Параграф. Инструкция по администрированию

Дата актуализации: 20.05.2025

САНКТ-ПЕТЕРБУРГ, 2025г.

С О Д Е Р Ж А Н И Е

1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Для целей настоящего Руководства администратора доступа (далее – настоящий документ) используются следующие понятия и определения:

Аутентификация – процесс подтверждения права пользователя на доступ при помощи логина и пароля.

Доступ – методы и средства физического и (или) логического доступа к компьютерам, сетям, операционным системам, автоматизированным системам, при этом доступ может сопровождаться вводом персонального идентификатора и пароля, в соответствии с установленными правилами – правами доступа.

Информационная система (ИС) – взаимосвязанная совокупность технических и программных средств, других объектов информационной инфраструктуры, содержащейся в базах данных информации и обеспечивающих ее обработку технологий.

КАИС КРО (ГИС СПб КАИС КРО) – государственная информационная система Санкт-Петербурга «Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга».

Логин – имя пользователя, которое используется для входа в систему.

Персональные данные (ПДн) – информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Приложение – функционально законченная часть программного обеспечения, предназначенная для выполнения определенных задач в рамках автоматизации бизнес-процессов.

Операция (действие) – действие, выполняемое в процессе обработки информации (добавление, редактирование, удаление и др.).

Пароль – ключ безопасности, состоящий из набора символов, использующийся для идентификации пользователя при входе в систему в паре с логином.

Поле – ячейка в экранной форме ИС, позволяющая ввести вручную или выбрать из предложенных значений характеристику (атрибут, свойство) объекта.

Пользователь – работник ОО, использующий ИС для решения стоящих перед ним задач в соответствии с его должностными обязанностями.

Права доступа – совокупность правил, регламентирующих порядок и условия выполнения пользователем тех или иных действий с объектами.

Роль – совокупность прав доступа, на основе которых проверяется возможность выполнения пользователем того или иного действия.

Учетная запись пользователя – запись с уникальным идентификатором, содержащая сведения, необходимые для идентификации пользователя, и назначенных ему правах доступа к объектам ИС и операциями с ними.

2. ВВЕДЕНИЕ

2.1. Назначение документа

2.1.1. Настоящий документ описывает действия администратора в подсистемах «Параграф», «Цифровая аналитика», «Электронная дидактическая среда» ГИС СПб КАИС КРО и предназначен для разграничения прав доступа Пользователей, достаточных для выполнения их должностных обязанностей. Документ содержит описание:

- входа в ИС, способа аутентификации в ИС;
- процесса формирования пользовательских учетных записей;

– механизма назначения ролей пользователей, операций работы с ролями, процесса настроек прав доступа для роли;
– процесса обновления прав доступа пользователей;
– процесса аудита действий с учетными записями, доступа к ПДн в системе и логирование системных событий.

2.2. Актуальность документа

2.2.1. Настоящий документ актуализируется со следующей периодичностью: с момента согласования до внесения следующего изменения.

3. ОРГАНИЗАЦИЯ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ

3.1. Описание входа в систему

3.1.1. Работа в ИС ведется в веб-интерфейсе.

3.1.2. Функционирование клиентской части программного обеспечения для просмотра данных осуществляется на персональных компьютерах пользователя со следующими показателями:

операционная система: Ubuntu 20.04 LTS, Astra Linux Special Edition 1.7 и выше, Windows 10 и выше.

один из следующих браузеров:
– Яндекс.Браузер 20 и выше;
– Microsoft Edge 44 и выше (только для Windows);
– Mozilla Firefox 102 и выше;
– Google Chrome 100 и выше.

3.1.3. Для доступа к подсистемам «Параграф», «Цифровая аналитика», «Электронная дидактическая среда» ГИС КАИС КРО используется единая точка входа и единая ролевая модель подсистемы «Параграф».

3.1.4. Для того чтобы выполнить вход в ИС требуется:
– в адресной строке браузера ввести адрес сервера, на котором установлена серверная часть подсистемы «Параграф», и нажать на клавиатуре клавишу [ENTER]: будет открыта главная страница веб-интерфейса ИС (Рис. 1)
– на открывшейся странице ввести логин и пароль пользователя в соответствующих полях и нажать кнопку «Войти».

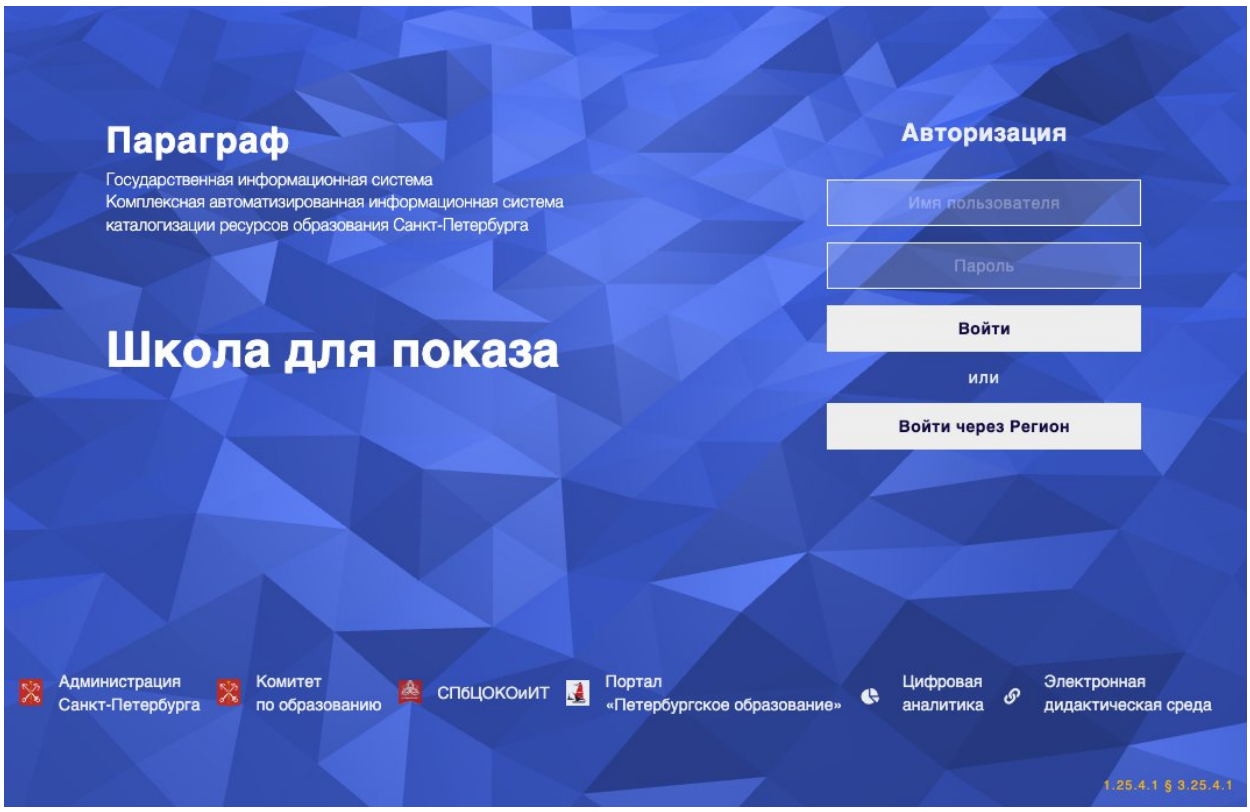


Рис. 1 Окно входа в ИС

3.1.5. Для того чтобы осуществить выход из ИС, необходимо нажать кнопку ☰. Затем в правом нижнем углу экрана выбрать «Выйти из системы» (Рис. 2). Сеанс работы завершится и откроется страница входа в подсистему «Параграф». Чтобы возобновить работу, достаточно заново выполнить вход в ИС.

