ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«РЕД ЕСАА»

Руководство администратора

RU.13230434.033 15

Содержание

1. Введение

В данном руководстве будет рассмотрено программное обеспечение «РЕД ЕСАА» версии 1.8 (далее – РЕД ЕСАА, Система). Содержит инструкцию по настройке, установке, запуску и использованию Системы и предназначено для системных администраторов и сотрудников отделов информатизации и обеспечения информационной безопасности, выполняющих настройку Системы. Программное обеспечение РЕД ЕСАА является платформенно-независимым Web-приложением, реализованным в соответствии со стандартной спецификацией Java Servlet в среде Servlet контейнера сервера приложений.

РЕД ЕСАА состоит из следующих подсистем:

- Системные объекты
- Информационной безопасности
- Администрирование
- Авторизация

В рамках данного руководства будут рассмотрены подсистемы «Системные объекты», «Информационной безопасности» и «Администрирование». Подсистема «Авторизация» рассматривается в руководстве пользователя.

2. Назначение

Программное обеспечение «РЕД ЕСАА» реализует централизованную аутентификацию пользователей Системы в рамках концепции единой точки входа (обмен криптозащищенными токенами аутентификации).

Программное обеспечение «РЕД ЕСАА» устанавливается на объекты автоматизации с целью:

- Централизованного управления учетными записями пользователей и их ролями в информационных системах зарегистрированных в РЕД ЕСАА к ресурсам которых осуществляется доступ (далее – клиентских системах);
- Централизованного управления клиентскими системами;
- Хранение идентификационной информации пользователей и предоставление сервиса аутентификации и авторизации для клиентских систем, которым требуется предоставлять доступ к каким-либо ресурсам.

3. Аппаратные и программные требования к Системе

3.1. Аппаратные требования

Технические средства, на которых функционирует программное обеспечение «РЕД ЕСАА» при минимальных нагрузках, должны удовлетворять требованиям, изложенным в таблице 3.1.

Таблица 3.1 – Минимальные требования аппаратных средств среды функционирования программного обеспечения «РЕД ЕСАА»

Наименование	Описание
Центральный процессор	8-ядерный процессор 64-бит с тактовой частотой 2 ГГц и выше
Оперативная память	24 ГБ и выше
Дисковая подсистема	Жесткий диск SSD 600 ГБ и более
Сетевой интерфейс	Ethernet порт 1000 BASE-T

3.2. Программные требования

Состав программного обеспечения, необходимый для функционирования программы, приведен в таблице 3.2.

Таблица 3.2 – Минимальные требования общесистемных программных средств среды функционирования программного обеспечения «РЕД ЕСАА»

Наименование	Описание
Операционная система	Семейства linux
Среда исполнения Java-программ	«Среда разработки и исполнения Java Axiom JDK Certified», версия Axiom JDK Certified 8;
Сервер приложений	Сервер приложений Libercat Certified, версия Libercat 9;

Наименование	Описание
Система управления базами данных	Ред База Данных 3.0 и выше
Веб-браузер	Mozilla Firefox 30 и выше и пр.

3.3. Требования безопасной эксплуатации Системы

Доступ к РЕД ЕСАА должен осуществляться только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Должно быть обеспечено взаимодействие РЕД ЕСАА только с доверенными системами, правила безопасности которых скоординированы с правилами безопасности организации, использующей РЕД ЕСАА.

Должны быть обеспечены установка, конфигурирование и управление РЕД ЕСАА в соответствии с эксплуатационной документацией на РЕД ЕСАА.

Аутентификация субъектов, осуществляющих попытку доступа к РЕД ЕСАА, должна осуществляться с использованием механизмов ОС, под управлением которой функционирует РЕД ЕСАА.

Функционирование РЕД ЕСАА должно осуществляться в среде функционирования, предоставляющей механизм аутентификации, обеспечивающий требуемый уровень защиты от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

Администраторы РЕД ЕСАА должны иметь квалификацию и опыт достаточные для выполнения инструкций, указанных в эксплуатационной документации на РЕД ЕСАА.

Предполагается наличие (одного или более) компетентных лиц, которые назначаются для управления безопасностью РЕД ЕСАА и информации в нем. Эти лица должны нести личную ответственность за следующие функции:

1. управление учетными записями пользователей;
2. первоначальное создание и присвоение учетным записям пользователям паролей, а также их смена в процессе эксплуатации в соответствии с требованиями правил безопасности организации;
3. создание и сопровождение ролей;
4. установление и сопровождение отношений между ролями;
5. назначение и аннулирование ролей, назначаемых пользователям.

Совместные действия уполномоченных на доступ к РЕД ЕСАА пользователей должны быть направлены исключительно на выполнение своих функциональных обязанностей.

4. Подготовка к работе

4.1. Установка РЕД ЕСАА

Для работоспособности и функционирования РЕД ЕСАА необходимо предварительно установить и настроить ПО из состава таблицы 3.2. Установка всех компонентов производится согласно эксплуатационной документации на них. Руководство по установке «РЕД ЕСАА» приведено ниже.

1. Находящийся на дистрибутивном диске архив формата «war» разместить в каталоге «webapps» сервера приложений.
2. Базу данных разместить в каталоге /opt/RedDatabase/ и дать права firebird:firebird. Затем в файле /opt/RedDatabase/databases.conf прописать путь до базы данных.

3. Необходимо установить переменную среды JAVA_HOME, в качестве значения которой вводится путь к каталогу установки среды исполнения JAVA.
4. Перезагрузить сервер.

Настройка файла конфигурации СУБД (firebird.conf). Необходимо добавить в конфигурационный файл следующие параметры:

```
ServerMode = Super
AuthServer = Legacy_Auth, Multifactor
AuthClient = Legacy_Auth, Multifactor
UserManager = Legacy_UserManager, Multifactor_Manager
WireCrypt = Disabled
ProviderName = 80
TrustedUser = SYSDBA
```

Данные параметры также необходимо добавить в конфигурационный файл СУБД на стороне каждой клиентской системы зарегистрированной в РЕД ЕСАА.

Перезагрузить сервер СУБД: systemctl restart firebird

Настройка файла конфигурации РЕД ЕСАА (ncore-properties.xml). Необходимо добавить в конфигурационный файл следующие параметры:

```
<entry key="ncore.security.vaadin.login.handler">biz.redsoft.sso.vaadin.auth.OAuthLoginHandler</entry>
<entry key="biz.redsoft.ncore.security.openid.enabled">true</entry>
<entry key="biz.redsoft.ncore.security.oauth2.factories">biz.redsoft.ncore.esia.openid.OpenIdFactory</entry>
<entry key="biz.redsoft.ncore.security.openid.scope">openid</entry>
<entry key="biz.redsoft.ncore.security.openid.authorization_path">/auth</entry>
<entry key="biz.redsoft.ncore.security.openid.access_token_path">/token</entry>
<entry key="biz.redsoft.ncore.security.openid.end_session_path">/logout</entry>
<entry key="biz.redsoft.ncore.security.openid.userinfo_path">/v1/userinfo</entry>
<entry key="biz.redsoft.ncore.security.openid.user_resolver">biz.redsoft.ncore.esia.openid.IdTokenLoginUserResolver</entry>
<entry key="biz.redsoft.ncore.security.openid.allow_new_user_creation">yes</entry>
<entry key="biz.redsoft.ncore.security.openid.reuse_existing_user">yes</entry>
<entry key="ncore.db.auth.ldap.rdb3mode">true</entry>
<entry key="security.cryptoapi.provider.type">80</entry>
<entry key="biz.redsoft.ncore.security.openid.button_caption">Вход ЕСАА</entry>
<entry key="ncore.db.mf.auth">true</entry>
<entry key="biz.redsoft.ncore.security.openid.trusted_db_auth">yes</entry>

<entry key="biz.redsoft.ncore.security.openid.client_id">sso-org</entry> (наименование зарегистрированной системы ЕСАА)
<entry key="biz.redsoft.ncore.security.openid.client_secret">secret1</entry> (секретный код зарегистрированной системы)
<entry key="biz.redsoft.ncore.security.openid.authorization_server">http://192.168.1.2:8080/sso/openid</entry> (адрес доступа Системы)
```

Перезагрузить сервер приложений.

Настройка файла конфигурации на стороне клиентской системы зарегистрированной в РЕД ЕСАА (ncore-properties.xml). Необходимо добавить в конфигурационный файл следующие параметры:

```
<entry key="biz.redsoft.ncore.esia.enabled">true</entry>
<entry key="biz.redsoft.ncore.security.openid.enabled">true</entry>
<entry key="biz.redsoft.ncore.security.oauth2.factories">biz.redsoft.ncore.esia.openid.OpenIdFactory</entry>
<entry key="biz.redsoft.ncore.security.openid.scope">openid</entry>
<entry key="biz.redsoft.ncore.security.openid.authorization_path">/auth</entry>
<entry key="biz.redsoft.ncore.security.openid.access_token_path">/token</entry>
<entry key="biz.redsoft.ncore.security.openid.end_session_path">/logout</entry>
<entry key="biz.redsoft.ncore.security.openid.userinfo_path">/v1/userinfo</entry>
<entry
key="biz.redsoft.ncore.security.openid.user_resolver">biz.redsoft.shg.application.oauth2.openid.ShgIdTokenLoginUserResolver
</entry>
<entry key="biz.redsoft.ncore.security.openid.allow_new_user_creation">yes</entry>
<entry key="biz.redsoft.ncore.security.openid.reuse_existing_user">yes</entry>
```

<entry key="ncore.db.mf.auth">true</entry>
<entry key="biz.redsoft.ncore.security.openid.trusted_db_auth">yes</entry>
<entry key="sso.update.user">true</entry>
<entry key="sso.delete.sys_user_role">true</entry>
<entry key="biz.redsoft.ncore.security.openid.button_caption">Вход ЕСАА</entry>

<entry key="biz.redsoft.ncore.security.openid.client_id">sh-gate</entry> (наименование клиентской системы)
<entry key="biz.redsoft.ncore.security.openid.client_secret">secret2</entry> (секретный код зарегистрированной системы)
<entry key="biz.redsoft.ncore.security.openid.redirect_url">http://192.168.1.3/shg</entry> (адрес клиентской системы)
<entry key="biz.redsoft.ncore.security.openid.authorization_server">http://192.168.1.2:8080/sso/openid</entry> (адрес сервера авторизации ЕСАА)

4.2. Порядок запуска Системы

Запуск программного обеспечения Системы осуществляется путем запуска 2 компонент:

СУБД: systemctl start firebird

Веб сервера:

..tomcat/bin/startup.sh

5. Подсистема «Системные объекты»

5.1. Планировщик заданий

Планировщик заданий позволяет назначать автоматически или вручную выполняемые задания, запуск которых производится в определенное время или при возникновении определенных событий в рамках Системы.

Для доступа к списку заданий планировщика необходимо:

1. Войти в Систему пользователем с ролью «Системный администратор».

2. На панели меню и навигации основного окна приложения перейти на вкладку «Системные объекты» → «Планировщик» → «Задачи планировщика». Произойдет инициализация формы списка элементов задач планировщика «Фоновая задача» (Рис. 5.1). Планировщик Системы содержит список предопределенных задач.

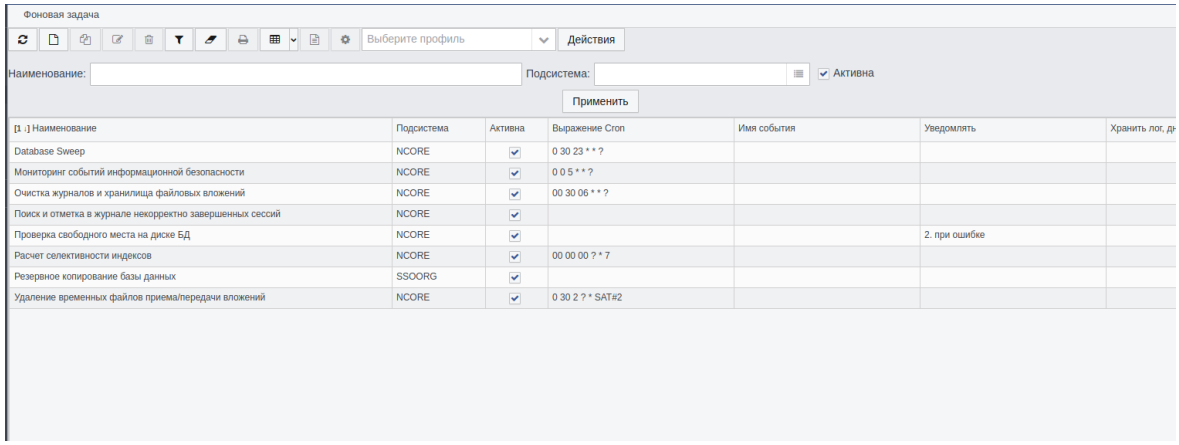


Рис. 5.1 Список задач планировщика

3. Для настройки периодичности выполнения задачи на форме списка «Фоновая задача» выбрать нужную задачу и на командной панели нажать на кнопку «Редактировать» (Рис. 5.1). Произойдет инициализация формы элемента задачи (Рис. 5.2).

