Руководство по эксплуатации Solar inView

Содержание

1 Общие сведения

1.1 Область применения

Solar inView – система разноуровневой аналитики и мониторинга эффективности средств и процессов SOC. Solar inView обеспечивает аккумулирование и анализ информации из разных подсистем безопасности и бизнес-систем с последующим её преобразованием и подачей в виде аналитических отчетов различного уровня детализации.

1.2 Краткое описание возможностей

Solar inView обеспечивает:

- анализ и представление данных, получаемых из бизнес-систем и систем обеспечения ИБ и ИТ (далее – системы-источники);
- централизованный контроль функционирования SOC (в том числе, в удаленных филиалах);
- использование различных типов объектов для визуализации отчетности (например, индикаторы, графики, диаграммы, таблицы).

2 Назначение ПО и условия выполнения программы

2.1 Назначение ПО

Solar inView предназначен для сбора, обработки и визуализации данных о состоянии информационной безопасности, поступающих от подключенных средств защиты информации, ИТ и бизнес систем (систем-источников).

Основные функции Solar inView:

- анализ и представление данных, получаемых из систем-источников;
- централизованный контроль функционирования SOC (в том числе, в удаленных филиалах);
- оценка результативности и эффективности подразделения SOC и процессов SOC.

2.2 Требования к программному обеспечению

2.2.1 Серверная часть

Для корректной работы Solar inView на серверном оборудовании должны быть установлены следующее программное обеспечение:

- Операционная система – Windows server 2012 или Linux;
- СУБД – PostgreSQL 16;
- WebServer – Tomcat 10;
- JAVA – OpenJDK 1.8 и другие версии выше.

Указанное программное обеспечение должно быть установлено перед началом работы с Solar inView. Описание его установки входит в документацию поставщиков ПО, а не в рамки данного документа.

2.2.2 Клиентское приложение

В состав программного обеспечения компьютера для АРМ пользователя Solar inView должна входить программа-клиент, предоставляющая пользователю возможность навигации и просмотра web-ресурсов (браузер). Рекомендуемые браузеры:

- Mozilla Firefox;
- Google Chrome.

Браузер должен быть установлен перед началом работы с Solar inView. Описание его установки входит в документацию поставщика ПО (браузера), а не в рамки данного документа.

Для корректной работы Solar inView рекомендуется в настройках браузера разрешить выполнение javascript и сохранение файлов cookies.

2.3 Требования к аппаратному обеспечению

2.3.1 Требования к серверному оборудованию

Для нормального функционирования Solar inView технические средства должны быть расположены на сервере, удовлетворяющем следующим минимальным требованиям:

- два восьми ядерных процессора Intel Core i8 x64 с тактовой частотой не ниже 2,0 ГГц;
- от 32 ГБ оперативной памяти;
- четыре жестких диска объемом 500 ГБ (в RAID1 с аппаратным RAID -контроллером);
- 1 порт Ethernet 10/100/1000.

2.3.2 Требования к АРМ администратора

АРМ администратора Solar inView должно быть оборудовано компьютером, обладающим следующими характеристиками:

- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой не менее 2 ГГц;
- объем оперативной памяти не менее 8 ГБ;
- объем жесткого диска не менее 100 ГБ;
- разрешение экрана при работе с управляющим интерфейсом от 1920x1080.

Кроме того, АРМ оператора Solar inView должно быть укомплектовано сетевым адаптером Ethernet.

2.3.3 Требования к АРМ пользователя

АРМ пользователя Solar inView должно быть оборудовано компьютером, обладающим следующими характеристиками:

- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой не менее 2 ГГц;
- объем оперативной памяти не менее 8 ГБ;
- объем жесткого диска не менее 100 ГБ;
- разрешение экрана при работе с управляющим интерфейсом от 1920x1080.

Кроме того, АРМ пользователя Solar inView должно быть укомплектовано сетевым адаптером Ethernet.

3 Выполнение программы

3.1 Основные принципы работы

3.1.1 Вход в систему

Для получения доступа в пользовательский интерфейс необходимо в адресной строке браузера ввести ссылку: «http://<ip-адрес хоста>:37799/webroot/security_dashboard» и нажать кнопку «Enter» (ip-адрес хоста задается администратором Solar inView).

На странице браузера появится окно для авторизации в Solar inView (см. Рис. 1).

Рис. 1 – Авторизация в Solar inView

Необходимо ввести логин и пароль пользователя, выданный системным администратором Solar inView.

При введении неверных идентификационных данных пользователю будет выдано сообщение об ошибке (см. Рис. 2).

Рис. 2 – Ошибка при вводе неверных идентификационных данных

Для того, чтобы завершить сессию пользователя необходимо кликнуть на иконку  в правом верхнем углу.

Сессия будет сброшена по таймауту по истечению 30 минут бездействия пользователя. После этого для того, чтобы продолжить работу с системой необходимо повторить процедуру входа.

3.1.2 Описания основных элементов интерфейса

Основные объекты, которые используются в Solar inView, представлены на Рис. 3.

Модель Solar inView – набор взаимосвязанных аналитических панелей.

Аналитическая панель (АП) – набор элементов (показателей и аналитических элементов), объединенных общей задачей.

Все элементы на АП разделяются на:

- индикаторы;
- диаграммы;
- графики,
- таблицы.

Элементы типа «Индикатор» отображают обобщенные показатели для оценки эффективности процессов управления и обеспечения ИБ. Такие показатели отображают срез на определенный момент времени и дают оценку сложившийся ситуации в качественных характеристиках (изменение цвета показателя говорит о переходе его значения в другую зону: красный – плохо, желтый – средне, зеленый – хорошо), пример см. на Рис. 3.

Элементы типа «Диаграмма» отображают аналитические показатели, предназначенные для мониторинга общего состояния ИБ и получения большей информации о значениях индикаторов. Диаграммы могут быть представлены в виде круговых диаграмм, гистограмм и др. (пример см. на Рис. 3).

Элементы типа «График» отображают статистику изменения какого-либо параметра во времени (пример см. на Рис. 3).