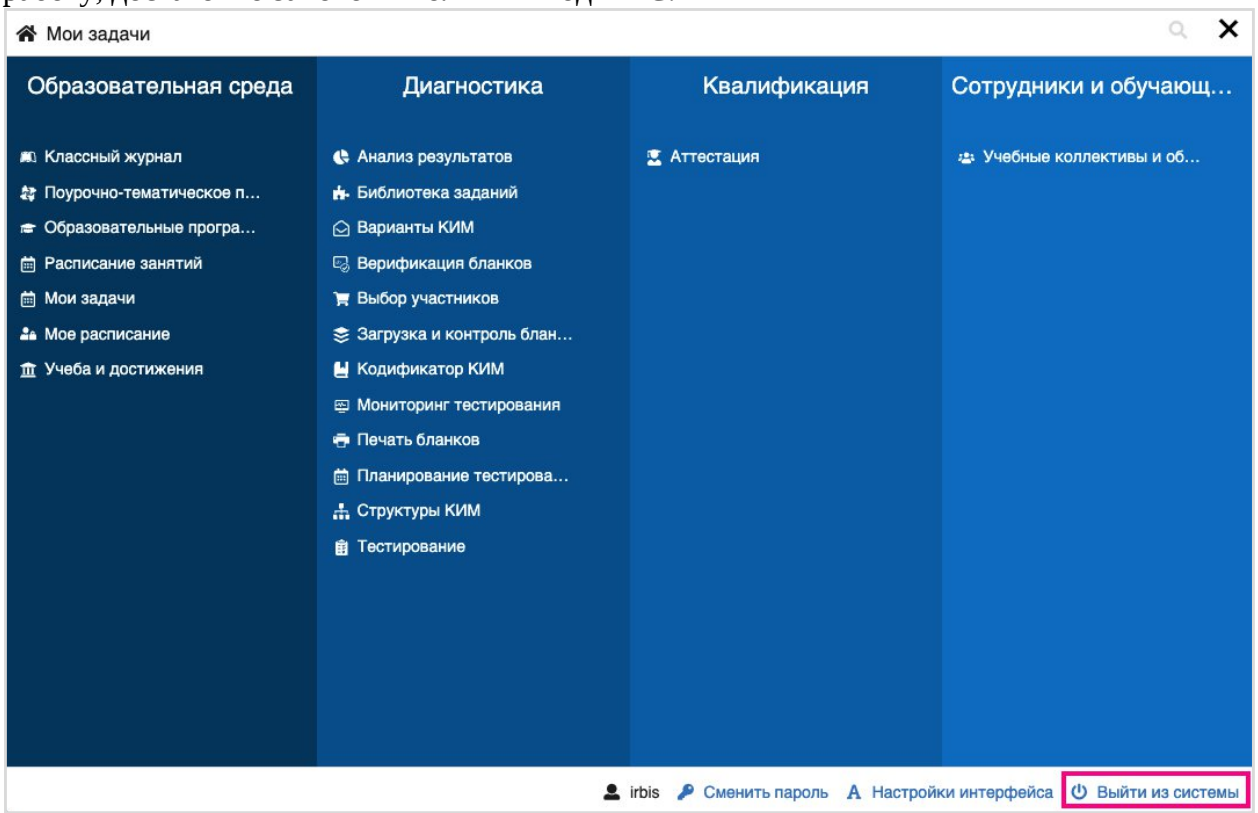


Рис. 2 Выход из ИС

3.1.6. При заданном периоде неактивности в файле settings.ini (см. п. 3.7.1 настоящего документа), сессия пользователя блокируется по истечение указанного времени (Рис. 3). Для разблокировки введите пароль пользователя в соответствующем поле. Для аутентификации под другой учетной записью – нажмите кнопку «Сменить пользователя».

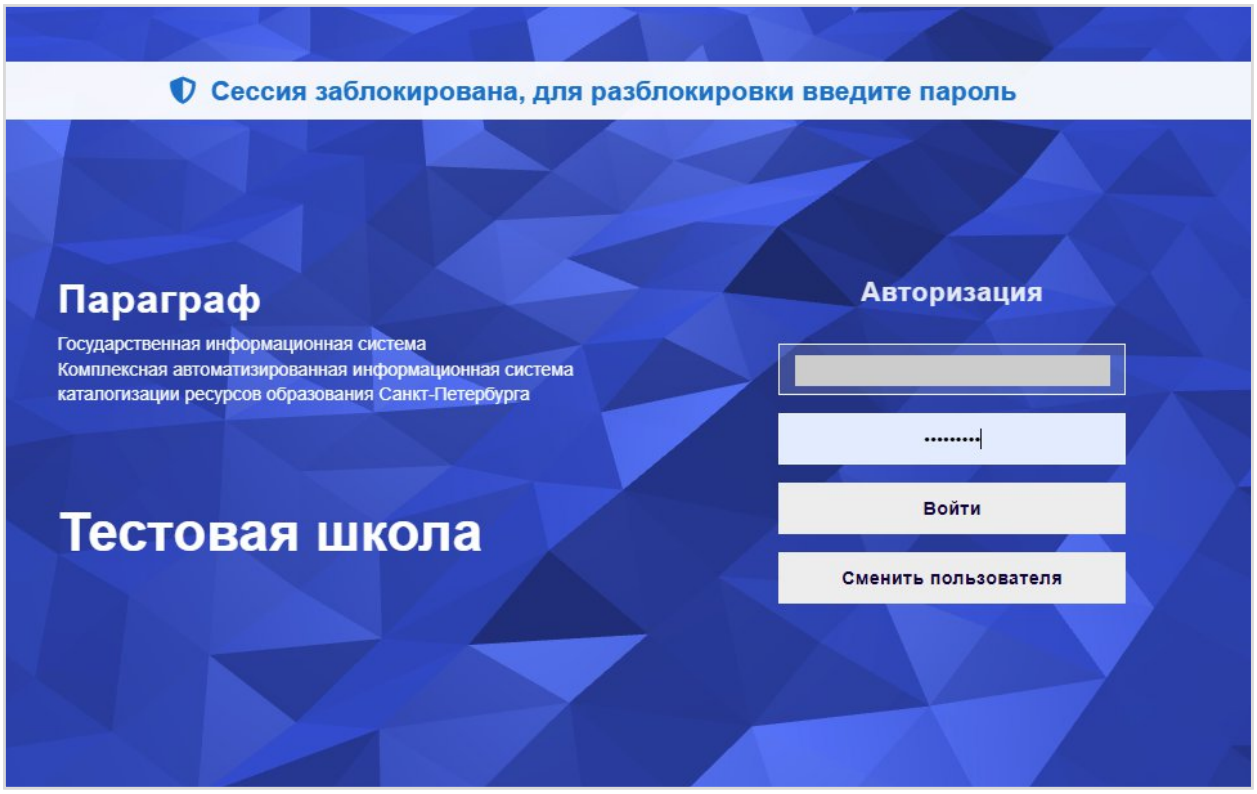


Рис. 3 Заблокирована сессия пользователя

3.1.7. При заданном параметре очистки cookies в файле settings.ini (см. п. 3.7.1 настоящего документа), сведения о состоянии входа в систему очищаются при закрытии браузера.

3.2. Аутентификация в системе

3.2.1. Аутентификация пользователя выполняется на основании совпадения идентификационной информации (имени и пароля), предъявленной пользователем, с информацией, хранящейся в системе.

3.2.2. При аутентификации происходит блокировка учетной записи пользователя на 15 минут при многократном неудачном вводе пароля (5 раз подряд). Это помогает усилить защиту ИС от взлома или неправомерного доступа.

3.2.3. Предусмотрена возможность аутентификации пользователя с ролями «Учитель», «Ученик» с использованием ЕСИА (кнопка «Войти через регион»). Для идентификации пользователя используются данные из полей «СНИЛС» и «Мобильный» (телефон). Значения в указанных полях подсистемы «Параграф» должны совпадать с данными, используемыми для аутентификации через ЕСИА в государственных сервисах.

3.3. Создание учетных записей

Для перехода к функциям администрирования и работы с учетными записями на верхней панели нажмите значок ☰ (Рис. 4) и открывшемся окне в разделе «Администрирование» выберите приложение «Администрирование пользователей».

Примечание: приложение доступно только тем пользователям, для которых настроены соответствующие права доступа.

