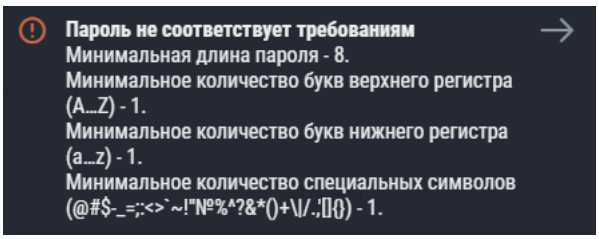

Рисунок 22. Предупреждение «Пароль не соответствует требованиям»

При первом входе пользователя в Систему CEDM потребуется смена временного пароля.

8.3.3. Редактирование учетной записи пользователя

Для редактирования учетной записи пользователя необходимо в левой части в экранной формы «Пользователи» выбрать нужную запись и в правой части экрана изменить доступные поля. Нажать кнопку «Сохранить». Данные учетной записи обновятся в Системе.

8.3.4. Удаление учетной записи пользователя

Для удаления учетной записи пользователя необходимо в левой части в экранной формы «Пользователи» выбрать нужную запись, в правой части нажать ••• и выбрать «Удалить пользователя». В диалоговом окне подтвердить операцию. Учетная запись пользователя будет удалена без возможности восстановления.

Учетную запись пользователя с логином, совпадающим с одним из удаленных, создать невозможно.

8.3.5. Настройка доступных IP-адресов

В настройках учетной записи пользователя возможно задать перечень разрешенных IP-адресов, с которых пользователь может осуществлять вход в Платформу CEDM. Для этого необходимо в левой части в экранной формы «Пользователи» выбрать нужную запись, в правой части экрана перейти в раздел «Доступные IP-адреса» (рисунок 23).

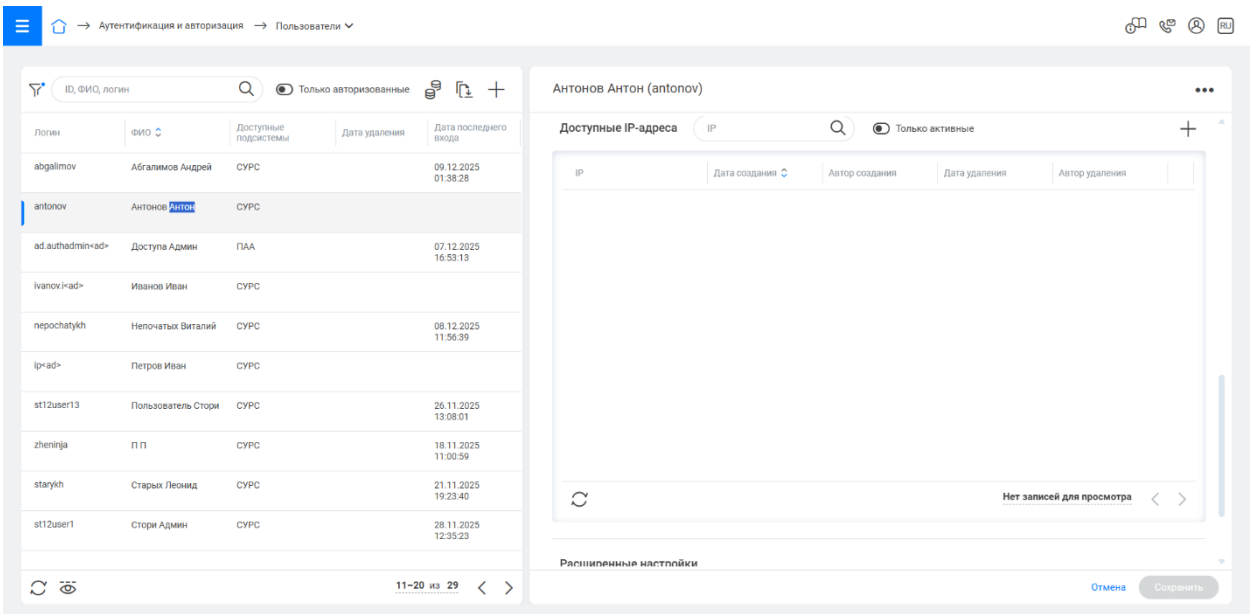

Рисунок 23. Окно настройки доступных IP-адресов

Для добавления IP-адреса необходимо нажать + и в появившемся диалоговом окне ввести IP-адрес и нажать «Применить» (рисунок 24). Созданная запись появится в таблице доступных IP-адресов.

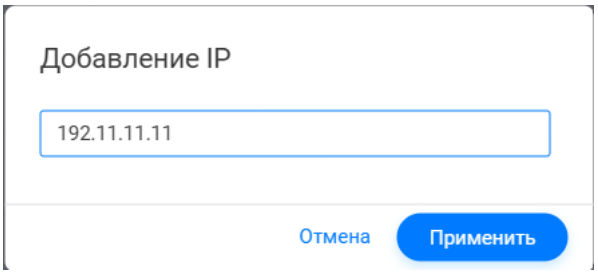

Рисунок 24. Окно ввода IP-адреса

При входе пользователя с IP-адреса, не входящего в перечень разрешенных, отобразится следующее сообщение: «IP-адрес подключения не соответствует установленным администратором для выбранной учетной записи».

8.3.6. Карточка учетной записи пользователя из Active Directory

Карточка учетной записи пользователя, импортированной из AD, отличается от локальной УЗ (рисунок 25) и имеет следующие отличительные атрибуты:

- актуальный – атрибут свидетельствует о том, учетная запись пользователя была передана в Систему при последней синхронизации с AD;
- внешняя система аутентификации – наименование внешней системы аутентификации – источника УЗ пользователя;
- memberOF – членство УЗ пользователя в организационных подразделениях (OU), группах (CN) и доменах (DC) AD;
- objectGUID – уникальный идентификатор учетной записи AD;
- JSON – выгрузка атрибутов УЗ в файл формата JSON.

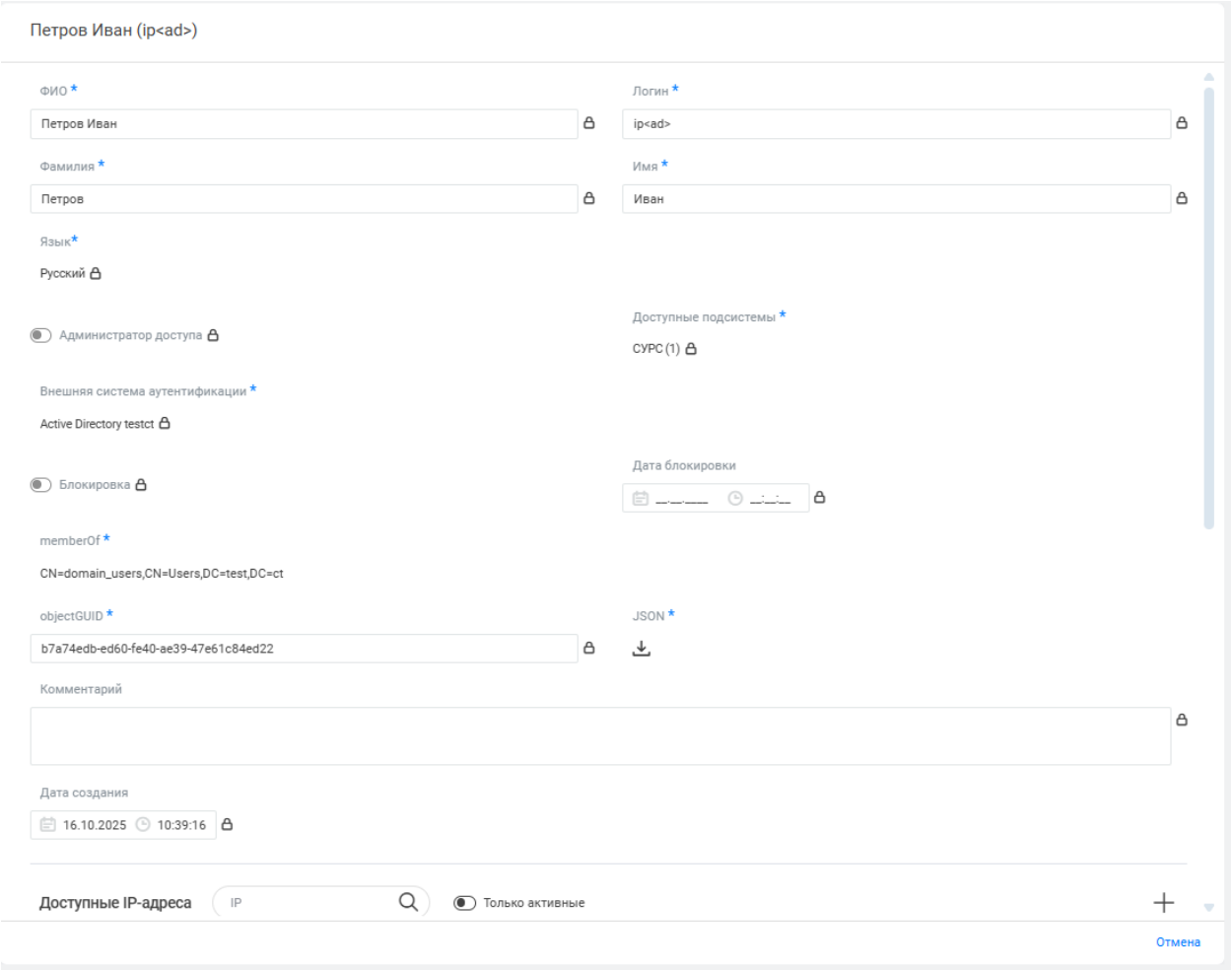

Рисунок 25. Карточка УЗ пользователя, полученной из AD

Атрибуты УЗ не доступны для редактирования за исключением настройки доступных IP-адресов (см. раздел 8.5 настоящего руководства).

8.3.7. Синхронизация списка пользователей

Подсистема аутентификации и авторизации осуществляет автоматическую синхронизацию списка пользователей как со внешней системой аутентификации, так и системой управления рабочими станциями. При необходимости администратор может синхронизировать данные принудительно.

Для принудительной выгрузки УЗ пользователей в СУРС необходимо выполнить следующие действия:

- нажать и в появившемся диалоговом окне выбрать «Выгрузка»;
- в пункте «Подсистема» выбрать СУРС;
- нажать «Ок».

Подсистема аутентификации и авторизации произведет синхронизацию данных УЗ пользователей с СУРС.

Для принудительной загрузки УЗ пользователей из Active Directory необходимо выполнить следующие действия:

нажать и в появившемся диалоговом окне выбрать «Загрузка»;

в пункте «Внешняя система аутентификации» выбрать источник.

Подсистема аутентификации и авторизации произведет синхронизацию данных УЗ пользователей со службой каталогов.

8.4. Настройка доступа (роли и пользователи)

Создание, управление и удаление ролей, а также назначение их пользователям осуществляется в разделе «Администрирование» -> «Настройка доступа» подсистемы СУРС.

8.4.1. Раздел «Роли»

Раздел «Роли» предназначен для создания, просмотра и настройки ролей пользователей (рисунок 26).

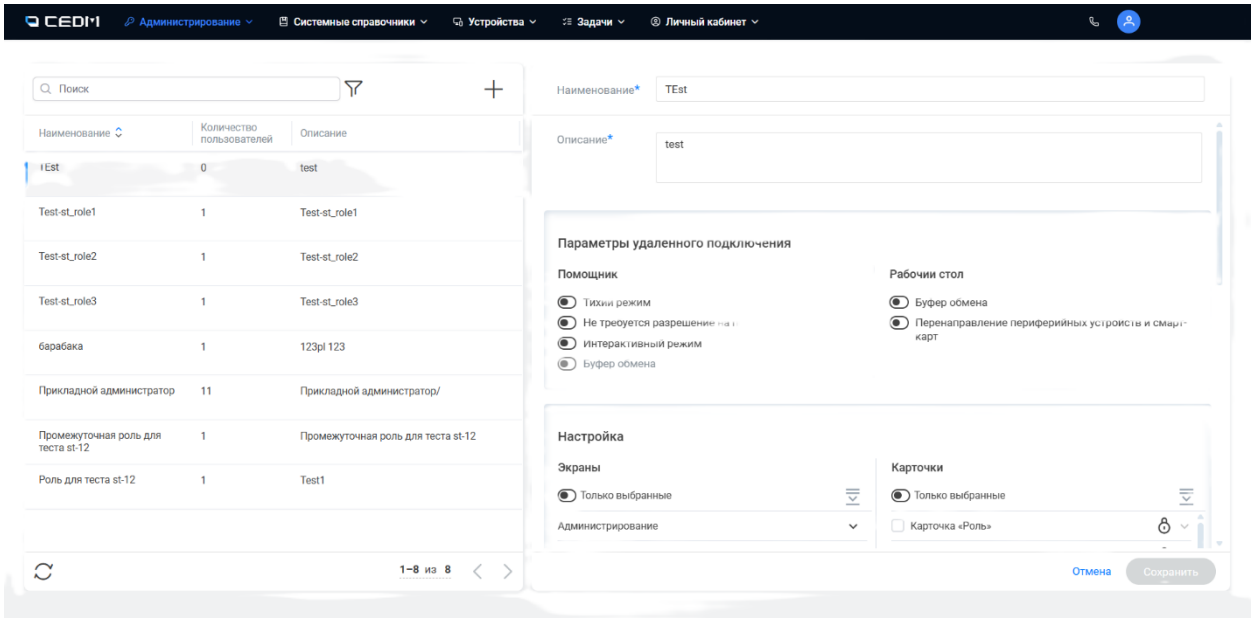

Рисунок 26. Экранная форма «Роли»

Параметры роли

Параметры роли сгруппированы на несколько функциональных блоков:

- «Параметры удаленного подключения» – настройка доступа пользователя CEDM к функциям удаленного рабочего стола;

- «Экраны» – настройка доступа пользователя к разделам веб-интерфейса CEDM;
- «Карточки» – настройка доступа к карточкам, вкладкам и функционалу разделов Системы.

Функциональный блок «Параметры удаленного подключения» включает два раздела:

- «Помощник» – настройка подключения к удаленному столу в сессию пользователя в режиме помощника;
- «Рабочий стол» – настройка подключения к удаленному столу в режиме перехвата сессии пользователя или в новую сессию.

Система CEDM позволяет осуществлять следующие настройки параметров удаленного подключения:

- «Тихий режим» – режим подключения к удаленному рабочему столу без запроса разрешения и уведомления пользователя удаленного устройства. Включение «Тихого режима» влечет включение режима «Не требуется разрешение на подключение»;
- «Не требуется разрешение на подключение» – режим подключения к удаленному рабочему столу без запроса разрешения, но с уведомлением пользователя оконечного устройства;
- «Интерактивный режим» – отвечает за доступ пользователя CEDM к управлению удаленным рабочим столом, включая мышь и клавиатуру, а также возможность использования комбинации горячих клавиш;
- «Буфер обмена» – доступ к возможности использовать общего буфера обмена для копирования текста с оконечного устройства рабочее место пользователя CEDM и обратно. Режим доступен при включенном «Интерактивном режиме».

Поиск роли

Для поиска роли необходимо выполнить следующие действия:

- перейти в экранную форму «Роли»;
- ввести часть названия роли в поисковой строке в верхней левой части рабочей области экранной формы и нажать кнопку  в правой части поля ввода (см. рисунок 26).

Фильтрация списка ролей

Для фильтрации списка ролей необходимо выполнить следующие действия:

- перейти в экранную форму «Роли»;
- нажать на кнопку в верхней части рабочей области экранной формы (см. рисунок 26);
- настроить фильтры (рисунок 27):

Экраны – множественный выбор из справочника;

Карточки – множественный выбор из справочника.

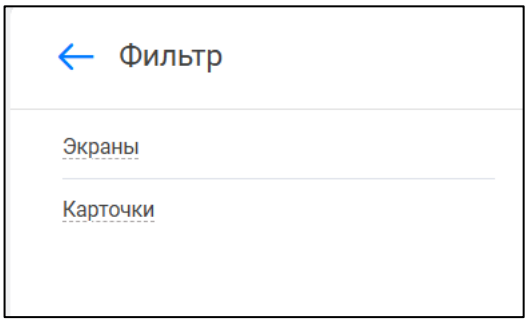

Рисунок 27. Фильтрация списка ролей

Просмотр роли

Для просмотра роли необходимо выполнить следующие действия:

- перейти в экранную форму «Роли»;
- нажать левой кнопкой мыши строку с ролью, в правой части откроется карточка роли (рисунок 28).

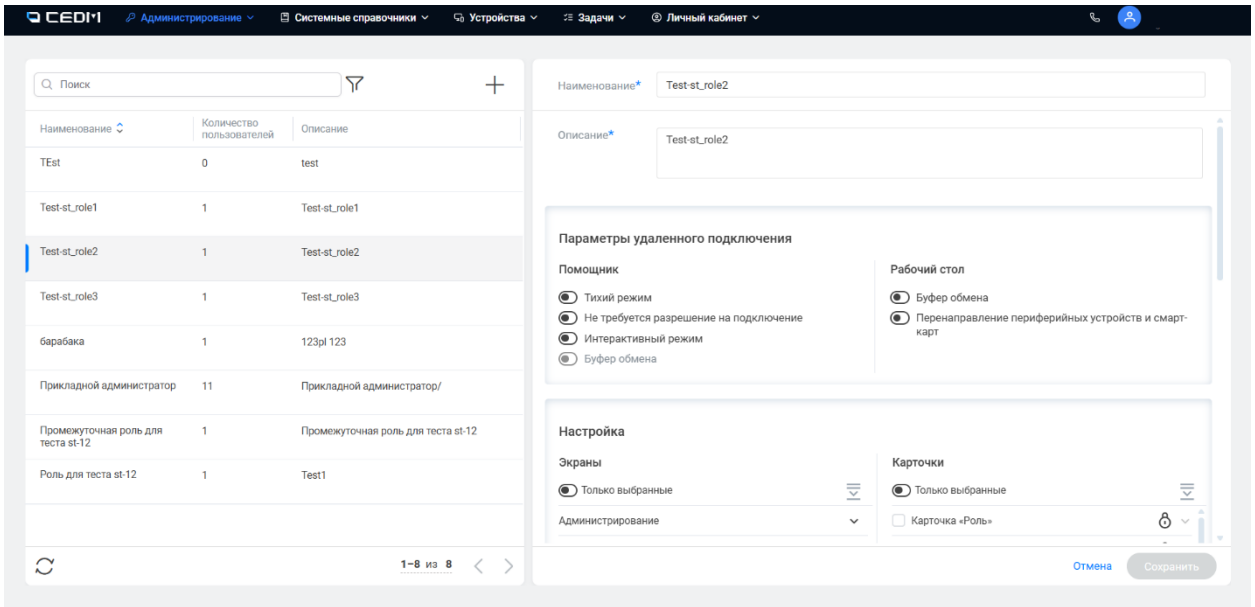

Рисунок 28. Карточка роли

Добавление новой роли

Для добавления роли необходимо выполнить следующие действия:

- перейти в экранную форму «Роли»;
- нажать кнопку + в верхней правой части списка ролей;
- заполнить карточку:
  - указать наименование;
  - заполнить описание;
  - предоставить доступ к экранам (для этого необходимо нажать на кнопку с изображением закрытого замка, после нажатия кнопка должна отображаться в виде открытого замка);
  - предоставить доступ к необходимым карточкам (переключая кнопку с на), вкладкам и их функциям (переключая чек-бокс в активное положение);
  - нажать кнопку «Сохранить».

В любой момент времени возможно прервать процесс добавления роли нажатием на кнопку «Отмена» (требуется подтверждение действия).

Удаление роли

Для удаления роли необходимо выполнить следующие действия:

- перейти в экранную форму «Роли»;
- нажать на роль, которую требуется удалить;
- нажать кнопку в правом верхнем углу рабочей области экранной формы;
- подтвердить удаление.

Редактирование роли

Для редактирования роли необходимо выполнить следующие действия:

- перейти в экранную форму «Роли»;
- нажать на роль, которую требуется изменить;
- внести изменения в роль, аналогично процессу добавления роли;

- после внесения необходимых изменений нажать на кнопку «Сохранить»;

В любой момент времени возможно прервать процесс редактирования роли нажатием на кнопку «Отмена» (требуется подтверждение действия).

8.4.2. Раздел «Пользователи»

Раздел предназначен для назначения групп устройств и ролей пользователям СУРС CEDM (рисунок 29), импортированных из подсистемы Аутентификации и авторизации (ПАА).

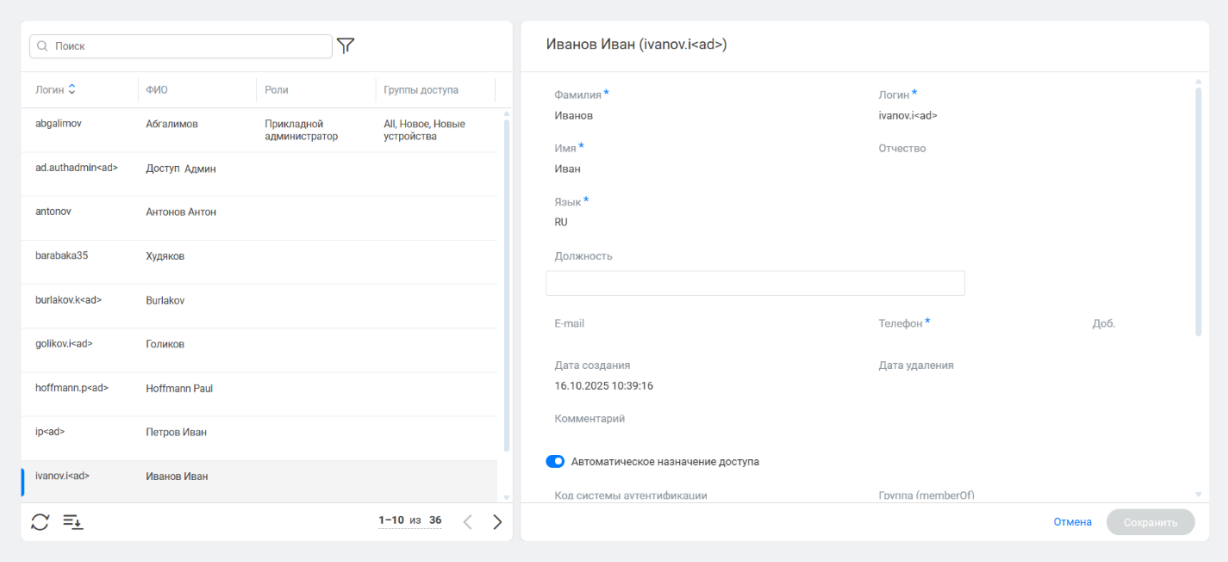

Рисунок 29. Экранная форма «Пользователи»

Поиск пользователя

Для поиска роли необходимо выполнить следующие действия:
перейти в экранную форму «Пользователи;
ввести часть названия ФИО или логина в поисковой строке в верхней левой части рабочей области экранной формы и нажать кнопку 🔍 в правой части поля ввода (см. рисунок 29).

Фильтрация списка пользователей

Для фильтрации списка пользователей необходимо выполнить следующие действия:

- перейти в экранную форму «Пользователи;
- нажать на кнопку ▽ в верхней части рабочей области экранной формы (см. рисунок 29).