Элемент типа «Таблица» представляет собой совокупную информацию по всем показателям эффективности и аналитическим элементам и предназначен для получения наиболее полной информации по интересующим пользователя показателям (пример см. на Рис. 3).

Фильтры позволяют быстро выбрать нужные параметры для отображения. Если в различных АП данные совпадают по месяцу либо году, то фильтрация будет выполнена по всем элементам таких АП. По умолчанию в фильтрах не выбрано ни одного значения (пример см. на Рис. 4).

1 - индикаторы 2 и 4- графики 3 - диаграмма 5 - таблица

Рис. 3 – Основные элементы интерфейса

Рис. 4 – Основные элементы интерфейса. Фильтры

3.1.3 Фильтрация данных

Фильтрация данных в системе осуществляется путем выбора интересующего значения на элементах АП и/или с помощью панели фильтрации.

Панель фильтрации находится в верху страницы. Панель фильтрации состоит из (Рис. 5):

– набор фильтров, доступных для текущей АП;

– кнопка «Очистить фильтры».

Для того, что провести фильтрацию данных необходимо выбрать левой кнопкой мыши одно или несколько значений в фильтре(ах). После этого данные на всех вкладках перестроятся в соответствии с сделанным выбором (см. Рис. 5).

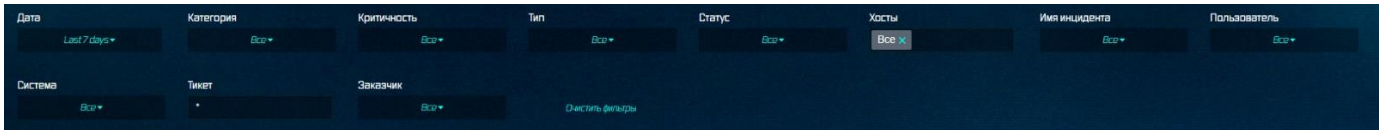

Рис. 5 – Фильтрация данных

Очистить выбор пользователя можно нажав на кнопку «Очистить фильтры».

Снять выбор одного или нескольких значений можно кликнув левой кнопкой мыши крестик рядом со значениями, выбор которых необходимо отменить.

Также сбросить все значения конкретного фильтра можно в поле фильтра нажав на рядом со значением.

Пример отображения фильтра см. Рис. 6.

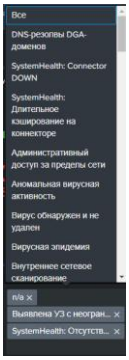

Рис. 6 – Пример работы фильтра

3.2 Использование Solar inView

Для каждого подключаемого СЗИ, ИТ- или бизнес-системы разрабатываются АП, которые позволяют контролировать процессы управления и обеспечения ИБ, автоматизируемые подключаемыми источниками.

Примеры отображения данных для источников приведены на Рис. 8, Рис. 9, **Ошибка! Источник ссылки не найден.**.

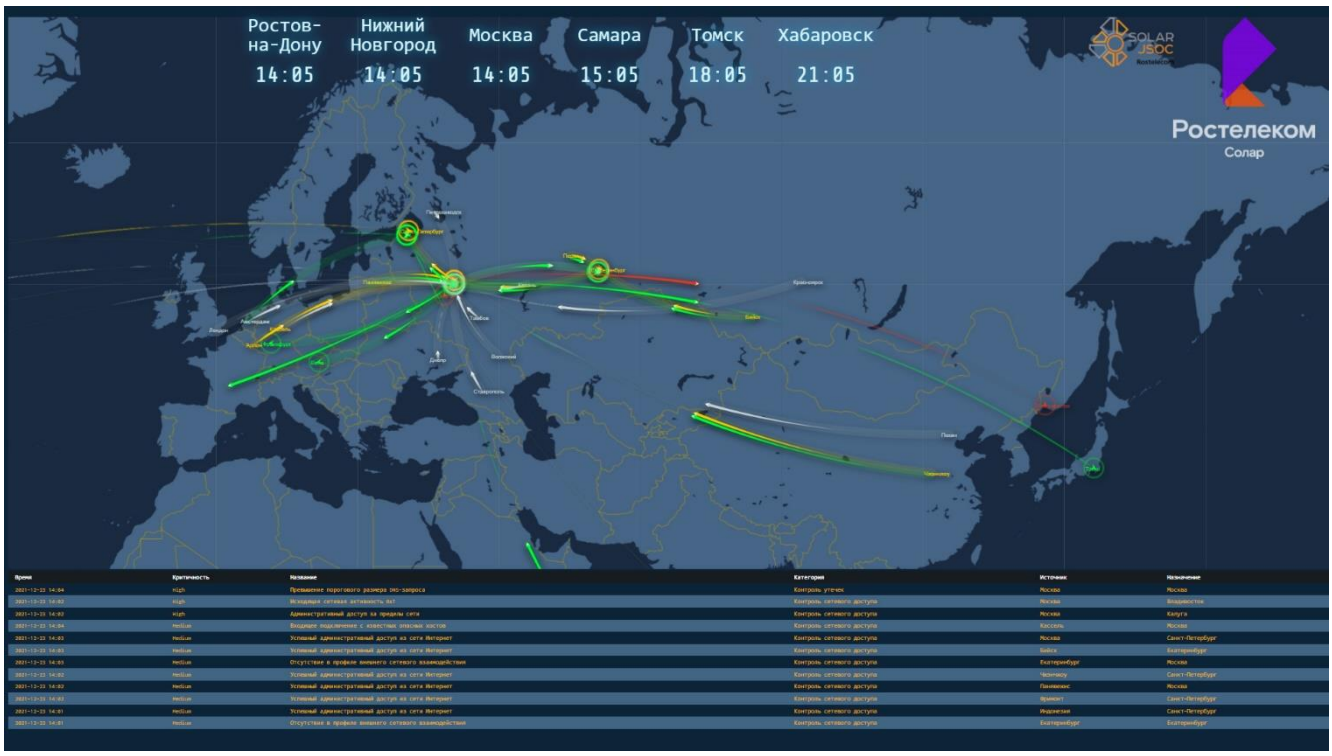

Рис. 7 – Аналитическая панель «Мониторинг кибератак»

