ЕДИНАЯ ЦИФРОВАЯ ПЛАТФОРМА.МИС 3.0

(ЕЦП.МИС 3.0)

Руководство пользователя. Подсистема "Администрирование" 3.0.5_3.

Модуль "Журнал разрешений" 3.0.5

Содержание

1 Введение 4

1.1 Область применения 4

1.2 Уровень подготовки пользователя 4

1.3 Перечень эксплуатационной документации, с которым необходимо ознакомиться пользователю 4

2 Назначение и условия применения 5

2.1 Виды деятельности, функции, для автоматизации которых предназначено данное средство автоматизации 5

2.2 Условия, при соблюдении которых обеспечивается применение средства автоматизации 5

3 Подготовка к работе 6

3.1 Порядок запуска Системы 6

3.2 Смена пароля 10

3.3 Контроль срока действия пароля 11

3.4 Порядок проверки работоспособности 11

4 Модуль "Журнал разрешений" 3.0.5 12

4.1 Общие сведения 13

4.2 Доступ к форме 13

4.3 Описание формы 14

4.3.1 Панель фильтров 14

4.3.2 Список разрешений 14

4.3.3 Раздел с детальной информацией по разрешению 15

4.3.4 Кнопки управления списком разрешений 15

4.3.5 Кнопки управления формой 16

4.4 Работа с формой 16

4.4.1 Добавление разрешения 16

4.4.2 Удаление разрешения 16

4.5 Правила при работе с разрешениями 17

5 Аварийные ситуации 19

5.1 Описание аварийных ситуаций 19
5.2 Действия в случае несоблюдения условий выполнения технологического процесса ..20
6 Эксплуатация модуля 22

1 Введение

1.1 Область применения

Настоящий документ описывает порядок работы с модулем "Журнал разрешений" 3.0.5 Единой цифровой платформы МИС 3.0 (далее – "ЕЦП.МИС 3.0", Система).

1.2 Уровень подготовки пользователя

Пользователи Системы должны обладать квалификацией, обеспечивающей, как минимум:

- базовые навыки работы на персональном компьютере с графическим пользовательским интерфейсом (клавиатура, мышь, управление окнами и приложениями, файловая Система);
- базовые навыки использования стандартной клиентской программы (браузера) в среде Интернета (настройка типовых конфигураций, установка подключений, доступ к веб-сайтам, навигация, формы и другие типовые интерактивные элементы);
- базовые навыки использования стандартной почтовой программы (настройка учетной записи для подключения к существующему почтовому ящику, создание, отправка и получение e-mail).

1.3 Перечень эксплуатационной документации, с которым необходимо ознакомиться пользователю

Перед началом работы пользователям рекомендуется ознакомиться с положениями данного руководства пользователя в части своих функциональных обязанностей.

2 Назначение и условия применения

2.1 Виды деятельности, функции, для автоматизации которых предназначено данное средство автоматизации

Модуль "Журнал разрешений" 3.0.5 предназначен для подписания документов от имени МО без участия пользователя.

2.2 Условия, при соблюдении которых обеспечивается применение средства автоматизации

Доступ к функциональным возможностям и данным Системы реализуется посредством веб-интерфейса. Работа пользователей Системы осуществляется на единой базе данных центра обработки данных (далее – ЦОД). Система доступна из любой организации (участника информационного обмена) при наличии канала связи в круглосуточном режиме.

Работа в Системе выполняется через автоматизированные рабочие места (далее – АРМ) персонала (в соответствии с местом работы, уровнем прав доступа к функциональным возможностям и данным Системы).

Настройка рабочего места (создание, настройка параметров работы в рамках медицинской организации (далее – МО), предоставление учетной записи пользователя) выполняется пользователем АРМ администратора МО. Настройка общесистемных параметров работы, конфигурация справочников выполняется пользователем АРМ администратора ЦОД.

Описание работы администраторов приведено в документе "Руководство администратора Системы".

3 Подготовка к работе

3.1 Порядок запуска Системы

Для входа в Систему необходимо выполнить следующие действия:

- запустите браузер, например, "Пуск" – "Все приложения" – "Firefox". Отобразится окно браузера и домашняя страница (рисунок 1).