- настроить фильтры (рисунок 30):
  - Тип роли – выпадающий список;
  - Роли – множественный выбор из справочника.

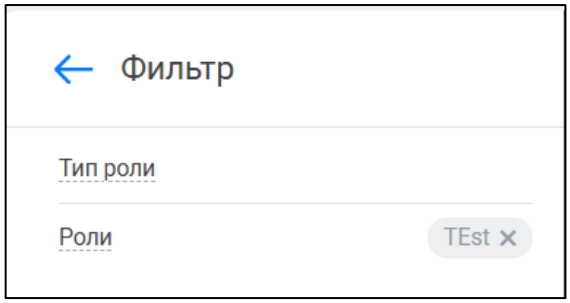

Рисунок 30. Фильтрация списка пользователей

Просмотр пользователя

Для просмотра пользователя необходимо выполнить следующие действия:

- перейти в экранную форму «Пользователи;
- нажать левой кнопкой мыши на строку с пользователем, в правой части откроется карточка пользователя (рисунок 31).

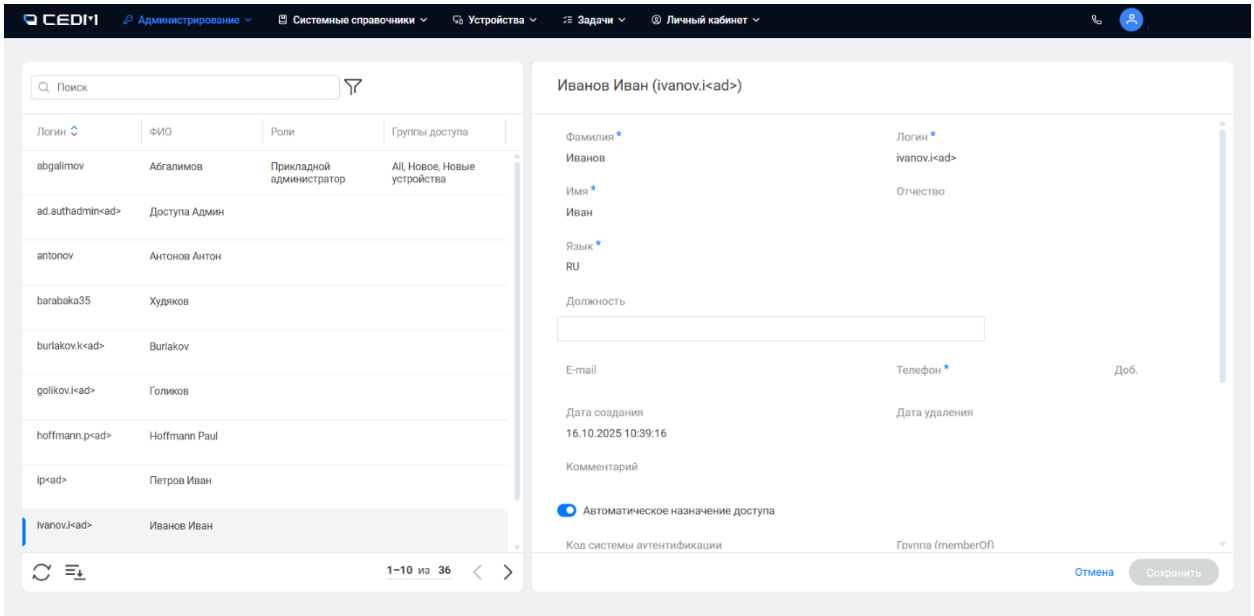

Рисунок 31. Карточка пользователя

Редактирование карточки пользователя

Для редактирования профиля пользователя необходимо выполнить следующие действия:

- перейти в экранную форму «Пользователи»;
- нажать на пользователя, которого требуется изменить;
- внести изменения в следующие доступные для изменения поля карточки пользователя:
  - Группы устройств – выбор устройств, к которым у пользователя будет доступ;
  - Настройка ролей – выбор ролей для пользователя из созданных в разделе «Роли» («Общая») или персональная настройка доступа («Персональная»). При выборе персональной настройки доступа открывается форма с параметрами доступа аналогичными рассмотренным в разделе 6.4.1;
  - после внесения необходимых изменений нажать кнопку «Сохранить».

В любой момент времени возможно прервать процесс редактирования пользователя нажатием на кнопку «Отмена» (требуется подтверждение действия).

8.4.3. Раздел «Автоматическое назначение доступа»

Раздел «Автоматическое назначение доступа» предназначен для автоматического назначения ролей и групп устройств пользователям при импорте их учетных записей из Active Directory. Механизм позволяет обеспечить соответствие между группами AD и правами доступа в системе CEDM.

Экранная форма «Автоматическое назначение доступа» содержит таблицу с правилами автоназначения со следующими полями (рисунок 32):

- ID – уникальный идентификатор правила;
- Активно – статус активности правила (Да/Нет);
- Код системы аутентификации – идентификатор внешней системы аутентификации;
- Группа (memberOf) – группа в Active Directory, для которой применяется правило;
- Назначаемые роли – роли в Системе CEDM, которые будут автоматически назначены пользователям из указанной группы AD;
- Назначаемые группы устройств – группы устройств в

Системе CEDM, к которым будет предоставлен доступ пользователям из указанной группы AD.

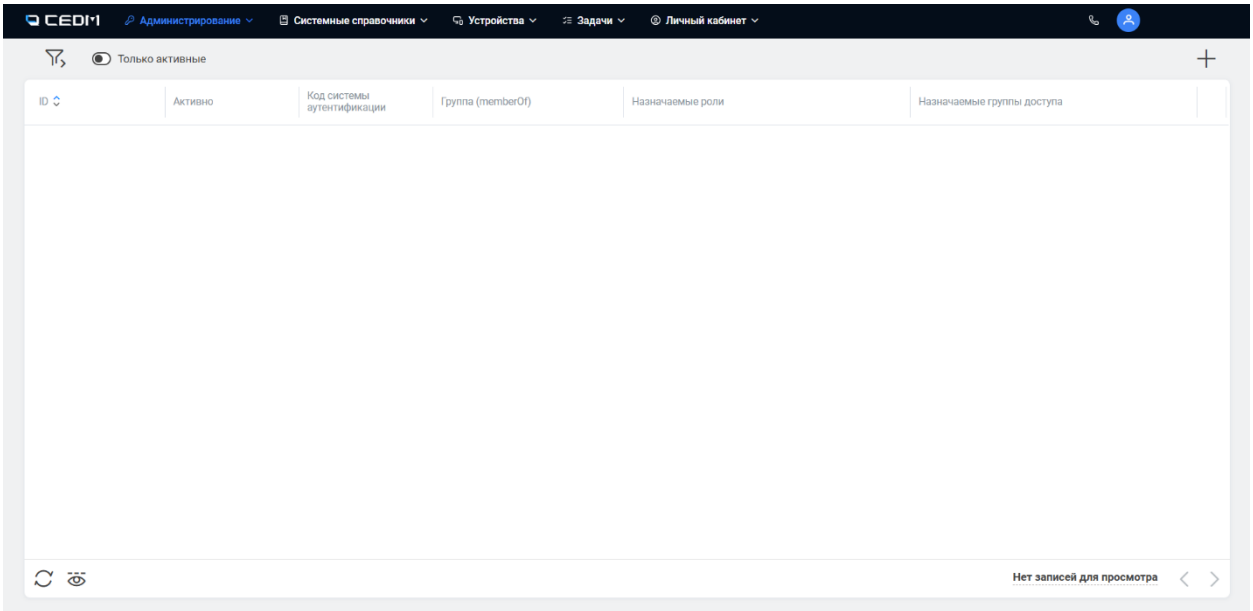

Рисунок 32. Автоматическое назначение ролей

Создание нового правила

Для создания нового правила нажать + в правом верхнем углу экрана. Откроется карточка автоматического назначения доступа (рисунок 33). В открывшейся карточке заполнить следующие блоки:

Основная информация

включить переключатель «Активно» для активации правила.

Условия назначения доступа

Код системы аутентификации* – указать код внешней системы аутентификации (например, AD);
Группа (memberOf)* – указать Distinguished Name (DN) группы в AD, для которой применяется правило. Задается через запятую без пробелов. Пример DN:

CN=CEDM_admin,CN=CEDM_Users,OU=IT_depart,DC=CEDM.compan_name,DC=ru

Назначаемые роли* – выбрать роли в Системе CEDM, которые будут назначены пользователям из указанной группы AD. Можно выбрать одну или несколько ролей;
Назначаемые группы устройств* – выбрать группы устройств в Системе CEDM, к которым будет предоставлен доступ пользователям из указанной группы AD. Можно выбрать одну или несколько групп

устройств.

Тип операции с учетной записью пользователя

Указать типы операций с учетной записью в подсистеме аутентификации и авторизации (ПАА), при выполнении которых будет срабатывать правило автоматического назначения доступа:

- Добавление – выполнять правило при добавлении нового пользователя в ПАА из AD;
- Редактирование – выполнять правило при изменении учетной записи в ПАА;
- Синхронизация с ПАА – выполнять правило при осуществлении полной выгрузки списка пользователей из ПАА.

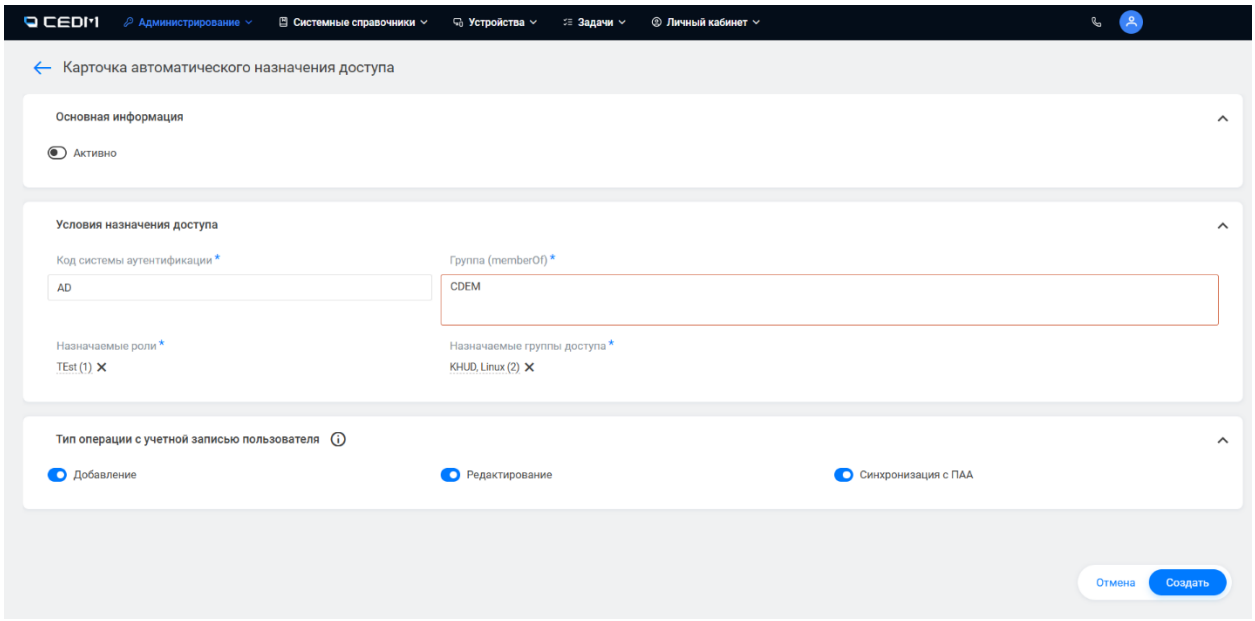

Рисунок 33. Создание правила автоматического назначения доступа

Нажать кнопку «Создать» для сохранения правила.

Примечание: поля, отмеченные звездочкой (*), обязательны для заполнения.

После создания правило начнет действовать автоматически при импорте новых пользователей AD из ПАА или при изменении существующих учетных записей AD в ПАА.

Удаления правила

Для удаления правила нажать 🗑. Появится диалоговое окно предупреждения (рисунок 34). Для удаления нажать «Подтвердить», для отмены удаления – «Отменить».

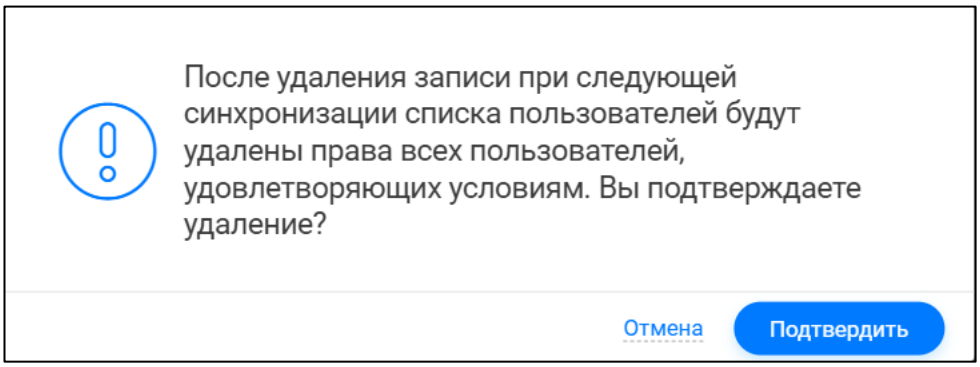

Рисунок 34. Диалоговое окно предупреждения

Примечание: при удалении правил, назначенные пользователям права доступа будут отозваны при очередной синхронизации с ПАА.

9. УПРАВЛЕНИЕ ПОДСИСТЕМОЙ ПАА

9.1. Настройка системных параметров ПАА

Настройка системных параметров осуществляется в разделе «Системные параметры» подсистемы ПАА. Экранная форма «Системные параметры» приведена на рисунке 35.

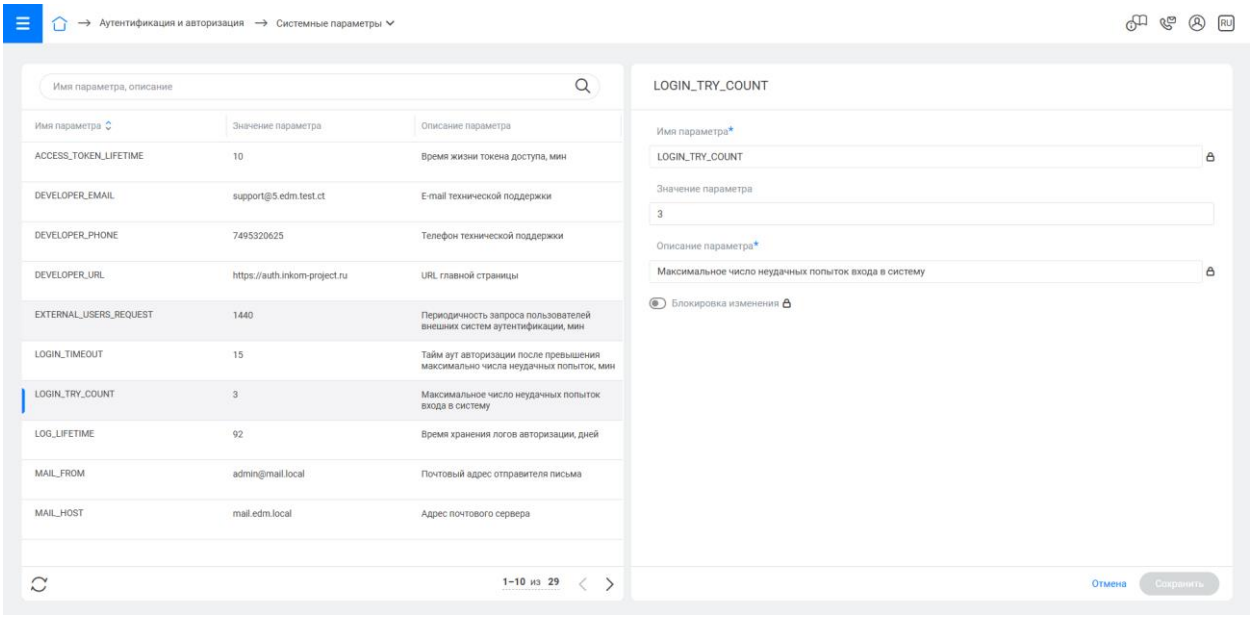

Рисунок 35. Экранная форма «Системные параметры»

Описание системных параметров приведено в таблице 3.

Таблица 3. Системные параметры CEDM

Наименование параметра	Описание параметра
ACCESS_TOKEN_LIFETIME	Время жизни токена доступа, мин. (от 1 до 10)
DEVELOPER_EMAIL	E-mail технической поддержки
DEVELOPER_PHONE	Телефон технической поддержки
DEVELOPER_URL	URL официальной страницы продукта
EXTERNAL_USERS_REQUEST	Периодичность запроса пользователей внешних систем аутентификации, мин
LOG_LIFETIME	Время хранения логов авторизации, дней
LOGIN_TIMEOUT	Тайм аут авторизации после превышения максимально числа неудачных попыток, мин.

LOGIN_TRY_COUNT	Максимальное число неудачных попыток входа в систему
PASS_COMPLEXITY_LENGTH	Минимальная длина пароля
PASS_COMPLEXITY_LOWERCASES	Минимальное количество букв нижнего регистра в пароле
PASS_COMPLEXITY_NUMBERS	Минимальное количество цифр в пароле
PASS_COMPLEXITY_SPECIAL_CHARACTERS	Минимальное количество спецсимволов в пароле
PASS_COMPLEXITY_UPPERCASES	Минимальное количество букв верхнего регистра в пароле
PASSWORD_MAX_LIFETIME	Максимальный срок действия пароля, дней
PASSWORD_MIN_LIFETIME	Минимальный срок действия пароля, дней
PASSWORD_MIN_NUM_CHANGING_CHARACTERS	Минимальное количество изменяемых символов при смене пароля
PASSWORD_RECOVERY_LINK_LIFETIME	Срок действия ссылки восстановления пароля, мин
PHONE_LENGHT	Количество символов в номере телефона в карточке пользователя
PRODUCT_FULL_NAME	Полное наименование продукта
PRODUCT_SHORT_NAME	Краткое наименование продукта
RECENT_PASSWORDS_BANNED_FROM_USE	Количество последних паролей, запрещенных к использованию
REFRESH_TOKEN_LIFETIME	Время жизни токена обновления, мин. (от 10 до 1440)

При изменении значения системных параметров из списка ниже будет необходима смена пароля всеми пользователями при следующем входе в Платформу:

- PASS_COMPLEXITY_UPPERCASES;
- PASS_COMPLEXITY_LOWERCASES;
- PASS_COMPLEXITY_NUMBERS;
- PASS_COMPLEXITY_SPECIAL_CHARACTERS;
- PASS_COMPLEXITY_LENGHT;
- PASSWORD_MAX_LIFETIME;

- PASSWORD_MIN_NUM_CHANGING_CHARACTERS.

9.2. Просмотр и редактирование нормативно-справочной информации (НСИ)

Просмотр и редактирование нормативно-справочной информации осуществляется в разделе НСИ. Экранная форма «НСИ» приведена на рисунке 36.

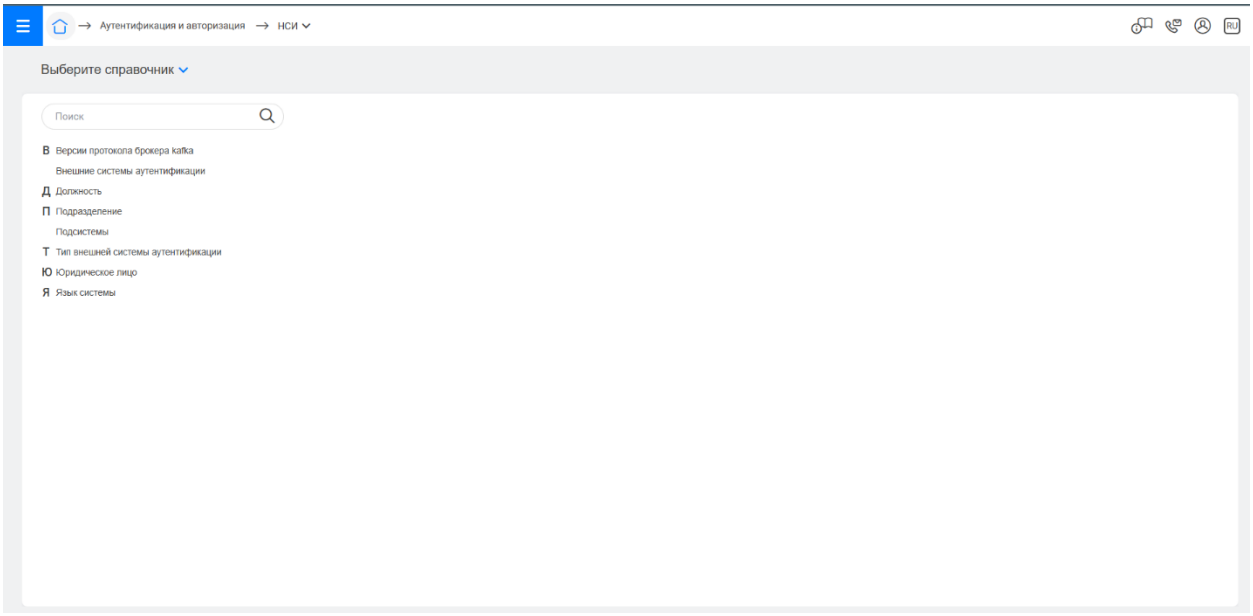

Рисунок 36. Экранная форма «НСИ»

9.2.1. Справочник «Подсистемы»

Справочник подсистемы предназначен для редактирования и добавления подсистем Системы CEDM (рисунок 37).

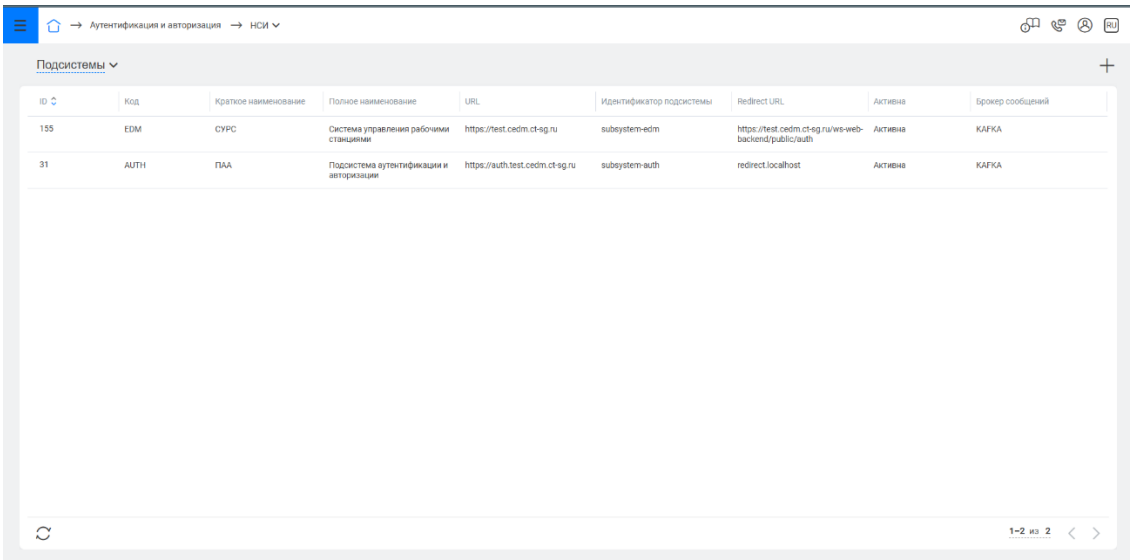

Рисунок 37. Экранная форма «НСИ». «Подсистемы»

Поля карточки «Подсистемы»:

- ID – уникальный цифровой идентификатор подсистемы;
- Код – уникальный буквенный идентификатор подсистемы;
- Краткое наименование – краткое пользовательское наименование подсистемы;
- Полное наименование – полное пользовательское наименование подсистемы;
- Наименование очереди – название топика системы брокера сообщений Kafka, в который из ПАА будут отправляться сообщения о затрагиваемых пользователях (добавление/изменение/удаление) для данной подсистемы;
- URL – адрес для осуществления переходов пользователей в подсистему;
- Идентификатор подсистемы – уникальная строка, идентифицирующая подсистему;
- Redirect URL – элемент реализации протокола авторизации OAuth2;
- Активна – статус подсистемы;
- IP-адрес брокера Kafka – адрес брокера сообщений Kafka;
- Версия протокола брокера Kafka – используемая подсистемой версия протокола брокера Kafka.