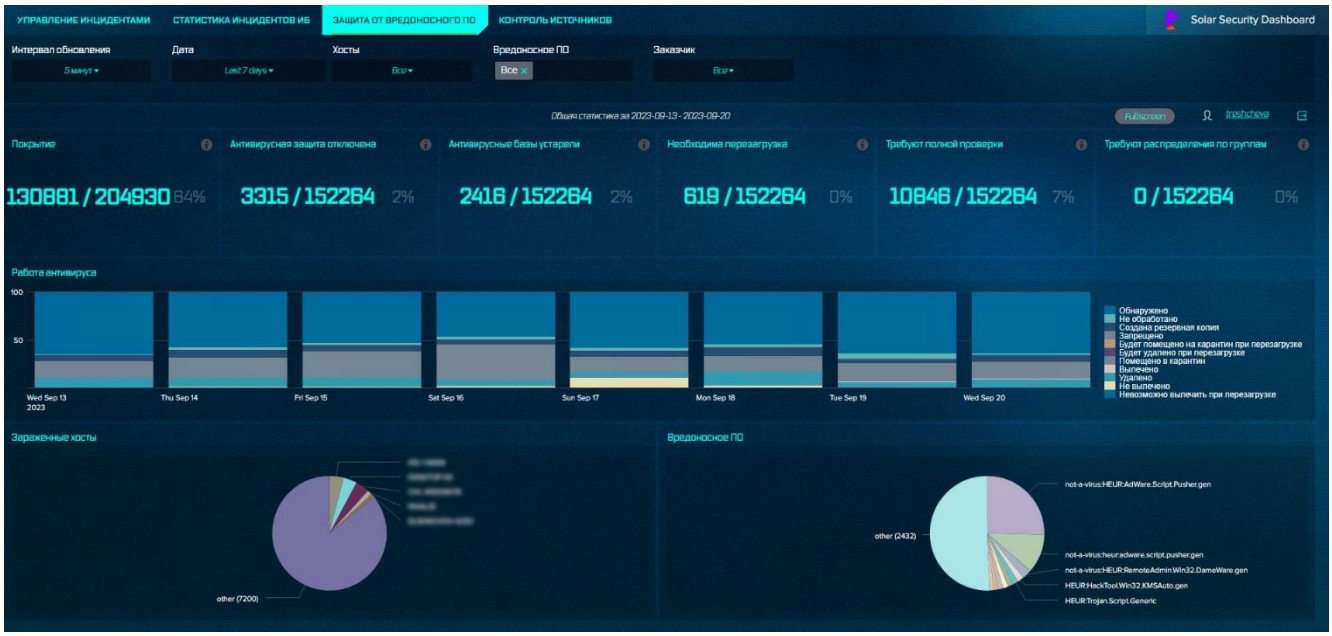

Рис. 8– Аналитическая панель «Защита от ВПО»

Рис. 9– Аналитическая панель «Управление инцидентами»

4 Подсистема нормативно-справочной информации

Для получения доступа в интерфейс подсистемы нормативно-справочной информации (НСИ) необходимо выбрать в выпадающем меню «Настройки» пункт «Система НСИ».

Примечание. Доступ к системе НСИ имеют только пользователи с правами аналитика.

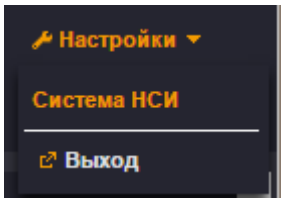

Рис. 10 – Переход к подсистеме нормативно-справочной информации

В системе НСИ есть набор справочников доступных для редактирования (Рис. 11)

Рис. 11 – Справочники

Для редактирования элементов справочника необходимо нажать кнопку «Редактировать»  напротив соответствующего элемента. После появится диалоговое окно, в котором отображены все доступные для редактирования атрибуты элемента (Рис. 12).

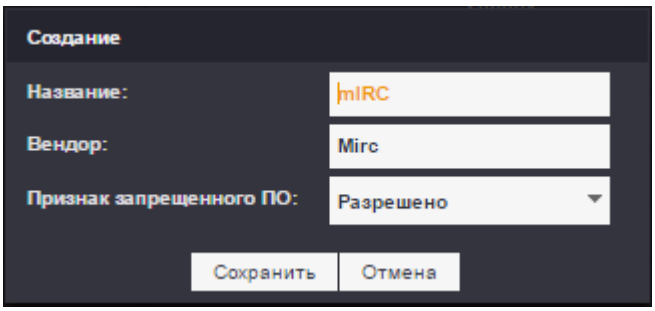

Рис. 12 – Редактирование элементов справочника

5 Интерфейс администрирования

5.1 Вход в систему

Для получения доступа в интерфейс администрирования необходимо в адресной строке браузера ввести ссылку: «http://<ip-адрес хоста, на котором установлена Solar inView>:8080/admin/» и нажать кнопку «Enter».

На странице браузера появится окно для авторизации в Solar inView (см. Рис. 1).

Рис. 13 – Авторизация в Solar inView

Необходимо ввести логин и пароль администратора, выданный системным администратором Solar inView.

Примечание. При установке системы по умолчанию созданы два пользователя: администратор Solar inView (admin/password) и пользователь (user/password). После первого входа в систему для данных учетных записей должны быть изменены пароли либо указанные учетные записи должны быть удалены после создания новых. Описание процесса создания нового пользователя/изменения пароля пользователя приведено в разделе 5.2 настоящего документа.

При введении неверных идентификационных данных администратору будет выдано сообщение об ошибке (см. Рис. 2).