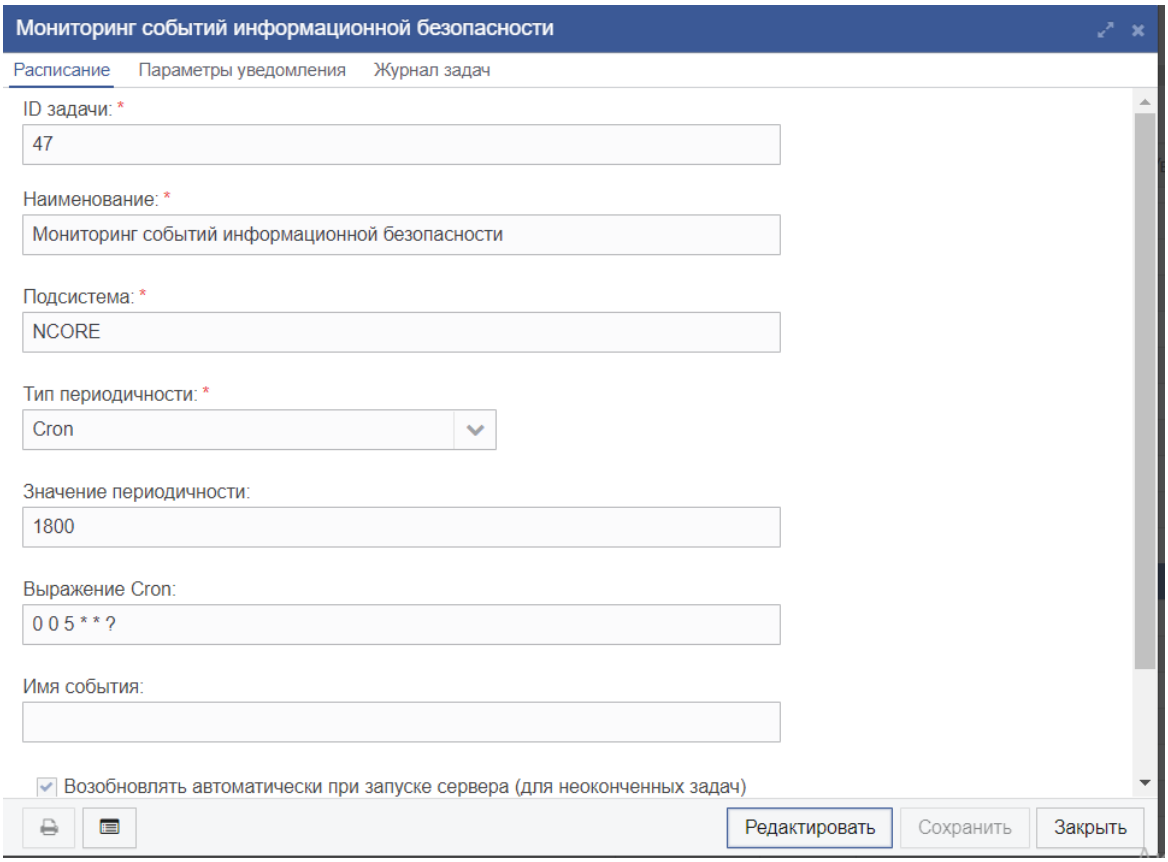


Рис. 5.2 Форма элемента задачи

Таблица 5.1.1 - Описание полей вкладки «Расписание»

Наименование элемента	Описание	Обязательность	Тип ввода
ID задачи	Номер, уникально идентифицирующий элемент задания	-	Заполняется автоматически
Наименование	Наименование выполняемой задачи	-	Вручную
Тип периодичности	Определяет тип периодичности выполнения задачи. Список имеет 3 предопределенных типа: 1. Cron – периодичность выполнения задачи задается выражением «Cron» 2. Циклически, каждые N секунд – периодичность выполнения задачи каждые N секунд. 3. Один раз при старте сервера – выполнение задачи провоцирует событие «Старт сервера»	-	Выбор из списка

Наименование элемента	Описание	Обязательность	Тип ввода
Значение периодичности	Определяет «цикличность» периодичность выполнения задачи в секундах. Доступно, если выставлено значение «Циклически, каждые N секунд» у поля «Тип периодичности»	-	Вручную
Выражение Cron	Определяет «цикличность» периодичность задачи выражением «Cron». Доступно, если выставлено значение «Cron» у поля «Тип периодичности». Структура выражения «cron»: * * * * * выполняемая команда - - - - - | | | | | | | | | ----День недели (1-7) | | | ------День (1 - 31) | | --------Час (0 - 23) | ----------Минута (0 - 59) ----------Секунда (0 - 59)	-	Вручную
Активна	Параметр активирует/деактивирует выполнение задачи планировщиком	-	Проставляется флаг

Таблица 5.1.2 - Описание полей вкладки «Журнал задач»

Наименование элемента	Описание	Обязательность	Тип ввода
Время запуска	Момент времени запуска задачи планировщиком	-	Заполняется автоматически
Время завершения	Момент времени завершения задачи	-	Заполняется автоматически
Сообщение об ошибке	Описания ошибки, возникающей в ходе выполнения задачи планировщиком	-	Заполняется автоматически

4. Для примера выполнить настройку следующим образом:

- Тип периодичности = Cron
- Выражение Cron = 0 40 12 * 1-5 ?

т.е. задача будет выполняться планировщиком каждый рабочий день в 12:40.

В меню «Системные объекты» → «Планировщик» → «Управление планировщиком задач» можно отслеживать статусы задач и их запуски. Для запуска задачи необходимо выделить требуемую задачу в списке и нажать кнопку «Выполнить задачу» (Рис. 5.3).

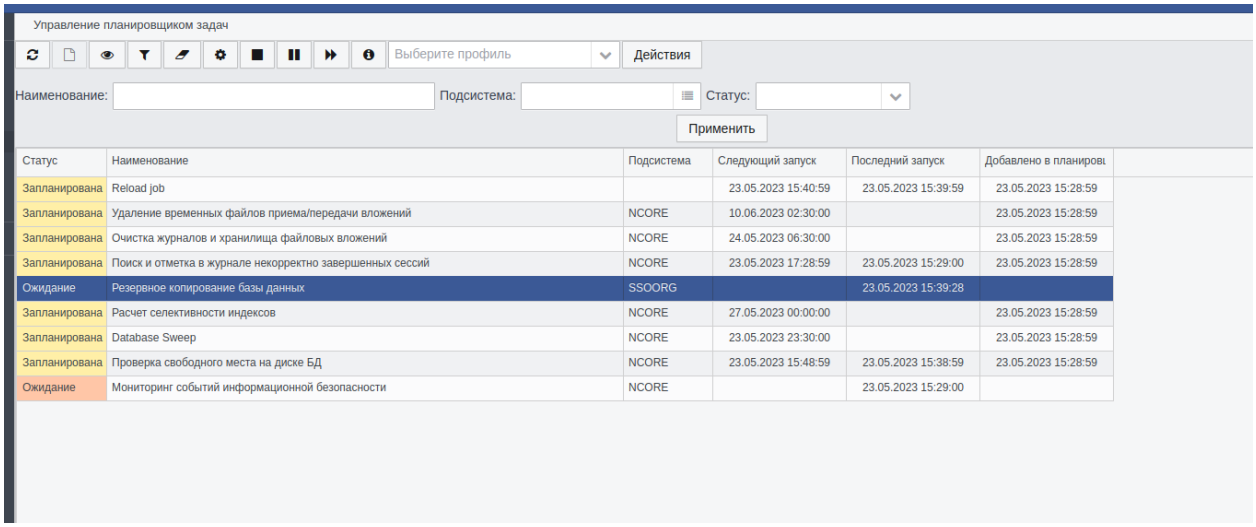


Рис. 5.3 Управление планировщиком задач

5.1.1. Проверка свободного места на диске БД

Для отслеживания свободного дискового пространства жесткого диска, на котором расположена база данных, реализована задача планировщика «Проверка свободного места на диске БД». По умолчанию регулярность проверки составляет 600 секунд (Рис 5.3.1).

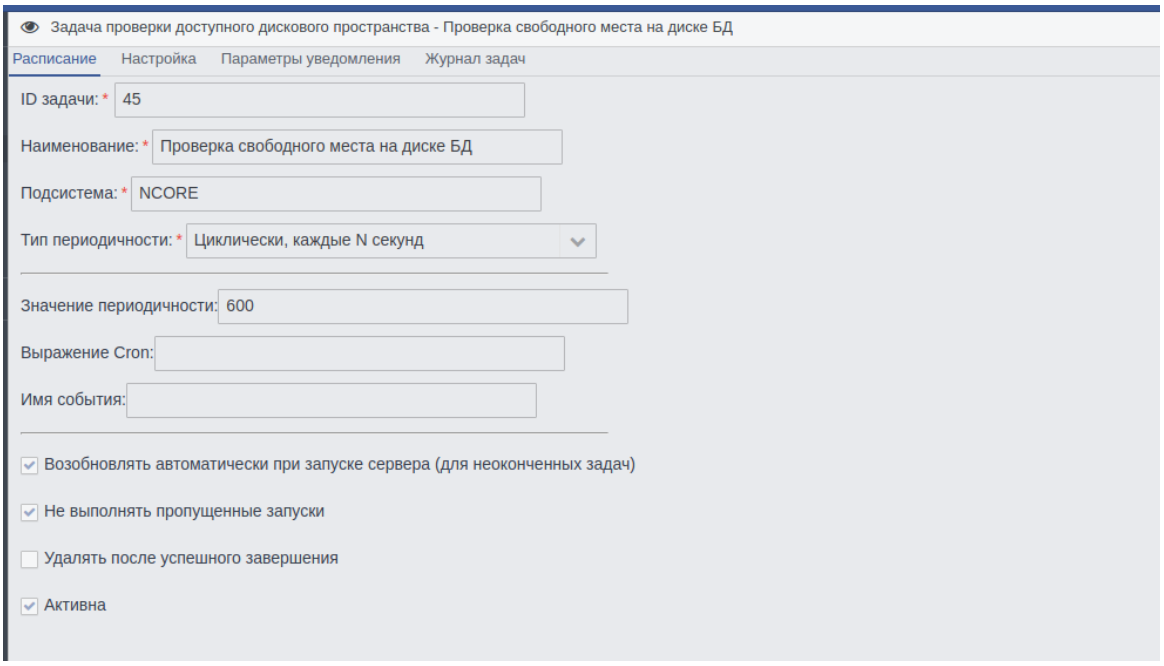


Рисунок 5.3.1. Задача проверки свободного места на диске БД

На форме «Настройка» настраивается объем дискового пространства и количество свободных транзакций в процентном соотношении, при достижении которых будут выполнены выбранные действия ниже (Рис 5.3.2). Либо сервер приложений будет остановлен, либо все подключенные пользователи будут отключены и БД будет переведена в сервисный режим (для возвращения БД в рабочий режим необходимо воспользоваться

утилитой СУБД и ввести команду*: /opt/RedDatabase/bin/gfix -online /БД*), либо оба действия одновременно.

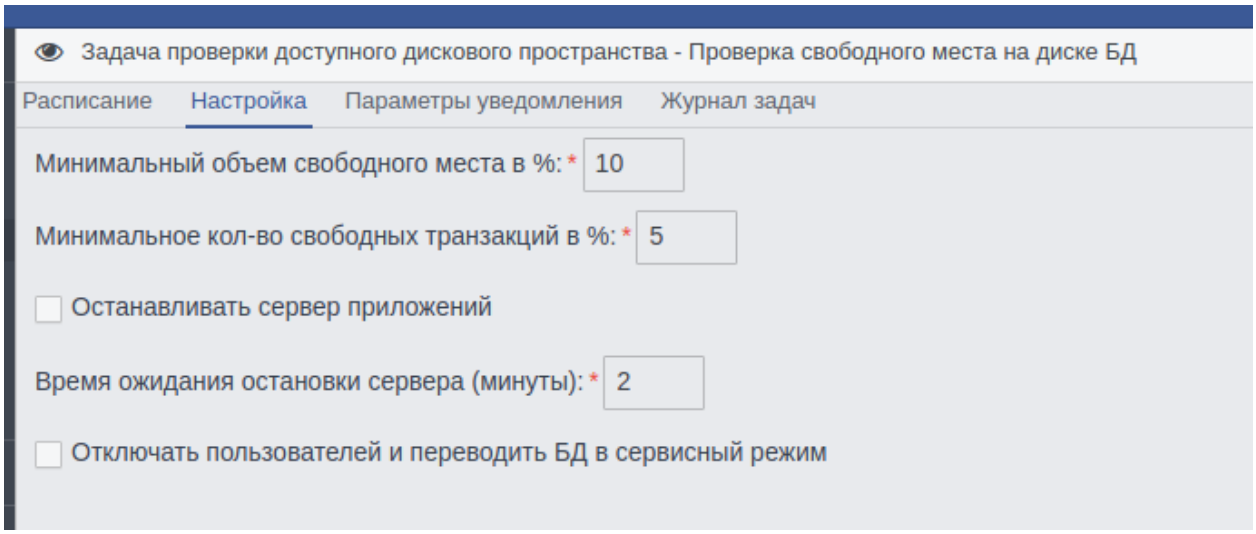
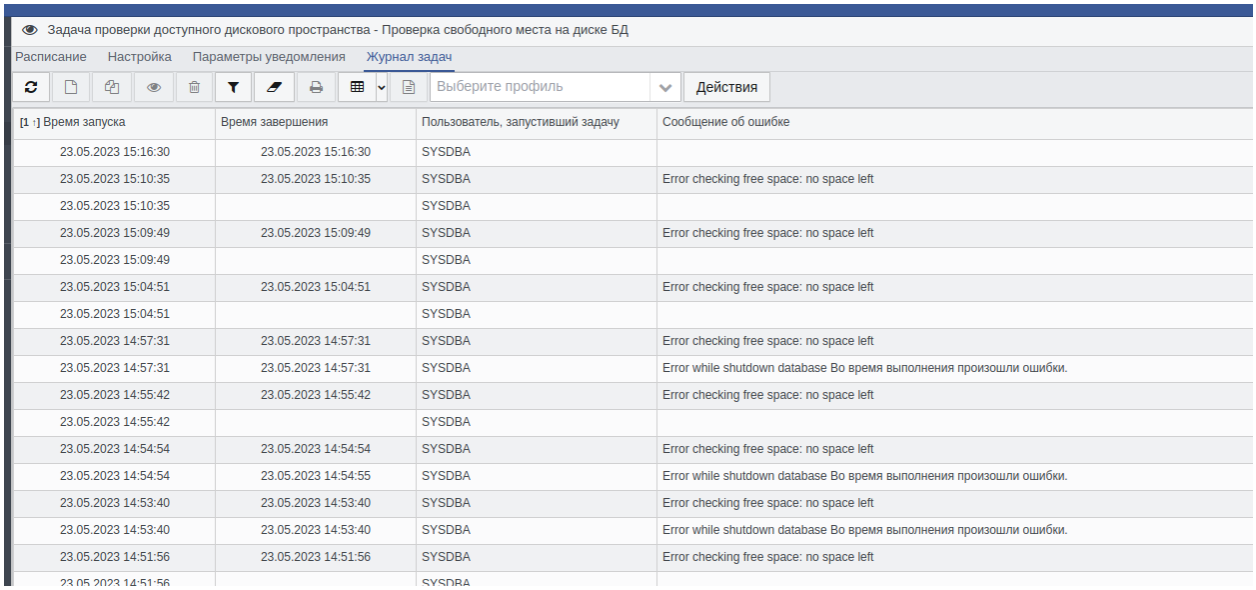