9.2.2. Справочник «Версии протокола брокера Kafka»

Содержит версии протокола брокера Kafka которые могут быть использованы в подсистемах CEDM.

9.2.3. Справочники «Должность», «Подразделение», «Юридическое лицо»

Справочники используются для хранения значений соответствующих полей учетной записи пользователя (см. раздел 6.3).

9.2.4. Справочник «Внешние системы аутентификации»

См. раздел «Интеграция CEDM со службой каталогов Active Directory».

9.2.5. Добавление значений в справочники

Для добавления значений в справочники необходимо выполнить следующие действия:

- нажать на кнопку + в верхнем правом углу экранной формы выбранного справочника (рисунок 38);

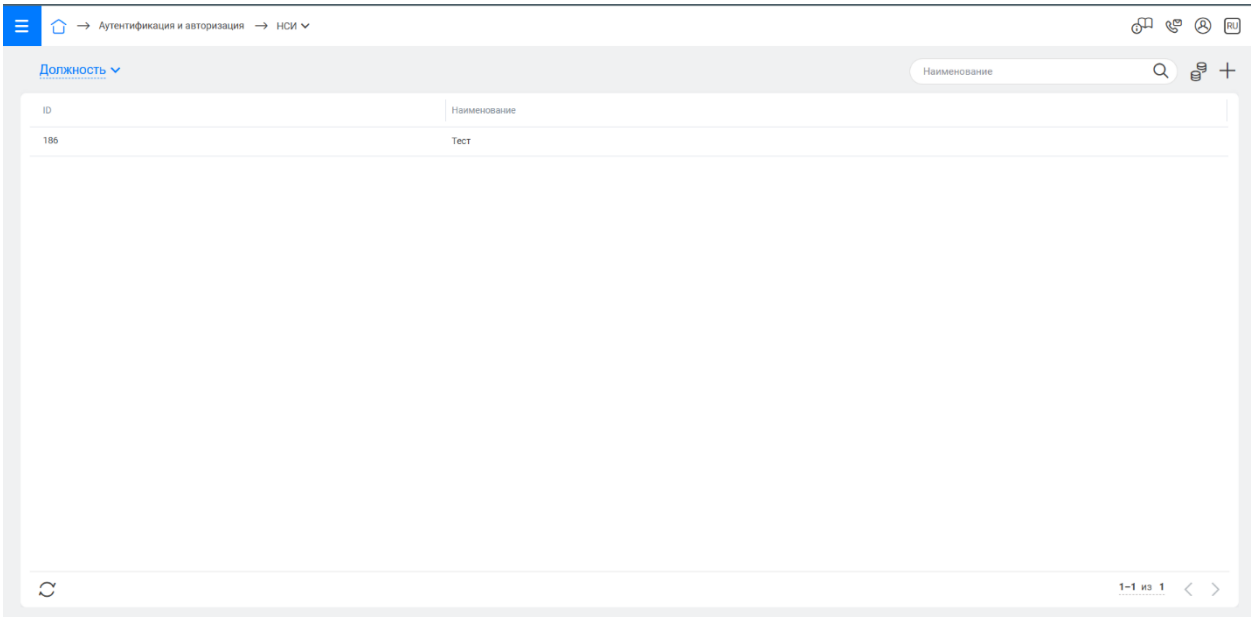

Рисунок 38. Экранная форма «НСИ». Справочник «Должность»

- в появившемся диалогом окне ввести название должности и нажать кнопку «Сохранить» (рисунок 39).

Рисунок 39. Диалоговое окно добавления записи в справочник

Добавленное значение отобразится в справочнике.

10. УПРАВЛЕНИЕ ПОДСИСТЕМОЙ СУРС

Управление подсистемой СУРС осуществляется в разделе «Администрирование».

10.1. Настройка Системы

10.1.1. Экранная форма «Настройки истории инвентаризации»

Экранная форма «Настройки истории инвентаризации» предназначена для настройки отслеживания изменений атрибутов инвентаризации оконечных устройств.

Структура экранной формы

В левой части отображается иерархическое дерево категорий инвентаризационных данных. При выборе категории в центральной части отображается список подкатегорий и элементов данной категории. При выборе конкретного элемента в правой части формы отображаются перечень его атрибутов в виде имени и чекбокса, отвечающего за включение/отключение его отслеживания (рисунок 40).

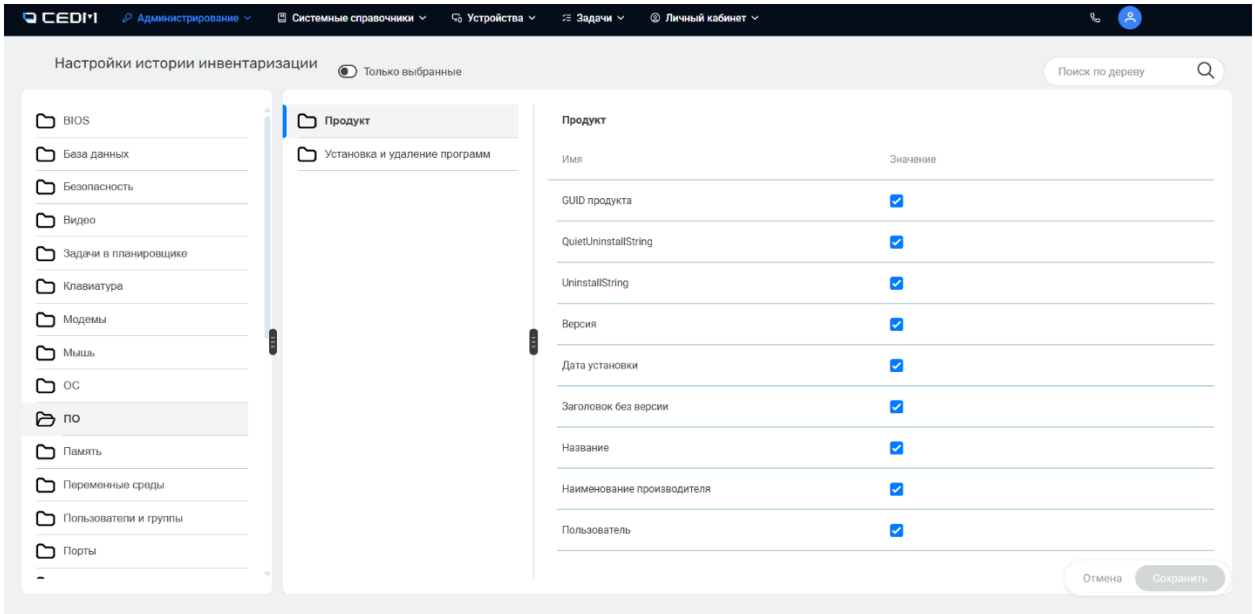

Рисунок 40. Экранная форма «Настройки истории инвентаризации»

Настройка отслеживания атрибутов

Для включения отслеживания изменений атрибута необходимо:

- выбрать категорию в дереве инвентаризации;
- в списке атрибутов активировать переключатель

напротив нужного атрибута;

- нажать кнопку «Сохранить».

Изменения значений отслеживаемых атрибутов будут доступны в карточке устройства на вкладке «Инвентаризация» – «История изменений».

10.1.2. Экранная форма «Системные параметры»

Экранная форма «Системные параметры» предназначена для настройки основных параметров работы Системы CEDM (рисунок 41).

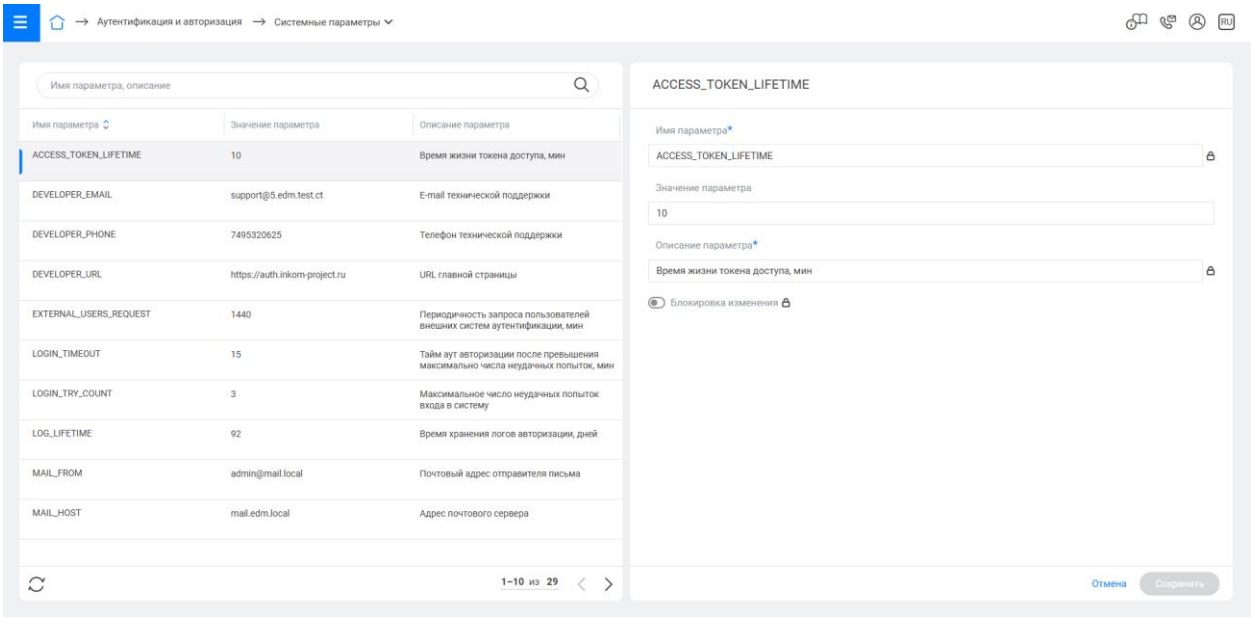

Рисунок 41. Экранная форма «Системные параметры»

Системные параметры CEDM

Описание системных параметров СУРС CEDM приведено в таблице 4.

Таблица 4. Системные параметры СУРС CEDM

Наименование параметра	Описание параметра
AGENT_CACHING_PERIOD	Период кэширования данных агентов (дней)
AGENT_CMD_QUEUE_CLEAR_DAYS	срок хранения данных в очереди команд агентам в случае отсутствия связи с агентом (дней)
AGENT_INSTALLERS_PAGE_PUBLIC	публичный доступ к веб-интерфейсу загрузки установщиков агентов (true или false)

AUTH_URL	URL подсистемы аутентификации и авторизации
FILE_SIZE	Максимальный размер загружаемого файла в файловое хранилище (Мб)
ORGANIZATION_NAME	Наименование вендора
PRODUCT_FULL_NAME	Полное наименование продукта
PRODUCT_SHORT_NAME	Краткое наименование продукта
REISSUE_AGENT_KEYS_BEFORE_EXPIRES_DAYS	Количество дней до окончания срока действия сертификата, за которое Система осуществляет его автоматический перевыпуск и отправку
SUPPORT_EMAIL	e-mail технической поддержки для обращений
SUPPORT_EMAIL_FROM	e-mail технической поддержки с которого отправляются рассылки
SUPPORT_PHONE	Телефон технической поддержки
TIMEOUT_ARCHIVE_TRANSFER	Если устройство не выходит на связь указанное количество дней, то ему будет присвоен статус «Архив». В случае появления устройства в сети после присвоения статуса «Архив» его статус снова будет изменен на «Активен»

10.1.3. Экранная форма «Расписание запуска задач»

Экранная форма «Расписание запуска задач» предназначена для управления системными задачами, которые выполняются по расписанию (рисунок 42).

Элементы расписания отображаются в таблице со следующими полями:

- Имя – системное имя задачи;
- Наименование – описательное название задачи;
- Тип – тип сервиса (Backend/Database);
- График запуска – расписание запуска в формате CRON;
- Статус выполнения – текущий статус задачи (Включено/Выключено);
- Логирование запусков – признак ведения журнала выполнения (Да/Нет);
- Код события – системный код события;
- Описание задачи – подробное описание

выполняемых действий.

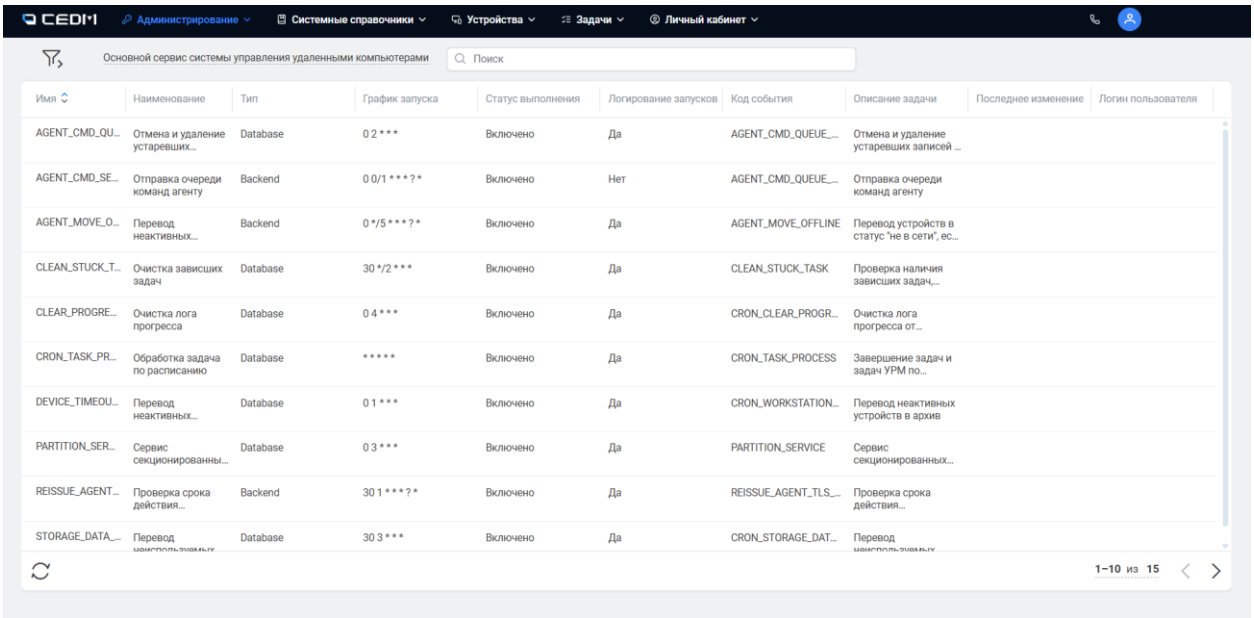

Рисунок 42. Экранная форма «Расписание запуска задач»

Редактирование расписания запуска задачи

Для редактирования расписания запуска задачи выполнить двойной щелчок на строке с требуемой задачей. Откроется карточка задачи (рисунок 43). В открывшейся карточке заполнить следующие поля:

- график запуска* – ввести текстовое выражение в формате CRON;
- Статус выполнения* – включить/выключить выполнение задачи.

Примечание: график запуска задается в формате CRON, где пять звездочек соответствуют: минуты (0-59), часы (0-23), день месяца (1-31), месяц (1-12), день недели (0-6, где 0 – воскресенье). Например:

- 0 2 * * * – запуск каждый день в 02:00
- 0 0/1 * * * ? – запуск каждый час
- 0 */5 * * * ? – запуск каждые 5 часов
- 0 3 * * 1 – запуск каждый понедельник в 03:00

Звездочка (*) означает «любое значение» в соответствующей позиции.

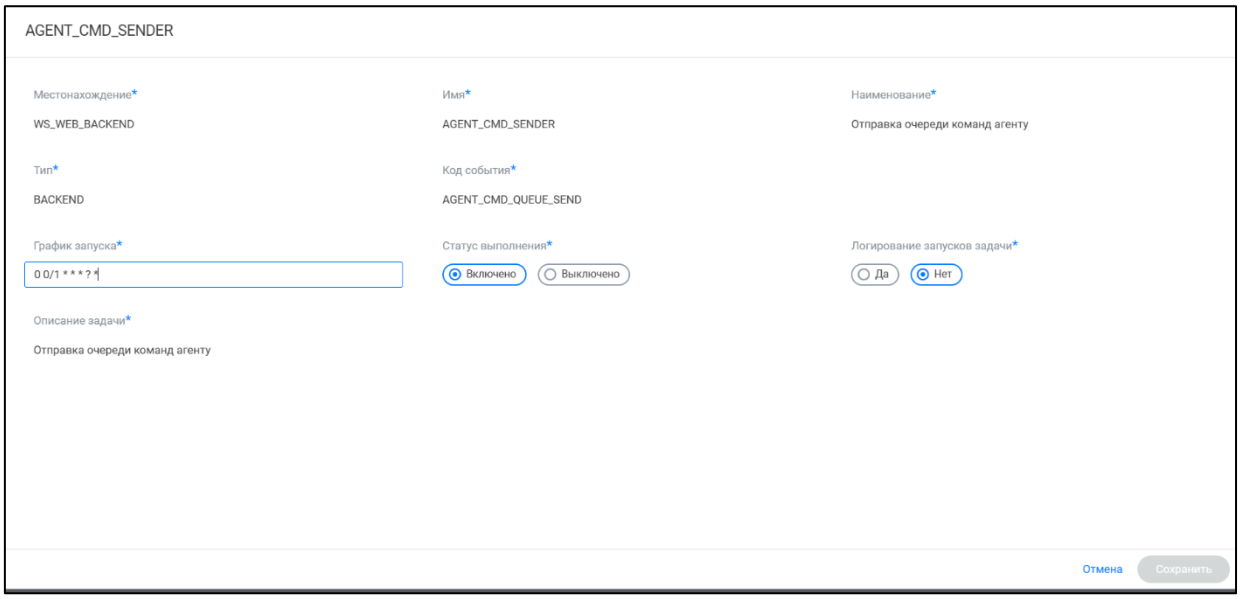

Рисунок 43. Карточка задачи

10.1.4. Экранная форма «Безопасность»

Раздел «Безопасность» предназначен для настройки параметров безопасного взаимодействия между агентами и сервером системы CEDM. В данном разделе администратор может:

- выбрать модель безопасности агент-серверного взаимодействия;
- настроить параметры аутентификации и шифрования;
- управлять сертификатами агентов и сервера;
- генерировать ключи и сертификаты;
- просматривать статистику безопасности.

Вкладка «Общие настройки»

Блок «Статистика»

В блоке «Статистика» отображается актуальная статистика по состоянию безопасности системы (рисунок 44):

- Успешно аутентифицировано агентов за последние сутки – количество аутентифицированных агентов, соответствующее фактическому числу подключенных агентов в Системе;
- Ошибок аутентификации агентов за последние сутки – количество агентов с неудачной аутентификацией;
- Ожидает подтверждения сертификата – количество агентов, ожидающих утверждения администратором;
- Требуется обновить агентов – количество агентов,

которые требуется обновить;

- Статистика по срокам действия сертификатов – количество агентов со сроком действия сертификатов менее 30 дней, менее 7 дней, а также с истекших сроком действия сертификата.

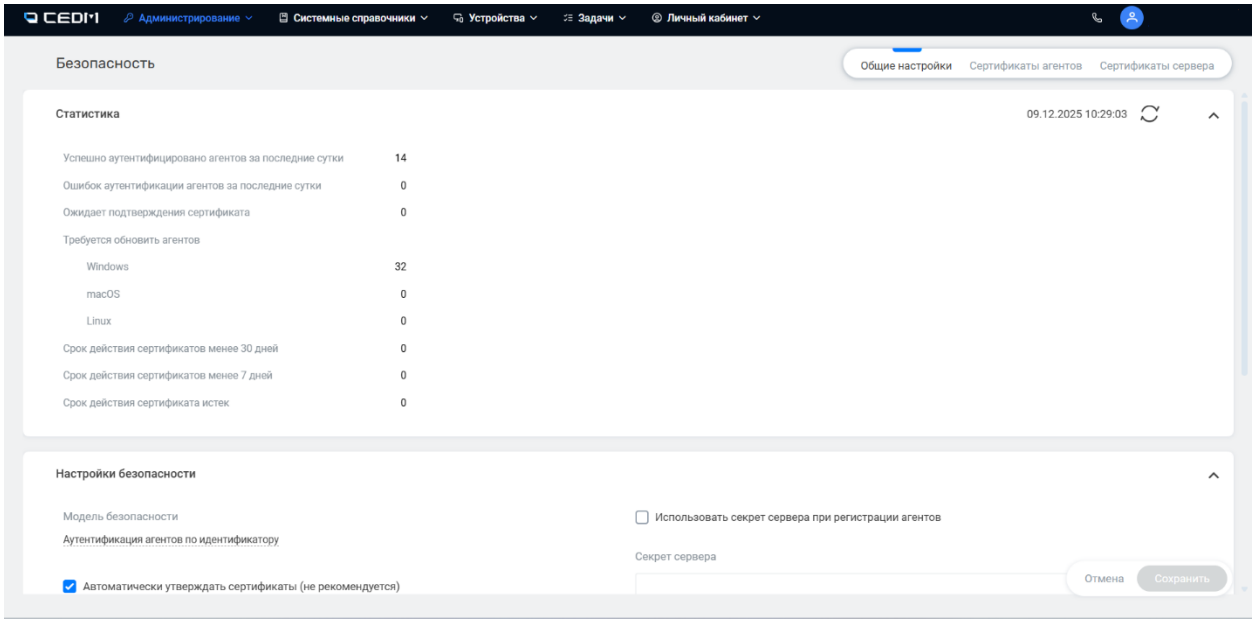

Рисунок 44. Экранная форма «Безопасность» – блок «Статистика»

Блок «Настройка безопасности»

Блок «Настройка безопасности» предназначен для управления основными параметрами безопасного взаимодействия агентов и сервера Системы CEDM (рисунок 45).