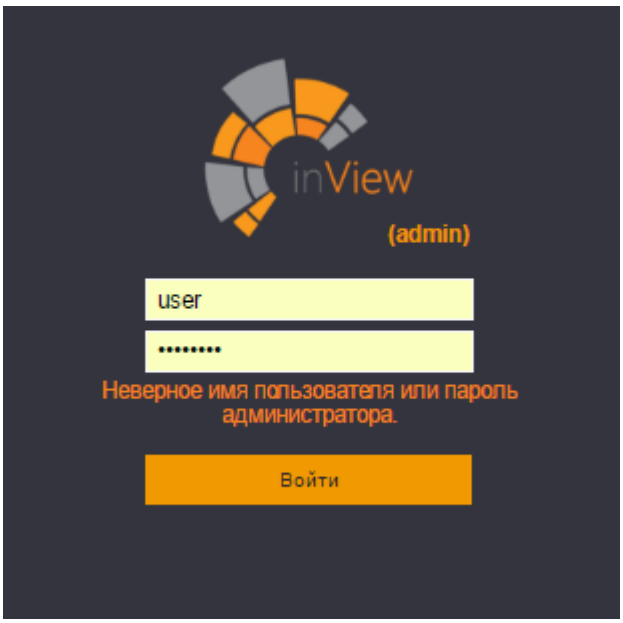

Рис. 14 – Ошибка при вводе неверных идентификационных данных

Для того, чтобы завершить сессию администратора необходимо выбрать в выпадающем меню «Настройки» пункт «Выход» (см. **Ошибка! Источник ссылки не найден.**).

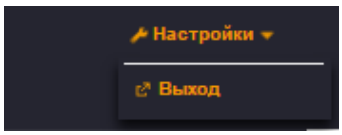

Рис. 15 – Выход из Solar inView

Сессия будет сброшена по таймауту по истечению 30 минут бездействия администратора. После этого для того, чтобы продолжить работу с системой необходимо повторить процедуру входа.

5.2 Управление учетными записями пользователей

5.2.1 Добавление пользователя

Для того, чтобы добавить нового пользователя Solar inView необходимо перейти на вкладку «Пользователи» (см. **Рис. 16**). На данной вкладке будет представлен перечень всех пользователей, имеющих доступ к Solar inView.

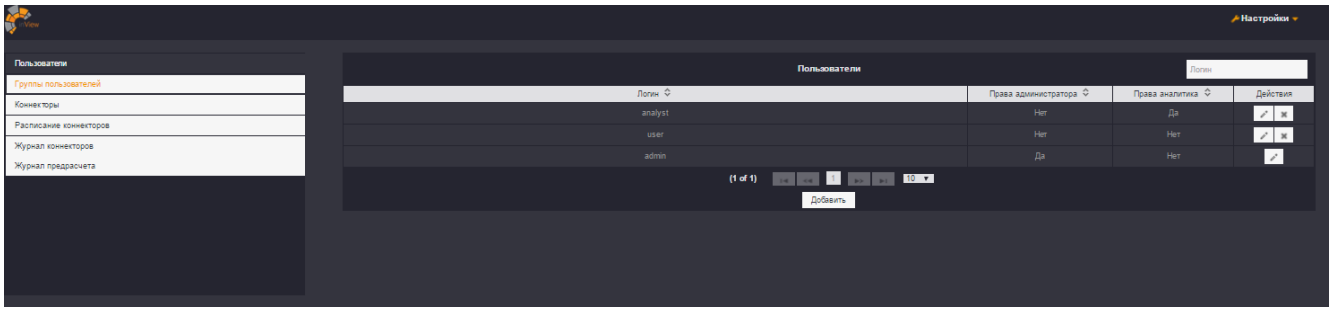

Рис. 16 – Вкладка «Пользователи»

Для того, чтобы добавить нового пользователя необходимо нажать кнопку «Добавить» и в открывшимся диалоговом окне ввести имя учетной записи в поле «Логин», задать пароль и при

необходимости, добавить пользователю права администратора или аналитика. После чего нажать кнопку добавить (см. Рис. 17).

Примечание 1. Права администратора устанавливаются в том случае, если создаваемый пользователь должен иметь административные полномочия в Solar inView.

Примечание 2. Права аналитика устанавливаются в том случае, если создаваемый пользователь должен иметь возможность работать с нормативно-справочной информацией.

Примечание 3. Для ввода пароля учетной записи администратору необходимо пригласить пользователя, для которого создается учетная запись, и попросить его лично ввести новый пароль.

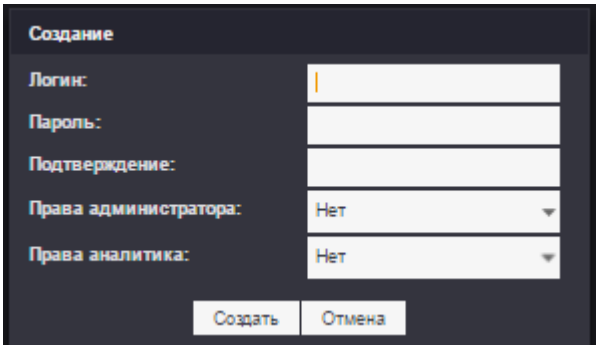

Рис. 17 – Добавление нового пользователя

Использование одинаковых логинов для учетных данных запрещено. В случае ввод уже используемого имени учетной записи администратору будет выдано сообщение об ошибке (см. Рис. 18.).

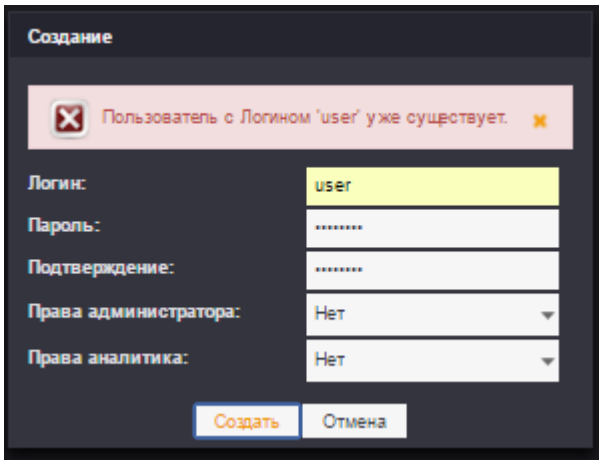

Рис. 18 – Ошибка при вводе логина пользователя

В случае если введенный пароль содержит менее 6 или более 20 символов, администратору будет выдано сообщение об ошибке (см. Рис. 19).