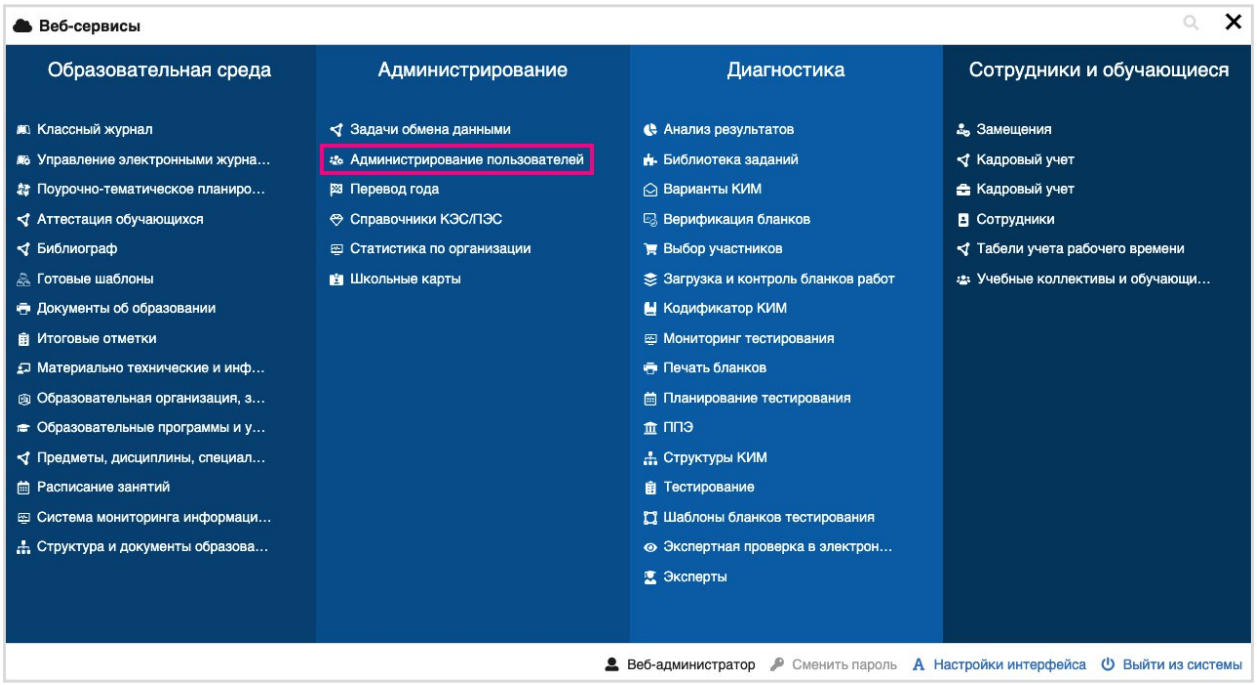


Рис. 4 Раздел «Администрирование»

В открывшемся окне нажмите по наименованию образовательной организации в дереве объектов. Откроется список пользователей, внесенных в базу данных, и возможности работы с ними (Рис. 5).

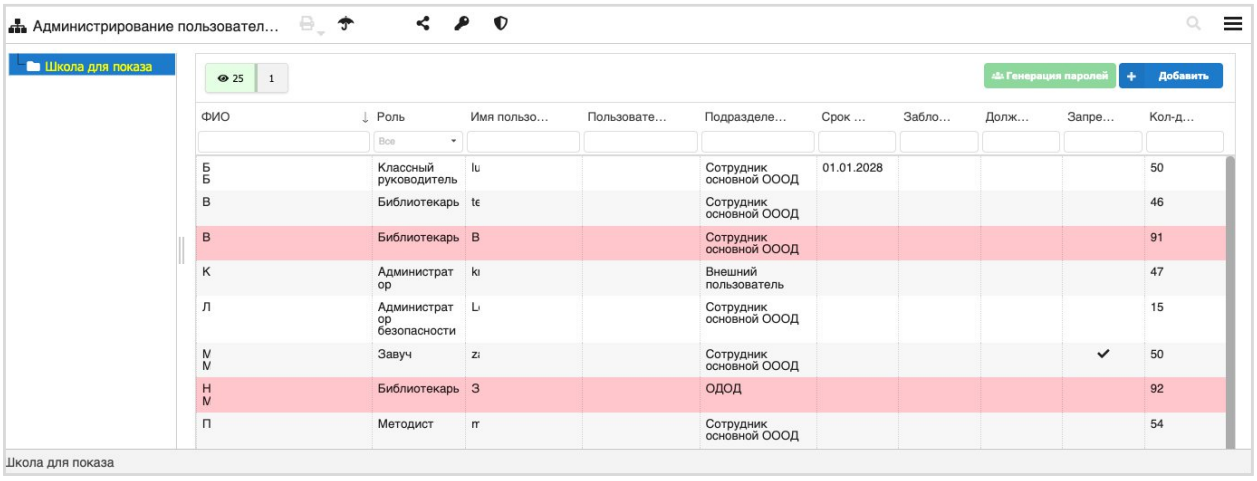


Рис. 5 Окно приложения «Администрирование пользователей»

Экранная форма содержит следующий список колонок:

- ФИО;
- Роль;
- Имя пользователя;
- Пользователь СДО;
- Подразделение;
- Срок действия учетной записи до (блокировки);
- Заблокирован;
- Должен изменить пароль;
- Запрет на изменение пароля (пользователем самостоятельно);
- Кол-во дней после смены пароля.

Красным цветом в таблице указаны учетные записи пользователей, срок действия которых превышает 90 дней (истёк). Галочками отмечены выбранные опции для пользователя.

В столбце «Кол-во дней после смены пароля» указывается количество дней после последней смены пароля (на 75 день система попросит изменить пароль, по истечение 90 дней – учетная запись будет заблокирована и выделена красным цветом).

Иконка 

отображает количество записей, доступных для просмотра в зависимости от выбранных настроек фильтрации и количество страниц, содержащих записи.

3.3.1. Учетные записи пользователей

Создание учетных записей в системе возможно двумя способами: регистрация нового пользователя из списка персон, внесенных в базу данных, и регистрация нового внешнего пользователя.

3.3.2. Регистрация нового пользователя из списка персон, внесенных в базу данных

По умолчанию в окне администрирования пользователей доступен список сотрудников. В системе предусмотрена возможность создания учетных записей для учащихся и законных представителей. Чтобы перейти к настройке прав доступа для этих категорий пользователей потребуется предварительно выбрать роль («Ученик», «Родитель») в соответствующей колонке — после фильтрации будет выведен список учащихся или законных представителей, внесенных в базу данных.

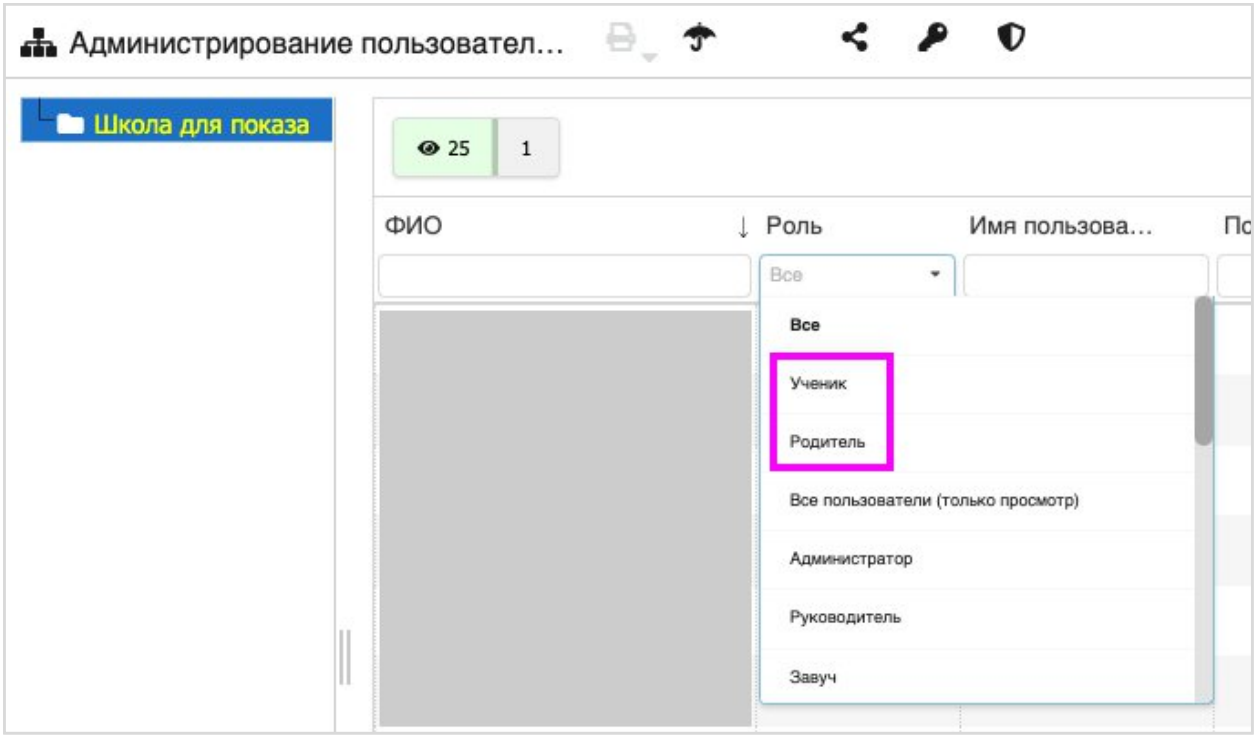


Рис. 6 Выбор роли для пользователей

Для настройки и создания учетных записей сотрудников предварительный выбор роли не требуется.