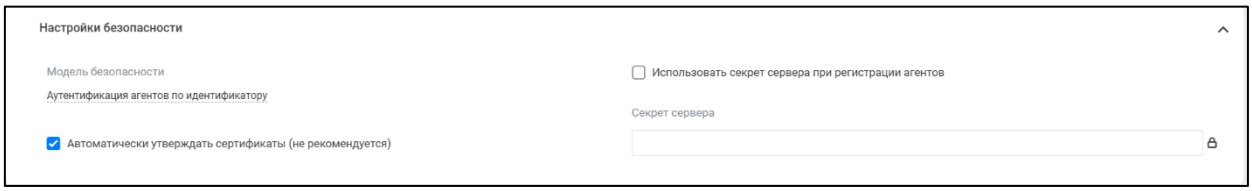

Рисунок 45. Экранная форма «Безопасность» – блок «Настройки безопасности»

В блоке доступны следующие настройки:

Модель безопасности – выбор модели безопасности агент-серверного взаимодействия.

В системе CEDM доступны следующие модели безопасности:

- Аутентификация агентов по идентификатору (значение по умолчанию) – базовая модель аутентификации.
- На основе сертификатов – защищенная модель

аутентификации с использованием mTLS.

Модель безопасности «Аутентификация агентов по идентификатору»

Преимущества модели:

- простота развертывания и настройки;
- быстрая регистрация новых агентов;
- минимальные требования к инфраструктуре.

Ограничения:

- базовый уровень безопасности по сравнению с моделью на основе сертификатов;
- отсутствие взаимной аутентификации;
- зависимость от защищенности канала передачи данных.

Модель безопасности «На основе сертификатов»

Преимущества модели:

- Взаимная аутентификация – и сервер, и агент проверяют подлинность друг друга;
- Криптографическая защита – использование проверенных алгоритмов шифрования;
- Защита от MITM-атак – невозможность перехвата и подмены трафика;
- Невозможность подделки агентов – каждый агент имеет уникальный подписанный сертификат;
- Защита целостности данных – гарантия неизменности передаваемых данных.

Ограничения:

- сложность первоначальной настройки – требует понимания PKI и сертификатов;
- риски при миграции развернутой Системы с подключенными агентами – потеря связи с агентами при неправильном переходе.

Параметры сертификатов определяются в блоке «Генерация ключей и сертификатов».

Автоматически утверждать сертификаты (не рекомендуется) – автоматическое утверждение сертификатов агентов при их подключении к серверу. По умолчанию отключено. Сертификаты утверждает администратор на вкладке «Сертификаты агентов»

Использовать секрет сервера при подключении агентов – дополнительная проверка при регистрации агентов. При включении данной опции:

- в конфигурацию агента при сборке установщика добавляется зашифрованный секрет (строка символов);
- при регистрации агент отправляет секрет для проверки;
- при несовпадении секрета регистрация не производится.

Секрет сервера – поле для указания секрета сервера. Становится доступным при включении опции «Использовать секрет сервера».

Примечание: при включении/отключении опции «Использовать секрет сервера при регистрации агентов» или изменении секрета сервера все имеющиеся установщики агентов становятся недействительными.

Блок «Генерация ключей и сертификатов»

Блок «Генерация ключей и сертификатов» предназначен для задания параметров агентских и серверных сертификатов, создаваемых Системой CEDM (рисунок 46).

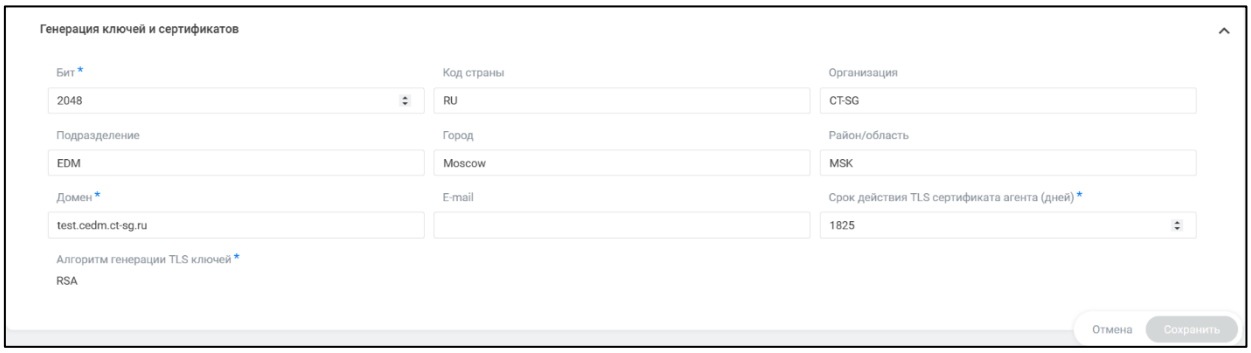

Рисунок 46. Экранная форма «Безопасность» – блок «Генерация ключей и сертификатов»

Доступны следующие параметры сертификатов:

- Бит* – длина ключа в битах;
- RU – двухбуквенный код страны согласно ISO 3166-1;
- Организация – название организации;
- Подразделение – название подразделения организации;
- Город – город регистрации организации;
- Район/область – район или область города;
- Домен* – доменное имя Системы CEDM. Должно

соответствовать реальному домену Системы CEDM;

- E-mail – электронная почта для связи;
- Срок действия TLS сертификата агента (дней)* – период действия сертификата агента;
- Алгоритм генерации TLS ключей* – алгоритм шифрования для генерации ключей.

Изменение параметров влияет только на новые генерируемые сертификаты, существующие остаются без изменений.

Вкладка «Сертификаты агентов»

Вкладка предназначена для управления ключами и сертификатами агентов, которые используются для защищенного агент-серверного взаимодействия по протоколу mTLS.

Сертификаты агентов отображаются в виде таблице со следующими полями (рисунок 47):

- Статус ключа – текущий статус ключа агента (Архив, Создан, Не утвержден, Утвержден, Заблокирован);
- Имя компьютера – сетевое имя устройства;
- ID устройства – уникальный идентификатор устройства в системе;
- Статус устройства – текущий статус устройства (Архив, Создан, Активен, Заблокирован, Ожидает подтверждения);
- В сети – наличие сетевого подключения устройства (В сети, Не в сети);
- Отпечаток – уникальный идентификатор (хеш) сертификата;
- Последнее подключение – дата и время последнего подключения устройства к серверу;
- Срок действия – дата окончания действия сертификата;
- Адрес – IP-адрес устройства;
- Устройство – вызов диалогового окна с детальной информации об устройстве.

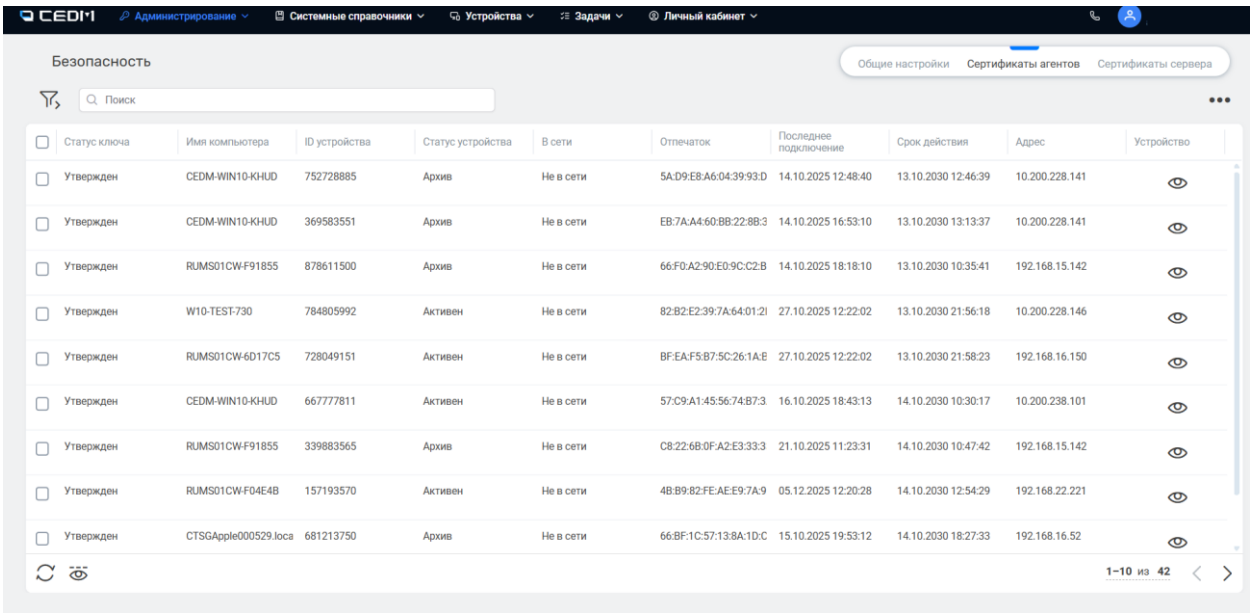

Рисунок 47. Экранная форма «Безопасность» – вкладка «Сертификаты агентов»

Управление сертификатами агентов

Управления сертификатами агентов осуществляется через выпадающее меню ●●● , которое включает следующие пункты:

Утвердить ключ агента – сервер подписывает сертификат агента своим закрытым ключом, отправляет подписанный сертификат агенту и переводит статус устройства в «Активен». Устройство получает возможность защищенного подключения к серверу.

Заблокировать ключ агента – временная блокировка доступа устройства к серверу. Устройство переводится в статус «Заблокирован». При попытке подключения устройства к серверу соединение будет отклонено.

Перевыпустить ключ агента – создание нового сертификата для устройства. Используется при компрометации текущего сертификата или плановой замене.

Разблокировать ключ агента – возобновление доступа ранее заблокированного устройства.

Вкладка «Сертификаты сервера»

Вкладка предназначена для управления сертификатами, используемыми сервером CEDM для защищенного взаимодействия с агентами (рисунок 48).

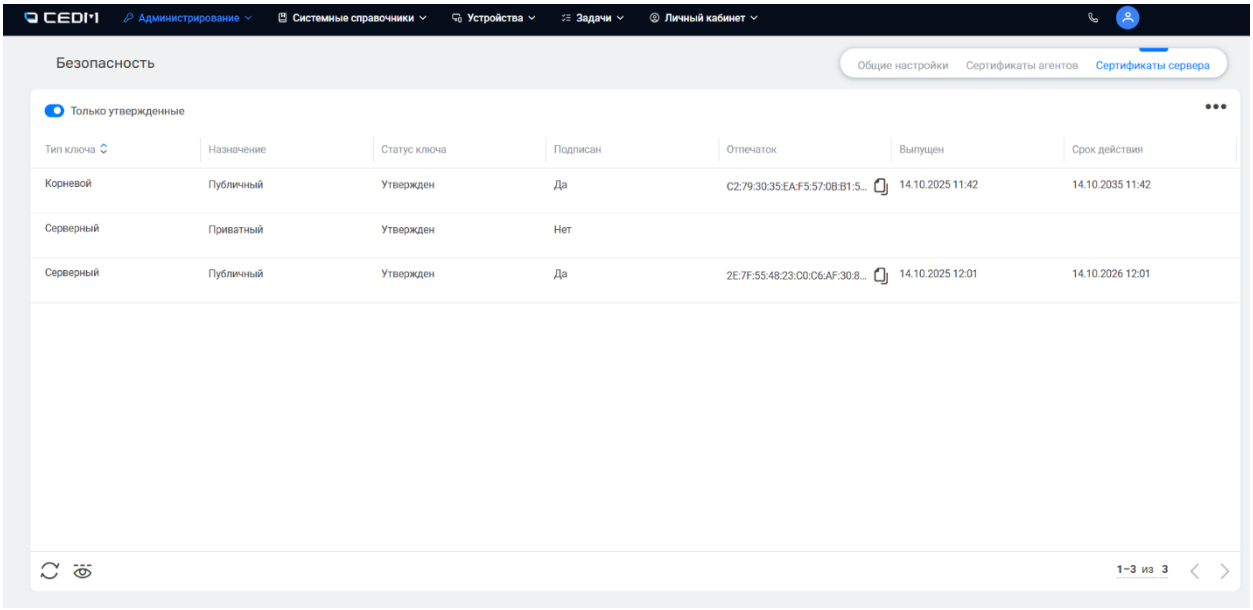

Рисунок 48. Экранная форма «Безопасность» – вкладка «Сертификаты сервера»

Сертификаты сервера отображаются в виде таблицы со следующими полями:

- Тип ключа – тип ключа (Корневой, Серверный);
- Назначение – назначение ключа (Публичный/Приватный);
- Статус ключа – текущий статус ключа (Утвержден, Не утвержден, Архив)
- Подписан – наличие подписи (Да/Нет);
- Отпечаток – уникальный идентификатор сертификата;
- Выпущен – дата и время выпуска сертификата;
- Срок действия – дата окончания срока действия сертификата.

Управление сертификатами сервера

Управление сертификатами сервера осуществляется через выпадающее меню ●●● , которое включает следующие пункты:

- **Загрузить корневой** – загрузка корневого сертификата;
- **Загрузить подписанный сертификат сервера** – загрузка подписанного публичного сертификата сервера;
- **Загрузить закрытый ключ сервера** – загрузка закрытого ключа сервера;

- **Генерировать закрытый ключ сервера** – создание закрытого ключа сервера;
- **Создать CSR** – создание запроса на подпись серверного сертификата.

Для имеющихся в системе сертификатов сервера доступны следующие действия через контекстное меню (по нажатию правой кнопки мыши):

Архивировать ключ сервера – перевод сертификата в статус «Архив». Такие сертификаты остаются в системе для обеспечения аудита, но не используются для новых подключений;

Скачать ключ сервера – скачивание файла сертификата в формате .crt;

Распространить корневой сертификат – отправка корневого сертификата на все активные агенты. Доступно только для корневого сертификата в статусе «Утвержден» с актуальной датой действия. При выполнении операции:

- уа все активные агенты создается запись в очереди команд с командой отправки корневого сертификата;
- при получении команды агент добавляет сертификат в свое хранилище, если такой сертификат отсутствует.

Утвердить – утверждение сертификата (для сертификатов в статусе «Не утвержден»).

При нажатии на строке таблицы отображается дополнительная информация о сертификате:

Алгоритм – алгоритм шифрования;

Бит – длина ключа в битах;

Код страны – двухбуквенный код страны;

Организация – организация, выпустившая сертификат;

Домен – доменное имя в формате FQDN, для которого выпущен корневой сертификат;

CRL – URL списка отозванных сертификатов.

Создание и добавление серверных ключей в Систему

1. **Добавление корневого сертификата в Систему**

Для добавления корневого сертификата в Систему выполнить следующие шаги:

- в выпадающем меню ••• выбрать пункт «Загрузить корневой сертификат».
- в появившемся стандартном диалоговом окне открытия файла выбрать корневой сертификат;
- в контекстном меню (по нажатию правой кнопки мыши) на строке с сертификатом выбрать «Утвердить».

2. Получение закрытого серверного ключа

Закрытый ключ сервера можно получить двумя способами: сгенерировать новый или загрузить существующий.

2.1. Генерация нового закрытого ключа сервера

Для создания нового закрытого ключа выполнить следующие шаги:

- в выпадающем меню ••• выбрать пункт «Генерировать закрытый ключ сервера».
- в появившемся диалоговом окне подтвердить действие;
- в диалоговом окне «Генерировать ключ» (рисунок 49) выбрать параметры закрытого ключа сервера и нажать «Продолжить»;
- в контекстном меню (по нажатию правой кнопки мыши) на строке с закрытым сертификатом выбрать «Утвердить».

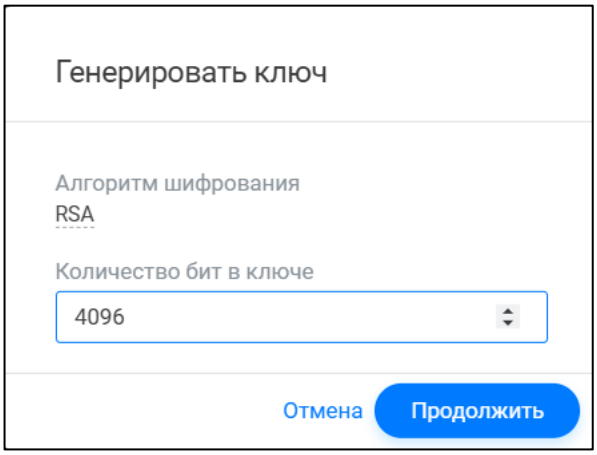

Рисунок 49. Выбор параметров закрытого ключа сервера

3. Создание запроса на подпись сертификата (CSR)

Для получения серверного сертификата, подписанного корневым, необходимо сформировать запрос на подпись (CSR) во внешний центр сертификации. Для этого:

- в выпадающем меню ••• выбрать пункт «Создать CSR»;
- Система отобразит диалоговое окно с метаданными CSR, полученными из блока «Генерация ключей и сертификатов» вкладки «Общие настройки»;
- проверить метаданными запроса, при необходимости скорректировать и нажать «Сохранить»;
- Система сохранит архив с файлом запроса в формате CSR на локальный диск рабочего места администратора CEDM.

4. **Загрузка открытого сертификата сервера**

Для загрузки подписанного сертификата выполнить следующие шаги:

- в выпадающем меню ••• выбрать пункт «Загрузить подписанный сертификат сервера»;
- в появившемся стандартном диалоговом окне открытия файла выбрать сертификат;
- в контекстном меню (по нажатию правой кнопки мыши) на строке с закрытым сертификатом выбрать «Утвердить».

5. Верификация корректности настройки

Минимальный набор должен состоять из трех сертификатов со статусом утвержден:

- корневой сертификат;
- серверный сертификат;
- серверный закрытый ключ.

Примечание: для подключения агентов корневой и серверный сертификаты должны иметь корректные поля CN, SAN и CRL, а также не истекшую дату срока действия.

Описание модели агент-серверного взаимодействия «Аутентификация агентов по идентификатору»

Модель «Аутентификация агентов по идентификатору» является базовой моделью безопасности в системе CEDM, используемой по умолчанию при развертывании Системы.

Принцип работы:

1. Регистрация агента на сервере

при первом подключении агент, установленный на устройстве, отправляет на сервер CEDM запрос на регистрацию;

сервер генерирует уникальный идентификатор агента и пароль сохраняет его в базе данных;
агент получает свои учетные данные и сохраняет их в локальном хранилище.

2. Аутентификация при подключении

при каждом подключении агент передает свой уникальный идентификатор;
сервер проверяет идентификатор в базе данных зарегистрированных агентов;
при успешной проверке устанавливается защищенное соединение.

3. Дополнительные параметры безопасности

возможно задать секрет сервера для защиты от подключений нелегитимных агентов (см. раздел «Настройки безопасности»).

Описание модели агент-серверного взаимодействия на основе сертификатов

Модель агент-серверного взаимодействия «На основе сертификатов» Системы использует механизм взаимной аутентификацию TLS (mutual TLS, mTLS) для обеспечения защищенного взаимодействия между агентами и сервером CEDM.

Принцип работы модели:

при сборке установщика агента в него добавляются:

- файл конфигурации агента;
- открытый корневой сертификат (см. раздел «Установщики агентов»).

после установки агента:

- на оконечном устройстве генерируется пара ключей (открытый и закрытый);
- параметры генерации ключей задаются в разделе «Установщики агентов» на вкладке «Конфигурации агентов» (см. раздел «Конфигурации агентов»).

при первом подключении к серверу агент:

- устанавливает TLS-соединение с сервером;
- проверяет сертификат сервера с помощью корневого сертификата;

отправляет запрос на регистрацию, включающий:

- свой открытый ключ (не подписанный);
- запрос на подпись сертификата (CSR);

- идентификационные данные устройства (Наименование, сетевой адрес, идентификатор).

сервер при получении запроса на регистрацию:

- проверяет отсутствие отпечатка открытого ключа агента в списке известных ключей;
- регистрирует агента в статусе «Ожидает утверждения»;
- сохраняет открытый ключ и CSR агента.

после утверждения администратором:

- сервер подписывает сертификат агента своим закрытым ключом;
- отправляет подписанный сертификат агенту;
- переводит статус устройства в «Активен».

агент при получении подписанного сертификата:

- сохраняет его в локальном хранилище;
- использует его для последующих подключений к серверу;
- отправляет подтверждение получения сертификата.

При каждом последующем подключении происходит взаимная аутентификация:

- сервер предоставляет свой сертификат, подписанный корневым;
- агент проверяет сертификат сервера;
- агент предоставляет свой сертификат, подписанный сервером;
- сервер проверяет подпись на сертификате агента.

Данный механизм обеспечивает:

- взаимную аутентификацию участников взаимодействия;
- защиту канала передачи данных;
- контроль доступа агентов к серверу;
- централизованное управление сертификатами.

Настройка модели агент-серверного взаимодействия «На основе сертификатов»

КРИТИЧЕСКИ ВАЖНО: процесс миграции развернутой Системы с подключенными агентами на модель безопасности «На

основе сертификатов» требует предварительного распространения на зарегистрированные в CEDM устройства корневых сертификатов с последующей перезагрузкой клиентских машин или перезапуском службы агента CEDM. Без распространенных сертификатов агенты **не смогут подключится к серверу**. При возврате Системы к модели «Аутентификация агентов по идентификаторам» потерявшие таким образом связь агенты также **не смогут подключится** автоматически. Потребуется перезапуск службы агента или **перезагрузка устройства** (подробности см. в разделе «Миграция с модели агент-серверного взаимодействия «Аутентификацию агентов по идентификатору» на модель «На основе сертификатов»).

Для настройки модели агент-серверного взаимодействия «На основе сертификатов» в «чистой» Системе (без подключенных агентов) необходимо выполнить следующие шаги:

1. Перейти в раздел «Безопасность» на вкладку «Сертификаты сервера».
2. Загрузить в Систему корневой сертификат (см. раздел Управление сертификатами сервера). Для этого:
   в выпадающем меню ••• выбрать пункт «Загрузить корневой сертификат»;
   в стандартном диалоговом окне выбрать файл сертификата.
3. Утвердить корневой сертификат. Для этого на строке с добавленным корневым сертификатом нажать правой кнопкой мыши и в выпадающем меню выбрать «Утвердить ключ».
4. Добавить в Систему закрытый ключ сервера (см. раздел Создание и добавление серверных ключей в Систему).
5. Утвердить закрытый ключ сервера.
6. Добавить в Систему подписанный сертификат Сервера (см. раздел Создание и добавление серверных ключей в Систему).
7. На вкладке «Общие настройки» модель безопасности установить «По сертификату».
8. собрать установщики агентов, в которые Система автоматически добавит утвержденный корневой или промежуточный сертификат (см. раздел «Установщики агентов»).

9. Система переведена на модель безопасности «По сертификатам».

Развертывание агентов

В случае выключенной опции «Автоматически утверждать сертификаты» при первом подключении устройства будут получать статус «Ожидает подтверждение». В данном случае для утверждения ключа агента выполнить следующие шаги:

1. Перейти в раздел «Безопасность» на вкладку «Сертификаты агентов»
2. В крайне левом столбце выбрать агентов, ключи которых необходимо утвердить
3. В выпадающем меню ••• выбрать утвердить ключ агента;
4. Ключ получит статус «Утвержден», а устройство – статус «Активен».

При включенной опции «Автоматически утверждать сертификаты» агенты будут регистрироваться в Системе в автоматическом режиме.