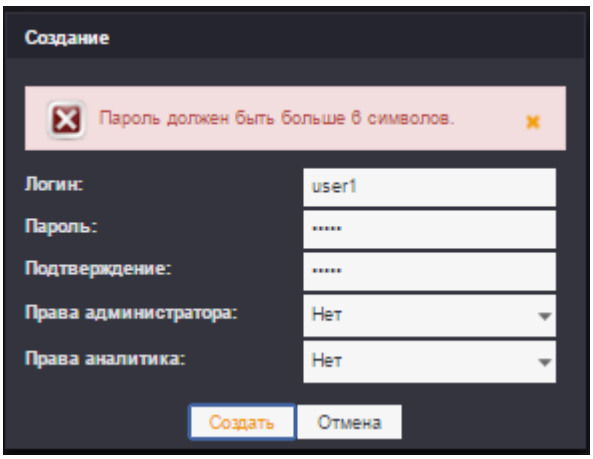

Рис. 19 – Ошибка при вводе пароля

Если все учетные данные введены верно, то новый пользователь появится в общем перечне (см. Рис. 20).

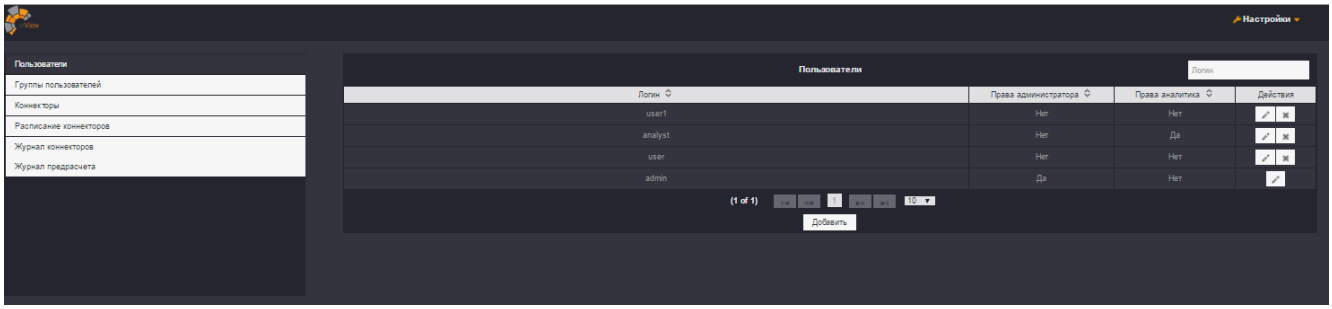

Рис. 20 – Успешное добавление нового пользователя

5.2.2 Редактирование и удаление учетной записи

Для того, чтобы изменить параметры учетной записи необходимо нажать кнопку «Редактировать»  напротив учетной записи, параметры которой необходимо изменить (см. Рис. 21).

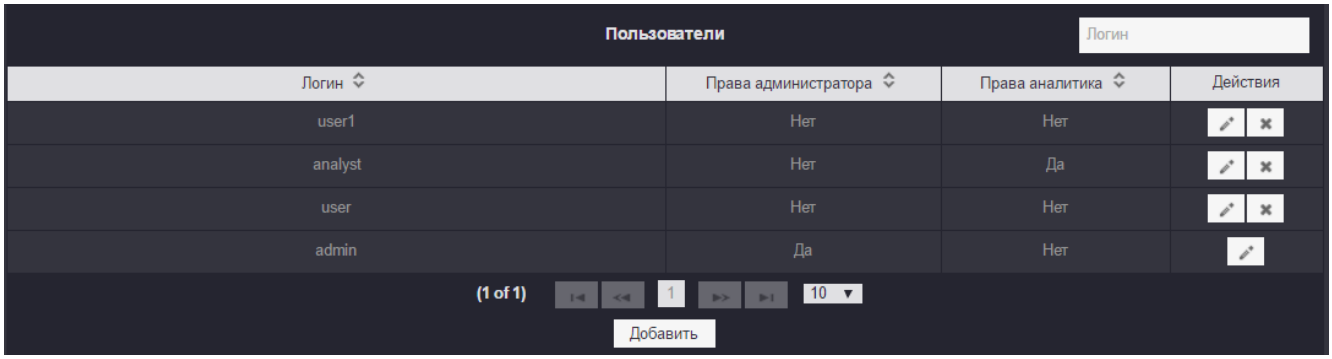

Рис. 21 – Редактирование учетной записи (шаг 1)

В поле «Добавление нового пользователя» появятся параметры выбранной для редактирования учетной записи (см. Рис. 22).

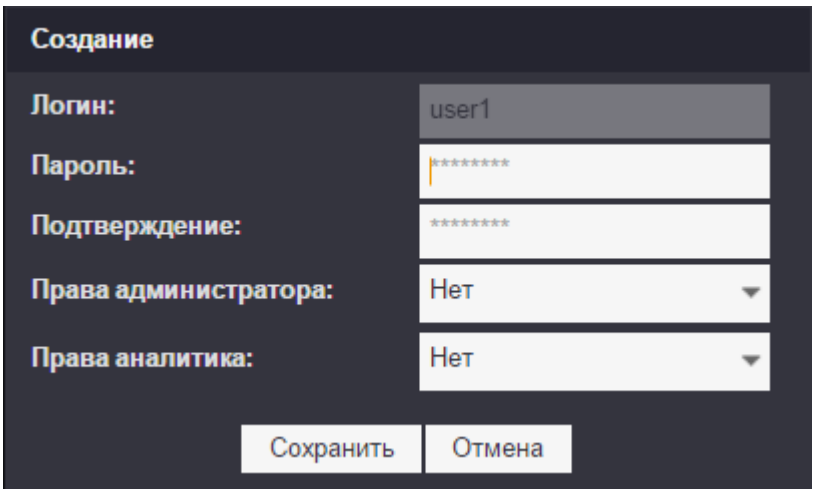

Рис. 22 – Редактирование учетной записи (шаг 2)

Далее необходимо изменить те параметры, которые требуется, и нажать кнопку «Сохранить».