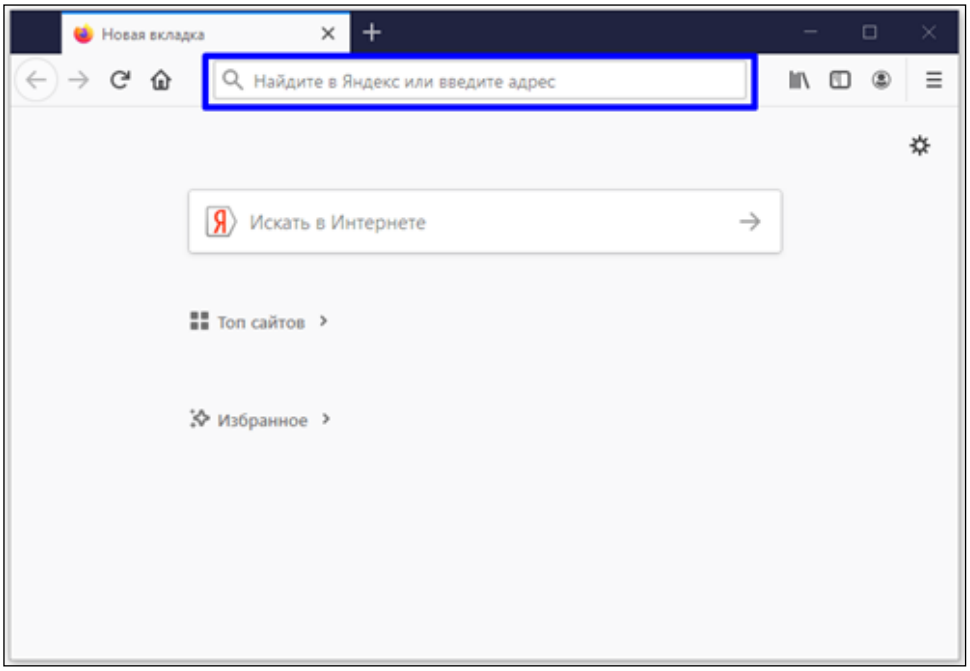


Рисунок 1 – Окно браузера и домашняя страница

- введите в адресной строке браузера IP-адрес страницы портала, нажмите клавишу "Enter". На главной странице Системы отобразится перечень программных продуктов.

Примечание – Адрес для подключения предоставляется администратором. Если страница Системы установлена в качестве домашней страницы, то она отобразится сразу после запуска браузера.

Для удобства использования рекомендуется добавить адрес Системы в закладки браузера, и/или сделать страницу Системы стартовой страницей.

Стартовое окно Системы представлено на рисунке 2.

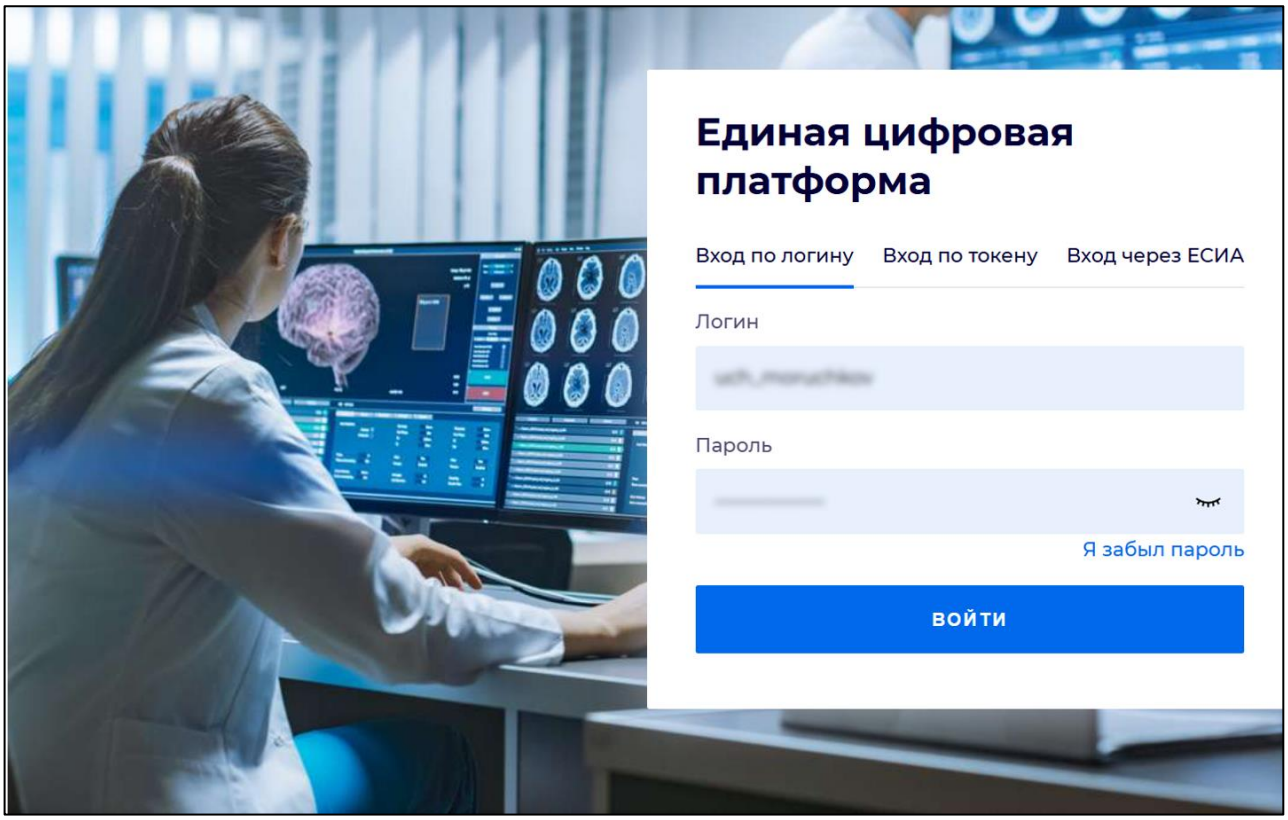


Рисунок 2 – Стартовое окно Системы

Вход в Систему возможен одним из способов:

- по логину;
- по токену;
- через ЕСИА.