Миграция с модели агент-серверного взаимодействия «Аутентификацию агентов по идентификатору» на модель «На основе сертификатов»

При наличии подключенных агентов перед переходом на модель безопасности «На основе сертификатов» необходимо выполнить предварительные шаги по подготовки Системы:

1. Перейти в раздел «Безопасность» на вкладку «Сертификаты сервера».
2. Загрузить в Систему корневой сертификат (см. раздел Управление сертификатами сервера). Для этого:

   в выпадающем меню ••• выбрать пункт «Загрузить корневой сертификат»;

   в стандартном диалоговом окне выбрать файл сертификата.
3. Утвердить корневой сертификат. Для этого на строке с добавленным корневым сертификатом нажать правой кнопкой мыши и в выпадающем меню выбрать «Утвердить ключ».
4. Добавить в Систему закрытый ключ сервера (см. раздел Создание и добавление серверных ключей в Систему).

5. Утвердить закрытый ключ сервера.
6. Добавить в Систему подписанный сертификат Сервера (см. раздел Создание и добавление серверных ключей в Систему).
7. Распространить коревой сертификат на агентах. Для этого на строке с корневым сертификатом нажать правой кнопкой мыши и выбрать «Распространить корневой сертификат».
8. Контролировать распространение сертификатов на агенты возможно в разделе «Мониторинг» в экранной форме «Очередь команд агентам».
9. Перейти в раздел «Безопасность» на вкладку «Общие настройки».
10. Включить опцию «Автоматически утверждать сертификаты».
11. Выбрать модель безопасности «На основе сертификатов».

⚠ После переключения модели безопасности агенты потеряют связь с сервером до перезагрузки устройств или перезапуска служб агентов.

12. Перезагрузить устройства или перезапустить службы агентов, после чего устройства подключатся к Системе.

⚠ Устройства, которые находятся не в сети не смогут получить сертификат. После изменения модели для таких УРМ необходимо выполнить дополнительные шаги:

13. Перейти в раздел «Безопасность» на вкладку «Сертификаты сервера» и скачать коревой сертификат. Для этого на строке с корневым сертификатом нажать правой кнопкой мыши и выбрать «Скачать ключ сервера».
14. Переименовать скаченный сертификат в root.crt и распространить его на устройства, поместив в установочную папку CEDM (по умолчанию c:\Program files\CEDM\desktopagent\ssl)
15. Перезапустить службу агента CEDM_desktop_agent
16. Система переведена на модель безопасности «По сертификатам».

⚠ После изменения модели безопасности на модель «На основе сертификатов» для распространения агентов на новые

устройства необходимо собрать установщик агента с актуальным корневым сертификатом.

Миграция с модели агент-серверного взаимодействия «На основе сертификатов» на модель «Аутентификацию агентов по идентификатору»

Для переключения между моделями «На основе сертификатов» на «Аутентификацию агентов по идентификатору» необходимо выполнить следующие шаги:

1. В экранной форме «Безопасность» выбрать модель безопасности «Аутентификация агентов по идентификатору».
2. Агенты отключаться от сервера и подключаться в соответствии с выбранной моделью агент-серверного взаимодействия.

10.1.5. Экранная форма «Настройки агентов»

9.1.5.1. Вкладка «Общие настройки»

Вкладка предназначена для просмотра и изменения настроек безопасности и аутентификации агентов CEDM (рисунок 50).

Перечень настроек представлен в таблице 5:

Таблица 5. Перечень настроек агентов и их описание

Настройка	Описание	Тип данных
Проверка FQDN сертификата	Активация проверки соответствия полного доменного имени (FQDN) в сертификате	Чек-бокс, в котором: • активный флаг соответствует значению «true» – настройка включена; • неактивный флаг соответствует значению «false» – настройка выключена
Проверка CRL сертификата	Включение проверки списка отозванных сертификатов	Чек-бокс, в котором: • активный флаг соответствует значению «true» – настройка включена; • неактивный флаг соответствует значению «false» – настройка выключена

Проверка срока действия сертификата	Активация проверки срока действия сертификатов	Чек-бокс, в котором: • активный флаг соответствует значению «true» – настройка включена; • неактивный флаг соответствует значению «false» – настройка выключена
URL WEB интерфейса администрирования	Адрес веб-интерфейса, для перехода из UI агента при использовании функций удаленного подключения	Строковое значение. Указывается в следующем формате: https://CEDM.test.ct/
Показывать ФИО Оператора Пользователю	Отображение полного имени оператора при удаленном подключении к устройствам пользователей	Чек-бокс, в котором: • активный флаг соответствует значению «true» – настройка включена; • неактивный флаг соответствует значению «false» – настройка выключена
Адреса сервера	Адрес proxy-серверов Системы CEDM для подключения агентов	Строковое значение. Указывается в следующем формате: <адрес_сервера>:<порт>

Для изменения значения параметра необходимо:

1) Выбрать требуемый параметр в списке и нажать на него.
2) Установить новое значение в поле «Значение». Для параметра «Адреса сервера» необходимо нажать напротив поля «Значение» кнопку , в всплывающем окне указать адрес и порт.
3) Нажать кнопку «Сохранить».

После изменения настроек нажать кнопку в правом верхнем углу страницы для синхронизации изменений с агентами.

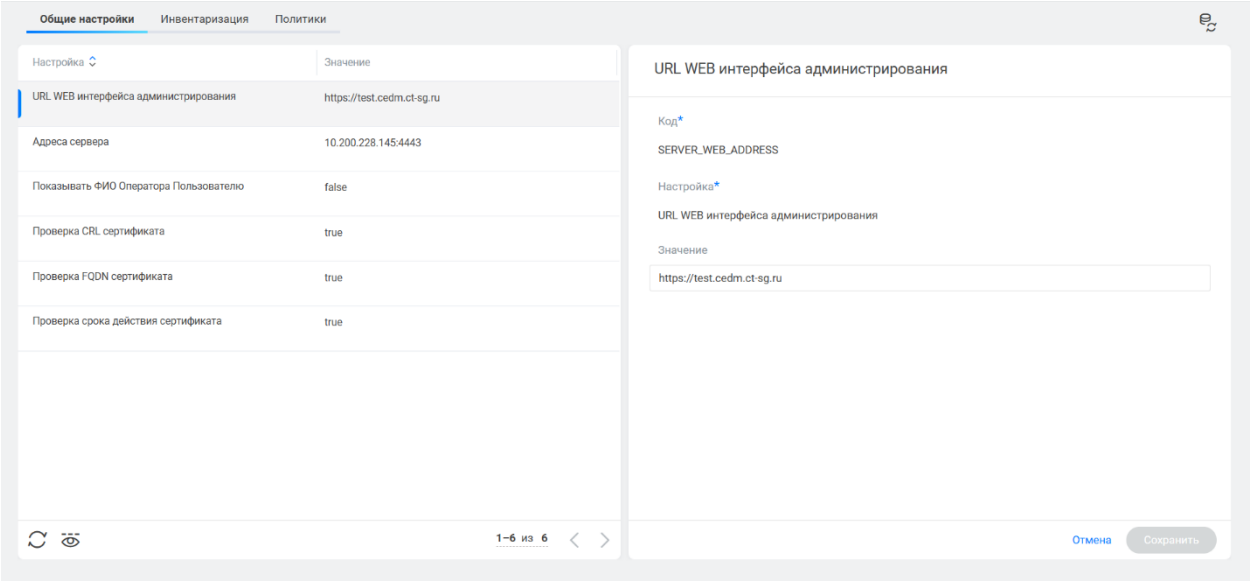

Рисунок 50. Экранная форма «Настройки агентов» – «Общие настройки»

9.1.5.2. Вкладка «Инвентаризация»

Вкладка «Инвентаризация» предназначена для настройки параметров сбора информации из реестра Windows на оконечных устройствах. В данном разделе администратор может указать конкретные ключи реестра, данные из которых будут собираться агентами CEDM в процессе инвентаризации (рисунок 51).

Инвентаризируемые в системе ключи реестра Windows отображаются в табличном виде со следующими полями:

«ID» – уникальный номер ключа в Системе. Генерируется автоматически после создания ключа;

«Имя атрибута» – пользовательское наименование собираемого параметра;

«Ветка реестра» – корневой раздел реестра Windows (например, HKEY_LOCAL_MACHINE);

«Путь» – путь к параметру в реестре без указания корневого раздела (например, SOFTWARE\Microsoft NT\CurrentVersion);

«Параметр» – имя параметра реестра, значение которого требуется получить (например, CurrentBuild).

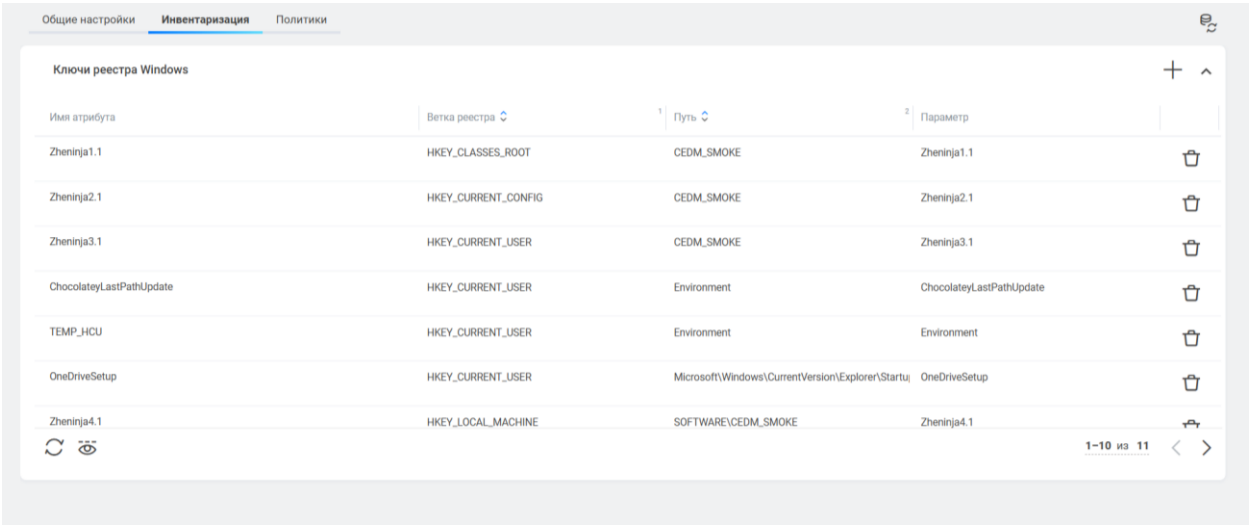

Рисунок 51. Экранная форма «Настройки агентов» – «Инвентаризация»

Управление списком собираемых ключей реестра

Для добавления нового ключа реестра необходимо:

1) Нажать кнопку + в правом верхнем углу списка.
2) В открывшейся форме «Новый ключ реестра Windows» заполнить поля:
   - «Имя атрибута»;
   - «Ветку реестра» (выбрать из выпадающего списка);
   - «Путь»;
   - «Параметр».
3) Нажать кнопку «Сохранить».

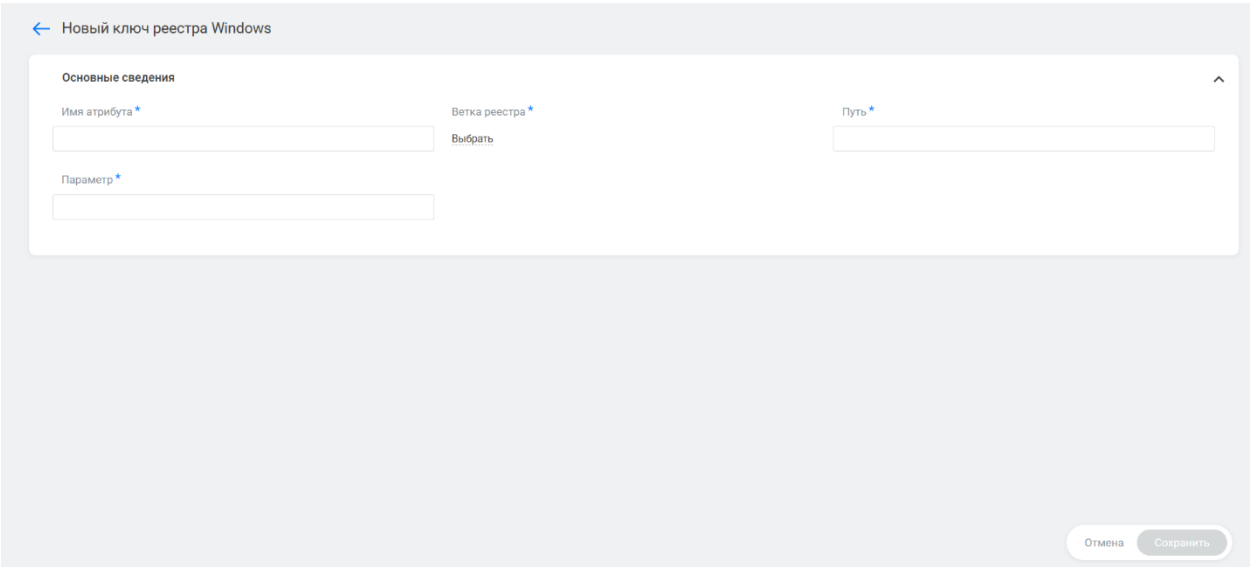

Рисунок 52. Добавление ключа реестра

Для удаления ключа реестра из списка инвентаризации необходимо нажать кнопку 🗑 в соответствующей строке.

После внесения изменений в перечень инвентаризируемых ключей нажать кнопку в правом верхнем углу страницы для синхронизации настроек с агентами.

Добавленные ключи реестра будут отображаться в карточке устройства. Для их просмотра требуется:

1) Перейти в раздел веб-интерфейса «Устройства».
2) Выбрать в списке необходимое устройство и дважды нажать на него.
3) В карточке устройства перейти на вкладку «Инвентаризация».
4) На странице «Дерево» выбрать папку «Реестр» и нажать на нее.

9.1.5.3. Вкладка «Политики»

Вкладка «Политики» предназначена для настройки параметров сбора событий с оконечных устройств. На вкладке в табличном виде отображается список политик со следующими полями (рисунок 53):

- «ID» – уникальный номер политики в Системе. Генерируется автоматически после создания политики;
- «Статус» – текущее состояние политики. Может принимать следующие состояния:
  - «Активен» – политика настроена и используется;
  - «Архив» – политика не используется;
  - «Черновик» – политика создана и сохранена, но не настроены источники событий.
- «Наименование» – название политики сбора событий;
- «ОС» – операционная система, для которой предназначена политика;
- «Устройств» – количество устройств, на которых применена политика;
- «Хранение» – максимальный период хранения собранных событий в днях на оконечном устройстве при отсутствии связи с сервером. При превышении максимального периода происходит ротация записей.

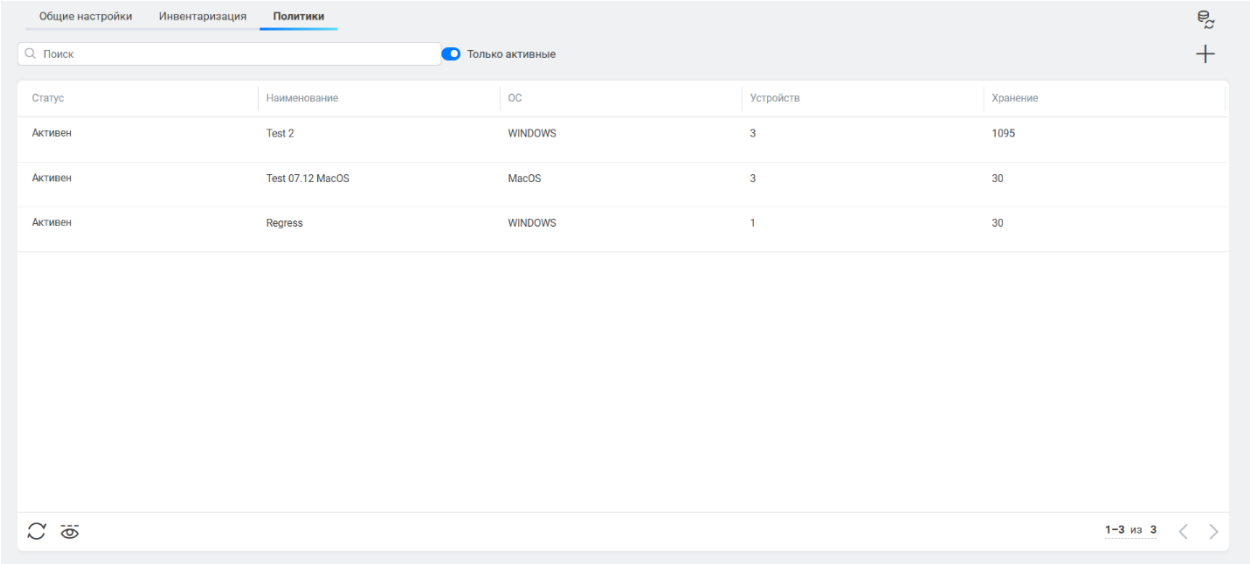

Рисунок 54. Экранная форма «Настройки агентов» – «Политики»

Создание новой политики сбора событий для ОС Windows

Для создания новой политики необходимо выполнить следующие действия:

1) Нажать кнопку + в правом верхнем углу экрана.
2) В открывшейся форме (рисунок 54) заполнить следующие поля:
   - «Наименование» – название политики;
   - «Операционная система» – выбрать из выпадающего списка тип Windows;
   - «Хранение, дней» – максимальный период хранения событий на оконечном устройстве при отсутствии связи с сервером;

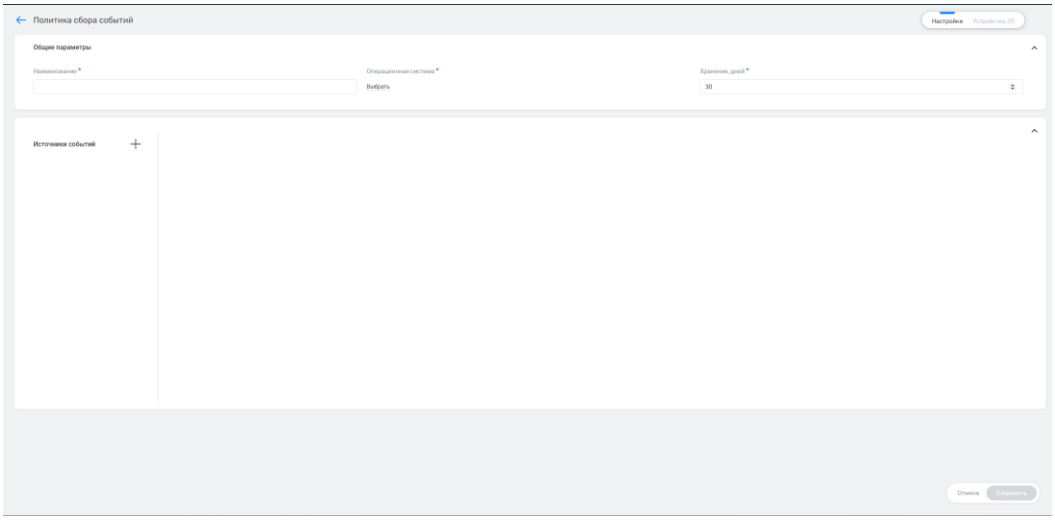

Рисунок 543. Создание политики

3) Добавить источники событий, нажав кнопку ┼. Далее требуется выбрать способ добавления источника событий:

«Добавить из справочника» – выбор стандартных источников событий. Необходимо нажать кнопку Выбрать и из выпадающего списка выбрать один из следующих типов источников:

- «Приложение»;
- «Безопасность»;
- «Установка»;
- «Система».

«Добавить вручную» – создание пользовательского источника событий с указанием значений для следующих параметров:

- «Наименование» – пользовательское название источника;
- «Полное имя источника» – путь к журналу событий в системе.

4) Указать общие параметры сбора событий:

«Период» – период обращения агента к журналу событий;

«Коды» – коды событий. Указываются через запятую;

«Уровень» – стандартные уровни регистрируемых событий:

- «Критическое»;
- «Ошибка»;
- «Предупреждение»;
- «Сведения»;
- «Подробности».

«Уровни» – нестандартные уровни событий:

- «Наименование» – пользовательское название

уровня событий;

– «Уровень» – числовое значение уровня события.

5) Нажать кнопку «Сохранить».
6) На вкладке «Устройства» указать устройства, к которым будет применена политика.
7) В меню ••• нажать «Активировать».

Обратите внимание, что в случае, если не указаны конкретные уровни регистрируемых событий, будет зафиксирована в обязательном порядке информация об определенных типах событий. Такие события имеют специальный уровень критичности (Level=0) и к ним относятся:

события аудита (успешные/неуспешные попытки входа в Систему);

операционные события (запуск/остановка системных процессов);

события, которые должны фиксироваться в журнале событий всегда, независимо от настроек;

события с особым жизненным циклом.

События с уровнем критичности «0» не будут фиксироваться, если будет указан любой другой конкретный уровень (или уровни). Если требуется фиксироваться события других уровней критичности, включая нулевой, то требуется все уровни указывать в явном виде в соответствующем поле.

Создание новой политики сбора событий для ОС macOS

Для создания новой политики необходимо выполнить следующие действия:

1) Нажать кнопку + в правом верхнем углу экрана.
2) В открывшейся форме заполнить следующие поля:

- «Наименование» – название политики;
- «Операционная система» – выбрать из выпадающего списка тип macOS;
- «Хранение, дней» – максимальный период хранения событий на оконечном устройстве при отсутствии связи с сервером;

3) Добавить источники событий, нажав кнопку +. Далее требуется выбрать способ добавления источника событий:

- «Добавить из справочника» – выбор стандартных источников событий. Необходимо нажать кнопку Выбрать и из

выпадающего списка выбрать один из следующих типов источников:

- «Начало работы системы»;
- «Начало работы (запуск) системы»;
- «Окончание (остановка) работы системы»;
- «Вход пользователя в систему»;
- «Выход пользователя из системы»;
- «Неуспешный вход в систему»;
- «Создание учетной записи»;
- «Удаление учетной записи»;
- «Блокировка (отключение) учетной записи»;
- «Разблокировка (включение) учетной записи»;
- «Назначение\исключение прав пользователя на объект»;
- «Смена пароля учетной записи»;
- «Создание группы (роли) пользователей»;
- «Удаление группы (роли) пользователей»;
- «Изменение прав группы 9/(роли) пользователей»;
- «Исключение пользователя из состава группы»; (роли)»;
- «Включение пользователя в состав группы (роли)»;
- «Очистка журнала событий».

- «Добавить вручную» – создание пользовательского источника событий с указанием пользовательского названия источника в поле «Наименование»;

4) Указать общие параметры сбора событий:

- «Подсистема» – подсистема ОС, в рамках которой будут собираться события;
- «Тип события» – тип собираемых событий;
- «Категория» – наименование области, к которым относятся собираемые события;
- «Фильтр(ы) по тексту сообщения» – регулярные выражения для фильтрации по тексту сообщений;
- «Типы сообщений» – типы собираемых событий и их уровни критичности.

5) Нажать кнопку «Сохранить».
6) На вкладке «Устройства» указать устройства, к которым будет применена политика.
7) В меню ••• нажать «Активировать».

Управление списком оконечных устройств в рамках политики

После настройки источников события необходимо перейти управлению списком оконечных устройств, к которым будет применена политика сбора событий. Это осуществляется на вкладке «Устройства» (рисунок 55) карточки политики сбора событий.