Рисунок 5.3.2 Настройки задачи

В форме «Журнал задач» отображаются записи о начале и завершение задачи, пользователях запустивших задачу и сообщений об ошибках. (Рис 5.3.3)



[1 ↑] Время запуска	Время завершения	Пользователь, запустивший задачу	Сообщение об ошибке
23.05.2023 15:16:30	23.05.2023 15:16:30	SYSDBA	
23.05.2023 15:10:35	23.05.2023 15:10:35	SYSDBA	Error checking free space: no space left
23.05.2023 15:10:35		SYSDBA	
23.05.2023 15:09:49	23.05.2023 15:09:49	SYSDBA	Error checking free space: no space left
23.05.2023 15:09:49		SYSDBA	
23.05.2023 15:04:51	23.05.2023 15:04:51	SYSDBA	Error checking free space: no space left
23.05.2023 15:04:51		SYSDBA	
23.05.2023 14:57:31	23.05.2023 14:57:31	SYSDBA	Error checking free space: no space left
23.05.2023 14:57:31	23.05.2023 14:57:31	SYSDBA	Error while shutdown database Во время выполнения произошли ошибки.
23.05.2023 14:55:42	23.05.2023 14:55:42	SYSDBA	Error checking free space: no space left
23.05.2023 14:55:42		SYSDBA	
23.05.2023 14:54:54	23.05.2023 14:54:54	SYSDBA	Error checking free space: no space left
23.05.2023 14:54:54	23.05.2023 14:54:55	SYSDBA	Error while shutdown database Во время выполнения произошли ошибки.
23.05.2023 14:53:40	23.05.2023 14:53:40	SYSDBA	Error checking free space: no space left
23.05.2023 14:53:40	23.05.2023 14:53:40	SYSDBA	Error while shutdown database Во время выполнения произошли ошибки.
23.05.2023 14:51:56	23.05.2023 14:51:56	SYSDBA	Error checking free space: no space left
23.05.2023 14:51:56		SYSDBA	

Рисунок 5.3.3 Журнал задачи

5.1.2. Резервное копирование БД

Резервное копирование необходимо для возможности быстрого и недорогого восстановления информации (в данном случае базы данных Системы) в случае утери (искажения) рабочей копии информации по какой-либо причине.

В автоматическом режиме полное резервное копирование базы данных Системы, производится в соответствии с заданием планировщика «Резервное копирование базы данных». Задача выполняет резервное копирование базы данных (файл с расширением .fdb в директории расположения базы данных) путем создания файла резервного копирования с именем базы и расширением .fbk, который архивирован в zip архив.

По умолчанию периодичность резервирования БД установлена на тип «вручную». Для настройки резервирования БД необходимо открыть задачу и перейти на форму «Параметры» (Рис. 5.3.4). В поле «База данных» указать абсолютный путь до файла базы данных или оставить поле пустым, в таком случае будет использоваться база из текущего подключения.

Указать путь до директории, в которой будут хранится резервные копии.

Для проверки успешности резервирования необходимо поставить флаг «Выполнять тестовое восстановление» и указать директорию в которой будет выполняться тестовое восстановление.

Указать директорию, в которую будут помещаться сжатые резервные копии БД.

В поле «Хранить резервных копий (не более)» указать максимальное количество хранимых резервных копий БД, после достижения указанного числа, первая копия будет уничтожена.

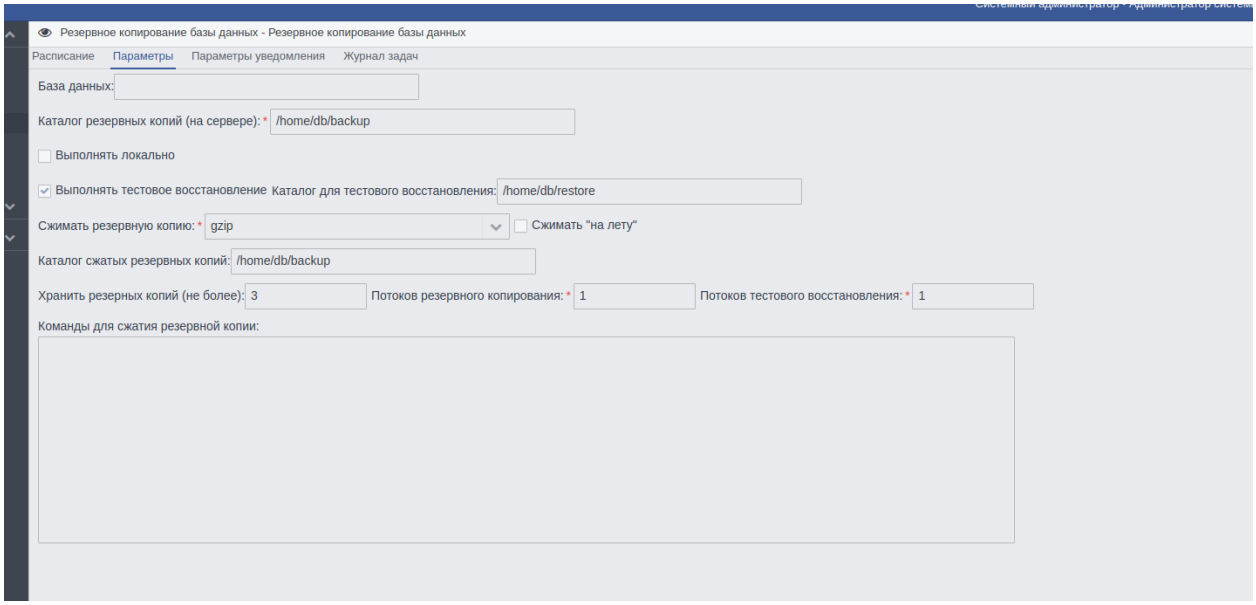


Рисунок 5.3.4 Настройки резервирования БД

После окончания выполнения задачи резервирования в указанной директории резервирования будет создана директория с названием в формате: дата и время завершения резервного копирования. Внутри директории будут два лог-файла (резервирвоания и восстановления) и архив с файлом резервной копии БД в формате имя_базы.fbk.

5.2. Информация о системе

Пункт меню «Системные объекты» → «Информация о системе» позволяет получить диагностическую информацию серверной части веб-приложения (Рис.5.4).

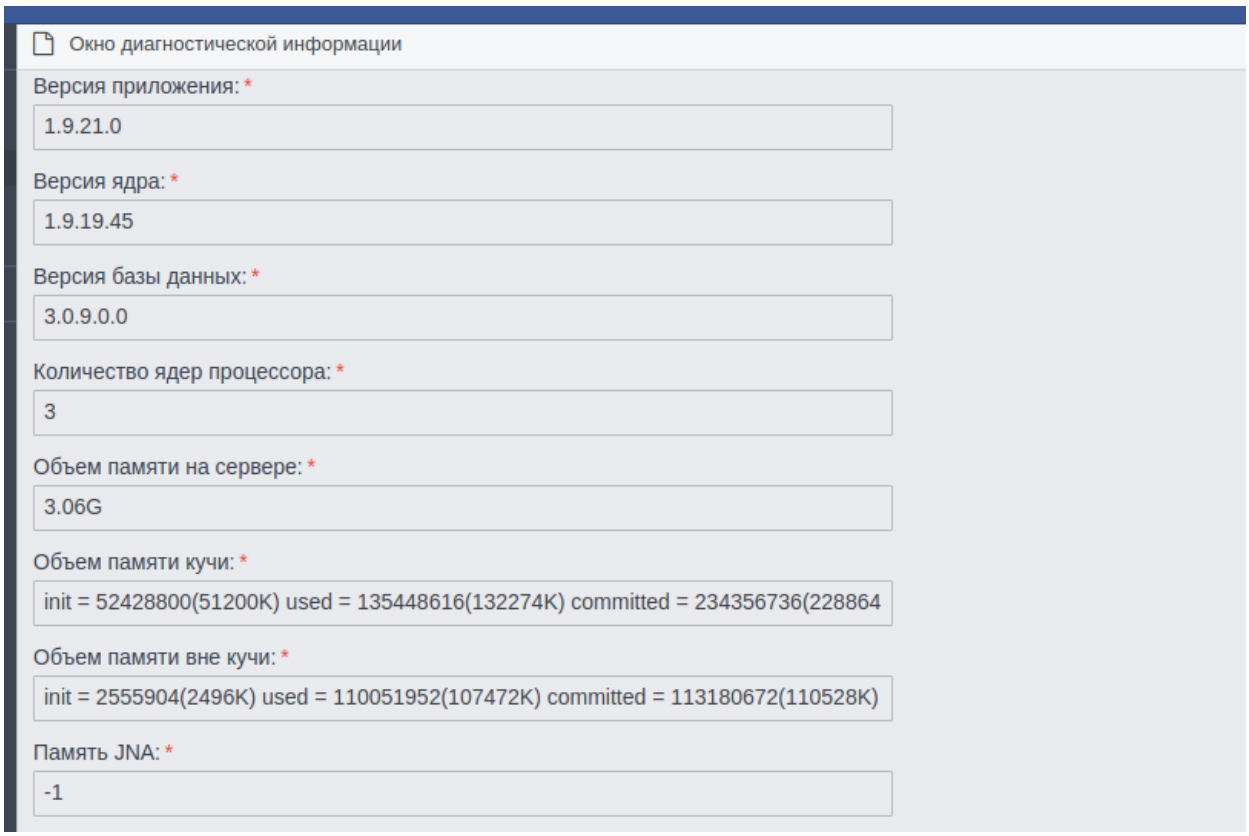


Рис 5.4 Информация о Системе

5.3. Сбросить кэш

Пункт меню «Системные объекты» → «Сбросить кэш» позволяет удалить содержимое, которое устарело или просрочено, тем самым устраняя некоторые проблемы при эксплуатации Системы.

6. Подсистема «Информационной безопасности»

6.1. Конфигурация ИБ

В подменю «Управление ИБ» → «Конфигурации ИБ» администратор может произвести настройки, относящиеся к информационной безопасности. (Рис. 6.1) Данные политики будут применены при смене пароля пользователем, у которого администратором Системы был установлен флаг «Требовать смену пароля».

Установить срок действия пароля в месяцах.

Установить сроки хранения журналов событий, после которых журналы будут удалены, а также блокировать авторизацию с одной учетной записи с разных ip-адресов.

Установить метрики качества секретов, удовлетворяющих необходимому уровню безопасности. При смене пароля пользователем Система будет проверять соответствие данных паролей заданным метрикам:

- наличие в пароле символов разного регистра;
- наличие в пароле и символов, и цифр;
- наличие в пароле имени учетной записи;
- проверка пароля на сложность.