В случае если меняются только параметры «Логин» и/или «Флаг «Админ», при нажатии кнопки «Сохранить» пароль пользователя остается прежним.

Для изменения пароля учетной записи пользователя администратору необходимо пригласить пользователя, учетная запись которого подлежит изменению, и попросить его лично ввести новый пароль. После введения нового пароля он будет изменен в Solar inView после нажатия кнопки «Сохранить».

Для того, чтобы удалить учетную запись необходимо нажать кнопку «Удалить» напротив соответствующей учетной записи (см. Рис. 23).

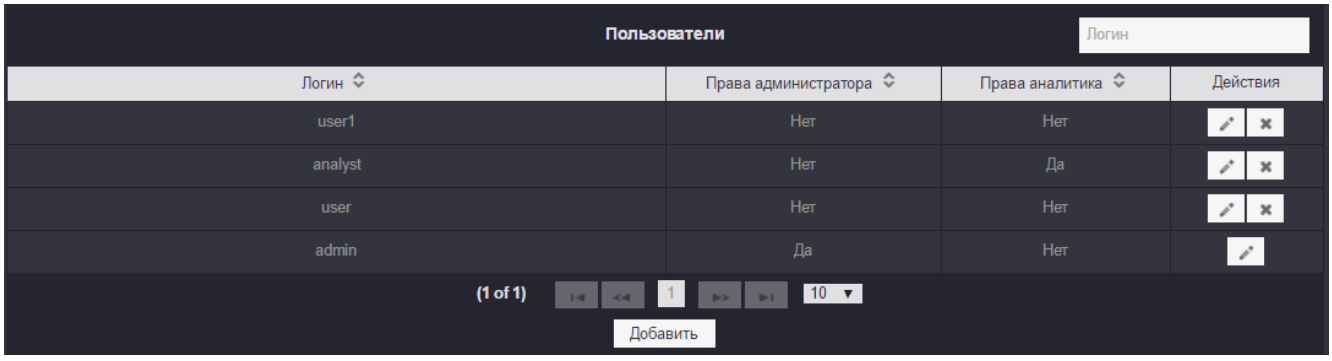

Рис. 23 – Удаление учетной записи

После этого учетная запись пользователя будет удалена из системы и перестанет отображать в перечне пользователей, имеющих доступ к Solar inView.

5.3 Подключение систем-источников

5.3.1 Общие положения

Управление коннекторами к системам-источникам осуществляется на вкладке «Коннекторы» (см. Рис. 24). К системе могут быть подключены следующие системы-источники:

- AD (источник справочных данных о сотрудниках организации);
- SIEM (ArcSight, MP SIEM, Kuma - источники информации о событиях ИБ);
- SAP (источник событий безопасности, обнаруженных в SAP);
- Другие источники необходимые для реализации дашбордов.

Перечень подключенных коннекторов приведен на вкладке «Коннекторы» (см. Рис. 24).

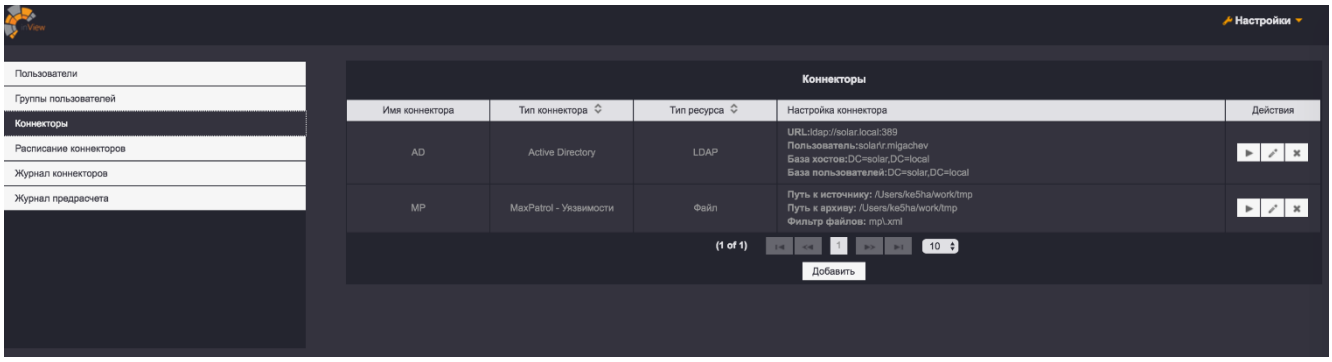

Рис. 24 – Вкладка «Коннекторы»

5.3.2 Подключение, редактирование и удаление коннектора

Для подключения коннектора необходимо в форме «Коннекторы» нажать кнопку «Добавить» и внести параметры подключения (см. **Ошибка! Источник ссылки не найден.**).