Выбрать устройства, к которым будет применена политика, можно одним из двух способов:

1) Нажать кнопку + и в открывшейся форме установить активный флаг напротив тех устройств, для которых необходимо применить политику. После этого нажать кнопку «Добавить».
2) Нажать кнопку и в открывшейся форме выбрать представление. После этого нажать кнопку «Применить».

После этого на вкладке «Устройства» будет отображаться список добавленных в рамках политики устройств.

Для удаления устройства из списка требуется напротив необходимого устройства нажать кнопку и подтвердить действие, нажав кнопку «Удалить».

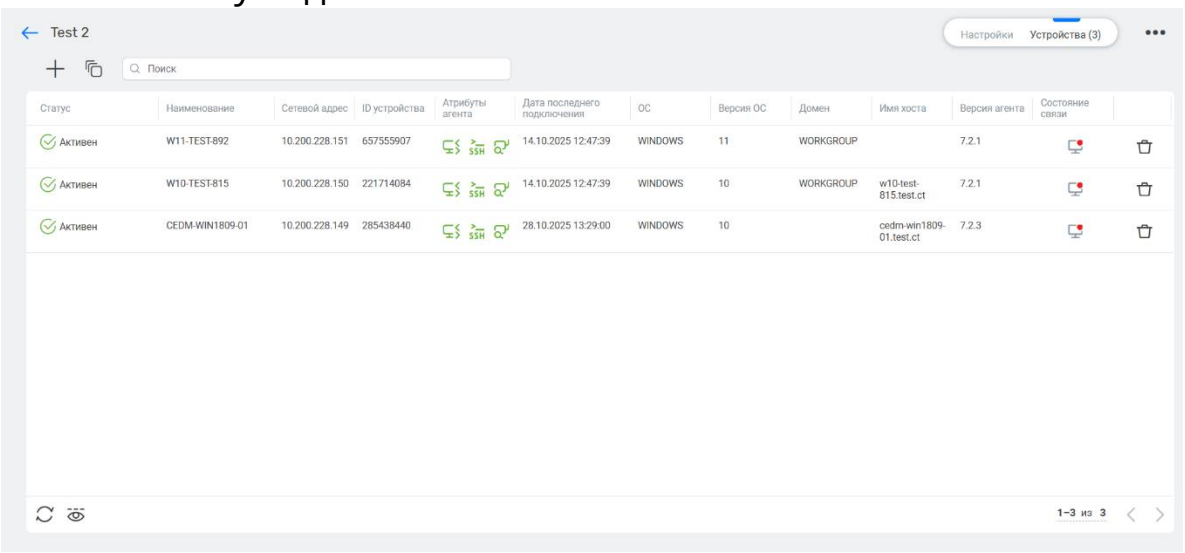

Рисунок 55. Создание политики. Вкладка «Устройства»

Управление политиками сбора событий

Управления политиками сбора событий осуществляется в карточке политики. При редактировании ранее созданной политики можно добавлять или удалять источники событий, а также изменять все параметры, кроме выбора ОС.

Для добавления новых источников событий необходимо повторить действия, которые выполнялись при создании политики.

Для удаления источников событий напротив необходимого источника требуется нажать кнопку 🗑 и подтвердить действие, нажав кнопку «Удалить».

Управление состояниями политик осуществляется с помощью выпадающего меню ••• . Доступны следующие действия:

- «В Архив» – отправить политику в архив;
- «Восстановить из Архива» – восстановить политику из архива;
- «В Архив» – сделать политику активной;
- «Синхронизировать» – отправить измененную политику на устройства, указанные на вкладке «Устройства» карточки политики сбора событий.

10.1.6. Экранная форма «Электронная почта»

Для отправки отчетов и оповещений CEDM на адреса электронной почты необходимо настроить подключение Системы к корпоративному почтовому серверу. Настройка подключения к почтовому серверу осуществляется в разделе «Электронная почта» (рисунок 56).

Настройки подключения:

- адрес почтового сервера – IP-адрес SMTP-сервера;
- порт – порт подключения к SMTP-серверу;
- имя пользователя – логин для аутентификации на почтовом сервере;
- пароль – пароль для аутентификации;
- SMTP: использовать TLS – включение/отключение TLS-шифрования.

Настройки отправителя:

- Адрес отправителя – адрес электронной почты, который будет указан в качестве адреса отправителя;

- Тема письма – текст, который будет указан в теме письма;
- Заголовок письма – текст, который будет указан в заголовке письма;
- Подпись письма – текст, который будет указан в подписи письма.

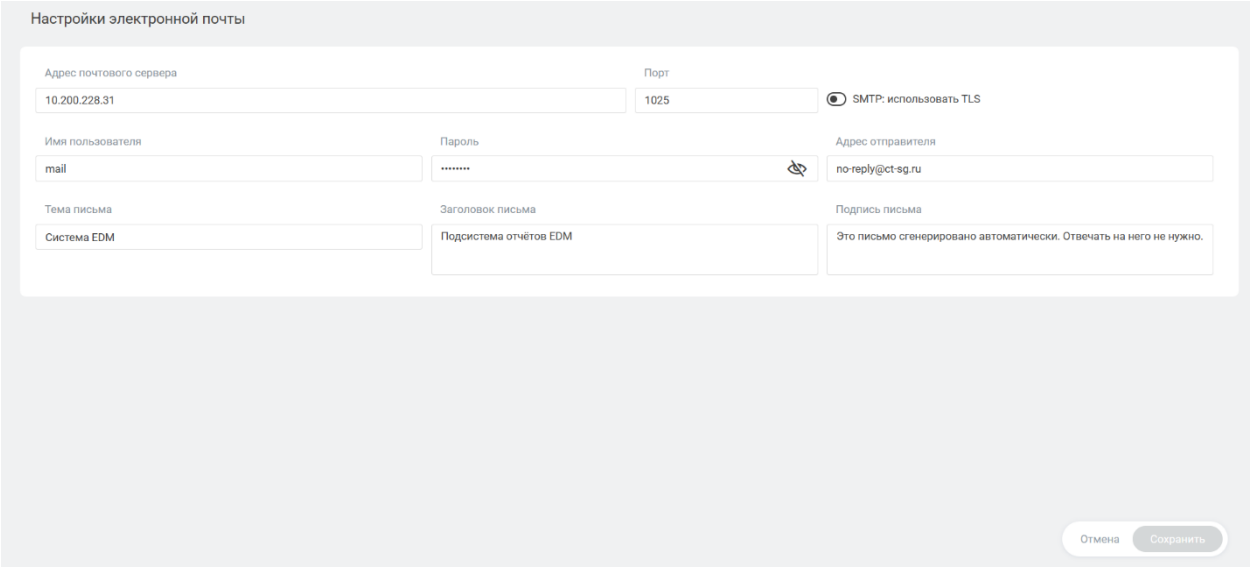

Рисунок 56. Экранная форма «Настройка электронной почты»

11. МОНИТОРИНГ. ЖУРНАЛ СОБЫТИЙ ПАА

Журнал событий ПАА предназначен для отображения и экспорта событий подсистемы аутентификации и авторизации (рисунок 57).

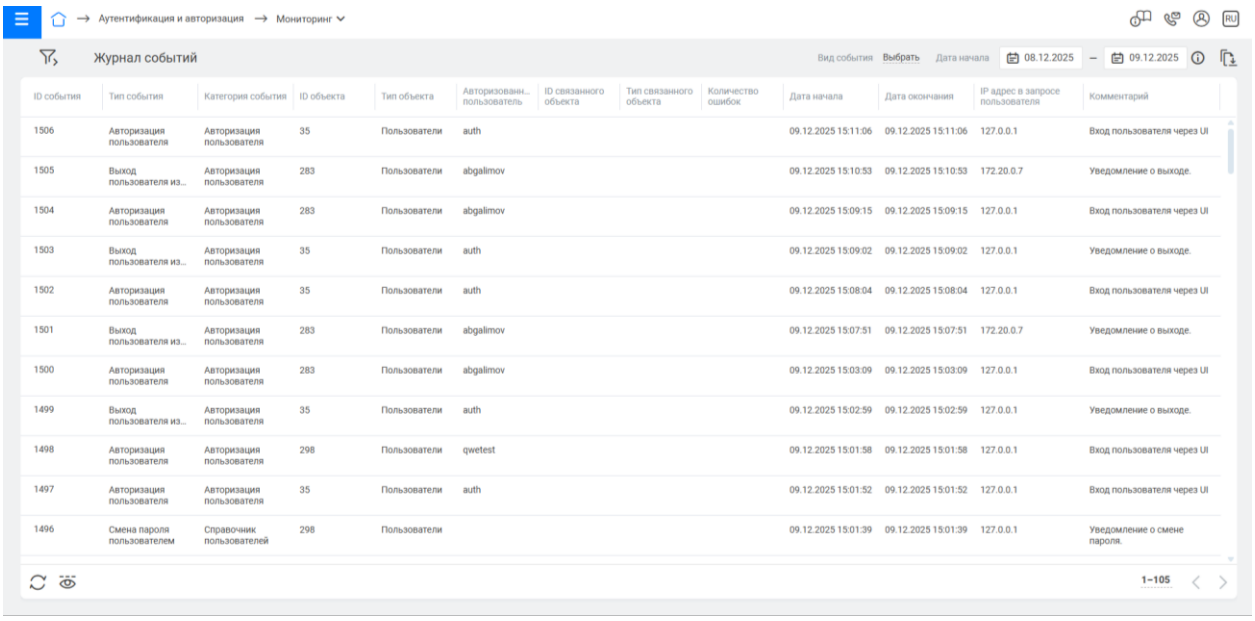

Рисунок 57. Экранная форма «Мониторинг»

11.1. Фильтрация событий

В журнале событий доступна фильтрация записей по любым полям таблицы. Условия всех выбранных фильтров работают по логическому «И» (рисунок 58).

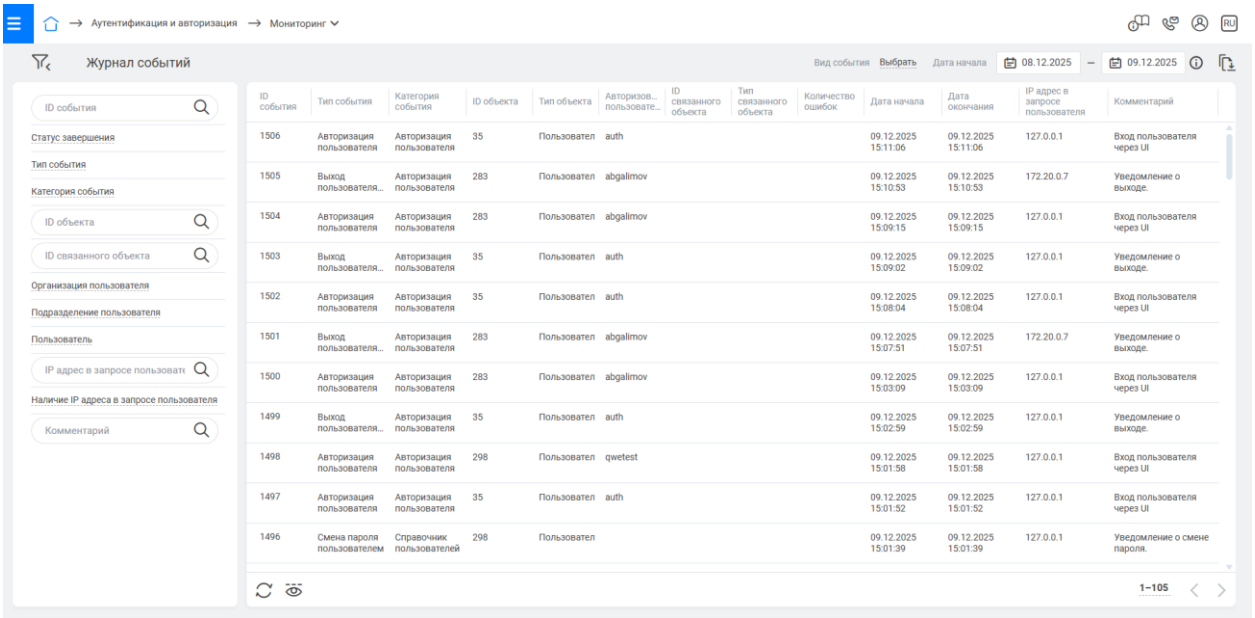

Рисунок 58. «Общий журнал событий». Фильтрация событий

11.2. Формирование отчета

Для формирования отчета необходимо нажать кнопку в правом верхнем углу экранной формы. В открывшимся диалоговом окне выбрать имя отчета, задать дату и время периода возникновения событий. В зависимости от типа отчета задать дополнительные параметры и нажать кнопку «Скачать» (рисунок 59).

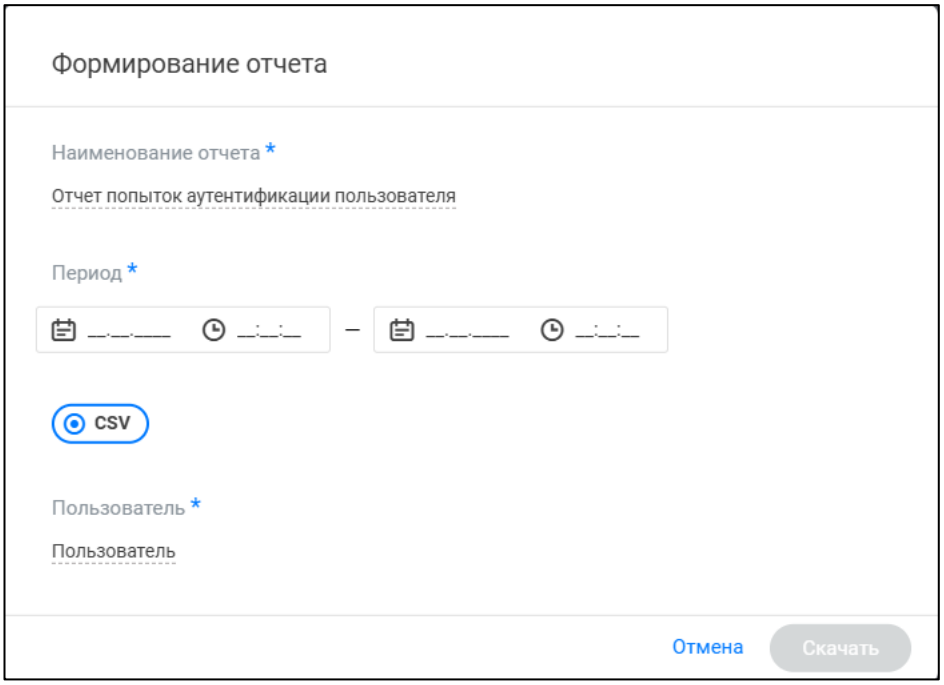

Рисунок 59. Диалоговое окно «Формирование отчета»

Перечень доступных для формирования отчетов:

- «Отчет попыток аутентификации пользователя»;
- «Отчет по событиям безопасности»;
- «Отчет действий пользователя»;
- «Отчет действий с выбранного IP»;
- «Отчет попыток аутентификации пользователей организации».

12. МОНИТОРИНГ. ЖУРНАЛ СОБЫТИЙ СУРС

12.1. Экранная форма «Общий журнал событий»

Общий журнал событий СУРС предназначен для отображения и экспорта событий СУРС (рисунок 60).

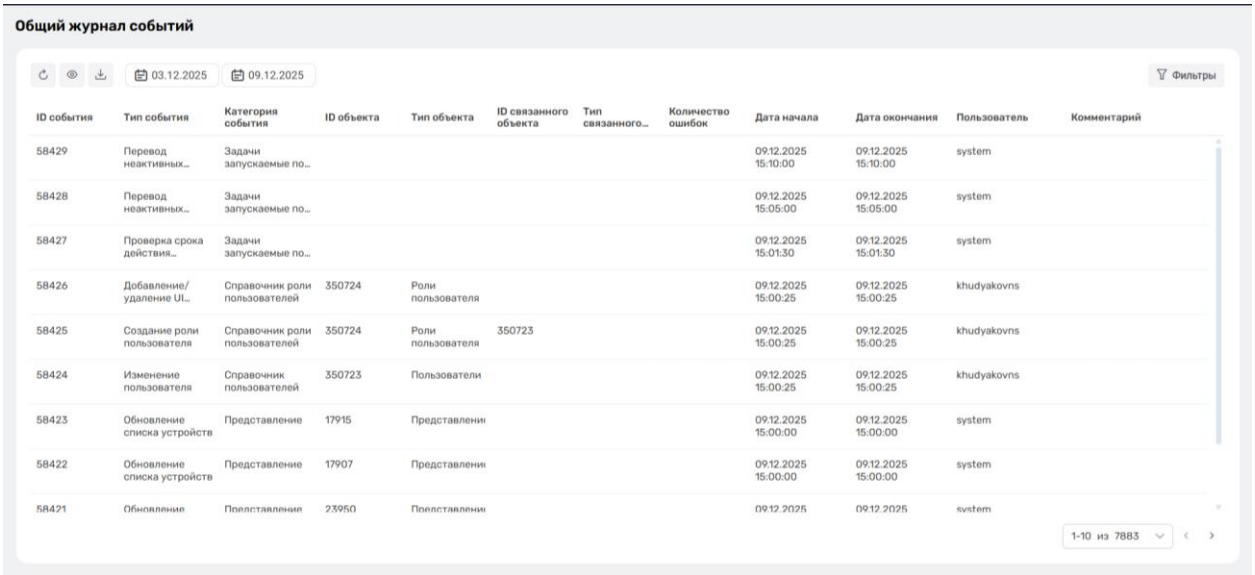

Рисунок 60. Экранная форма «Общий журнал событий»

Примечание: отображение записей в журнале событий ограничено периодом в одни сутки и не более 1000 строк.

12.1.1. Фильтрация общего журнала событий

Для фильтрации списка параметров необходимо выполнить следующие действия:

- перейти на экранную форму «Общий журнал событий»;
- отфильтровать список, выбрав один из сервисов в верхней левой части рабочей области экранной формы;
- настроить фильтры панели фильтрации (рисунок 61):
  - ID события – строка поиска;
  - Тип события – множественный выбор из справочника;
  - Категория события – множественный выбор из справочника;
  - ID объекта – строка поиска;
  - ID связанного объекта – строка поиска;
  - Пользователь – множественный выбор из справочника;

– Комментарий – строка поиска.

- настроить фильтр периода. Фильтр периода не может быть задан на период более суток.

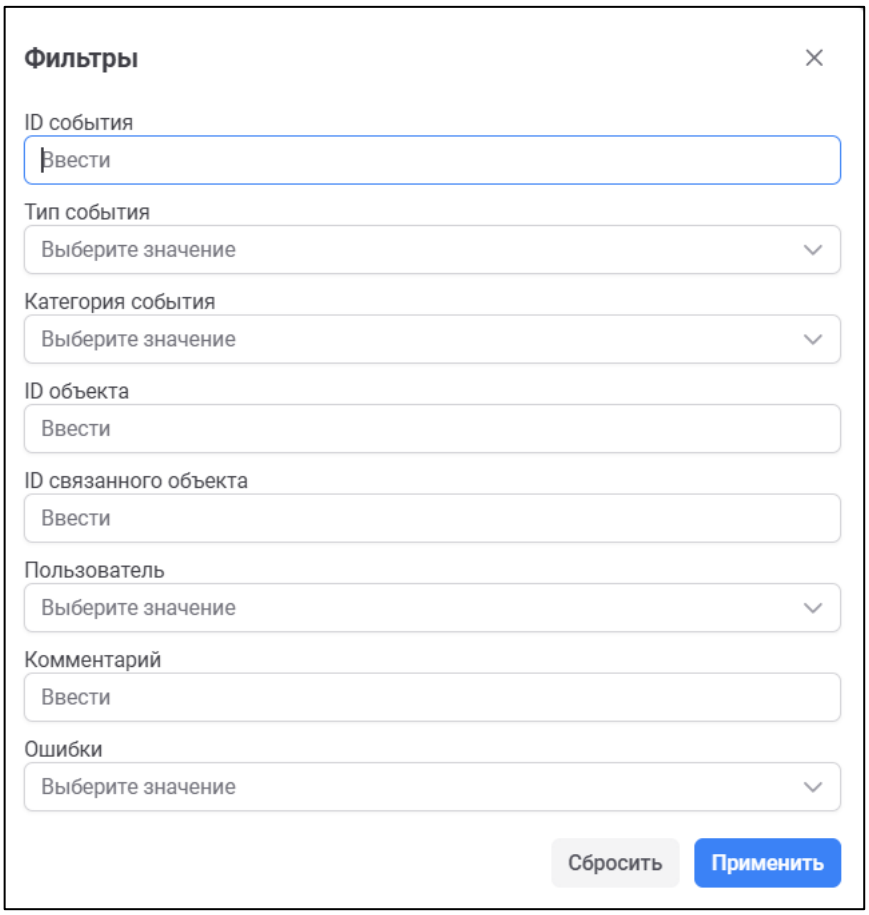

Рисунок 61. Фильтры общего журнала мониторинга

12.1.2. Просмотр карточки события

Для просмотра карточки события выполнить следующие действия:

- перейти на экранную форму «Общий журнал событий»;
- нажать на строку с событием, откроется окно карточки события (рисунок 62).

Рисунок 62. Карточка события

12.2. Экранная форма «Журнал сеансов удаленного помощника»

Журнал сеансов удаленного помощника СУРС предназначен для отображения информации о сеансах подключения операторов к удаленному рабочему столу пользователей оконечных устройств. Журнал содержит следующие поля (рисунок 63):

- Наименование устройства оператора – имя устройства, с которого было инициировано подключение;
- ID устройства оператора – внутренний идентификатор устройства оператора;
- Наименование устройства пользователя – имя оконечного устройства, к которому выполнялось подключение;
- ID устройства пользователя – внутренний идентификатор оконечного устройства;
- Состояние – текущий статус сеанса (Активно, Завершен, Запрос создан);
- Подключение – дата и время начала сеанса подключения;
- Отключение – дата и время завершения сеанса подключения;
- Причина – причина завершения сеанса;
- Ошибка – информация об ошибках, если они возникли во время сеанса;
- Авторизация – метод авторизации при подключении

(TOKEN или PASSWORD).