Для регистрации нового пользователя из числа сотрудников выберите в списке персон подходящего сотрудника — нажмите на его ФИО. Откроется карточка настройки прав доступа (Рис. 7).

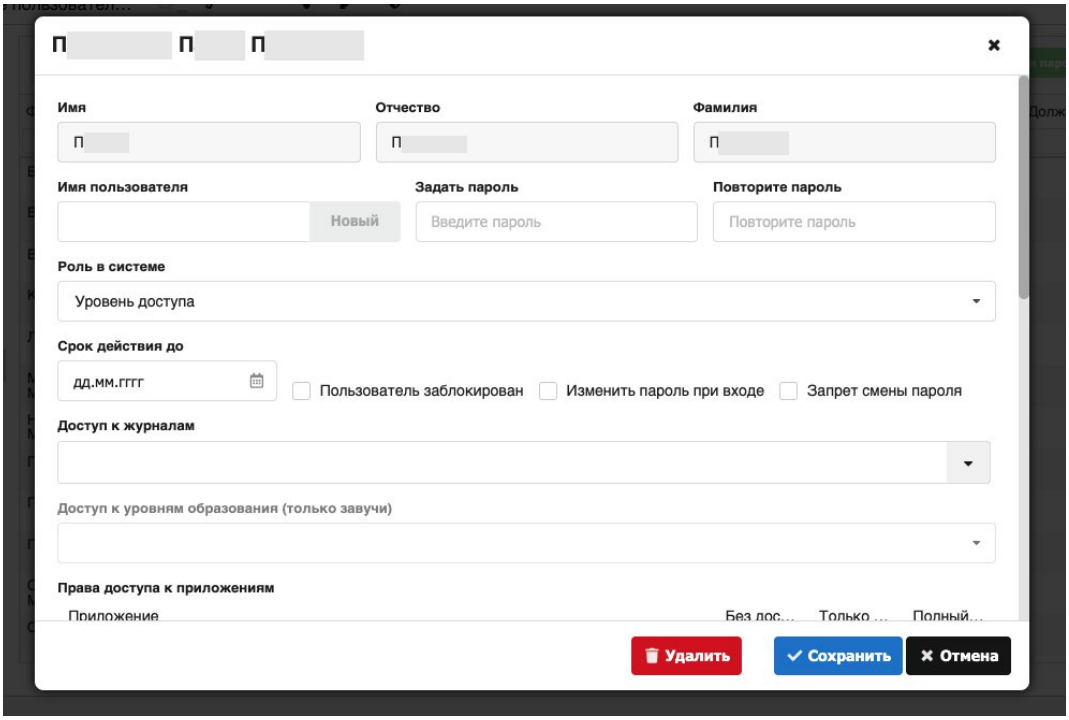


Рис. 7 Окно создания учетной записи

3.3.2.1. Общие рекомендации по заполнению карточки нового пользователя

Заполнять поля следует последовательно сверху вниз, чтобы не нарушить логику автоматического заполнения полей.

Поля *«Имя»*, *«Отчество»*, *«Фамилия»* являются не редактируемыми для персоны, внесенной в базу данных. Изменить сведения в этих полях можно только в соответствующем приложении.

Введите *имя пользователя* — допускается использование букв русского, латинского алфавитов, цифр и специальных символов. Запрещено использовать имя пользователя, уже имеющееся в системе. Запрещено повторно использовать имя пользователя, ранее удаленного из системы, ранее, чем через год после его удаления.

Задайте *пароль* и повторите его в поле рядом. Должны выполнятся следующие требования к паролю:

- длина пароля не менее шести символов;
- пароль содержит как минимум одну букву верхнего регистра, одну букву нижнего регистра, цифру и специальный символ (кроме пробела);
- буквы допустимо использовать только из латинского алфавита.

Укажите *роль* пользователя в системе. Каждой роли в системе соответствуют преднастроенные права на доступ к документам, справочникам, отчетам, действиям. Дополнительно настраивается доступ к приложениям.

Обратите внимание: в ИС предусмотрено две административных роли — «Администратор» и «Администратор безопасности». Администратор безопасности может просматривать не только журналы аудита учетных записей, но также имеет доступ к журналу фактов обращений к персональным данным.

При необходимости укажите *срок действия пароля* пользователя. По умолчанию срок действия составляет пароля составляет 75 дней, это значение в поле не указывается. Срок действия пароля может быть сокращен, но не увеличен.

Если пользователю требуется *изменить пароль при входе* или наоборот, *запретить* самостоятельно *изменять пароль* — установите галочки в соответствующих чекбоксах.

3.3.2.2. Доступ к журналам

Если пользователю требуется предоставить доступ к журналам (обычно для пользователей с ролями «Завуч», «Учитель предметник», «Классный руководитель») в

конце поля «Доступ к журналам» нажмите кнопку . В открывшемся окне поставьте галочки напротив наименования журналов, для которых необходимо предоставить полный доступ (для редактирования) или открыть для просмотра. В этом же окне настраивается доступ к просмотру и редактированию календарного плана воспитательной работы и плана мероприятий.

3.3.2.3. Доступ к уровням образования

Для пользователя с ролью «Завуч» дополнительно можно настроить доступ к объектам и персонам в системе по уровню образования. Разверните список и выберите столько уровней.

По умолчанию завучу доступны все имеющиеся уровни образования, выполнять настройки требуется только для ограничения доступа.

3.3.2.4. Доступ к приложениям

Раздел «Права доступа к приложениям» позволяет гибко настроить права доступа пользователей. Отметьте галочками в разделе те приложения, к которым у пользователя будет доступ на просмотр или полный доступ (для редактирования).

По умолчанию пользователю доступен интерфейс подсистемы «Цифровая аналитика» и перечень приложений, доступных для его роли без учета настроек отдельных прав доступа.

3.3.2.5. После того как поля в окне регистрации нового пользователя будут заполнены нажмите кнопку «*Сохранить*».

3.3.3. Регистрация нового внешнего пользователя

Регистрация внешних пользователей недоступна для ролей «Ученик» и «Родитель».

Чтобы создать учетную запись внешнего пользователя, нажмите кнопку «+ Добавить» в правой части окна (Рис. 8).

Рис. 8 Кнопка «+ Добавить» для регистрации внешних пользователей

Откроется окно регистрации нового пользователя. Воспользуйтесь шагами из пункта 3.3.2 для заполнения карточки нового пользователя.

Дополнительно укажите фамилию, имя, отчество добавляемого пользователя, а также краткое описание.

Не рекомендуется предоставлять внешним пользователям доступ к приложениям, содержащим персональные данные!

После заполнения полей нажмите кнопку «Добавить» внизу окна для создания новой учетной записи внешнего пользователя.

3.3.4. Настройка ранее созданной учетной записи пользователя

Для настройки существующей учетной записи пользователя выберите его в списке пользователей в окне приложения «Администрирование пользователей» (для настройки прав доступа пользователей с ролями «Ученик», «Родитель» потребуется предварительно установить фильтр в колонке «Роль»). Далее, воспользуйтесь шагами из пункта 3.3.2 для настройки учетной записи пользователя.

После заполнения полей нажмите кнопку «Сохранить» внизу окна для сохранения новых настроек ранее созданной учетной записи пользователя.

3.4. Отзыв доступа и блокировка учетной записи

Отзыв доступа пользователя и блокировка учетной записи пользователя осуществляется в карточке пользователя.