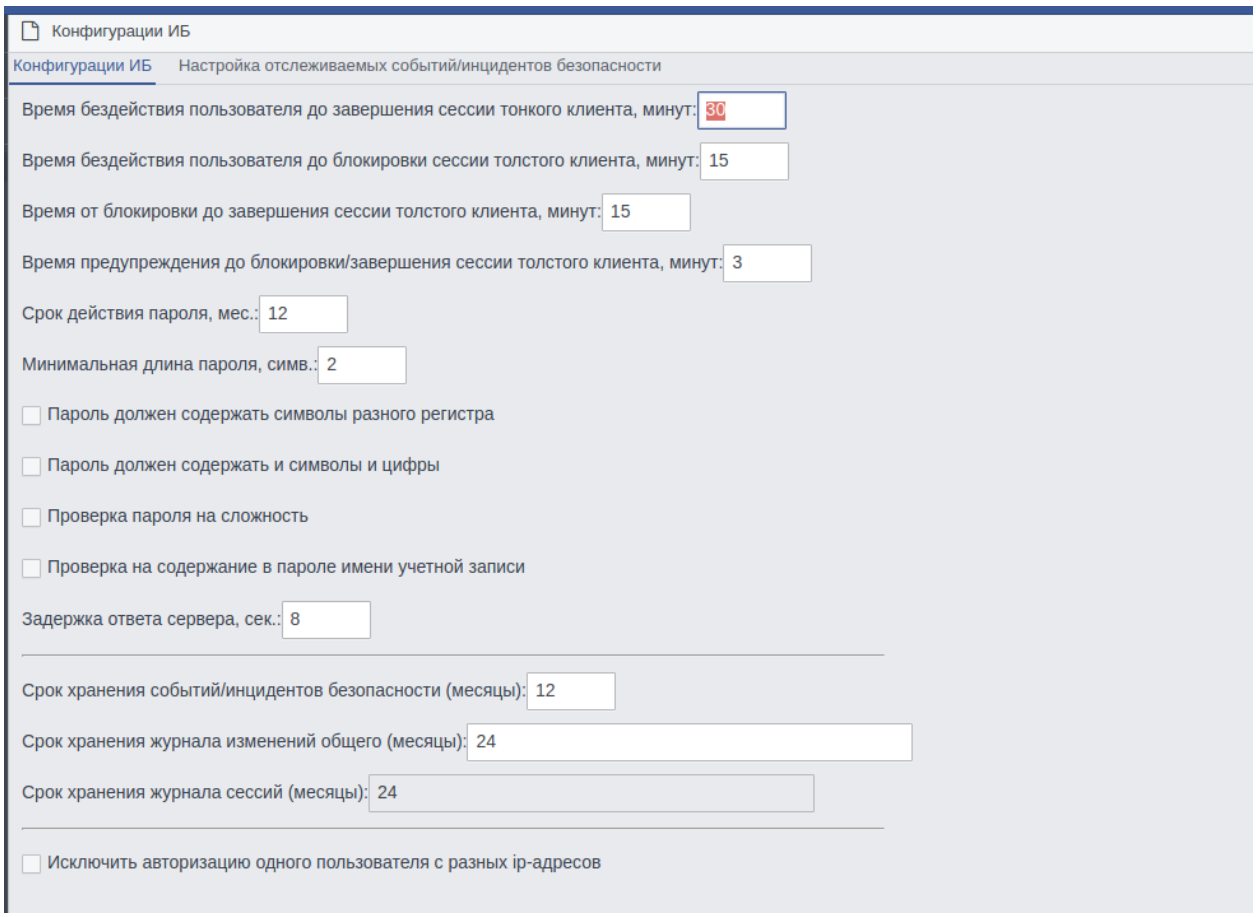


Рисунок 6.1 Конфигурации ИБ

Также в этом окне настраивается время, определяющее интервалы, через которые будет производится разрыв сессий и завершение работы Системы в случае бездействия пользователя.

Администратор может настроить метрики сложности пароля, используемые при назначении новых и смене уже действующих. Здесь можно изменить минимальную длину пароля и используемые символы.

При проверке в пароле имени учетной записи пользователя, происходит поиск логина пользователя в изменяемом пароле. При этом не важно, в каком месте пароля будет размещен логин пользователя и в каком регистре будут использованы буквы, важным будет только полное вхождение логина пользователя.

Для проверки пароля на сложность используется специальный словарь. Администратор заполняет это словарь наиболее распространенными паролями, которые могут быть использованы злоумышленниками для подбора аутентификационной информации пользователей. Для заполнения словаря можно использовать любые средства для работы с БД (например, утилиту ISQL входящую в комплект поставки СУБД «Ред База Данных»). Необходимо заполнить таблицу ss_password_dictionary БД ПК словами, которые могут быть использованы для перебора пароля. Для утилиты ISQL последовательность команд, следующая:

SQL> insert into ss_password_dictionary(id, suser_password) values (1, 'admin'); SQL> commit;

Далее, при смене пароля пользователем происходит проверка на полное и точное вхождение пароля в данный словарь. В случае если данный пароль не встречается в словаре, то Система дает разрешение на операцию по изменению пароля пользователя. Администратор Системы может включать/выключать данные метрики по своему усмотрению и комбинировать их любым способом, исходя из действующих в данный момент политик безопасности.

Во вкладке «Настройка отслеживаемых событий/инцидентов безопасности» администратор может изменить состав событий, отслеживаемых в журналах аудита:

- Вход пользователя в подсистему;
- Выход пользователя из подсистемы;
- Неиспользование УЗП последние два месяца.

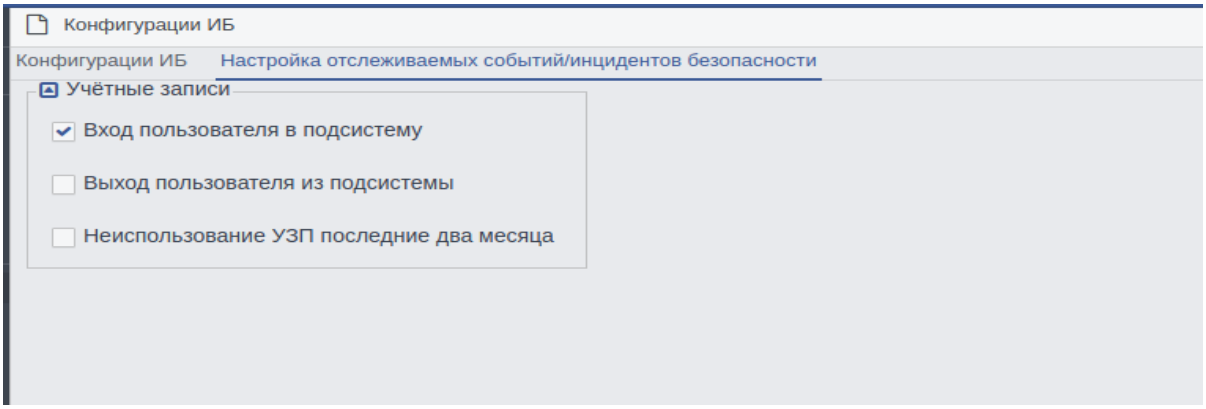


Рисунок 6.2 Настройка отслеживаемых событий

Изменение параметров формы «Конфигурации ИБ» также регистрируются в журнале и управляются задачей «Мониторинг событий информационной безопасности» в форме «Задачи планировщика», если отключить эту задачу данные события перестанут регистрироваться в журнале инцидентов (Рис 6.3).

[1 ↓] Наименование	Подсистема	Активна	Выражение Cron
Database Sweep	NCORE	☑	0 30 23 * * ?
Мониторинг событий информационной безопасности	NCORE	☑	0 0 5 * * ?
Очистка журналов и хранилища файловых вложений	NCORE	☑	00 30 06 * * ?
Поиск и отметка в журнале некорректно завершенных сессий	NCORE	☑	
Проверка свободного места на диске БД	NCORE	☑	
Расчет селективности индексов	NCORE	☑	00 00 00 ? * 7
Удаление временных файлов приема/передачи вложений	NCORE	☑	0 30 2 ? * SAT#2

Рисунок 6.3 Задача мониторинга событий ИБ

6.2. Журнал событий и инцидентов ИБ

Для просмотра записей событий ИБ необходимо перейти в Управление ИБ –> Журнал событий и инцидентов ИБ. В открывшемся списке отображаются записи произошедших событий и инцидентов ИБ, по котором ведется аудит. Есть возможность

сортировки и фильтрации по определенным событиям их статусам и даты возникновения события. (Рис. 6.4)

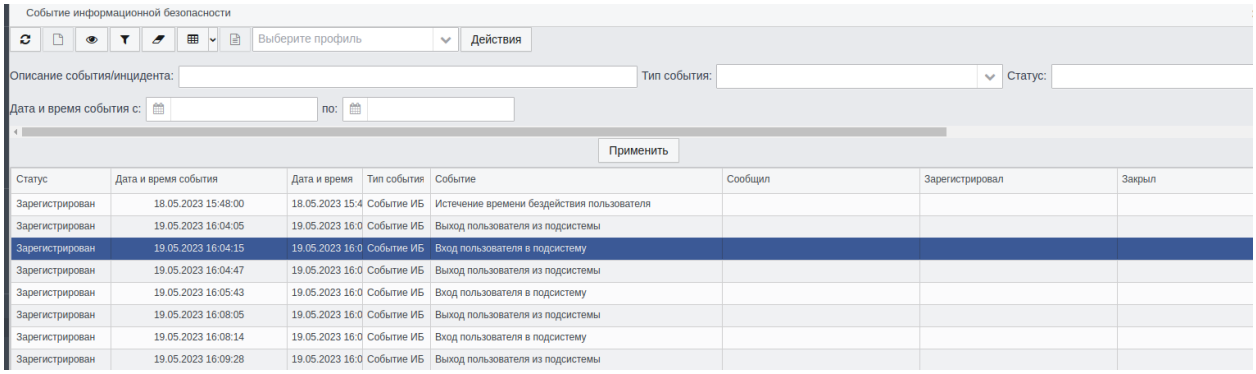


Рисунок 6.4 Журнал событий ИБ

При выборе конкретной записи двойным щелчком мыши, открывается подробная информация о событии, а также с возможностью обработать событие и изменить его статус (Рис. 6.5)

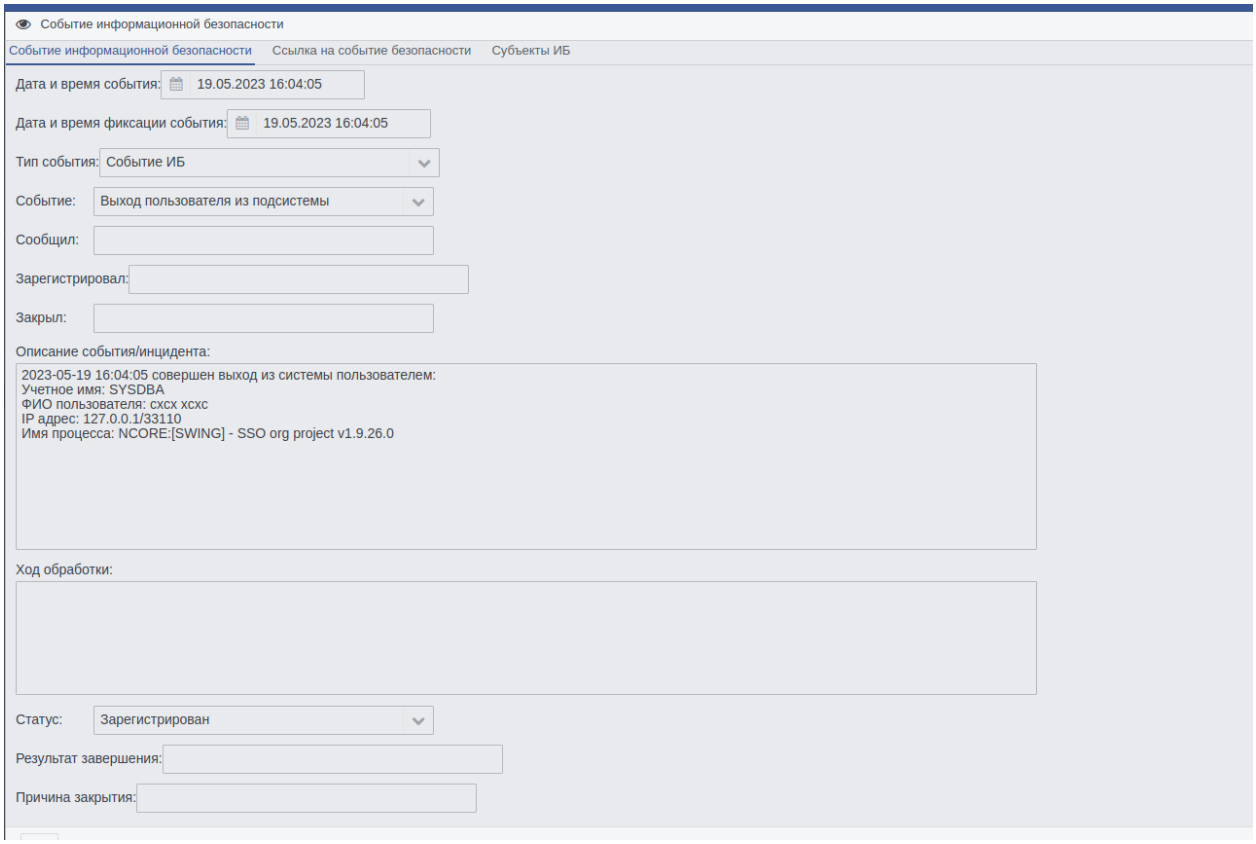


Рисунок 6.5 Карточка события ИБ

6.3. Журнал активных соединений

В меню Управление ИБ –> Активные соединения отображен список осуществленных соединений с базой данных с указанием от каких пользователей, процессов, ip-адресов осуществлено соединение. Дата и время подключения и последней активности. Некоторые соединения осуществлены от системных пользователей, например «Cash Writer» и «Garbage Collector» которые выполняют системные функции для нормальной работы Системы. (Рис. 6.6)

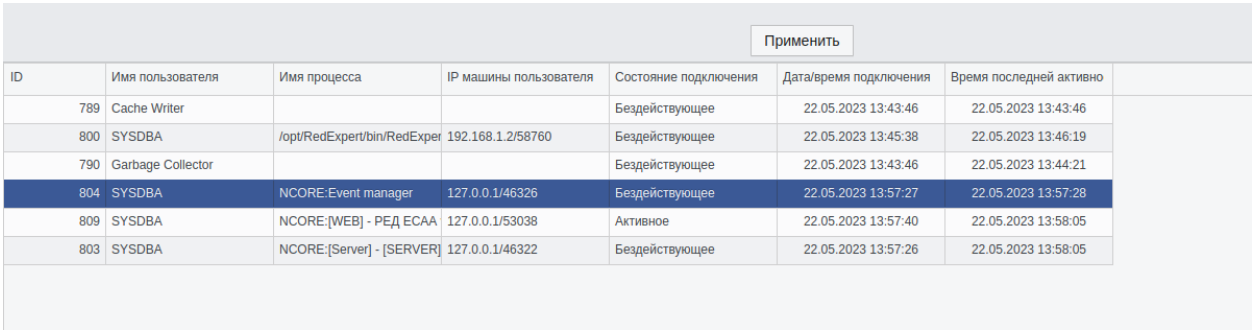


Рисунок 6.6 Активные соединения

Отображение столбцов и сортировка настраивается кликом правой кнопки мыши на наименование столбцов.