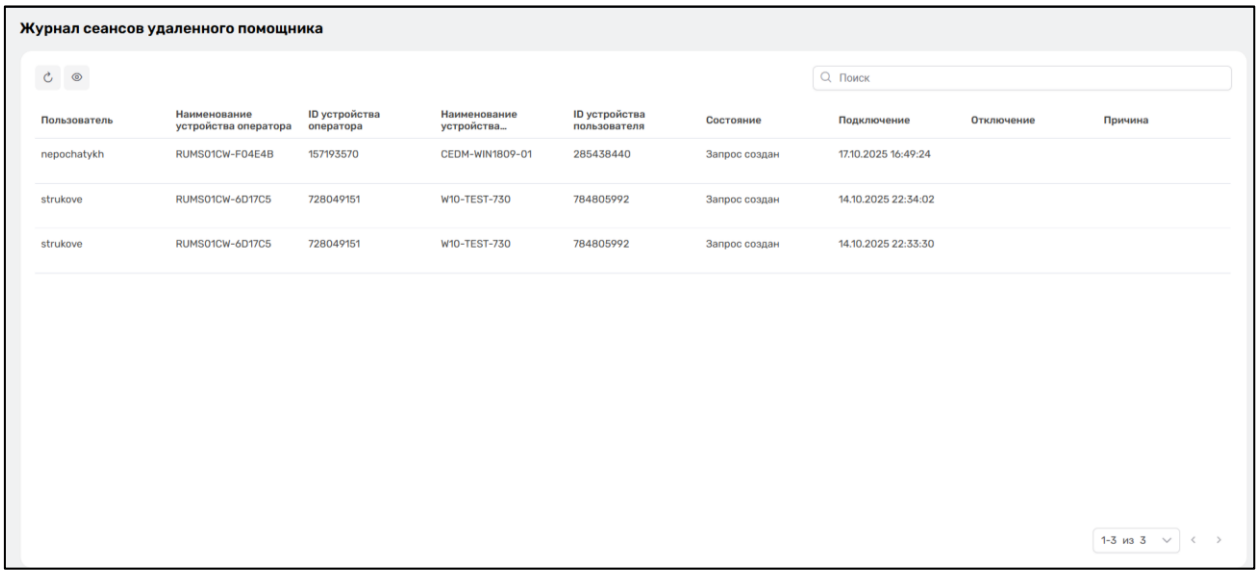

Рисунок 63. Экранная форма «Журнал сеансов удаленного помощника»

12.3. Экранная форма «Очередь команд агентам»

Экранная форма «Очередь команд агентам» (рисунок 64) предназначена для отображения информации о командах агентам. Данные отображаются в табличном виде со следующими полями:

- Команда – тип отправляемой команды агенту;
- Статус – текущее состояние команды;
- ID устройства – внутренний идентификатор устройства;
- Наименование устройства – имя устройства, на которое отправлена команда;
- Состояние связи – текущий статус подключения устройства;
- Создана – дата и время создания команды
- Срок действия – период действия команды;
- JSON – нажать для скачивания детальной информации о команде в формате JSON;
- Ошибка – информация об ошибках при выполнении команды.

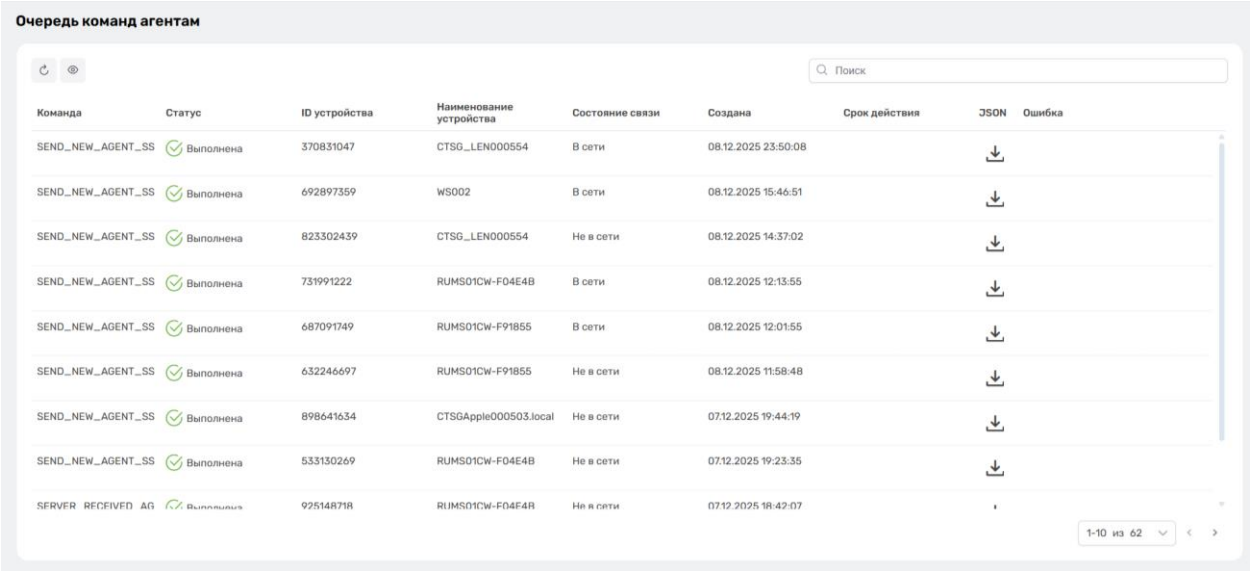

Рисунок 64. Экранная форма «Очередь команд агентам»

12.4. Экранная форма «Журнал ошибок»

Экранная форма «Журнал ошибок» предназначена для отображения информации об ошибках, возникающих в СУРС (рисунок 65). Данные отображаются в табличном виде со следующими полями:

- Дата и время – дата и время возникновения ошибки;
- Ошибка – краткое описание ошибки;
- ID объекта – уникальный идентификатор объекта, связанного с ошибкой;
- Тип объекта – тип объекта (Устройство, Пользователь, Задача и т. д.);
- Наименование объекта – имя объекта;
- ID дочернего объекта – идентификатор связанного дочернего объекта;
- Тип дочернего объекта – тип дочернего объекта;
- Категория ошибки – категория ошибки;

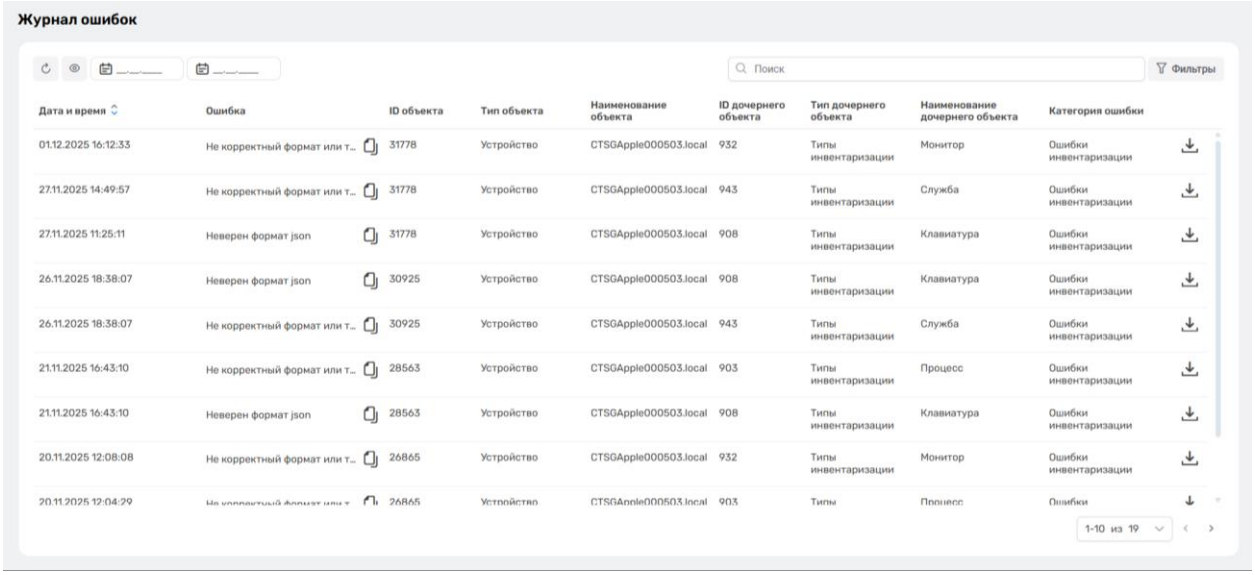

Рисунок 65. Экранная форма «Журнал ошибок»

12.4.1. Фильтрация журнала ошибок

Для фильтрации записей:

- нажать для вызова панели фильтрации;
- настроить фильтры панели фильтрации;
- настроить фильтр периода.

12.4.2. Просмотр карточки события

Для просмотра подробной информации об ошибке выполнить двойной щелчок мышью на соответствующей строке. Откроется карточка ошибки (рисунок 66). В поле «Дополнительная информация» карточки ошибки содержится расширенное техническое описание ошибки.

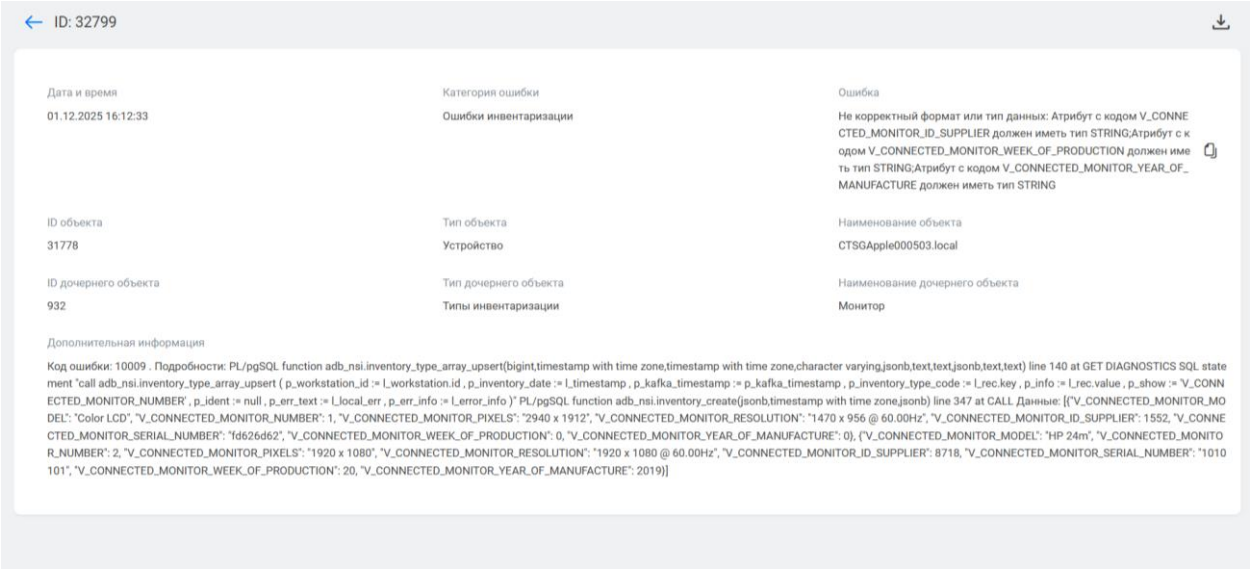

Рисунок 66. Карточка ошибки

12.4.3. Выгрузка ошибки в текстовый файл

Для выгрузки ошибки в текстовый файл перейти в карточку ошибки и нажать в правом верхнем углу. Система выгрузит файл в формате txt на рабочее место администратора Системы CEDM.

13. КОМПОНЕНТЫ СИСТЕМЫ

13.1. Установщики агентов

Раздел «Установщики агентов» предназначен для управления установочными пакетами агентов CEDM. В табличном виде отображается информация о доступных установщиках агентов для различных операционных систем и их версиях.

13.1.1. Вкладка «Установщики агентов»

На вкладке в табличном виде отображается информация о доступных установщиках агентов для различных операционных систем и их версиях (рисунок 67).

Таблица содержит следующие поля:

- Статус – текущее состояние установщика (Активен, Архив, Недействителен)
- Версия – версия агента CEDM;
- ОС – тип операционной системы, для которой предназначен установщик (Windows, Linux, MacOS);
- Архитектура – архитектура процессора (x86_64, arm);
- Дистрибутив Linux – ОС для установщиков семейства Linux (РЕД ОС, Astra Linux Special Edition, Альт Рабочая станция);
- Тип установки – тип агента («Полная установка» или «Легкий агент»[1]).
- Файл – имя установочного файла с возможностью скачивания;
- Архивация – нажать для перевода установщика в архив.

[1] Легкий агент – агент, предназначенный только для удаленного доступа и не имеющий функций инвентаризации и выполнения задач.

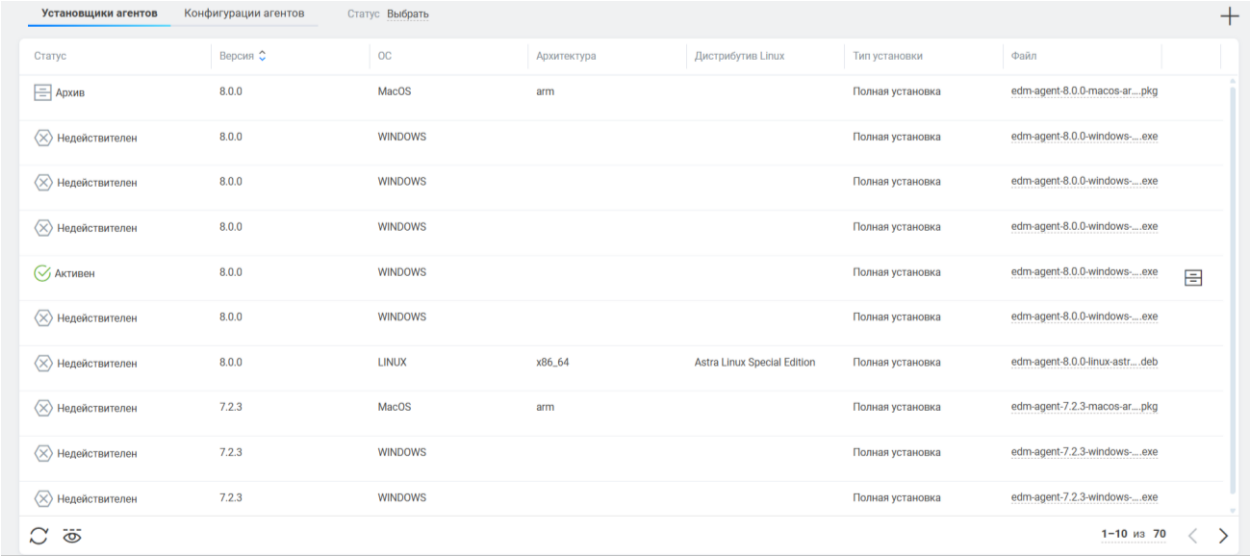

Рисунок 67. Экранная форма «Установщики агентов»

Действия с установщиками

На вкладке доступны следующие действия:

- создать новый установщик (кнопка + в правом верхнем углу);
- скачать установочный файл (кнопка в колонке «Файл»);
- открыть карточку установщика (двойной щелчок на сроке таблицы);
- фильтровать таблицу по статусу (выпадающий список «Статус»).

13.1.2. Вкладка «Конфигурации агентов»

Вкладка «Конфигурации агентов» предназначена для настройки параметров подключения и безопасности агентов CEDM. На данной вкладке задаются основные параметры взаимодействия агентов с сервером CEDM (рисунок 58).

Параметры подключения:

- Адрес сервера* – IP-адрес и порт сервера CEDM для подключения агентов (например, 192.168.12.21:443);
- URL сервера* – веб-адрес сервера CEDM (например, https://CEDM-test.ru/);

Параметры безопасности:

- Использовать секрет сервера* – переключатель для включения/отключения использования секрета при

подключении;

- Количество бит в ключе – размер ключа шифрования в битах (например, 4096);
- Модель безопасности – тип используемой модели безопасности (см. раздел «Настроек Системы» – «Безопасность»);
- Корневой сертификат – открытый корневой сертификат, зашиваемый в установщик и используемый для проверки подлинности сервера (см. раздел «Настроек Системы» – «Безопасность»);

Алгоритм шифрования – используемый алгоритм шифрования для защиты SSH-соединения между агентом и сервером (например, aes-128-cbc);

Примечание: поля, отмеченные звездочкой (*), являются обязательными для заполнения.

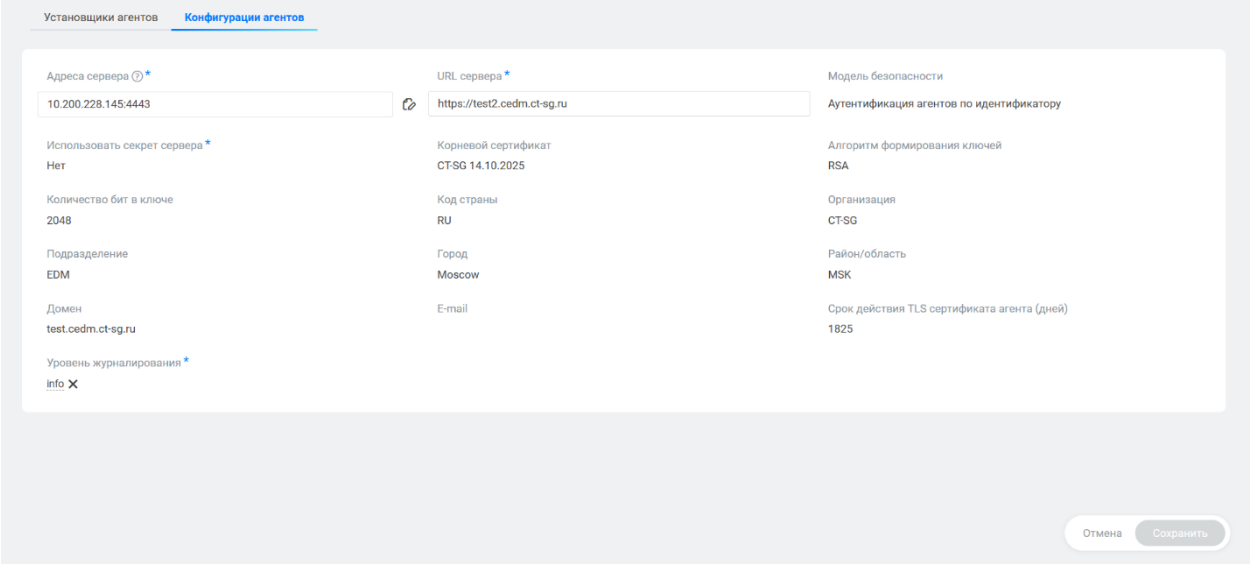

Рисунок 68. Экранная форма «Установщики агентов» – «Конфигурация агентов»

13.1.3. Добавление нового установщика

Для создания нового установщика агента необходимо выполнить следующие действия:

- нажать кнопку + в правом верхнем углу раздела «Установщики агентов». Откроется форма «Новый установщик агентов»;
- в открывшейся форме заполнить следующие поля:

- Версия* – версия создаваемого установщика агента;
- ОС* – тип операционной системы, для которой создается установщик.
- Дистрибутив Linux – название операционной системы для ОС семейства Linux;
- Тип установки* – тип создаваемого установщика:
  - Полная установка;
  - Легкий агент (только удаленный доступ).
- Исходный файл* – загрузить базовый установочный пакет, на основе которого будет создан установщик;
- Комментарий – дополнительная информация об установщике (опционально).

нажать кнопку «Сохранить». Установщик получает статус «Черновик»;

в выпадающем меню ••• выбрать «Собрать установщик». Подтвердить действие во всплывающем диалогов окне.

После сборки установщик появится в таблице на вкладке «Установщики агентов» и будет доступен для скачивания.

Примечание: поля, отмеченные звездочкой (*), являются обязательными для заполнения.

14. О СИСТЕМЕ

Раздел «О системе» содержит общую актуальную информацию о системе CEDM и состоянии ее компонентов, а именно:

- текущая версия системы;
- дата установки;
- информация о зарегистрированных приложениях.

Информация о зарегистрированных приложениях представляет собой таблицу с перечнем компонентов системы. Для каждого приложения отображаются следующие данные (рисунок 69):

- «Приложение» – название приложения;
- «Экземпляр» – уникальный идентификатор экземпляра приложения;
- «Версия» – номер версии последней сборки приложения;
- «Адрес» – IP-адрес приложения;
- «Порт» – сетевой порт приложения;
- «Хеш коммита» – уникальный идентификатор коммита;
- «Время сборки» – время последней сборки приложения;
- «Время регистрации» – время регистрации сборки в Системе;
- «Время последнего оповещения» – время последнего ответа приложения.

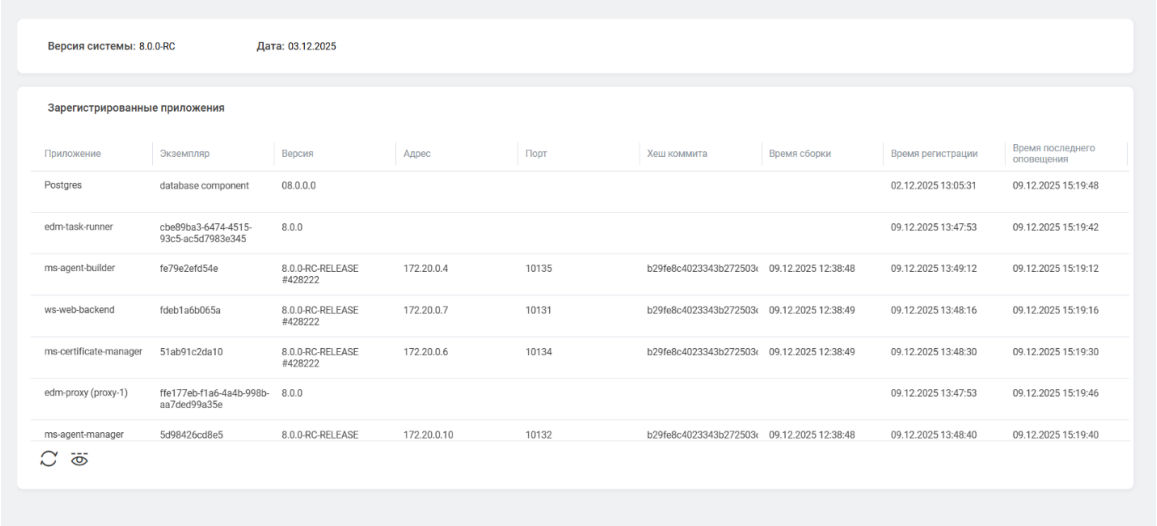

Рисунок 69. Экранная форма «О системе»

15. РЕЗЕРВНОЕ КОПИРОВАНИЕ БД POSTGRESQL И ФХ HDFS

15.1. Конфигурация БД по умолчанию

По умолчанию CEDM-север имеет следующую конфигурацию баз данных:

- БД СУРС: CEDM_test;
- docker-контейнер с БД СУРС: test_CEDM-db01-1;
- порт БД: 5432;
- БД ПАА: auth_test;
- docker-контейнер с БД_ПАА: test_CEDM-db_oauth_01-1;
- порт БД ПАА: 5433;

15.2. Резервное копирование базы данных

Для создания резервных копий баз данных нам необходим установленный клиент PostgreSQL на рабочем месте, с которого будут выполняться запросы. Для установки клиента PostgreSQL выполнить команду:

```
sh
dnf install PostgreSQL15
```

1. Передать пароль базы данных переменной окружения для использования утилитой pg_dump.

```
sh
export PGPASSWORD=DB_PASSWORD
```

где:

DB_PASSWORD – пароль пользователя БД

2. Создать резервную копию базы данных с помощью встроенной в PostgreSQL утилиты pg_dump

```
sh
pg_dump -U DB_USER -h IP_СУБД -p DB_PORT DB_NAME > DB_NAME-
`date --iso`.sql
```

где:

DB_USER – имя пользователя БД;

IP_СУБД – IP адрес хоста, на котором расположена БД;

DB_NAME – имя БД для резервирования;

DB_PORT – порт, на котором работает PostgreSQL;

> DB_NAME-date --iso.sql – перенаправляет вывод команды в файл. Имя файла формируется из имени базы данных и текущей даты в формате ISO (YYYY-MM-DD). Например, CEDM_test-2024-07-16.sql.