Способ №1:

- выберите регион в поле "Регион";
- введите логин учетной записи в поле "Логин";
- введите пароль учетной записи в поле "Пароль";
- нажмите кнопку "Войти".

Способ №2:

- перейдите на вкладку "Вход по токену". Отобразится окно входа в систему по токену (рисунок 3);

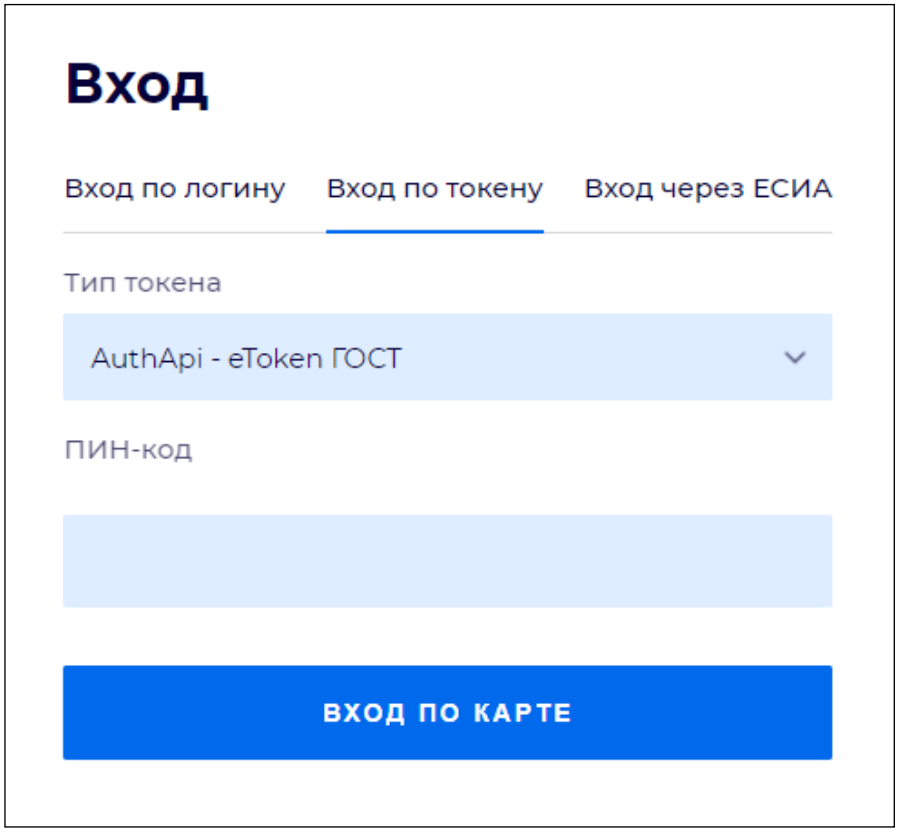


Рисунок 3 – Окно входа в систему по токену

- выберите тип токена;
- введите пароль от электронной подписи (далее – ЭП) в поле "ПИН-код"/"Сертификат" (расположенное ниже поля "Тип токена"). Наименование поля зависит от выбранного типа токена;
- нажмите кнопку "Вход по карте".

Примечания

1 На компьютере пользователя предварительно должно быть установлено и запущено программное обеспечение для выбранного типа токена.

2 Предварительно может потребоваться установить сертификаты пользователей администратором системы в программном обеспечении выбранного типа токена.

При неправильном вводе имени пользователя и (или) пароля отобразится соответствующее сообщение. В этом случае необходимо повторить ввод имени пользователя и (или) пароля.

Способ №3:

- перейдите на вкладку "Вход через ЕСИА". Будет выполнен переход на страницу авторизации через ЕСИА.
- введите данные для входа, нажмите кнопку "Войти".

Примечания

1 Для авторизации с помощью токена на компьютере пользователя предварительно должно быть установлено и запущено программное обеспечение для выбранного типа токена. Может потребоваться установка сертификатов пользователей администратором системы в программном обеспечении выбранного типа токена.

2 Для авторизации через ЕСИА учетная запись пользователя должна быть связана с учетной записью человека в ЕСИА. Учетная запись пользователя должна быть включена в группу "Авторизация через ЕСИА".