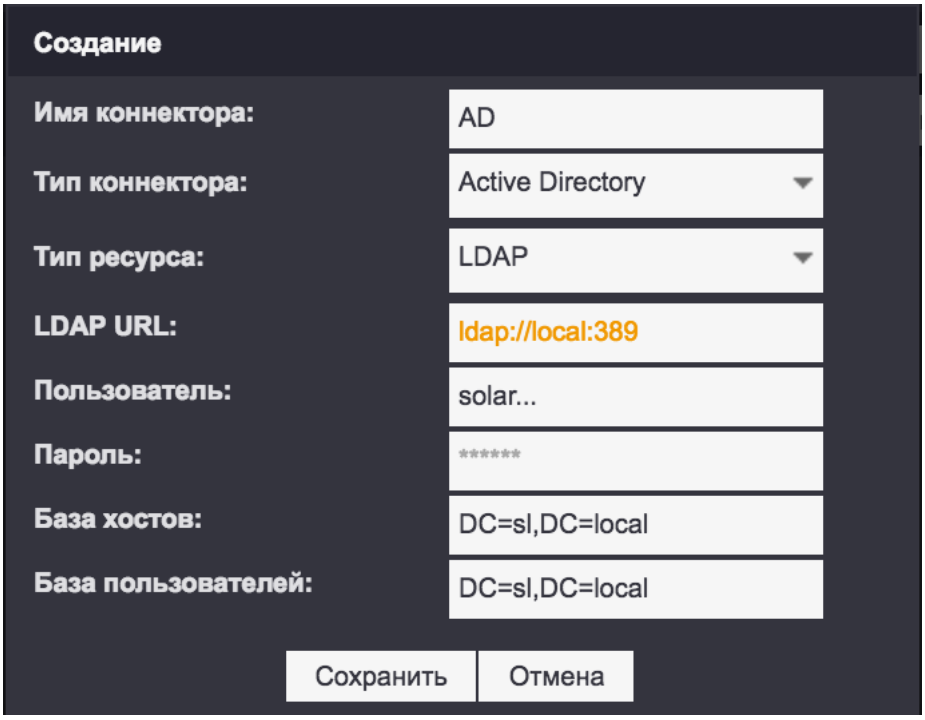

Рис. 25 – Подключение коннектора типа «БД/LDAP»

Если настройки подключения будут введены некорректно, то администратору будет выдано сообщение об ошибке (см. Рис. 26).

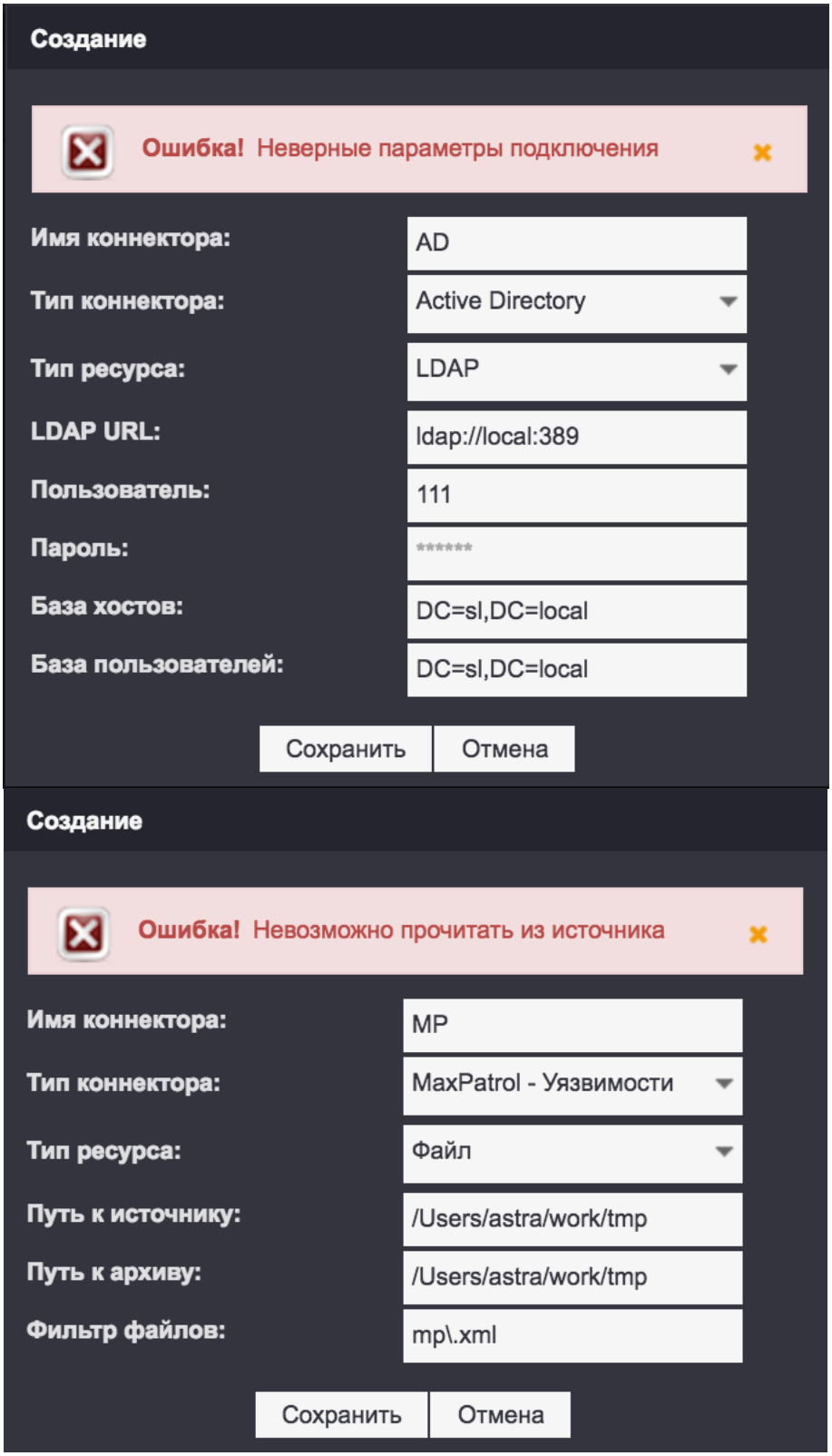

Рис. 26 – Ошибка при указании неверного пути к исходным данным

При попытке добавить коннектор, который в системе уже существует, администратору будет выдано соответствующее сообщение.

Для редактирования коннектора необходимо нажать кнопку «Редактировать» напротив соответствующего коннектора. После этого откроется диалоговое окно с настройками

коннектора (см. **Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**).

Для того, чтобы отключить коннектор необходимо нажать кнопку «Удалить» напротив соответствующего коннектора. После коннектор удаляется из системы и данные от системы-источника, к которой относился коннектор, более не обрабатываются/не обновляются в Solar inView.

Для того, чтобы принудительно обновить данные от коннектора необходимо нажать кнопку «Запустить» напротив соответствующего коннектора. После коннектор будет добавлен в очередь на обработку.

5.3.3 Расписание выполнения коннекторов

Для настройки автоматического запуска коннекторов, необходимо перейти на вкладку «Расписание коннекторов» (Рис. 27).