6.4. Журнал сессий

В меню Управление ИБ –> Журнал сессий отображаются все удачные аутентификации пользователей в Систему с указанием информации о подключившемся пользователе, времени и дате начала и окончания каждой сессии, активна ли в данный момент сессия (Рис. 6.7).

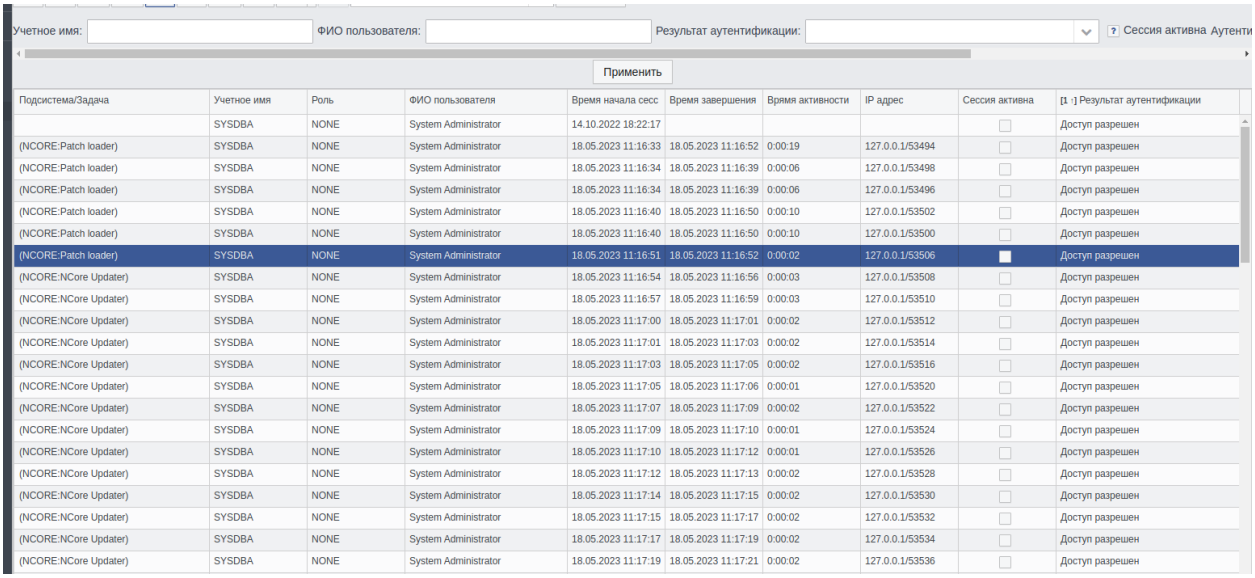


Рисунок 6.7 Журнал сессий

Отображение столбцов и сортировка настраивается кликом правой кнопки мыши на наименование столбцов. Фильтры поиска находятся в верхней части окна.

7. Подсистема «Администрирование»

7.1. Клиентские системы

Создание, управление и редактирование клиентскими системами осуществляется в меню Администрирование –> Клиентские системы. При переходе отображены созданные клиентские системы и информация о них (Рис 7.1). Отображение столбцов и сортировка настраивается кликом правой кнопки мыши на наименование столбцов. Фильтры поиска находятся в верхней части окна.

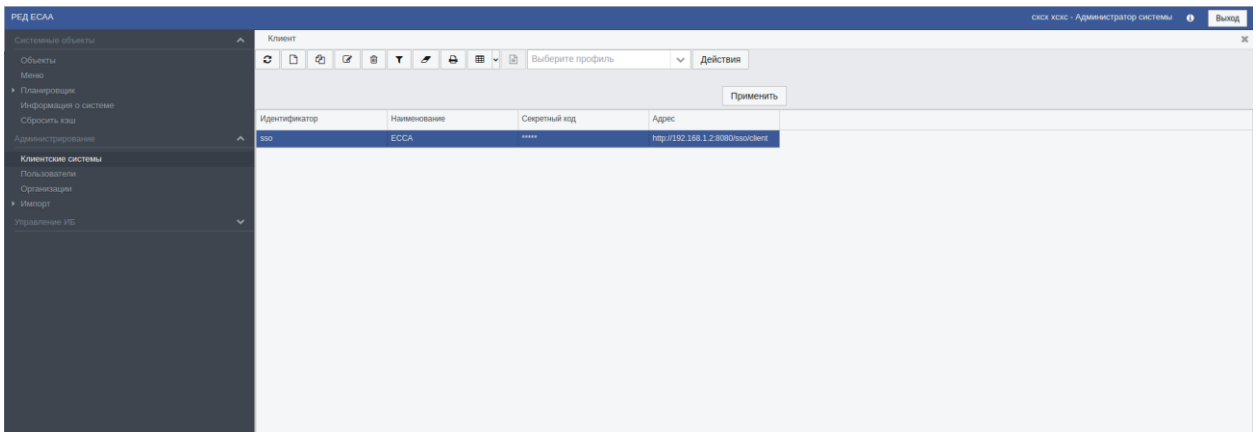


Рисунок 7.1 Форма клиентских систем

Так как сама Система должна быть зарегистрирована как клиентская система, по умолчанию она добавлена в список клиентских систем с секретным кодом – secret1, код для безопасной эксплуатации Системы необходимо сменить.

Для удаления или редактирования клиентской системы из списка необходимо выделить нужную систему и нажать кнопку «Удалить» или «Редактировать».

Для добавления новой клиентской системы необходимо нажать кнопку «Создать» после чего заполнить формы: клиент, организации, роли и пользователи.

В форме «Клиент» в поле «Идентификатор» необходимо придумать и ввести уникальный идентификатор, по которому будет отслеживаться добавляемая система-клиент.

В поле «Наименование» ввести название клиентской системы для более легкой идентификации ее в Системе.

В поле «Секретный код» вводится набор символов, который клиентская система будет использовать при получении доступа к РЕД ЕСАА. Секретный код является паролем для доступа к РЕД ЕСАА, он должен храниться в секрете, его утечка может привести к несанкционированному доступу к защищенным ресурсам.

В поле «Адрес» вводится URL-адрес клиентской системы, к которой необходим доступ пользователей. (пример – http://192.168.1.2:8080/sso/client) (Рис 7.2)

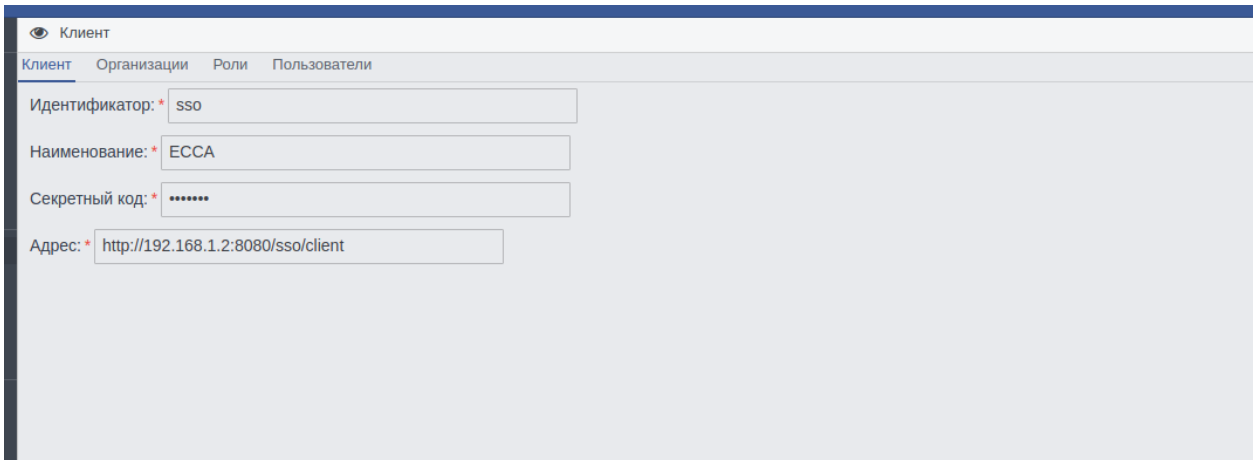


Рисунок 7.2. Форма клиент

В форме «Организации» по необходимости в случае наличия организаций в клиентской системе для их синхронизации необходимо воспроизвести структуру организаций, их наименования и коды идентичные клиентской системы (Рис 7.3).

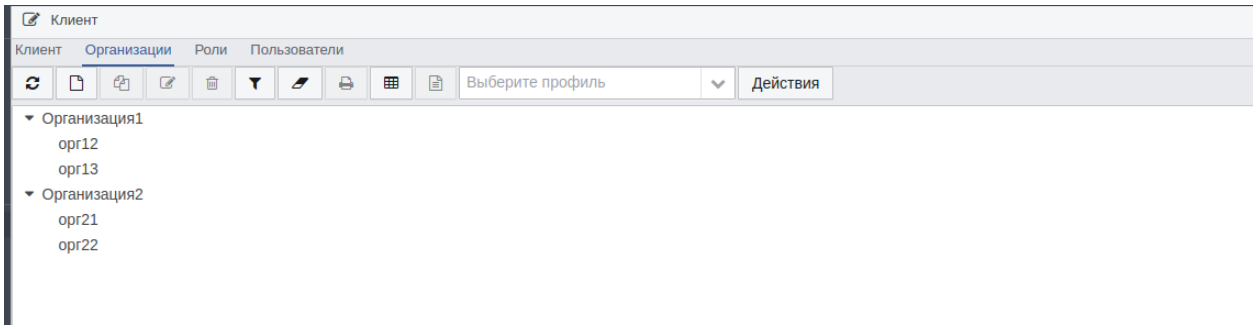


Рисунок 7.3 Структура организаций

Для добавления новой организации в структуру необходимо нажать кнопку «Создать». В случае необходимости создание родительской или дочерней организации необходимо выделить нужную организацию и после этого нажать кнопку «Создать» – будет создана дочерняя выделенной организации. Для создание корневой организации необходимо нажать кнопку «Создать» без выделения какой-либо организации.

После нажатия кнопки «Создать» необходимо ввести наименование организации и ее код соответствующие организации в клиентской системе (Рис 7.4).

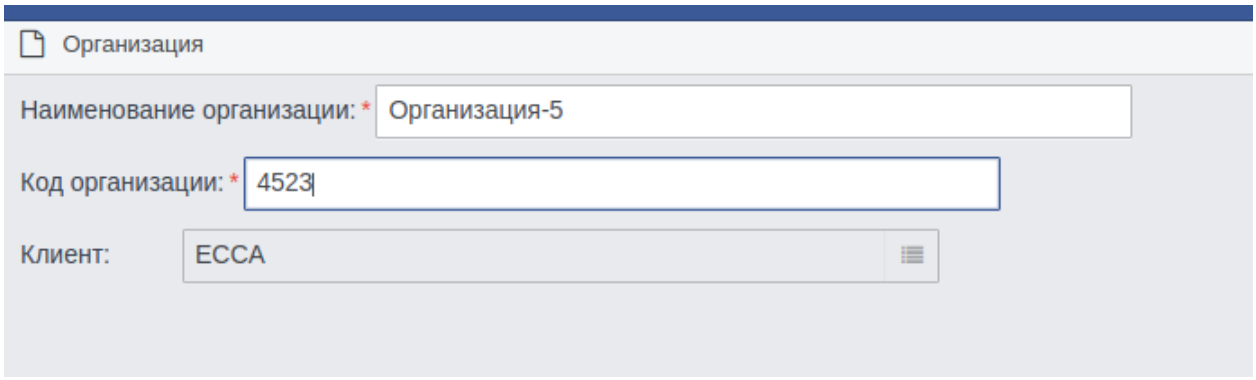


Рисунок 7.4 Создание организации

В форме «Роли» находится перечень уже добавленных ролей клиентской системы (Рис 7.5). В РЕД ЕСАА предусмотрены две роли «Системный администратор» и «Пользователь» более подробно о которых рассказано ниже.