При неправильном вводе имени пользователя и (или) пароля отобразится соответствующее сообщение. В этом случае необходимо повторить ввод имени пользователя и (или) пароля;

- отобразится форма выбора МО. Вид формы выбора МО представлен на рисунке 4;

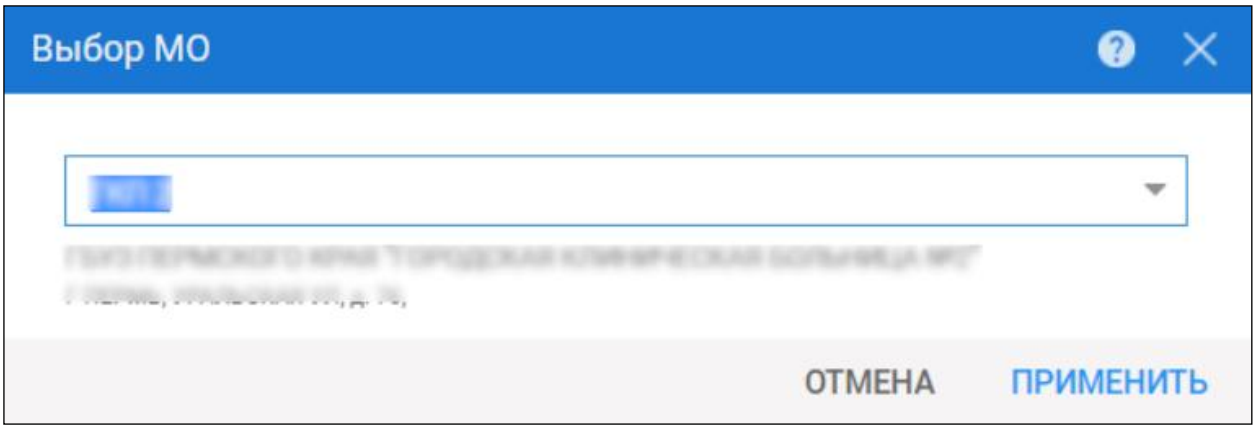


Рисунок 4 – Форма выбора МО

- укажите необходимую МО и нажмите кнопку "Применить";
- отобразится форма выбора АРМ по умолчанию. Вид формы выбора АРМ по умолчанию представлен на рисунке 5;

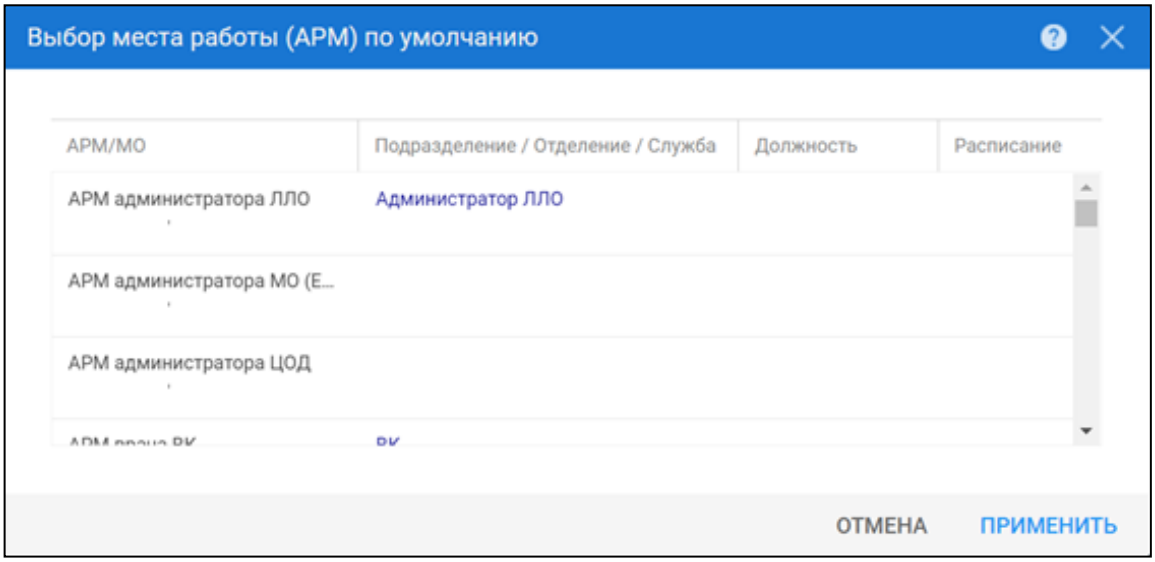


Рисунок 5 – Форма выбора АРМ по умолчанию

Примечание – Форма отображается, если ранее не было выбрано место работы по умолчанию, или при входе была изменена МО. После выбора места работы указанный АРМ будет загружаться автоматически после авторизации.

- выберите место работы в списке, нажмите кнопку "Применить". Отобразится форма указанного АРМ пользователя.

3.2 Смена пароля

При регистрации учетной записи администратор присваивает ей временный пароль. При первом входе в Систему пользователь должен сменить временный пароль, выданный администратором.

После ввода имени пользователя, пароля и нажатия кнопки "Войти в систему" выполняется проверка актуальности пароля, как временного, так и постоянного.

Если истек срок действия временного пароля (срок действия пароля определяется настройками в параметрах системы, то отобразится сообщение пользователю: "Истек срок действия временного пароля. Обратитесь к Администратору системы". Далее процесс аутентификации не производится.