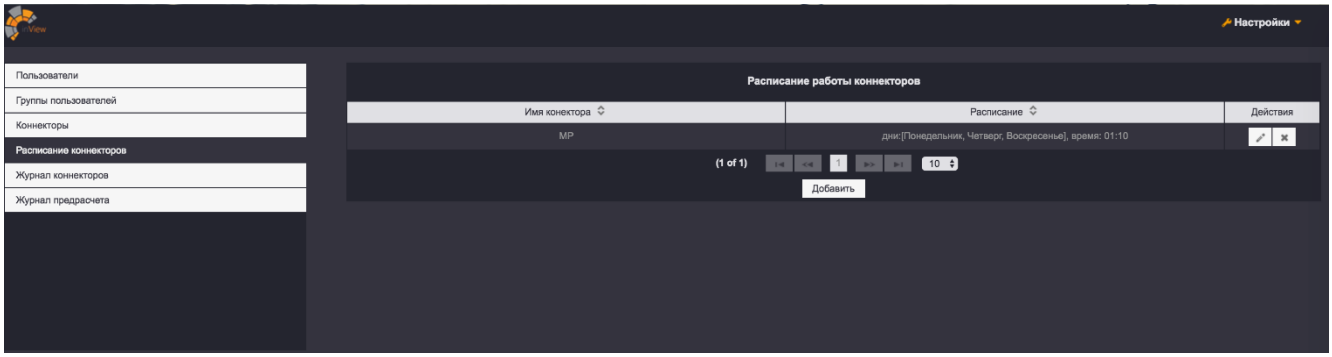

Рис. 27 – Вкладка «Расписание коннекторов»

Для добавления расписание необходимо нажать на кнопку «Добавить», после чего появится диалоговое окно, в котором необходимо задать параметры задачи на обновление данных (Рис. 28).

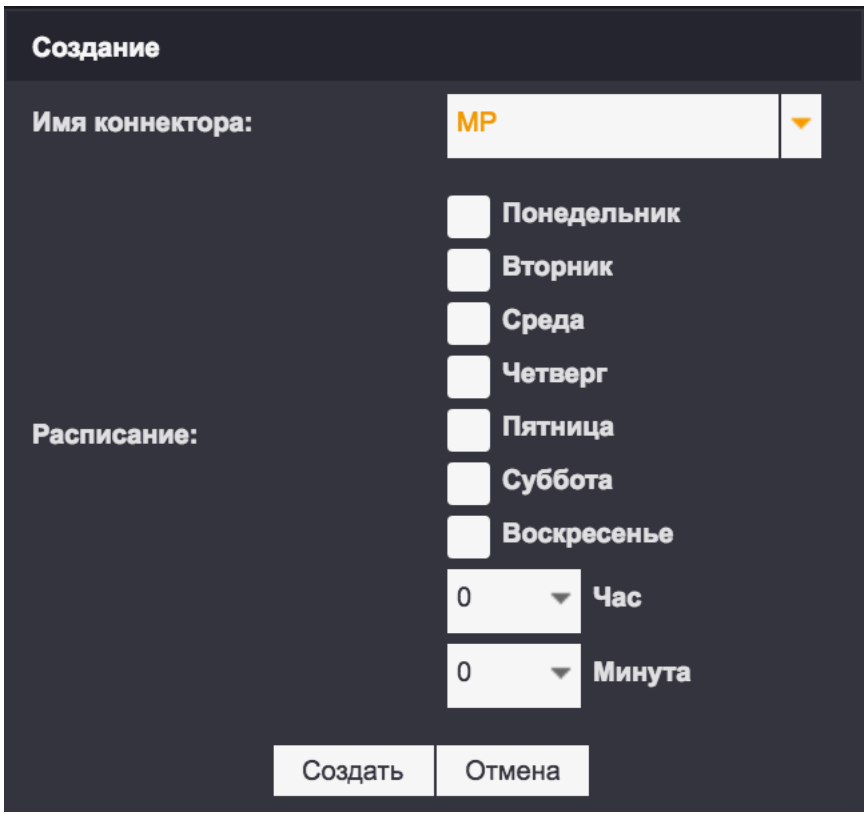

Рис. 28 – Создание задачи на обновление данных от коннектора

5.3.4 Журнал коннекторов

Все коннекторы после постановки задачи на автоматическое обновление или запуска вручную ставятся в очередь на обработку (Рис. 29).

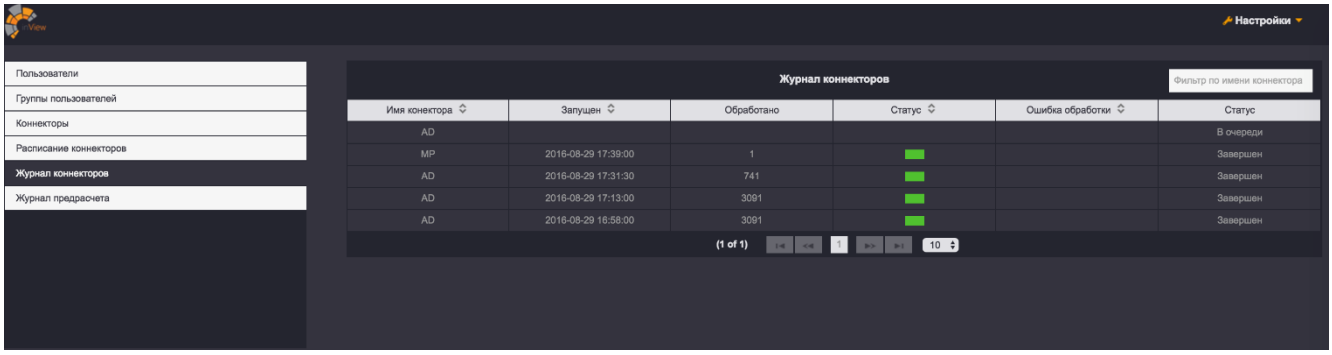

Рис. 29 – Очередь обработки коннекторов

6 Перечень принятых сокращений

АП	Аналитическая панель
АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
ПО	Программное обеспечение