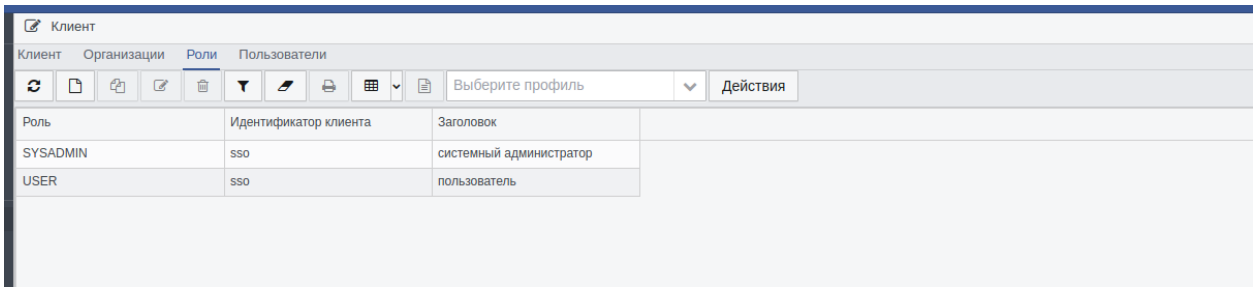


Рисунок 7.5 Перечень ролей клиентской системы

Для добавления роли необходимо нажать кнопку «Создать» и ввести в поле «Роль» наименование роли идентичное наименованию в клиентской системе. В поле «Заголовок» можно ввести любое удобное наименование для отображения (Рис 7.6).

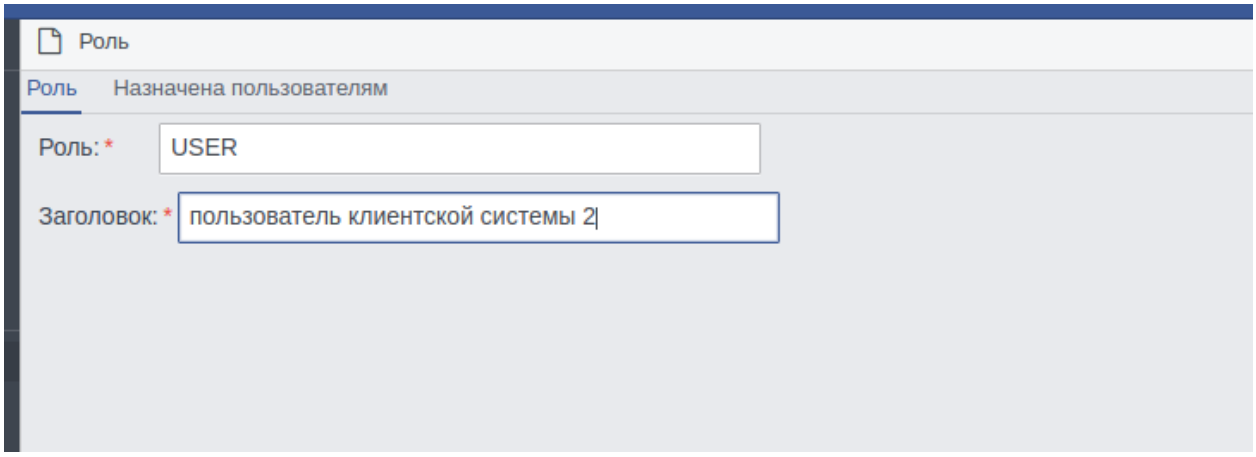


Рисунок 7.6 Форма создания роли клиентской системы

На вкладке «Назначена пользователям» можно посмотреть каким пользователям данная роль уже назначена.

На форме «Пользователи» отображается список уже добавленных пользователей в данную клиентскую систему (Рис 7.7)

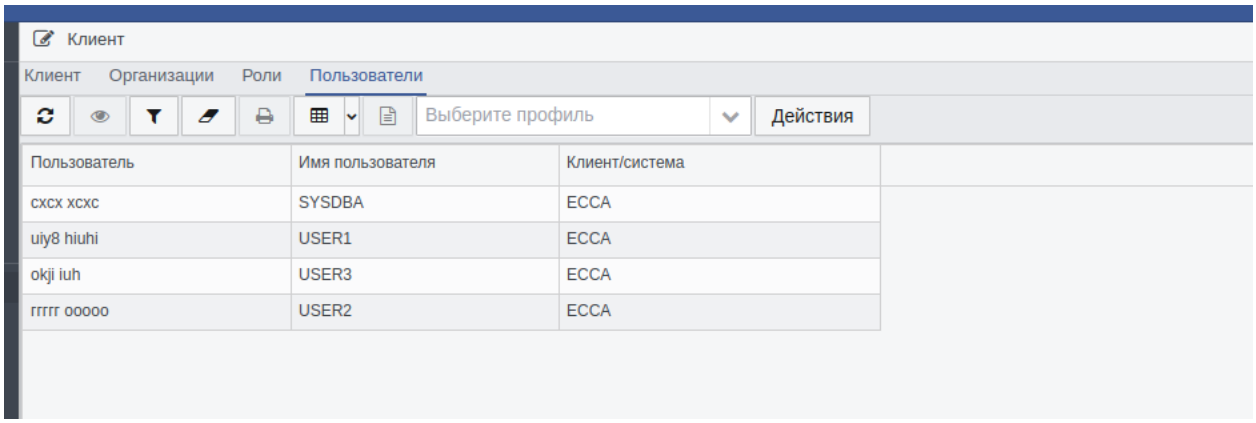


Рисунок 7.7 Форма пользователи клиентской системы

Для получения более подробной информации о пользователе необходимо открыть его двойным кликом левой кнопки мыши (Рис 7.8).

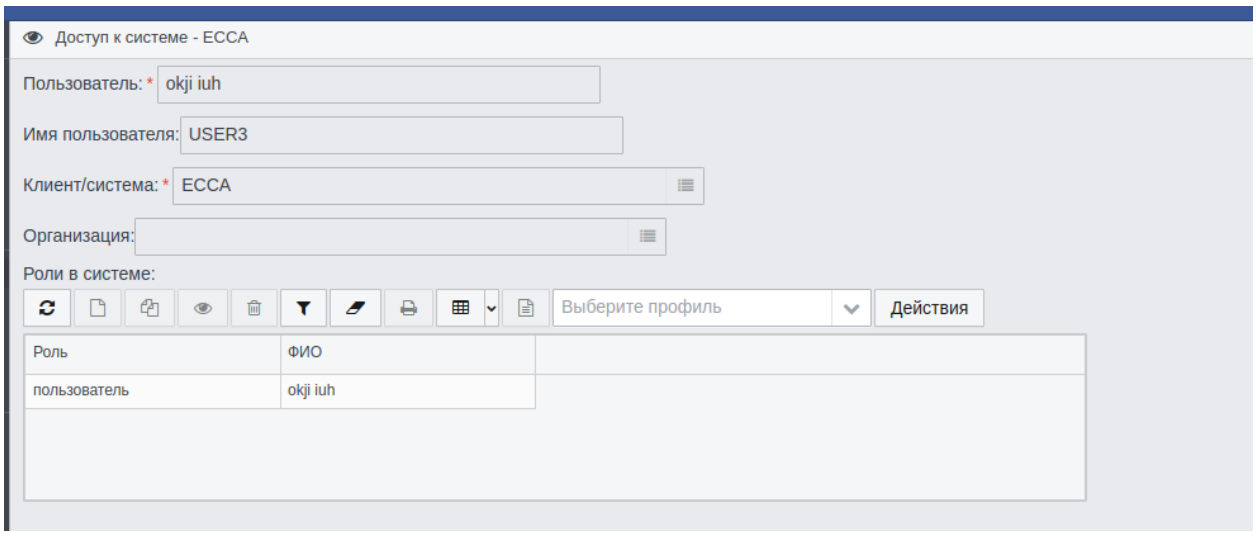


Рисунок 7.8 Дополнительная информация о пользователе

После завершения настроек клиентской системы необходимо нажать кнопку «Сохранить».

Далее необходимо в конфигурационный файл клиентской системы, чтобы авторизация осуществлялась через РЕД ЕСАА, добавить следующие параметры:

<entry key="biz.redsoft.ncore.security.openid.enabled">true</entry>
<entry key="biz.redsoft.ncore.security.oauth2.factories">biz.redsoft.ncore.esia.openid.OpenIdFactory</entry>
<entry key="biz.redsoft.ncore.security.openid.client_id">**sso**</entry> – **идентификатор зарегистрированной клиентской системы**
<entry key="biz.redsoft.ncore.security.openid.client_secret">**secret2**</entry> – **секретный код зарегистрированной клиентской системы**
<entry key="biz.redsoft.ncore.security.openid.scope">openid</entry>
<entry key="biz.redsoft.ncore.security.openid.authorization_server">**http://192.168.1.2:8080/sso/**openid</entry> – **URL-адрес сервера РЕД ЕСАА**
<entry key="biz.redsoft.ncore.security.openid.authorization_path">/auth</entry>
<entry key="biz.redsoft.ncore.security.openid.access_token_path">/token</entry>
<entry key="biz.redsoft.ncore.security.openid.end_session_path">/logout</entry>
<entry key="biz.redsoft.ncore.security.openid.userinfo_path">/v1/userinfo</entry>
<entry key="biz.redsoft.ncore.security.openid.redirect_url">**http://192.168.1.3/system2**</entry> – **URL-адрес системы клиента**
<entry key="biz.redsoft.ncore.security.openid.user_resolver">biz.redsoft.shg.application.oauth2.openid.ShgIdTokenLoginUserResolver</entry>
<entry key="biz.redsoft.ncore.security.openid.allow_new_user_creation">yes</entry>
<entry key="biz.redsoft.ncore.security.openid.trusted_db_auth">yes</entry>
<entry key="biz.redsoft.ncore.security.openid.reuse_existing_user">yes</entry>
<entry key="sso.update.user">true</entry>
<entry key="sso.delete.sys_user_role">true</entry>

7.2. Пользователи

Создание, управление и редактирование пользователей всех клиентских систем осуществляется в меню Администрирование –> Пользователи. При переходе отображены зарегистрированные пользователи и информация о них (Рис 7.9). Отображение столбцов и сортировка настраивается кликом правой кнопки мыши на наименование столбцов. Фильтры поиска находятся в верхней части окна.

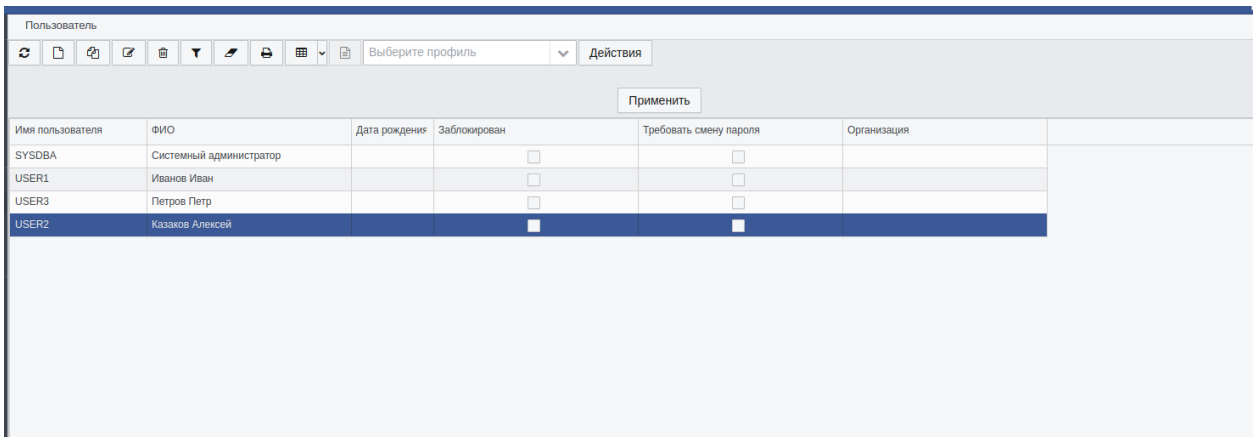


Рисунок 7.9 Список зарегистрированных пользователей

По умолчанию в РЕД ЕСАА зарегистрирован пользователь с ролью системного администратора «SYSDBA» в клиентской системе РЕД ЕСАА.

Для удаления или редактирования пользователей из списка необходимо выделить нужного пользователя и нажать кнопку «Удалить» или «Редактировать».

Для регистрации нового пользователя необходимо нажать кнопку «Создать» после чего заполнить формы «пользователь» и «доступные системы».

В форме «Пользователь» в поле «Имя пользователя» указывается имя пользователя идентичное уже существующему в клиентской системе – в этом случае информация об этом пользователе в клиентской системе будет обновлена или указывается имя нового пользователя, который при первой попытке авторизации будет создан в клиентской системе. Заполняются прочие поля. Флаг «Заблокирован» означает, что пользователь не сможет авторизоваться в клиентской системе, флаг «Требовать смену пароля» означает, что при следующей авторизации пользователя, ему будет необходимо ввести старый пароль, а после придумать новый пароль, который должен соответствовать текущим политикам пароля, указанным в «Конфигурации ИБ». (Рис 7.10)

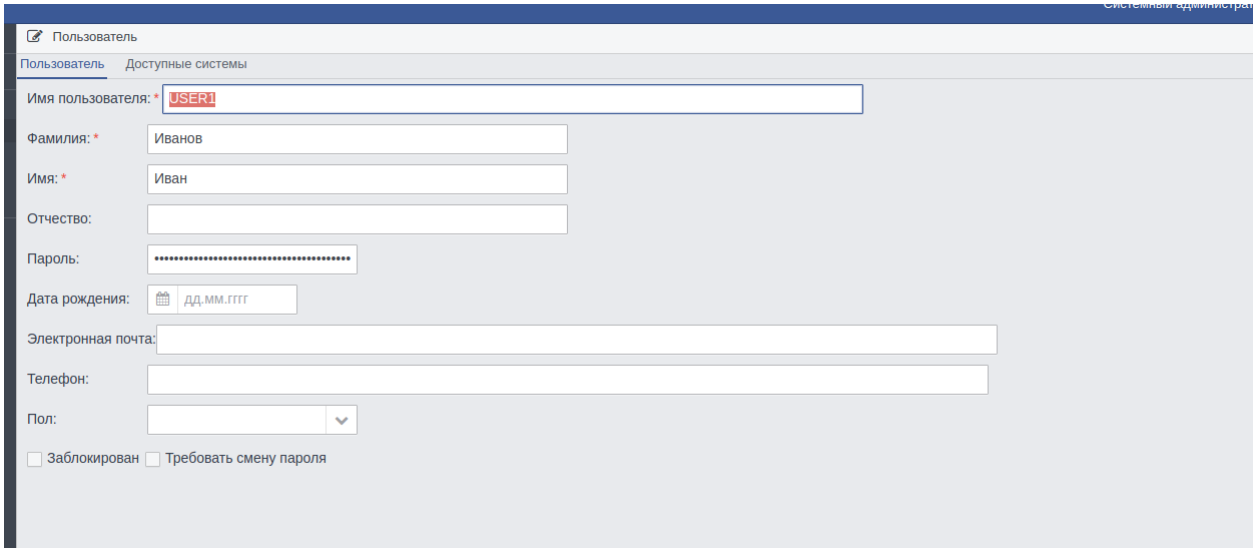


Рисунок 7.10 Форма «Пользователь»

В форме «Доступные системы» отображается список клиентских систем, к которым пользователь уже имеет доступ (Рис. 7.11).