Если временный пароль прошел проверку на актуальность, на форме отображаются поля для смены пароля. Рядом с полями отобразится подсказка с требованиями к паролю (указывается минимальная длина и допустимые символы).

При смене временного пароля на постоянный (при первом входе в систему) выполняется проверка на соответствие пароля установленным требованиям безопасности (минимальная длина, пользовательский пароль должен отличаться от временного на указанное количество символов и т.д.).

Вход в Систему возможен, если введен актуальный временный пароль, новый пароль соответствует всем требованиям (требования к паролю указаны в параметрах системы), значения полей "Новый пароль" и "Новый пароль еще раз" идентичны. В процессе ввода нового пароля рядом с полем должна отобразиться зеленая галочка, если введенный пароль удовлетворяет всем требованиям. В процессе подтверждения нового пароля рядом с полем "Новый пароль еще раз" отобразится зеленая галочка, если значения полей "Новый пароль" и "Новый пароль еще раз" идентичны.

При входе в систему происходит сохранение нового пароля.

3.3 Контроль срока действия пароля

При каждом входе в систему выполняется проверка срока действия пароля. Срок действия пароля определяется настройками системы (рассчитывается от даты создания пароля).

За несколько дней до истечения срока действия пароля при входе в систему выводится информационное сообщение "До истечения срока действия пароля осталось %кол-во дней% дней. Пароль можно сменить в личном кабинете".

При входе в систему в последний день актуальности пароля, на форме авторизации отобразятся поля для смены пароля.

Вход в систему возможен, если введен верный старый пароль, а новый пароль соответствует всем требованиям (требования к паролю указаны в параметрах системы), значения поле "Новый пароль" и "Новый пароль еще раз" идентичны.

В процессе ввода нового пароля рядом с полем отобразится зеленая галочка, если введенный пароль удовлетворяет всем требованиям.

В процессе подтверждения нового пароля рядом с полем "Новый пароль еще раз" отобразится зеленая галочка, если значения полей "Новый пароль" и "Новый пароль еще раз" идентичны.

При входе в систему происходит сохранение нового пароля.

3.4 Порядок проверки работоспособности

Для проверки работоспособности системы необходимо выполнить следующие действия:

- выполните вход в Системе и откройте АРМ;
- вызовите любую форму.

При корректном вводе учетных данных должна отобразиться форма выбора МО или АРМ, либо АРМ пользователя. При выполнении действий должно не должно отображаться ошибок, система должна реагировать на запросы пользователя, например, отображать ту или иную форму.

4 Модуль "Журнал разрешений" 3.0.5

Система предоставляет доступ к журналу разрешений пользователю, обладающему любой из групп прав: "Администратор ЦОД", "Администратор ЛПУ", "Автоматическое подписание сертификатом ЭП МО";

Для настройки разрешений пользователь вносит сведения в Систему в зависимости от группы прав:

- "Администратор ЦОД":
  - организация действия разрешения;
  - уполномоченное лицо;
  - файл и период разрешения;
  - файл ключа электронной подписи;
  - пароль от ключа электронной подписи.
- "Администратор ЛПУ":
  - уполномоченное лицо;
  - файл разрешения;
  - срок действия разрешения;
  - файл ключа электронной подписи;
  - пароль от ключа электронной подписи.
- "Автоматическое подписание сертификатом ЭП МО":
  - файл разрешения;
  - срок действия разрешения;
  - файл ключа электронной подписи;
  - пароль от ключа электронной подписи.

Файл ключа электронной подписи предоставляется в виде zip архива, состоящего из файлов: header.key, masks.key, masks2.key, name.key, primary.key, primary2.key.

Система выполняет проверку уникальности разрешений на автоматическое подписание от МО.

Для одной организации может быть использовано одно разрешение и один ключ электронной подписи. При настройке пользователем нового разрешения для ранее настроенной организации Системой выполняется замена существующих данных.

4.1 Общие сведения

Форма "Журнал разрешений" предназначена для просмотра и управления разрешениями на применение ЭП уполномоченного лица МО или организации, от имени которой будет выполняться автоматическое подписание.