3.4.1. Автоматическая блокировка учетной записи пользователя

Автоматическая блокировка учетной записи пользователя осуществляется в случае, если учетная запись пользователя была неактивна более 90 дней.

3.4.2. Блокировка и удаление учетной записи пользователя через интерфейс системы

Для блокировки или удаления существующей учетной записи пользователя выберите его в списке пользователей в окне приложения «Администрирование пользователей» (для настройки прав доступа пользователей с ролями «Ученик», «Родитель» потребуется предварительно установить фильтр в колонке «Роль»).

В открывшемся коне доступны следующие действия:

– заблокировать пользователю доступ в систему;
– полностью удалить учетную запись из системы.

Поставьте галочку в чекбоксе «Пользователь заблокирован» для блокировки пользователя до последующей отмены блокировки администратором ИС вручную (Рис. 9). Нажмите кнопку «Сохранить» для сохранения изменений. В списке пользователей учетная запись будет помечена галочкой в колонке «Заблокирован».

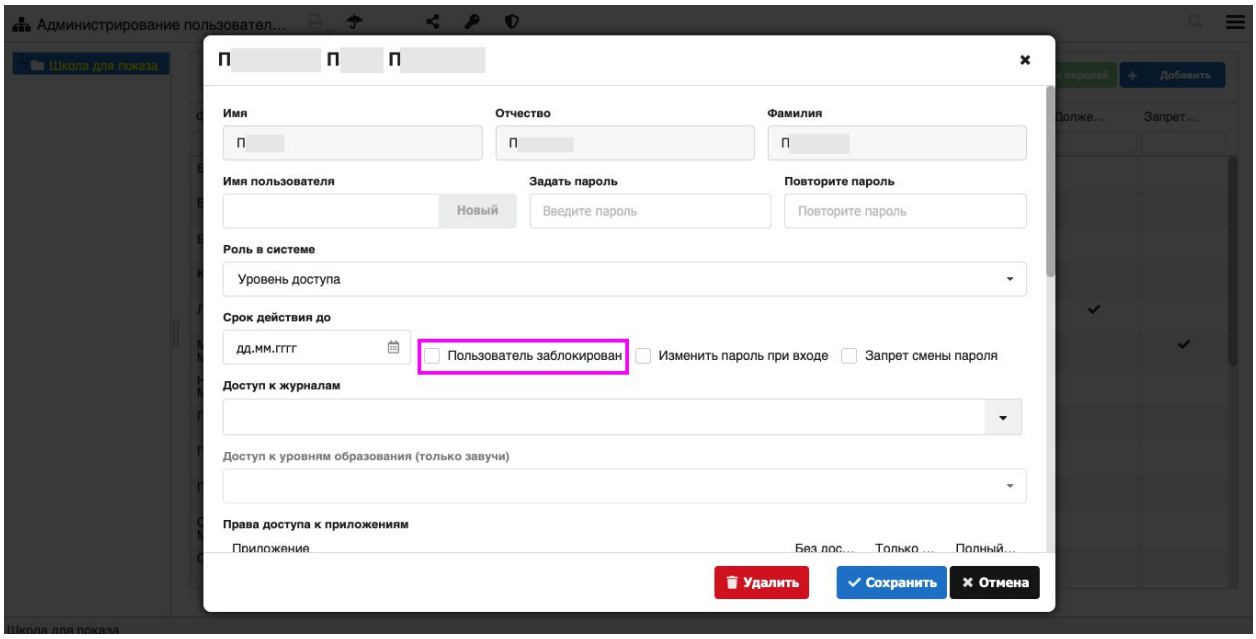


Рис. 9 Чек-бокс блокировки пользователя

Для удаления учетной записи пользователя нажмите кнопку «Удалить» (Рис. 10) в окне настройки учетной записи пользователя. Подтвердите удаление, нажав в появившемся окне кнопку «Удалить» ещё раз.

Если была удалена учетная запись пользователя, внесенного в базу данных, то будут удалены только настройки доступа и аутентификационные данные. Запись персоны в списке будет присутствовать. При необходимости можно повторно выбрать ту же персону и заново создать для нее учетную запись.

Если была удалена учетная запись внешнего пользователя – она также будет удалена из списка пользователей.

Обратите внимание: в системе запрещено повторное использование удаленного логина в течение года.

Важно: удаление учетной записи пользователя является необратимой операцией!

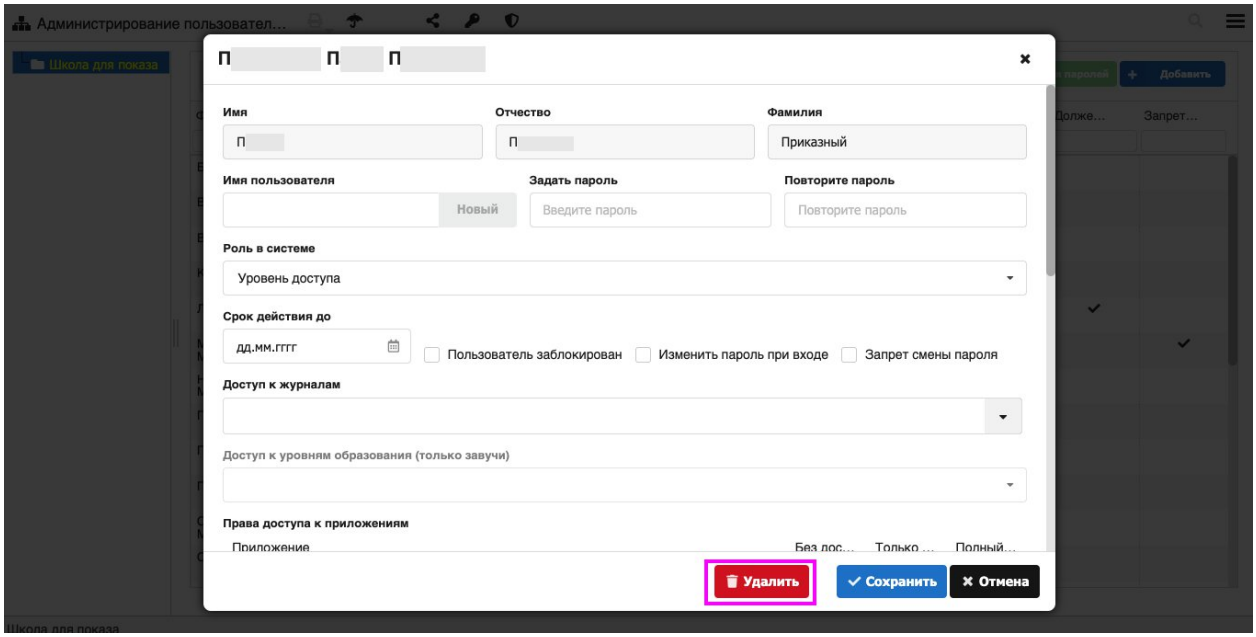


Рис. 10 Кнопка «Удалить» в окне настройки учетной записи

3.5. Разблокировка учетной записи и сброс пароля

3.5.1. Разблокировка учетной записи

Если пользователю был заблокирован вход в систему, разблокировать доступ можно окне настройки учетной записи пользователя – снимите галочку в чек-боксе «Пользователь заблокирован» (Рис. 9) и сохраните изменения.

3.5.2. Изменение пароля Пользователя

Доступны следующие варианты изменения пароля:

- изменение администратором системы в окне настроек учетной записи;
- изменение пользователем по инициативе пользователя;
- изменение пользователем по требованиям системы.

Должны выполнятся следующие требования к паролю:

- длина пароля не менее шести символов;
- пароль содержит как минимум одну букву верхнего регистра, одну букву нижнего регистра, цифру и специальный символ (кроме пробела);
- буквы допустимо использовать только из латинского алфавита.

3.5.2.1. Изменение пароля администратором системы

Для изменения пароля существующей учетной записи пользователя выберите его в списке пользователей в окне приложения «Администрирование пользователей» (для настройки прав доступа пользователей с ролями «Ученик», «Родитель» потребуется предварительно установить фильтр в колонке «Роль»).

Нажмите кнопку «Сменить пароль» (Рис. 11).

В открывшемся окне введите новый пароль для учетной записи и подтвердите его. Нажмите кнопку «Сохранить».

Изменения будут сохранены, а окно настроек учетной записи пользователя будет закрыто.