В результате в каталоге запуска команды создается SQL-файл с резервной копией указанной базы данных.

15.3. Восстановление базы данных из резервной копии

В качестве примера рассматривается ситуация восстановления данных на CEDM-сервер СУБД, где создан контейнер с БД, но самой БД нет, пользователь БД не создан. Файл резервной копии находится на сервере.

Для восстановления данных из резервной копии выполнить следующие действия:

1. На CEDM-сервере с СУБД подключится к терминалу PostgreSQL, расположенному в docker-контейнере, от имени пользователя postgres:

```
sh
docker exec -it DB_CONTAINER_NAME su postgres -c "psql"
```

где:

DB_CONTAINER_NAME – имя docker-контейнера с БД.

2. Создать пользователя и назначить ему роли:

```
SQL
create role DB_USER password 'DB_PASSWORD' createdb createrole
inherit login
```

где:

DB_USER – имя создаваемого пользователя;

'DB_PASSWORD' – пароль создаваемого пользователя;

createdb – дает пользователю право создавать новые базы данных;

createrole – позволяет пользователю создавать другие роли и пользователей;

inherit – новый пользователь автоматически получает привилегии ролей, членом которых она является;
login – позволяет пользователю входить в систему (т.е. это создается учетная запись, а не просто набор разрешений).

3. Назначить роли DB_USER пользователю admin:

```
SQL
grant DB_USER to admin
```

4. Создать чистую БД и дать права на нее ранее созданному пользователю:

```
SQL
CREATE DATABASE DB_NAME WITH OWNER = DB_USER ENCODING = 'UTF8'
TABLESPACE = pg_default TEMPLATE = template0 LC_COLLATE =
'ru_RU.UTF-8' LC_CTYPE = 'ru_RU.UTF-8' CONNECTION LIMIT = -1
```

где:
DB_NAME – имя создаваемой БД;
DB_USER – имя пользователя, созданного на шаге 2.

5. Выйти из терминала PostgreSQL:

```
SQL
postgres=# \q
```

6. Скопировать файл резервной копии в контейнер с БД в домашний каталог пользователя postgres (/home/postgres):

```
sh
docker cp backup_file.sql DB_CONTAINER_NAME:/home/postgres
```

где:
backup_file.sql – имя файла и полный путь к нему внутри docker-контейнера;
DB_CONTAINER_NAME – имя docker-контейнера с БД.

7. Выполнить восстановление данных из резервной копии:

```
sh
docker exec -it DB_CONTAINER_NAME su postgres -c "psql -d
DB_NAME -f /home/postgres/backup_file.sql"
```

где:

DB_CONTAINER_NAME – имя docker-контейнера с БД;
DB_NAME – имя созданной на шаге 4 БД;
backup_file.sql - имя файла с резервной копией.

8. Дождаться завершения процесса восстановления данных.

15.4. Конфигурация ФХ HDFS по умолчанию

По умолчанию CEDM-север имеет следующую конфигурацию ФХ HDFS:

- расположение ФХ HDFS: CORE-сервер с основными приложениями;
- путь к ФХ HDFS:

/var/lib/docker/volumes/test_CEDM_dfs_data/_data/datanode,

где:

test_CEDM_dfs_data – имя docker-volume, которое создается в системе для контейнера с ФХ HDFS. Оно может отличаться. Узнать его имя можно командой

```
sh
docker volume ls | grep dfs_data docker
```

- имя docker-контейнера с ФХ:

test_CEDM-ms_file_storage_data_node-1

- путь к ФХ внутри docker-контейнера:

/usr/share/hdfs

15.5. Резервное копирование ФХ HDFS

Для доступа к контейнерам в командах имя контейнера получается путем применения фильтров к списку контейнеров системы.

15.5.1. Способ 1: Архивирование каталога с ФХ

1. Остановить контейнер с ФХ HDFS:

```
sh
docker stop $(docker ps --format "table {{.Names}}" |grep stor-
age)
```

2. Архивировать каталог с ФХ HDFS:

```
sh
tar czvf hdfs-`date --iso`.tar.gz /var/lib/docker/vol-
umes/test_CEDM_dfs_data/_data/datanode/
```

В результате выполнения команды создается архив с именем hdfs-YYYY-MM-DD.tar.gz, где YYYY-MM-DD – текущая дата.

3. Запустить контейнер:

```
sh
docker start $(docker ps -a --format "table {{.Names}}" |grep
storage)
```

Восстановление ФХ HDFS из архива

1. Остановить контейнер с ФХ HDFS:

```
sh
docker stop $(docker ps --format "table {{.Names}}" |grep stor-
age)
```

2. Распаковать архив с резервной копией:

```
sh
tar xzvf hdfs-2024-04-02.tar.gz  -C /
```

3. Запустить контейнер:

```
sh
docker start $(docker ps -a --format "table {{.Names}}" |grep
storage)
```

15.5.2. Способ 2: Резервное копирование docker volume

Для резервного копирования docker volume потребуется дополнительный контейнер. В данном Руководстве используется образ легковесного контейнера с набором утилит BusyBox.

Подготовка

1. Если на сервере CORE нет доступа в Интернет, то необходимо доставить файл с образом контейнера в Систему.
2. Загрузить доставленный образ в локальный репозиторий docker:

```
sh
docker load -i busybox.tar
```

Резервное копирование docker volume

1. Выполнить команду запуска временного контейнера и создания архива:

```
sh
docker run --rm --volumes-from test_CEDM-ms_file_stor-
age_data_node-1 -v $(pwd):/backup busybox tar cvf /backup/hdfs-
`date --iso`.tar /usr/share/hdfs
```

где:

test_CEDM-ms_file_storage_data_node-1 – имя контейнера ФХ (используется по умолчанию);

hdfs-`date --iso`.tar – имя конечного архива;

/usr/share/hdfs – путь к ФХ внутри docker-контейнера (используется по умолчанию).

В результате работы команды без остановки основного контейнера будет создана резервная копию данных HDFS в архив с именем hdfs-YYYY-MM-DD.tar (где YYYY-MM-DD – текущая дата).

Восстановление docker volume архива

1. Выполнить команду запуска временного контейнера и распаковки архива с резервной копией:

```
sh
```

```
docker run --rm --volumes-from test_CEDM-ms_file_stor-
age_data_node-1 -v $(pwd):/backup busybox tar cvf /backup/hdfs-
`date --iso`.tar /usr/share/hdfs
```

где:

test_CEDM-ms_file_storage_data_node-1 – имя контейнера ФХ (используется по умолчанию);

hdfs-YYYY-MM-DD.tar – имя архива с резервной копией;

2. Перезапустить контейнер с ФХ:

```
sh
docker restart $(docker ps -a --format "table {{.Names}}" |grep
storage_data)
```

Примечание: операция восстановления может перезаписать существующие данные в томах HDFS, поэтому ее следует использовать с осторожностью и только когда вы уверены в необходимости восстановления данных из этой конкретной резервной копии.

В текущей реализации HDFS оба способа 100% гарантии сохранения данных не дают.

16. СПРАВОЧНАЯ ИНФОРМАЦИЯ

16.1. Журналирование событий компонентов Системы CEDM

16.1.1. Расположение и доступ к журналам компонентов Системы CEDM

Журналы компонентов Системы имеют следующую структуру хранения:

/var/lib/docker/containers/{container_id}/*.log,

где *container_id* – уникальный идентификатор контейнера Docker, генерируемый при установке системы.

Для доступа к журналу заданного компонента необходимо на сервере с основными приложениями выполнить следующие действия:

1. Отобразить имена всех имеющихся контейнеров Docker, выполнив команду:

docker ps --format "table {{.Names}}"

2. Получить идентификатор контейнера Docker командой:

docker inspect --format="{{.Id}}" container_name,

где *container_name* – имя нужного контейнера из списка, полученного на шаге 1.

3. Открыть файлы журнала событий командой:

/var/lib/docker/containers/{container_id}/.log,*

где *container_id* – идентификатор контейнера Docker, полученный на шаге 3.

4. Альтернативная команда получения логов по имени контейнера Docker:

docker logs *container_name,*

где *container_name* – имя контейнера из списка, полученного на шаге 1.

В таблице 6 приведено местонахождение журналов событий компонентов Системы CEDM.

Таблица 6. Расположение журналов с логами CEDM и команды для их просмотра

Приложение	**Сервер**	**Каталог с логами**	**Фор-мат**	**Команды для просмотра логов**
ms-app-registry	CORE	/var/lib/docker/containers/{container_id}/*.log	json	*cat /var/lib/docker/containers/{container_id}/*.log* *docker logs {container_name}*
ws-web-backend	CORE	/var/lib/docker/containers/{container_id}/*.log	json	
ms-file-storage-data_node	CORE	/var/lib/docker/containers/{container_id}/*.log	json	
ms-file-storage-name_node	CORE	/var/lib/docker/containers/{container_id}/*.log	json	
ms-agent-manager	CORE	/var/lib/docker/containers/{container_id}/*.log	json	
ws-web-proxy	CORE	/var/lib/docker/containers/{container_id}/*.log	json	
ws-web-proxy	CORE	/var/lib/docker/containers/{container_id}/*.log	json	
nginx	CORE	/var/lib/docker/containers/{container_id}/*.log	json	
web_frontend_auth	CORE	/var/lib/docker/containers/{container_id}/*.log	json	
ws_auth	CORE	/var/lib/docker/containers/{container_id}/*.log	json	
web_frontend	CORE	/var/lib/docker/containers/{container_id}/*.log	json	
agent-task-runner-service	Task Manager	/opt/agent-task-runner-service/logs/	txt	*cat /opt/agent-task-runner-service/logs/daily_log_ `date +'%Y-%m-%d'` `*
agent-proxy-service	Proxy Gate	/opt/agent-proxy-service/logs/	txt	*cat /opt/agent-proxy-service/logs/daily_log_ `date +'%Y-%m-%d'` `*
kafka	CORE	/opt/kafka/logs/server.log	txt	*cat /opt/kafka/logs/server.log*

16.1.2. Журналирование ПАА

Журналирование событий ПАА осуществляется в развернутой на сервере СУБД базе данных auth_test.

В таблице 7 приведены схемы, наименования и описания журналов.

Таблица 7. Журналирование ПАА

Схема	Наименование	Описание
Журналы		
adb_event	event_log	Журнал событий
adb_event	error_log	Журнал ошибок
Справочники		
adb_event	nsi_event_category	Справочник «Категория события»
adb_event	nsi_event_type	Справочник «Тип события»
adb_event	rmm_event_type_category	Допустимые события по категориям
auth_data	nsi_object_type	Справочник «Тип объекта»
adb_event	nsi_error_category	Справочник «Категория ошибок»
adb_event	nsi_error_type	Справочник «Тип ошибки»
adb_event	object_info_v	Представление «Список объектов системы»

16.1.3. Журналирование событий СУРС

Журналирование событий СУРС осуществляется в развернутой на сервере СУБД базе данных CEDM_test.

В таблице 8 приведены схемы, наименования и описания журналов.

Таблица 8. Журналирование СУРС

Схема	Наименование	Описание
Журналы		
adb_event	event_log	Журнал событий
adb_event	error_log	Журнал ошибок
adb_event	state_log	Журнал перехода состояний объектов
adb_nsi	remote_assistant_log	Журнал сеансов удаленного помощника
adb_nsi	workstation_event_log	Журнал событий устройства
adb_nsi	rmm_workstation_task	Журнал задач устройства
Справочники		
adb_event	nsi_event_category	Справочник «Категория события»
adb_event	nsi_event_type	Справочник «Тип события»
adb_event	rmm_event_type_category	Допустимые события по категориям
adb_nsi	nsi_object_type	Справочник «Тип объекта»
adb_event	nsi_error_category	Справочник «Категория ошибок»
adb_event	nsi_error_type	Справочник «Тип ошибки»

adb_event	object_info_v	Представление «Список объектов системы»
adb_nsi	nsi_state	Справочник «Статусы»
adb_nsi	nsi_state_reason	Справочник «Причины состояний»
adb_nsi	workstation	Устройства
adb_nsi	nsi_session_state	Справочник «Состояние сеанса»
adb_nsi	nsi_disconnect_reason	Справочник «Причина отключения»
adb_nsi	nsi_workstation_event_type	Справочник «Тип события устройства»
adb_nsi	nsi_workstation_event	Справочник «Событие устройства»
adb_nsi	task_template	Шаблон задач

16.2. Метрики для постановки на мониторинг

Данный раздел описывает ключевые метрики, которые необходимо отслеживать для обеспечения стабильной работы системы CEDM. Метрики разделены по сервисам и важности, что позволяет администраторам Системы приоритизировать свои действия в случае возникновении проблем.

16.2.1. Общие принципы мониторинга

Все серверы и ключевые сервисы системы CEDM должны быть подключены к системе мониторинга.

Для каждой метрики определен уровень важности: «высокая», «средняя» или «предупреждение».

Метрики охватывают различные аспекты работы системы: от состояния файловой системы до работы конкретных сервисов и контейнеров.

16.2.2. Ключевые метрики для постановки на мониторинг

В таблице 9 представлены ключевые метрики для постановки на мониторинг на примере системы мониторинга Zabbix. При использовании других систем мониторинга может потребоваться адаптация названий и параметров метрик. Администраторам CEDM рекомендуется настроить оповещения на основе этих метрик в соответствии с их важностью.

Таблица 9. Метрики постановки на мониторинг

Метрика	Важность	Сервис	Сервер	Пояснение	Описание
Disk space is critically low	средняя	ФС	все	Мониторинг свободного места на диске	Место на диске занято больше чем на 90%
Disk space is low	предупреждение	ФС	все	Мониторинг свободного места на диске	Место на диске занято больше чем на 80%
Filesystem has become read-only	средняя	ФС	все	Мониторинг возможности записи информации на диск	Файловая система перешла в режим read-only
/boot: Disk space is critically low	средняя	ФС	все	Мониторинг свободного места на диске	Место на загрузочном разделе /boot занято больше чем на 90%
/boot: Disk space is low	предупреждение	ФС	все	Мониторинг свободного места на диске	Место на загрузочном разделе /boot занято больше чем на 80%
/boot: Filesystem has become read-only	средняя	ФС	все	Мониторинг возможности записи информации на диск	Файловая система загрузочного раздела /boot перешла в режим read-only
agent-proxy-service is not running	высокая	agent-proxy-service	Proxy Gate	Мониторинг состояния службы agent-proxy-service	Служба agent-proxy-service не запущена
agent-task-runner-service is not running	высокая	agent-task-runner-service	Task Manager	Мониторинг состояния службы agent-task-runner-service	Служба agent-task-runner-service не запущена
Container *NAME*: An error has occurred in the container	предупреждение	docker	CORE, СУБД	Мониторинг состояния контейнера	Контейнер работает с ошибкой

Container *NAME*: Container has been stopped with error code	средняя	docker	CORE, СУБД	Мониторинг состояния контейнера	Работа контейнера была завершена с ошибкой
Container *NAME*: Health state container is unhealthy	высокая	docker	CORE, СУБД	Мониторинг состояния контейнера	Статус контейнера - UNHEALTHY
Docker: Service is down	средняя	docker	CORE, СУБД	Мониторинг состояния службы docker	Служба docker не запущена
health ms-agent-manager is no data more 1h	высокая	docker	CORE	Мониторинг actuator/health контейнера ms-agent-manager	Данных от приложения ms-agent-manager за последний час не поступало
health ms-app-registry is no data more 1h	высокая	docker	CORE	Мониторинг actuator/health контейнера ms-app-registry	Данных от приложения ms-app-registry за последний час не поступало
health ws-web-backend is no data more 1h	высокая	docker	CORE	Мониторинг actuator/health контейнера ws-web-backend	Данных от приложения ws-web-backend за последний час не поступало
health ws-web-proxy is no data more 1h	высокая	docker	CORE	Мониторинг actuator/health контейнера ws-web-proxy	Данных от приложения ws-web-proxy за последний час не поступало.
Interface ens18: Link down	средняя	сетевой интерфейс	все	Мониторинг сетевого интерфейса	Пропала связь до сетевого интерфейса
Linux: High CPU utilization	предупреждение	ОС	все	Мониторинг нагрузки системы	Последние 5 минут нагрузка на ЦПУ выше 90%
Linux: High memory utilization	средняя	ОС	все	Мониторинг нагрузки системы	Последние 5 минут используется больше 90% ОЗУ
Linux: High swap space usage	предупреждение	ОС	все	Мониторинг нагрузки системы	Последние 5 минут свободной своп-памяти меньше 50%
Linux: Lack of available memory	средняя	ОС	все	Мониторинг нагрузки системы	Последние 5 минут свободно меньше 20МБ ОЗУ

Linux: Zabbix agent is not available	средняя	zabbix-agentd zabbix-agent2	все	Мониторинг состояния службы zabbix-agentd или zabbix-agent2	zabbix-agent на клиенте не доступен с сервера мониторинга.
DB [db_name]: Deadlock occurred	средняя	PostgreSQL	СУБД	Мониторинг данных БД	Больше 5 минут число дедлоков больше 0.
DB [db_name]: Number of locks is too high	средняя	PostgreSQL	СУБД	Мониторинг данных БД	Количество блокировок последние 5 минут больше 100.
DB [db_name]: Too many slow queries	средняя	PostgreSQL	СУБД	Мониторинг данных БД	Медленных запросов за последние 5 минут больше 5
Kafka process is down more 2m	высокая	kafka	CORE	Мониторинг состояния службы kafka	Служба kafka не активна более 2 минут.

16.2.3. Настройка мониторинга

Для эффективного мониторинга рекомендуется:

1. Использовать систему мониторинга Zabbix или аналогичную, способную отслеживать указанные метрики. При использовании других систем может потребоваться адаптация названий и параметров метрик.
2. Настроить систему мониторинга для отслеживания всех указанных метрик.
3. Установить пороговые значения для каждой метрики в соответствии с указанными в таблице критериями.
4. Настроить оповещения для администраторов с учетом важности каждой метрики.
5. Регулярно проверять и обновлять настройки мониторинга для обеспечения их актуальности.

16.2.4. Действия при срабатывании оповещений

При получении оповещения администратору следует:

1. Определить важность проблемы на основе сработавшей метрики.
2. Проверить состояние затронутого сервиса или компонента системы.
3. Предпринять необходимые меры для устранения проблемы в соответствии с ее важностью.

4. Зафиксировать инцидент и принятые меры в журнале обслуживания системы.
5. Проанализировать причины возникновения проблемы и, при необходимости, внести изменения в конфигурацию системы для предотвращения подобных ситуаций в будущем.

17. ДИАГНОСТИКА И РЕШЕНИЕ ПРОБЛЕМ

17.1. Общие рекомендации по диагностике

Общие рекомендации по диагностике:

- проверить журналы компонентов Системы, в которых возникла ошибка (см. подраздел 14.1 настоящего руководства);
- проверить состояние сетевых подключений между компонентами Системы;
- выполнить перезагрузку контейнеров компонентов, в которых возникла ошибка.

17.2. Часто встречающиеся проблемы и их решения

17.2.1. Проблемы с аутентификацией пользователей

Проблема: Пользователь не может войти в систему.
Возможные причины и решения:

- неверные учетные данные: проверить корректность логина и пароля;
- блокировка учетной записи: проверить статус УЗ в ПАА;
- проблемы с интеграцией AD: проверить настройки подключения к AD.

17.2.2. Проблемы с производительностью системы

Проблема: Система работает медленно.
Возможные причины и решения:

- высокая нагрузка на сервер: проверить загрузку CPU, памяти и диска;
- проблемы с базой данных: проверить производительность запросов к БД;
- сетевые задержки: проверить пропускную способность сети;

17.2.3. Ошибки при интеграции с внешними системами

Проблема: не работает интеграция с Active Directory.
Возможные причины и решения:

- неверные настройки подключения: проверить параметры в разделе «Внешние системы аутентификации»

- проблемы с сетевым доступом: проверить доступность сервера AD;
- недостаточно прав: проверить права доступа учетной записи для интеграции.

17.2.4. Ошибки сервера CORE после перезагрузки сервера или его восстановления из снапшота (Snapshot)

Симптомы:

- после перезагрузки или восстановления из снапшота сервера CORE при входе пользователя в Систему отображается ошибка «502 Bad Gateway» (рисунок 70);

Рисунок 70. Ошибка «502 Bad Gateway»

- служба Kafka не запускается.

Решение:

Остановить службы zookeeper и kafka

```bash
systemctl stop zookeeper.service
systemctl stop kafka.service
```

Удалить журналы событий сервиса Zookeeper:

```bash
rm -rf /tmp/zookeeper
```

- удалить журналы событий сервиса Kafka:

```
bash
rm -rf /data/kafka/kafka-logs
```

- запустить службы zookeeper и kafka:

```
bash
systemctl start zookeeper.service
systemctl start kafka.service
```

- перезапустить все контейнеры:

```
bash
docker restart $(docker ps -q)
```

На сервере с компонентом CEDM Task Runner проверить службу agent-task-runner-service на наличие ошибок.

```
bash
systemctl status agent-task-runner-service
```

Если есть ошибки перезапустить службу:

```
bash
systemctl restart agent-task-runner-service
```

На сервере с компонентом CEDM Proxy проверить службу *agent-proxy-service* на наличие ошибок:

```
bash
systemctl status agent-proxy-service
```

Если есть ошибки перезапустить службу:

```
bash
systemctl restart agent-proxy-service
```

18. ОБРАЩЕНИЕ В ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ

18.1. Порядок подачи обращений в службу технической поддержки

Обращения в службу поддержки компании «ООО «Кросстех Солюшнс Групп» (Вендор) в гарантийных случаях необходимо производить через электронную почту support@ct-sg.ru.

18.2. Требования к содержанию обращений

При подаче обращения через портал технической поддержки для ускорения предоставления решения по обращению необходимо максимально подробно заполнить все поля и приложить файлы с необходимой информацией (журналы событий, скриншоты, другие файлы).

Требования к оформлению обращений:

1. Одно обращение описывает одну проблему, возникшую в процессе работы системы.
2. Наименование обращения кратко описывает имеющуюся проблему.
3. Указан приоритет устранения проблемы:
    - критичный – существование дефекта приводит к масштабным последствиям катастрофического характера, например: потеря данных, раскрытие конфиденциальной информации;
    - средний – существование дефекта слабо влияет на типичные сценарии работы пользователей, и/или существует обходной путь достижения цели, например: диалоговое окно не закрывается автоматически после нажатия кнопок «OK»/«Cancel»;
    - низкий – существование дефекта редко обнаруживается незначительным процентом пользователей и (почти) не влияет на их работу, например: опечатка в глубоко вложенном пункте меню настроек.
    - Описание проблемы подробное и содержит следующие пункты:
    - окружение – версия ОС и ее разрядность, версия продукта, дополнительные параметры (браузеры и их версии или приложения и их версии);

- шаги воспроизведения – алгоритм в форме пошаговой инструкции воспроизведения ошибки, где одно действие указано как один шаг;
- ожидаемый результат – описание того, как система должна работать после выполнения шагов, указанных выше;
- фактический результат – описание того, как система работает после воспроизведения вышеуказанной последовательности шагов;
- вложенные файлы – дополнительная информация: скриншоты, текстовые файлы, журналы событий, видео выполняемых действий.

Дополнительные параметры: предусловие, постусловие, дополнения.