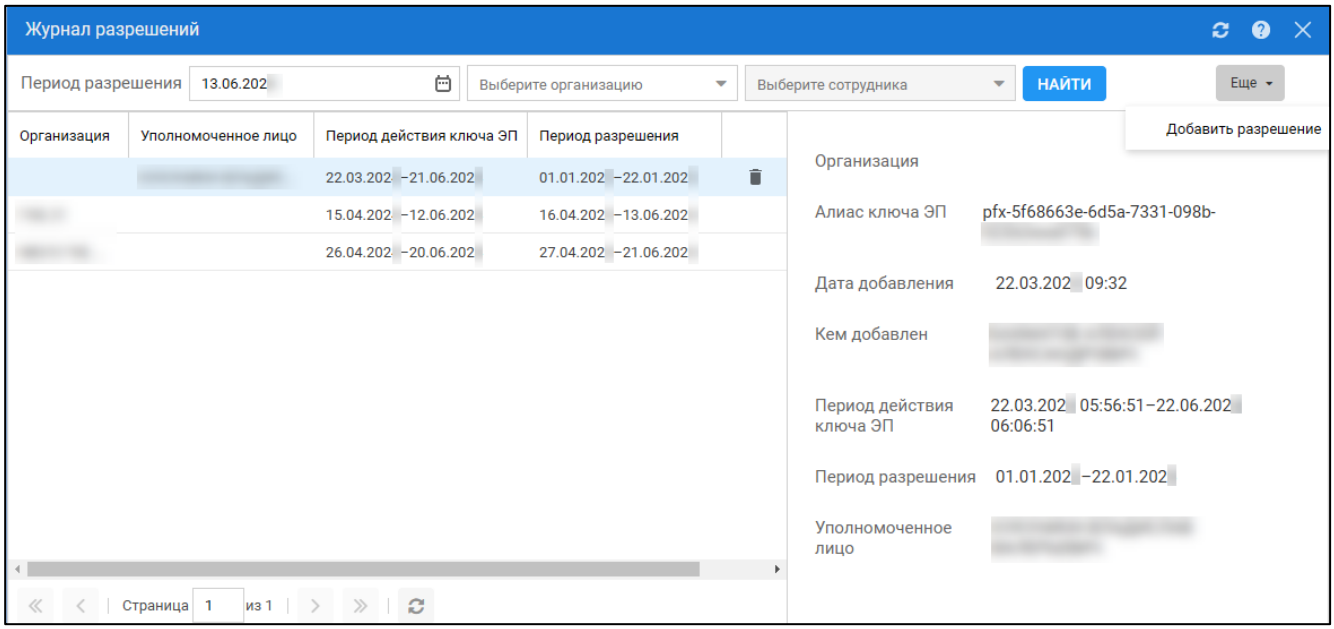


Рисунок 6 – Журнал разрешений

4.2 Доступ к форме

Форма доступна пользователям:

- АРМ администратора ЦОД и АРМ администратора организации:
  - нажмите кнопку "Сервис" в главном меню Системы;
  - выберите пункт "Журнал разрешений для автоподписания от МО" в выпадающем меню.
- АРМ администратора МО:
  - откройте главное меню Системы;
  - перейдите в раздел "Сервис";
  - выберите пункт "Журнал разрешений для автоподписания от МО".
- других АРМ, если их учётной записи назначена группа прав доступа "Автоматическое подписание сертификатом ЭП МО". Доступ к форме аналогичен описанному для АРМ администратора ЦОД или АРМ администратора МО – в зависимости от интерфейса АРМ.

Пользователям АРМ администратора ЦОД настройка разрешений доступна по МО и организациям всего региона, пользователям АРМ администратора МО и АРМ администратора

организации – в рамках своей МО или организации, пользователь с группой прав доступа "Автоматическое подписание сертификатом ЭП МО" может управлять только своим разрешением.

4.3 Описание формы

Форма содержит:

- панель фильтров;
- список разрешений;
- раздел детальной информации по разрешению;
- кнопки управления списком разрешений;
- кнопки управления формой.

4.3.1 Панель фильтров

Панель фильтров содержит поля для фильтрации списка разрешений:

- "Период разрешения" – по дате или периоду действия разрешения;
- "Выберите организацию" – по МО или организации уполномоченного лица, на которого оформлено разрешение;
- "Выберите сотрудника" – по уполномоченному лицу, на которого оформлено разрешение. Поле доступно для заполнения после заполнения поля "Выберите организацию".

Для фильтрации списка разрешений заполните поля на панели фильтров и нажмите кнопку "Найти".

4.3.2 Список разрешений

Список разрешений представлен в табличном виде со столбцами:

- "Организация" – МО или организации, от имени которой выполняется автоматическое подписание видов СЭМД (в случае выполнения настроек, описанных в справке "Автоматическое подписание СЭМД от имени МО или организации");
- "Уполномоченное лицо" – Ф. И. О. уполномоченного лица МО или организации, от имени которой выполняется автоматическое подписание видов СЭМД;
- "Период действия ключа ЭП" – период действия ключа ЭП уполномоченного лица МО или организации, от имени которой выполняется автоматическое подписание видов СЭМД. Отобразится предупреждение, если до даты истечения действия ключа ЭП осталось меньше недели;

- "Период разрешения" – период действия разрешения на применение ЭП для автоматического подписания видов СЭМД.

4.3.3 Раздел с детальной информацией по разрешению

Раздел отображается после выбора записи о разрешении на применение ЭП, в правой части формы.