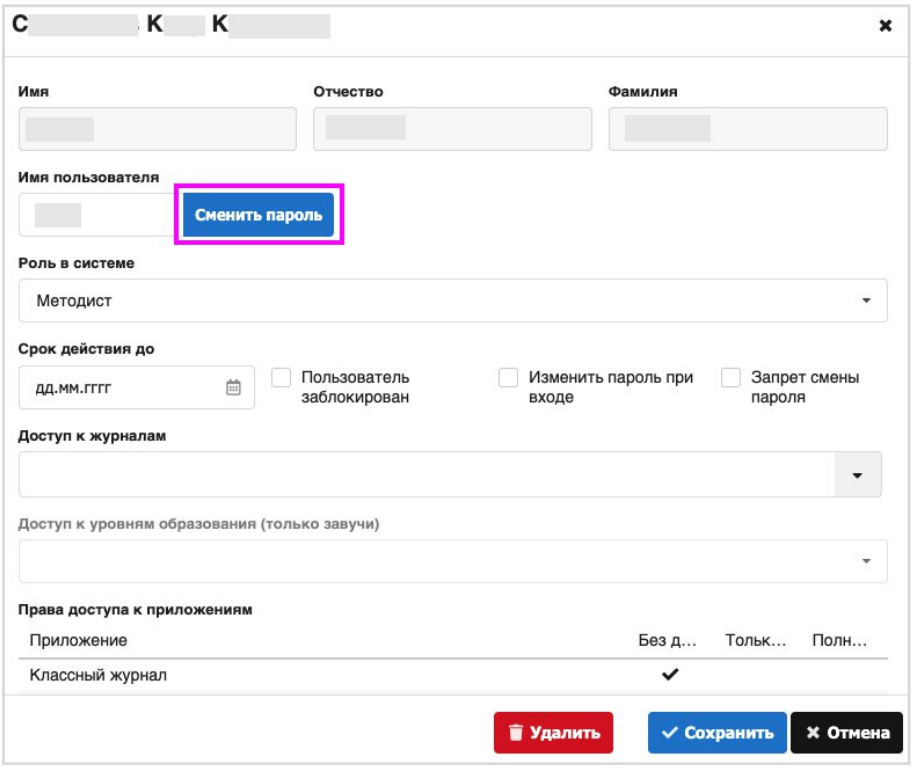


Рис. 11 Кнопка «Сменить пароль» в окне настройки учетной записи

3.5.2.1. Изменение пароля пользователем по инициативе пользователя

Если для пользователя не был установлен запрет на самостоятельную смену пароля, то в окне, содержащем список приложений системы, в правом нижнем углу будет доступна кнопка «Сменить пароль» (Рис. 12).

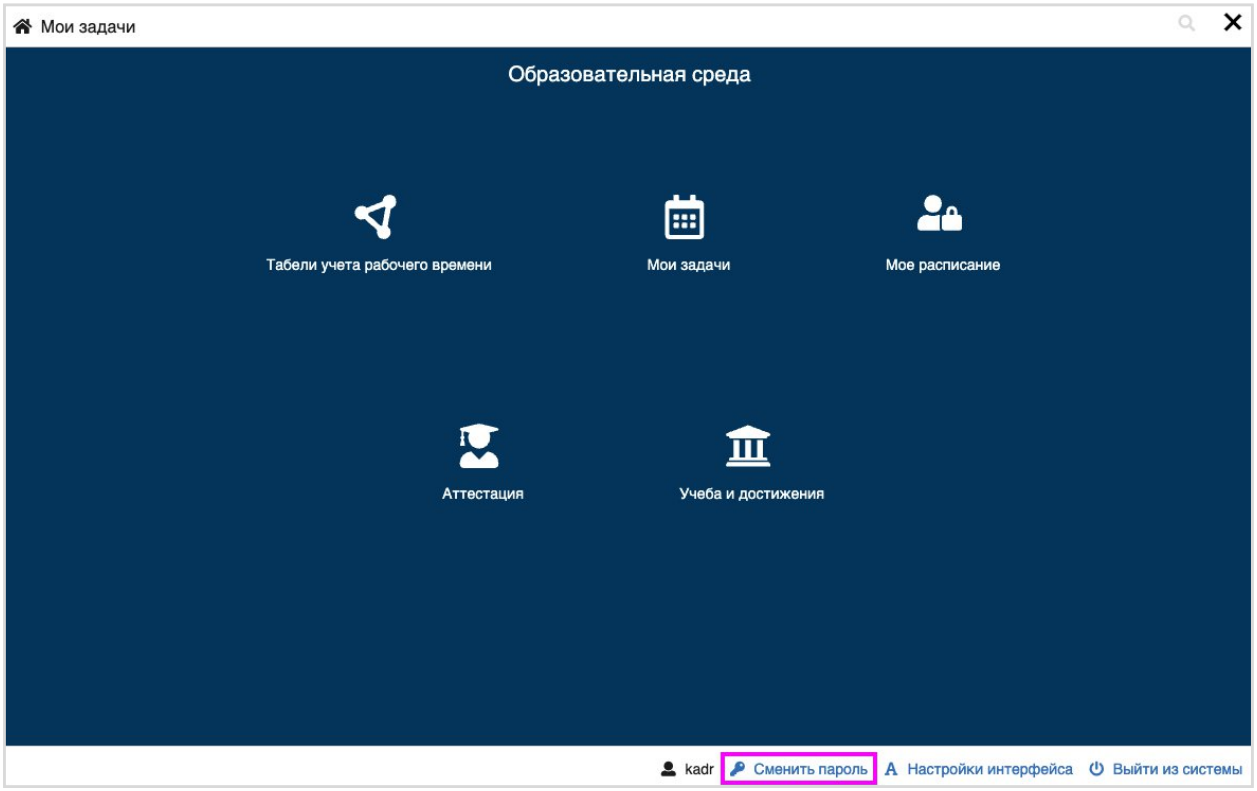


Рис. 12 Кнопка «Сменить пароль» в окне списка приложений

Нажатие на кнопку откроет окно (Рис. 13), в котором пользователю необходимо ввести свой текущий пароль, а затем новый и его подтверждение.

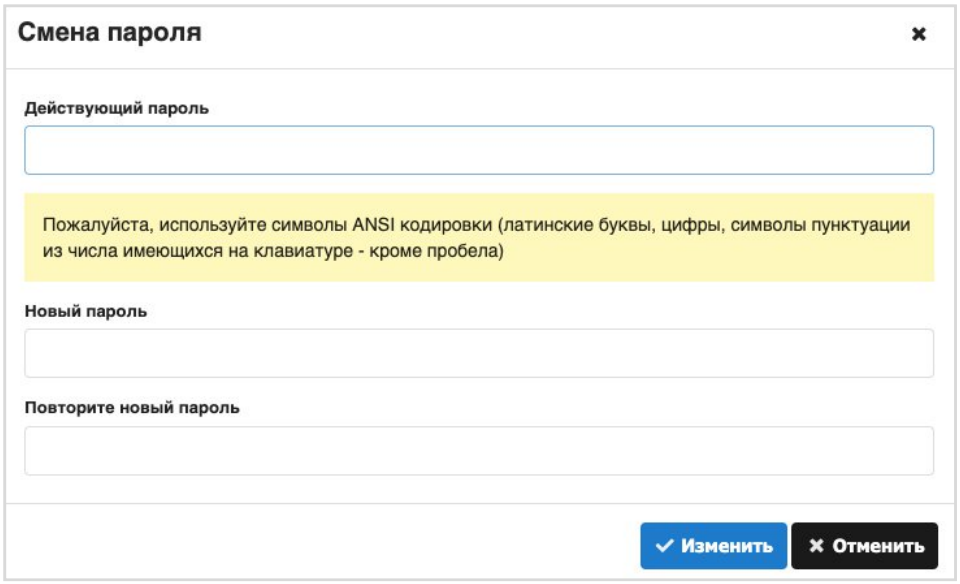


Рис. 13 Окно смены пароля

Если все требования к паролю были соблюдены, корректно введен действующий пароль, новый пароль и его подтверждение, то нажатие кнопки «Изменить» сохранит новые настройки. Будет также выведено всплывающее окно об успешном сохранении нового пароля.

Пользователь с ролью «Веб администратор» (суперадминистратор) не может изменить пароль самостоятельно в веб-интерфейсе. Для изменения пароля потребуется вносить изменения в файл settings.ini.