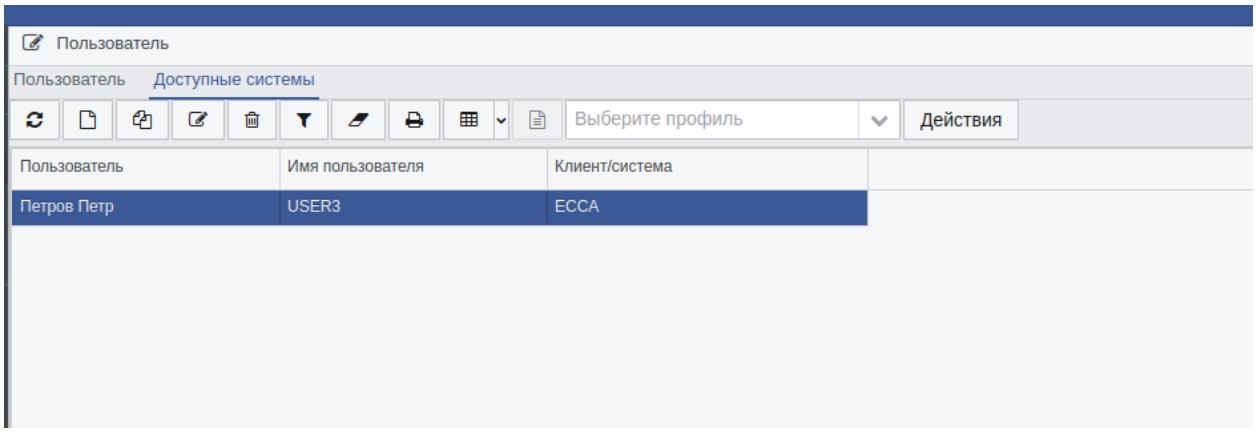


Рисунок 7.11 Доступные пользователю клиентские системы

При выборе нужной клиентской системе и двойном щелчке левой кнопкой мыши открывается форма дополнительной информации с отображением присвоенных ролей и организации пользователя в выбранной клиентской системе. (Рис 7.12)

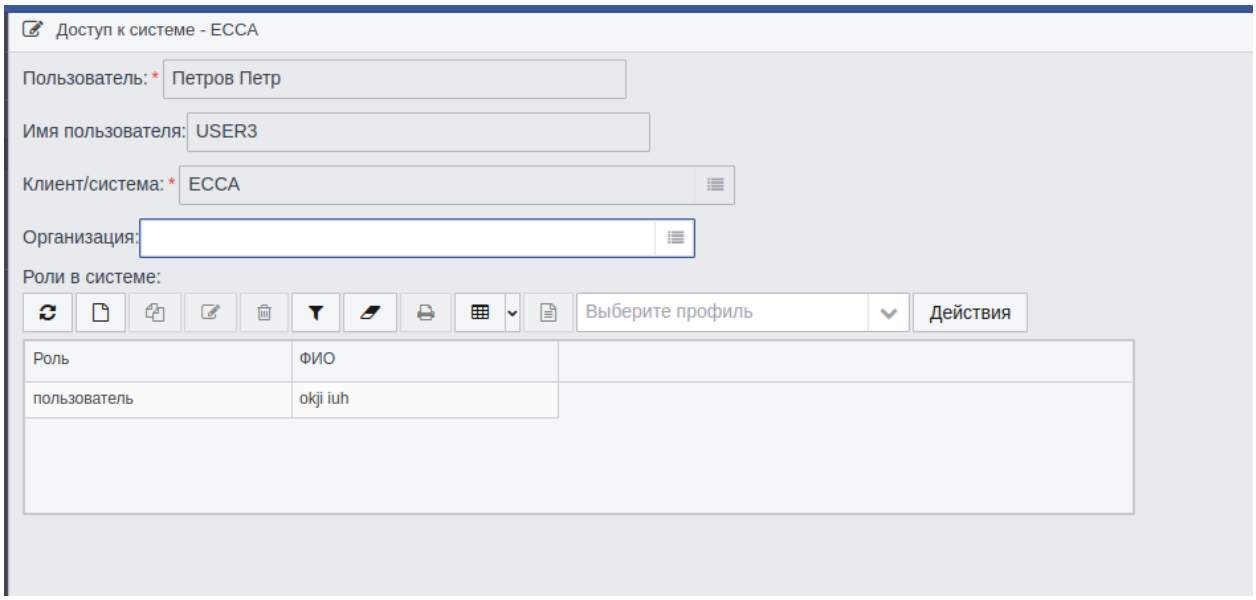


Рисунок 7.12 Подробная информация о доступе пользователя к клиентской системе

Для регистрации пользователя в новой клиентской системе необходимо из формы «Доступные системы» нажать кнопку «Создать», выбрать из зарегистрированных клиентских систем необходимую, добавить из списка по необходимости организацию в которой находится пользователь (Рис 7.13)

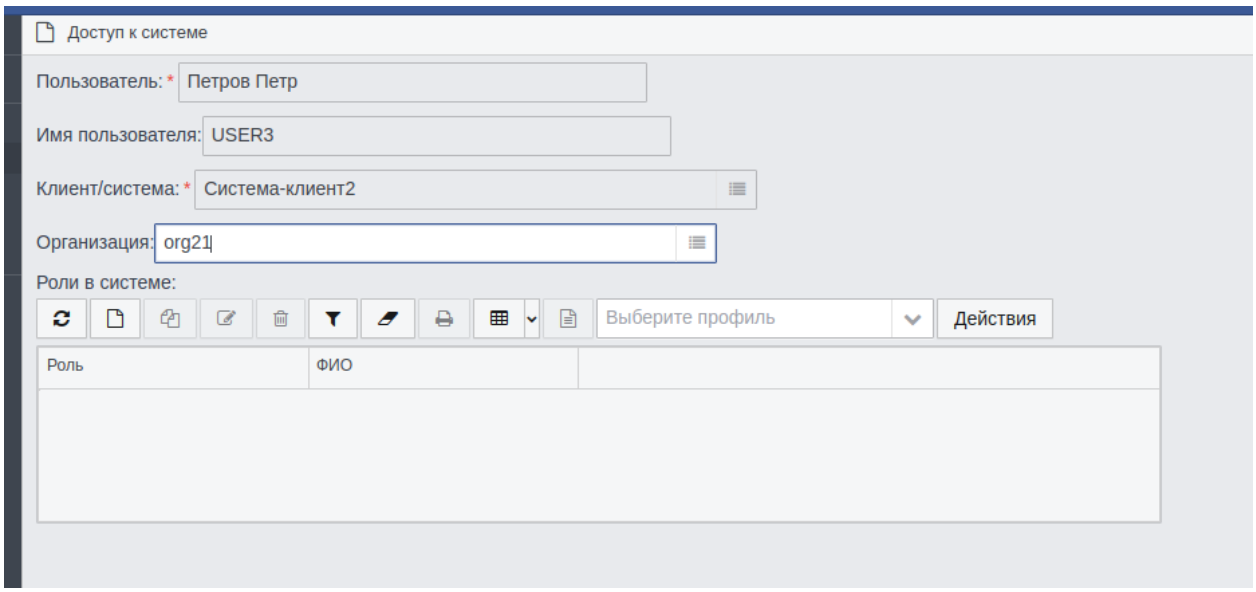


Рисунок 7.13 Регистрация пользователя в клиентской системе

Для добавления роли необходимо на форме «Доступ к системе» нажать кнопку «Создать» и выбрать или из уже имеющихся ролей или создать роль с названием идентичным в клиентской системе. (Рис 7.14)

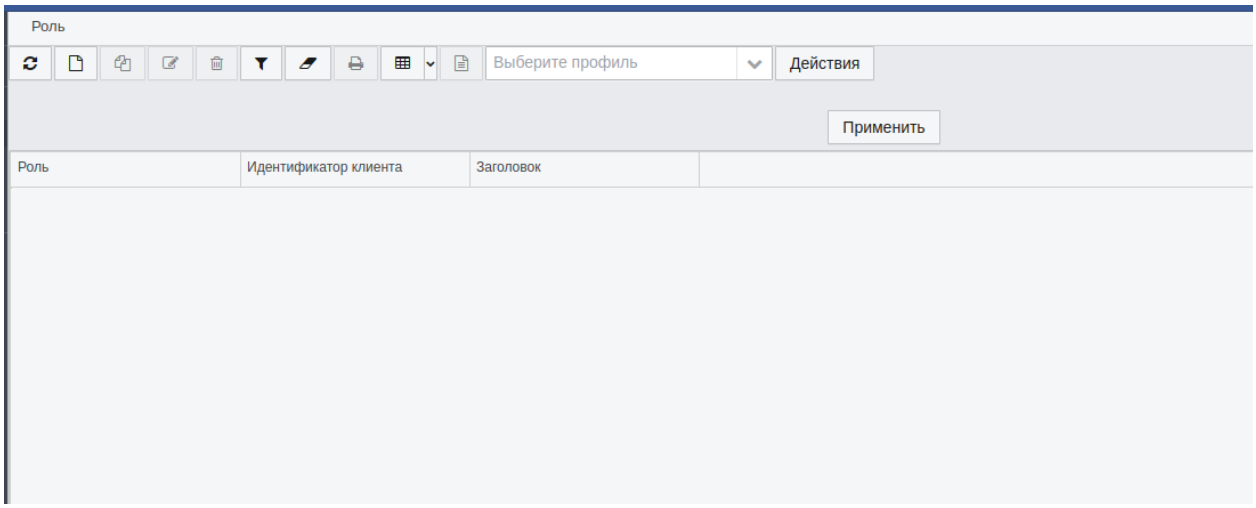


Рисунок 7.14 Добавление ролей пользователю

По окончанию настройки пользователя нажать кнопку «Сохранить».

7.3. Организации

Создание, управление и редактирование организаций всех клиентских систем осуществляется в меню Администрирование –> Организации. При переходе отображены созданные организации. Дочерние организации раскрываются нажатием стрелки слева от названия организации (Рис 7.15). Фильтры по наименованию организации и клиентской системе, в которой находятся организации находятся в верхней части окна.

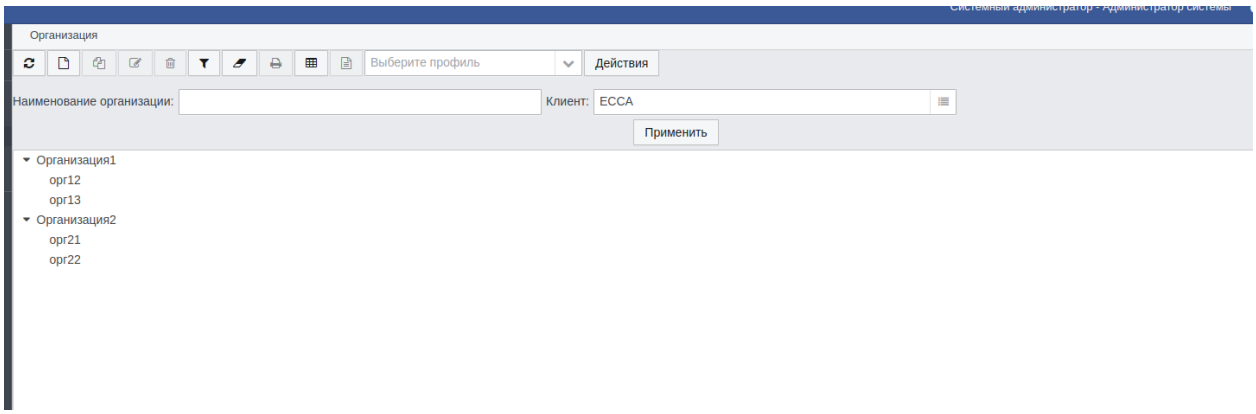


Рисунок 7.15 Список организаций для клиентской системы ECAA

Для осуществления верной привязки пользователей и организаций клиентской системы и РЕД ECAA, структура, названия и код организаций должны быть идентичны клиентской системы.