Раздел содержит сведения:

- "Организация" – МО или организации, от имени которой выполняется автоматическое подписание видов СЭМД (в случае выполнения настроек, описанных в справке "Автоматическое подписание СЭМД от имени МО или организации");
- "Алиас ключа ЭП" – алиас ключа ЭП;
- "Дата добавления" – дата и время добавления разрешения на применение ЭП;
- "Кем добавлен" – Ф. И. О. добавившего разрешение на применение ЭП пользователя;
- "Период действия ключа ЭП" – период действия ЭП уполномоченного лица МО или организации, от имени которой выполняется автоматическое подписание видов СЭМД. Отобразится предупреждение, если до истечения срока действия ЭП осталось меньше недели;
- "Период разрешения" – период действия разрешения на применение ЭП для автоматического подписания видов СЭМД. Отобразится предупреждение, если до истечения срока действия разрешения осталось меньше недели;
- "Уполномоченное лицо" – Ф. И. О. уполномоченного лица МО или организации, от имени которой выполняется автоматическое подписание видов СЭМД.

4.3.4 Кнопки управления списком разрешений

Кнопки управления списком разрешений:

- "Добавить разрешение" – для добавления разрешения на применение ЭП для автоматического подписания видов СЭМД. При нажатии отобразится форма "Разрешение на автоматическое подписание от имени организации" в режиме добавления;
- "Удалить" – для удаления выбранной записи о разрешении на применение ЭП.

4.3.5 Кнопки управления формой

Кнопки управления формой:

- "Закрыть" – для закрытия формы;
- "Обновить" – для обновления отображаемых на форме сведений;
- "Помощь" – для вызова информационной справки по работе с формой;
- "Обновить" – обновление отображаемых записей журнала;
- кнопки перелистывания страниц журнала:
  - – кнопки перехода к первой/последней странице записей журнала;
  - – кнопки перехода к предыдущей/последующей странице записей журнала.

4.4 Работа с формой

От имени МО или организации в Системе может существовать только один действующий ключ ЭП. Поэтому при добавлении для МО или организации нового разрешения предыдущее разрешение автоматически удаляется.

4.4.1 Добавление разрешения

Для добавления разрешения на применение ЭП для автоматического подписания видов СЭМД:

- нажмите кнопку "Добавить разрешение" на форме "Журнал разрешений";
- отобразится форма "Разрешение на автоматическое подписание от имени организации". Заполните на форме обязательные и, при необходимости, необязательные поля;
- сохраните введённые на форме значения.

Добавленная запись о разрешении на применение ЭП для автоматического подписания видов СЭМД отобразится в Журнале разрешений.

4.4.2 Удаление разрешения

Для удаления разрешения на применение ЭП:

- выберите запись о разрешении на форме "Журнал разрешений";
- нажмите кнопку "Удалить". Отобразится форма для подтверждения действия по удалению и предупреждение, что удаление без возможности восстановления. Нажмите

на ней кнопку "Да" для подтверждения (кнопка "Нет" используется для отказа от удаления).

Запись о разрешении будет удалена.

4.5 Правила при работе с разрешениями

Если правило не соблюдается, при сохранении записи о разрешении на применение ЭП отобразится информирующее о том сообщение.

Т а б л и ц а 1 – Правила для разрешений

№ п/п	Правило	Сообщение пользователю в случае нарушения правила
1	Для МО или организации актуальным (используемым для подписания) может быть только одно разрешение	–
2	Ключ ЭЦП, указанный при добавлении разрешения, должен быть действующим	"Ключ ЭЦП должен действовать на момент загрузки. Срок действия истек <дата окончания действия криптоконтейнера>"
3	Период действия разрешения должен быть в пределах периода действия ключа ЭП	"Период действия разрешения должен входить в период действия ключа ЭЦП. Период действия ключа ЭЦП <дата начала действия криптоконтейнера>–<дата окончания действия криптоконтейнера>" (действие разрешения должно истекать не позднее предыдущей даты относительно времени окончания действия ключа ЭЦП)"
4	Одно разрешение предоставляет согласие на использование одного ключа ЭП для автоматического подписания	
5	Для подписания от имени МО или организации может быть использован ключ ЭП, принадлежащий данной МО или организации (ОГРН выданного	"ОГРН ключа ЭЦП <ОГРН из криптоконтейнера> не совпадает с ОГРН указанной организации <краткое наименование текущей организации>"

№ п/п	Правило	Сообщение пользователю в случае нарушения правила
	ключа соответствует ОГРН организации)	
6	Дата начала действия разрешения для Системы должна быть равна дате его добавления (текущей дате)	"Дата начала действия разрешения должна быть равна дате добавления <текущая дата>"
7	Алиас ключа ЭП должен быть уникальным среди алиасов других используемых для подписания ключей ЭП (т. е. среди ключей ЭП, соответствующих действующим разрешениям). Обеспечивается удостоверяющим центром, предоставляющим ключи для ЭП	–

5 Аварийные ситуации

5.1 Описание аварийных ситуаций

Надежность Системы обеспечивается при следующих аварийных ситуациях:

- отказ Системы;
- сбой Системы.

Отказом Системы следует считать событие, состоящее в утрате работоспособности Системы и приводящее к невыполнению или неправильному выполнению контрольных примеров или задач функциональных модулей.

Сбоем Системы следует считать событие, состоящее во временной утрате работоспособности Системы и характеризуемое возникновением ошибки при выполнении контрольных примеров или задач функциональных модулей.