3.5.2.2. Изменение пароля пользователем по требованиям системы

Система автоматически запрашивает изменение пароля у пользователя в следующих случаях:

- истек срок действия пароля, установленный администратором;
- прошло более 75 дней с момента предыдущей смены пароля;
- администратором установлено требование изменения пароля пользователем при его следующем входе в систему.

Сразу после аутентификации пользователя в системе будет выведено всплывающее окно, в котором необходимо ввести текущий пароль пользователя, новый пароль и его подтверждение (Рис. 13), затем нажать кнопку «Изменить».

Если все требования к паролю были соблюдены, корректно введен действующий пароль, новый пароль и его подтверждение, то нажатие кнопки «Изменить» сохранит новые настройки. Будет также выведено всплывающее окно об успешном сохранении нового пароля.

Обратите внимание: для пользователей с истекшим сроком действия пароля (более 75 дней) автоматически выставляется галочка в чек-боксе «Изменить пароль при следующем входе». Снятие галочки в чек-боксе не отменяет необходимость выполнения процедуры смены пароля!

3.6. Аудит действий в системе

В ИС предусмотрено логирование событий и три журнала аудита действий в системе:

- журнал регистрации действий с пользователями;
- журнал авторизации;

- журнал доступа к персональным данным.

В таблице 1 представлена матрица доступа административных ролей к возможностям аудита.

Таблица 1

	Администратор (назначаемая роль)	Администратор безопасности (назначаемая роль)	Веб-администратор (системная роль)
Журнал регистрации действий с пользователями	+	+	+
Журнал авторизации	+	+	+
Журнал доступа к персональным данным	-	+	+
Лог событий	-	+	+

Журналы доступны для просмотра в приложении «Администрирование пользователей». Выделите образовательную организацию в окне приложения, чтобы в верхнем меню появились иконки журналов (Рис. 14).

Рис. 14 Кнопки просмотра журналов аудита

Лог событий доступен в приложении «Задачи обмена данными» раздела «Администрирование» (Рис. 15).

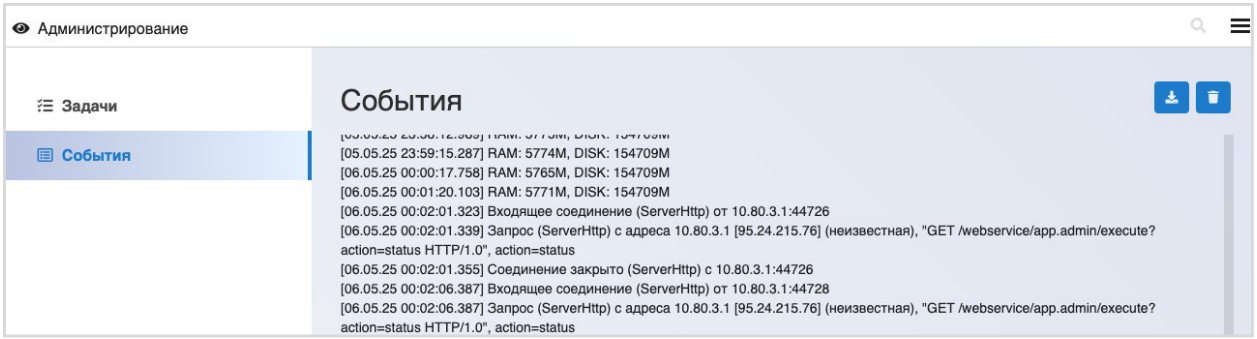


Рис. 15 Пункт «События» в окне приложения «Задачи обмена данными»

3.6.1. Журнал регистрации действий с пользователями

Нажмите кнопку , чтобы открыть журнал регистрации действий с пользователями (Рис. 16).

Рис. 16 Журнал регистрации действий с пользователями

Журнал содержит колонки:

- Метка времени (регистрации события);
- USER_ID (внутренний ID пользователя в базе данных);
- Имя пользователя (с учетной которого записью выполнялись действия);
- Персона (ФИО, соответствующие USER ID и учетной записи);
- Тип события (системный);
- Детали события;
- Кто изменил (указывается пользователь, отличный от веб-администратора).

Предусмотрена возможность фильтрации по одной / нескольким колонкам, сортировка в прямом или обратном порядке (по однократному/повторному нажатию на заголовок колонки).

Иконка  отображает количество записей, доступных для просмотра в зависимости от выбранных настроек фильтрации и количество страниц, содержащих записи.

3.6.2. Журнал авторизации

Нажмите кнопку  , чтобы открыть журнал авторизации (Рис. 17).

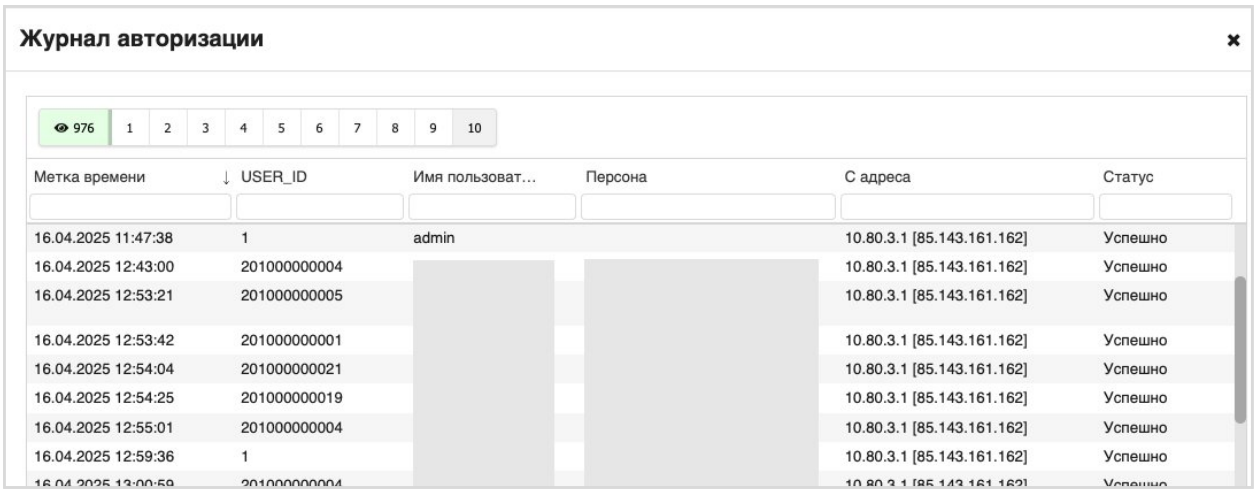


Рис. 17 Журнал авторизации

Журнал содержит колонки:

- Метка времени (регистрации события);
- USER_ID (внутренний ID пользователя в базе данных);
- Имя пользователя (выполнявшего аутентификацию в системе);
- Персона (ФИО, соответствующие USER ID и учетной записи);

- С адреса (IP адрес сервера и клиента);
- Статус.

Предусмотрена возможность фильтрации по одной / нескольким колонкам, сортировка в прямом или обратном порядке (по однократному/повторному нажатию на заголовок колонки).

Иконка 

отображает количество записей, доступных для просмотра в зависимости от выбранных настроек фильтрации и количество страниц, содержащих записи.

3.6.3. Журнал доступа к персональным данным

Нажмите кнопку  , чтобы открыть журнал доступа к персональным данным (Рис. 18).