Для создания новой организации необходимо нажать кнопку «Создать». В появившейся форме «Организация» необходимо заполнить поля «Наименование организации» и «Код организации», а также выбрать из списка для какой клиентской системы будет создана организация и нажать кнопку «Сохранить» (Рис 7.16)

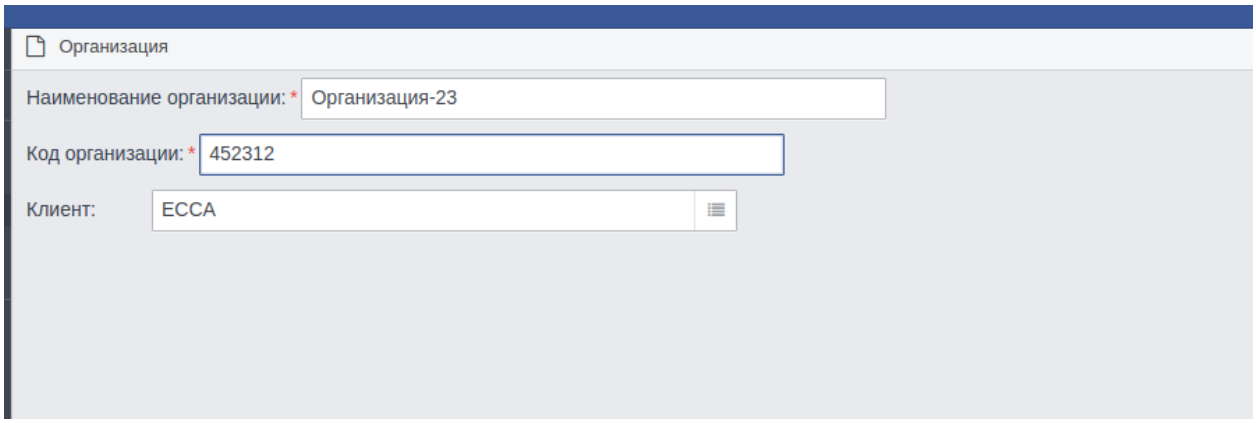


Рисунок 7.16 Создание организации

7.4. Роли пользователей

В Системе предустановлены две роли: Системного администратора – SYS_ADMIN и пользователя – USER.

Роль SYS_ADMIN имеет полный доступ ко всему функционалу Системы и служит для настройки и администрирования Системы, управления учетными записями и клиентскими системами.

Роль USER необходима пользователям клиентских систем, которые авторизуются с помощью РЕД ECAA. Данная роль не имеет доступа к пунктам меню Система.

В случае назначения одной учетной записи пользователя нескольких ролей, будет предоставлен доступ к объектам системы в соответствии с ролью, которая имеет наивысший приоритет.

8. Сообщения оператору

8.1. Система зависла и не отвечает на действия пользователя

В случае если был введен неверный пароль или происходит смена пароля – в связи с настройками безопасности система не будет отвечать на действия пользователя одну-две минуты. Если действия пользователя не были связаны с вводом или сменой пароля и во время работы система перестала реагировать на действия пользователя, появился красный индикатор работы системы (Рисунок 5.1.1) и ситуация не меняется в течении нескольких минут, закройте вкладку браузера и заново запустите систему в браузере по адресу системы.

Рисунок 5.1.1 - Индикатор работы системы

Если это не помогло – обратитесь в службу технической поддержки.

8.2. Ошибка соединения

При проблемах с сетевым соединением или проблемах на сервере возможно возникновение «Ошибки соединения» (Рисунок 5.2.2). Закройте вкладку браузера и через несколько минут попробуйте зайти в систему снова в браузере по адресу системы.

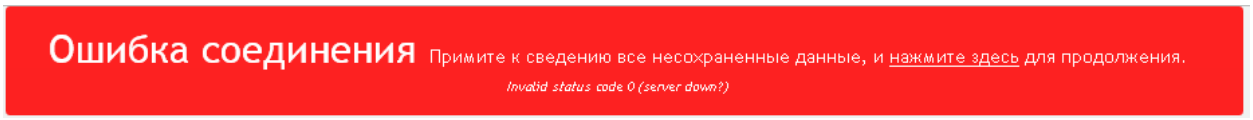


Рисунок 5.2.2 - Ошибка соединения

Если это не помогло – обратитесь в службу технической поддержки.

8.3. Сессия истекла

Если пользователь не использовал систему в течении 15 минут, в целях обеспечения безопасности его сессия прерывается (5.3.1). Для продолжения работы нажмите на ссылку «Нажмите здесь» и заново введите логин и пароль.

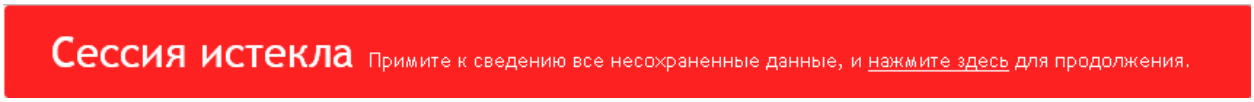


Рисунок 5.3.1 - Сессия истекла

8.4. Не заполнены обязательные поля

Если при создании запроса или ответа в нем не заполнены обязательные поля, при попытке сохранить карточку пользователя или системы-клиента появится предупреждающее сообщение с указанием полей, которые необходимо заполнить (Рисунок 5.4.1).

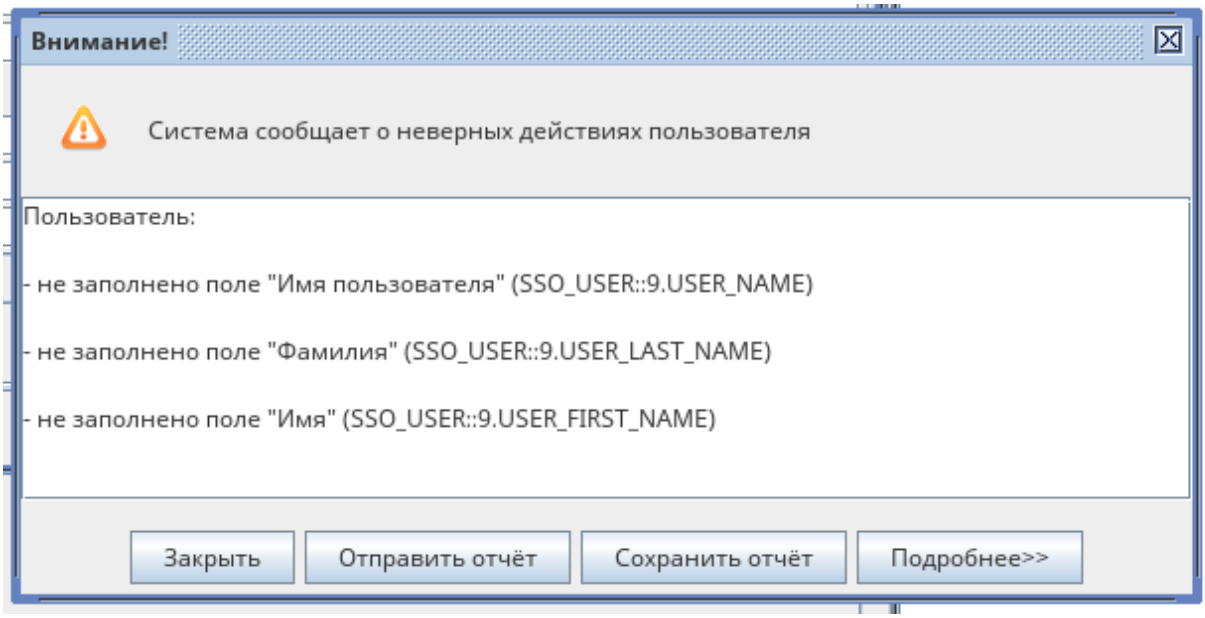


Рисунок 5.4.1 - Не заполнены обязательные поля

8.5. Системная ошибка

При работе системы крайне редко возможно возникновение системных ошибок (Рисунок5.5.1). При возникновении системной ошибки нажмите на кнопку «Подробнее» (Рисунок5.5.2), сохраните описание и передайте его в службу технической поддержки. Попробуйте продолжить дальнейшую работу, если система зависла и не отвечает, закройте вкладку браузера и заново запустите систему в браузере по адресу системы.

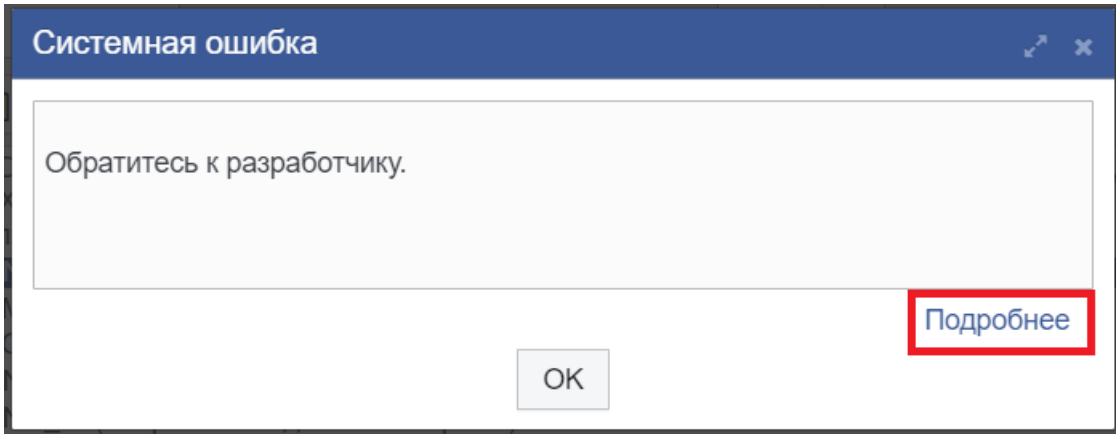


Рисунок5.5.1 - Системная ошибка

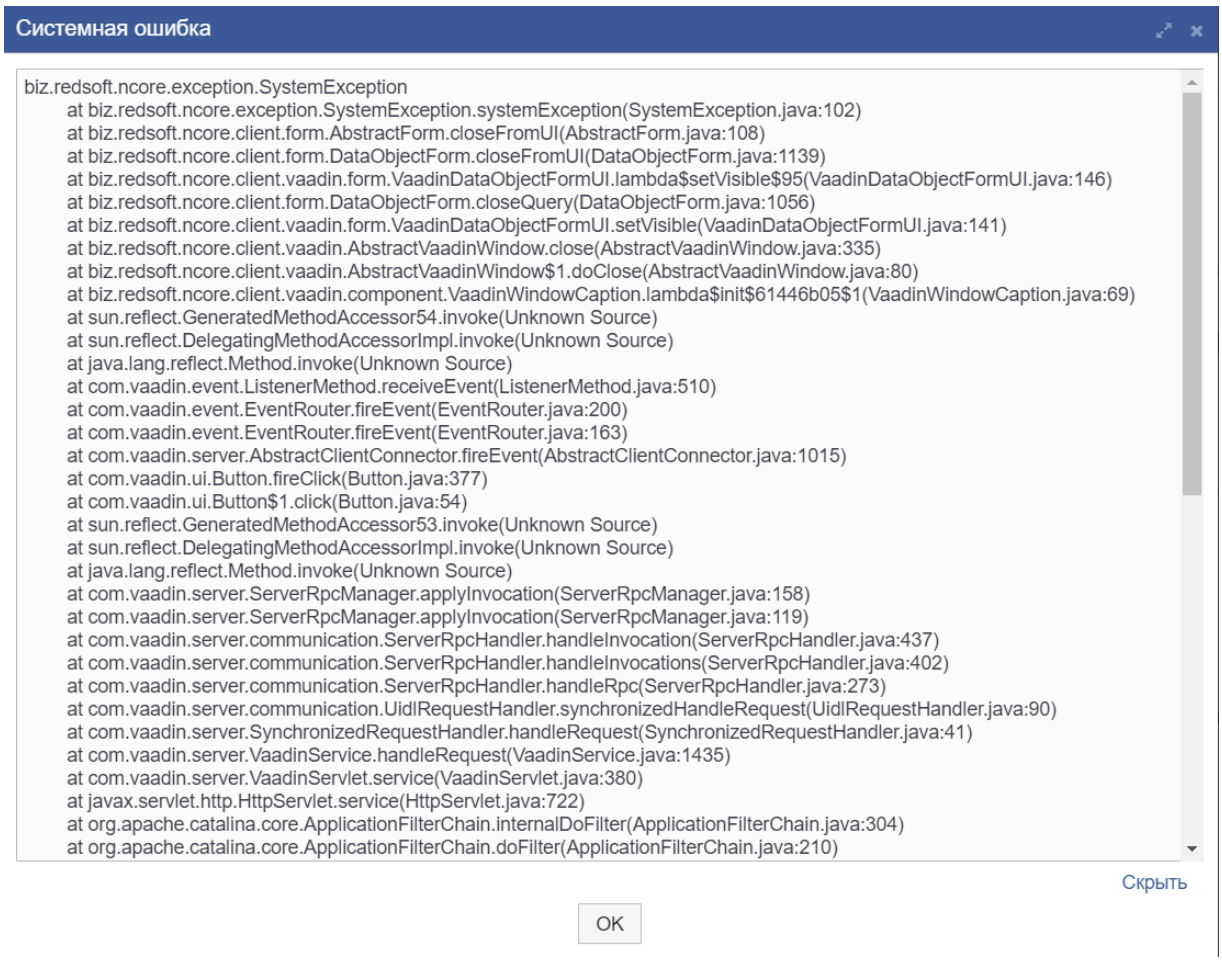


Рисунок5.5.2 - Подробное описание системной ошибки