В Системе предусмотрено автоматическое восстановление обрабатываемой информации в следующих аварийных ситуациях:

- программный сбой при операциях записи–чтения;
- разрыв связи с клиентской программой (терминальным устройством) в ходе редактирования/обновления информации.

В Системе предусмотрена возможность ручного восстановления обрабатываемой информации из резервной копии в следующих аварийных ситуациях:

- физический выход из строя дисковых накопителей;
- ошибочные действия обслуживающего персонала.

В Системе предусмотрено автоматическое восстановление работоспособности серверной части Системы в следующих ситуациях:

- штатное и аварийное отключение электропитания серверной части;
- штатная перезагрузка Системы и загрузка после отключения;
- программный сбой общесистемного программного обеспечения, приведший к перезагрузке Системы.

В Системе предусмотрено полуавтоматическое восстановление работоспособности серверной части Системы в следующих аварийных ситуациях:

- физический выход из строя любого аппаратного компонента, кроме дисковых накопителей – после замены компонента и восстановления конфигурации общесистемного программного обеспечения;
- аварийная перезагрузка системы, приведшая к нефатальному нарушению целостности файловой системы – после восстановления файловой системы.

Для восстановления Системы после отказа или сбоя, необходимо сначала устранить причину отказа/сбоя (заменить неисправное оборудование, устранить системные ошибки и др.), а затем предпринять следующие действия:

- установить операционную систему, а затем – соответствующий пакет обновления; проверить правильность работы домена.
- установить СУБД, а затем – соответствующий пакет обновления.
- восстановить базу данных из резервной копии; перезагрузить сервер после восстановления базы данных.
- проверить доступность Системы; чтобы убедиться в правильности работы, запустите сценарий проверки основных функций.
- активировать возможность работы пользователей в штатном режиме.

В случае отказа или сбоя Системы, связанного с неисправностью оборудования, работы проводит Администратор Заказчика.

В случае отказа или сбоя Системы, связанного с системной ошибкой, работы проводит Администратор Исполнителя.

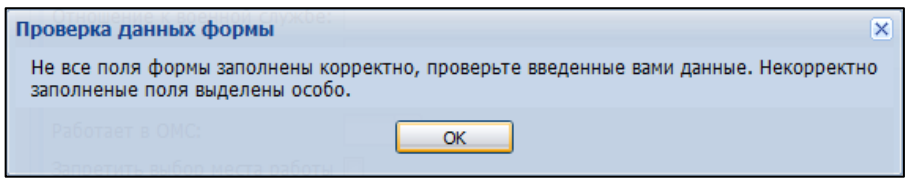
5.2 Действия в случае несоблюдения условий выполнения технологического процесса

При работе с Системой пользователю могут отображаться сообщения нескольких типов:

- сообщение об успешном завершении действия;
- сообщение об ошибке;
- предупреждение;
- сообщение о неисправности системы.

Сообщение об успешном завершении действия содержит краткое резюме операции. Для закрытия сообщения нажмите кнопку "**ОК**".

Сообщение об ошибке отображается в случае, когда дальнейшее выполнение действия в Системе невозможно. Как правило, в таком сообщении содержится краткое описание причины возникновения ошибки. Для закрытия сообщения об ошибке нажмите кнопку "**ОК**".



Предупреждение отображается в том случае, если действия, совершенные оператором, могут повлечь за собой какие–либо особенности в выполнении операции, но не приведут к ошибке.

Например, если оператор укажет у сотрудника ставку менее 0,1, то отобразится сообщение, что такая ставка не будет учитываться при выгрузке. Для того чтобы продолжить выполнение действия, нажмите кнопку "**Да**"/"**Продолжить**". Для того чтобы прекратить действие, нажмите кнопку "**Нет**"/"**Отмена**".

В случае возникновения ошибки о неисправности системы, пользователю системы следует обратиться к администратору системы.

Администратор системы для решения проблем обращается к эксплуатационной документации, настоящему руководству, онлайн справочной системе.

В случае невозможности разрешения ситуации следует обратиться в техническую поддержку.

6 Эксплуатация модуля

Система предназначена для функционирования 24 часа в сутки 7 дней в неделю. Обеспечивается возможность взаимодействия с пользователями в круглосуточном режиме без перерывов, в том числе при доступе пользователей из других по отношению к серверной части временных зон.

Для программного обеспечения Системы определены следующие режимы функционирования:

- штатный режим (режим, обеспечивающий выполнение функций Системы);
- предаварийный режим (режим, предшествующий переходу в аварийный режим);
- аварийный режим (характеризуется отказом одного или нескольких компонентов программного и/или аппаратного обеспечения. В данном режиме функционируют ресурсы, которые в штатном режиме находятся в режиме горячего резерва)
- сервисный режим (режим для проведения реконфигурирования, обновления и профилактического обслуживания).

Информационный обмен со стороны Системы построен через:

- интеграционную шину Системы с соблюдением правил информационной безопасности;
- Сервисы интеграции.

Подробное описание приведено в документе "Регламент эксплуатации".