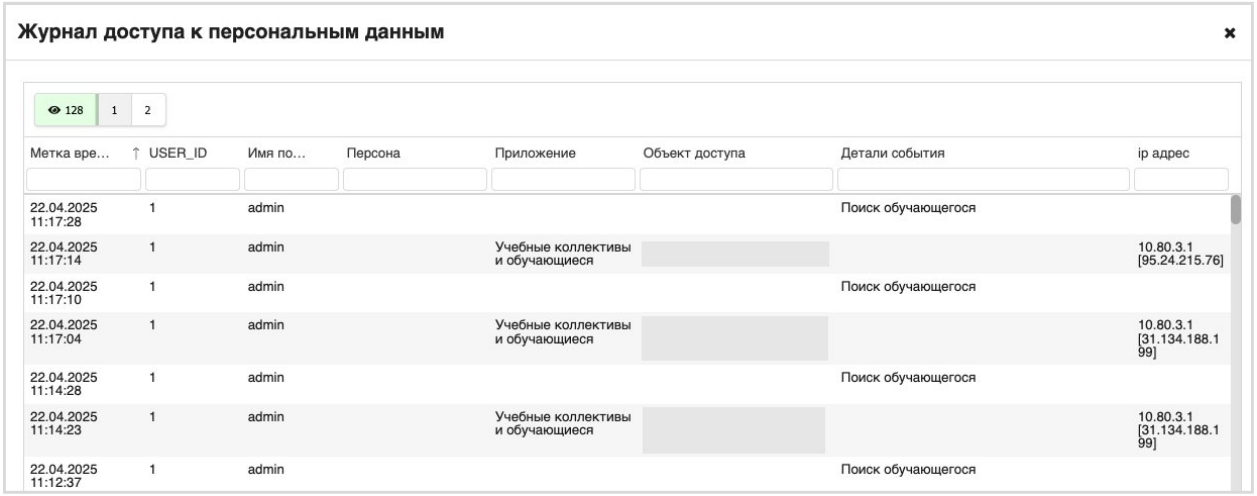
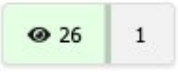


Рис. 18 Журнал доступа к персональным данным

Журнал содержит колонки:

- Метка времени (регистрации события);
- USER_ID (внутренний ID пользователя в базе данных);
- Имя пользователя (получившего доступ к ПДн);
- Персона (ФИО, соответствующие USER ID и учетной записи);
- Приложение (в котором был осуществлен доступ к ПДн);
- Объект доступа (сведения о персоне, к чьим данным осуществлялся доступ);
- Детали события (указывается действие, отличное от открытия карточки персоны);
- ip адрес (сервера и клиента).

Предусмотрена возможность фильтрации по одной / нескольким колонкам, сортировка в прямом или обратном порядке (по однократному/повторному нажатию на заголовок колонки).

Иконка 

отображает количество записей, доступных для просмотра в зависимости от выбранных настроек фильтрации и количество страниц, содержащих записи.

3.6.4. Лог событий

Перейдите в приложение «Задачи обмена данными», чтобы открыть лог событий системы.

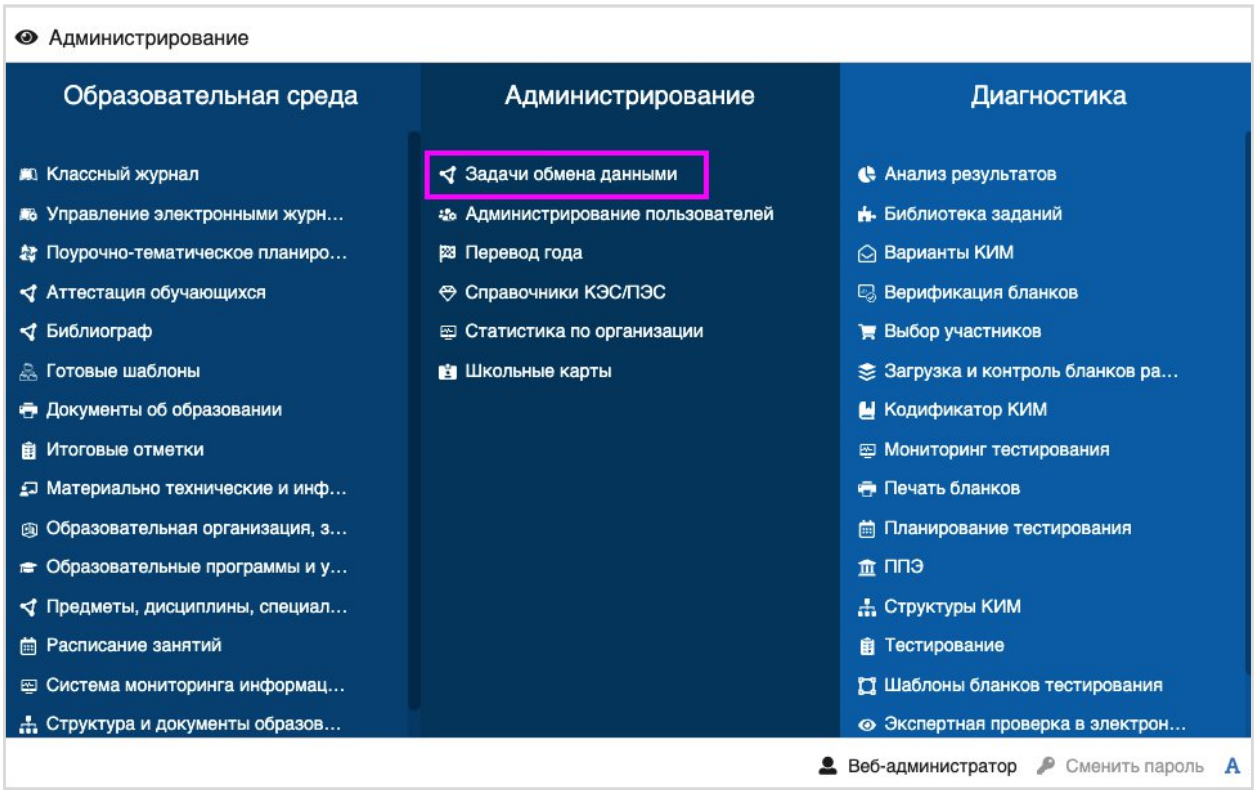


Рис. 19 Приложение «Задачи обмена данными»

В логе событий сохраняются сведения обо всех действиях пользователей в системе: аутентификации, результатах выполнения задач обмена, результатах действий в системе (например, фильтрации данных в таблицах), сведения об использовании оперативной памяти сервера и т.д.

Используйте кнопку  в правом углу окна «События» (Рис. 15), чтобы сформировать архив текущих логов и сохранить его на компьютер.

3.7. Дополнительные настройки безопасности в системе

Для дополнительных настроек безопасности внесите изменения в файл settings.ini из папки IVC/Datagate.

После внесения изменений потребуется перезапустить службу DatagateAppServer.

3.7.1. Отключение анимации на экране входа

Для улучшения быстродействия системы и отключения анимации заставки на экране авторизации укажите дополнительный параметр в секции [System]:

NoAnimation=XXX (где 0 – анимация включена, 1 – анимация выключена).

3.7.2. Блокировка сессии

Укажите дополнительные параметры в секции [System]:

ScreenLockTime=XXX – где вместо «XXX» указать количество секунд, по истечению которых будет автоматически заблокируется сессия пользователя.

CookiesClearOnClose=1– при установке параметра с таким значением файлы cookies будут автоматически очищаться при закрытии окна ИС.

3.7.3. Отправка сообщения администратору об инциденте безопасности

При превышении установленного лимита оперативной памяти и/или памяти жесткого диска, администратору будет отправлено сообщение на электронную почту.

Укажите дополнительные параметры в секции [System]:

AdminAddress= smtp:XXX – где вместо «XXX» указать адрес электронной почты, на который будут отправляться сообщения.

MemoryFreeLimit=XXX - где вместо «XXX» указать минимальное допустимое количество байт оперативной памяти.

DiskFreeLimit=XXX - где вместо «XXX» указать минимальное допустимое количество байт памяти на жестком диске.

Укажите дополнительные параметры в секции [SMTP] (при отсутствии секции в файле settings.ini – добавьте предварительно саму секцию):

Host=XXX - где вместо «XXX» указать адрес почтового сервера для отправки электронной почты.

Port=XXX - где вместо «XXX» указать порт почтового севера.

UserName=XXX - где вместо «XXX» указать логин пользователя на почтовом сервере, от имени которого будет происходить отправка сообщения.

Password=XXX - где вместо «XXX» указать пароль пользователя на почтовом сервере, от имени которого будет происходить отправка сообщения.

AuthType=Default – тип аутентификации (может принимать значения: Default – определять автоматически, none – отсутствует, SASL – использовать только конкретный тип идентификации SASL).

TLS=None – тип защиты соединения (может принимать значения: None – без защиты соединения; или один из типов: Require; Implicit; Explicit).

DefaultSender=XXX - где вместо «XXX» указать адрес электронной почты отправителя системного сообщения.

3.7.4. Изменение пароля Веб-администратора

Измените параметр в секции [System]:

AuthPassword=XXX – где вместо «XXX» указать пароль Веб-администратора (по умолчанию принимает значение PPdpHgBg).