



**АО ТРЭИ**

---

**Unimod PRO**  
**версия 2**

**Руководство администратора**

RU.TREI.00010-01 31 02-1



---

© 2023 АО ТРЭИ.

Россия,

440028, Пенза,

ул. Титова, 1Г

Тел: +7(8412)49-95-39

е-mail: [tr-penza@trei.biz](mailto:tr-penza@trei.biz)

<http://www.trei.biz>

---

**СОДЕРЖАНИЕ**

<b>ВВЕДЕНИЕ .....</b>	<b>5</b>
<b>1. ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫЕ МЕРЫ .....</b>	<b>6</b>
1.1 ПРОЦЕДУРЫ ПОСТАВКИ .....	6
1.1.1 <i>Общий порядок поставки</i> .....	6
1.1.2 <i>Комплектность упаковки</i> .....	6
1.1.3 <i>Процедуры и меры безопасности при распространении ОО к месту назначения</i> .....	6
1.1.3.1 <i>Контроль целостности программного обеспечения компонентов ОО</i> .....	6
1.1.3.2 <i>Контроль целостности файлов установочного диска</i> .....	6
1.1.3.3 <i>Контроль сохранности упакованного комплекта</i> .....	7
1.1.3.4 <i>Поддержка безопасности доставки</i> .....	7
1.2 ТРЕБОВАНИЯ БЕЗОПАСНОСТИ К СРЕДЕ ИТ .....	7
<b>2. СТРУКТУРА ПРОГРАММЫ .....</b>	<b>8</b>
2.1 КОМПОНЕНТ КОНФИГУРАЦИИ КОНТРОЛЛЕРА .....	8
2.2 КОМПОНЕНТ ЗАГРУЗКИ КОНФИГУРАЦИИ OPC СЕРВЕРА .....	8
2.3 ГРАФИЧЕСКИЙ ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС (GUI) .....	8
2.4 ГРАФИЧЕСКИЙ РЕДАКТОР ДЛЯ ЯЗЫКОВ FBD/LD .....	9
2.5 ГРАФИЧЕСКИЙ РЕДАКТОР ДЛЯ ЯЗЫКА ST .....	9
2.6 КОМПОНЕНТ МОДЕЛИ ДАННЫХ ПРОЕКТА И СИСТЕМНОЙ БИБЛИОТЕКИ .....	10
2.7 МЕНЕДЖЕР ВЗАИМОДЕЙСТВИЯ МЕЖДУ ПРОГРАММНЫМИ КОМПОНЕНТАМИ .....	10
2.8 КОМПОНЕНТ АУТЕНТИФИКАЦИИ И РАЗГРАНИЧЕНИЯ ДОСТУПА .....	10
2.9 КОМПОНЕНТ ЭМУЛЯЦИИ ВЫПОЛНЕНИЯ ТЕХНОЛОГИЧЕСКОГО ПРИЛОЖЕНИЯ .....	11
2.10 КОМПОНЕНТ СВЯЗИ С КОНТРОЛЛЕРОМ И ОТЛАДКИ ТЕХНОЛОГИЧЕСКОГО ПРИЛОЖЕНИЯ В РЕАЛЬНОМ ВРЕМЕНИ .....	11
2.11 КОМПОНЕНТ ГРАФИЧЕСКИХ ИНТЕРФЕЙСОВ ОТЛАДЧИКА .....	12
2.12 КОМПИЛЯТОР .....	12
2.13 КОМПОНЕНТ РЕДАКТИРОВАНИЯ НАСТРОЕК .....	12
2.14 КОМПОНЕНТ ПРИЕМА КОНФИГУРАЦИИ OPC СЕРВЕРА .....	12
2.15 КОМПОНЕНТ OPC UA СЕРВЕРА .....	13
<b>3. НАСТРОЙКА ПРОГРАММЫ .....</b>	<b>14</b>
3.1 СИСТЕМНЫЕ ТРЕБОВАНИЯ .....	14
3.2 УСТАНОВКА И УДАЛЕНИЕ В ОС «ASTRA LINUX» .....	14
3.3 ОПИСАНИЕ СТАРТА И ПРОЦЕДУРА ПРОВЕРКИ ПРАВИЛЬНОСТИ СТАРТА .....	16
3.4 О ПРОГРАММЕ .....	17
<b>4. НАСТРОЙКА ПОДСИСТЕМЫ БЕЗОПАСНОСТИ .....</b>	<b>17</b>
4.1 ОБЩИЕ СВЕДЕНИЯ .....	17
4.2 ЗАЩИЩЕННЫЙ РЕЖИМ .....	18
4.3 СМЕНА ПАРОЛЯ .....	23
4.4 РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ .....	23

## Введение

**Unimod PRO** – является инструментальной системой, которая предназначена для конфигурирования промышленных контроллеров серии **TREI-5B** и разработки технологических приложений на языках стандарта МЭК 61131-3 (ST, FBD, LD). **Unimod PRO** включает в себя набор компонент для обеспечения процесса подготовки исходного кода технологической программы, описания связей переменных с их физическими представлениями (каналами ввода-вывода), компиляции, загрузки и отладки приложения.

В состав инструментальной системы **Unimod PRO** входят средства и компоненты, при помощи которых возможно выполнение следующих действий:

- структурирование данных технологического приложения;
- описание технологической задачи в графическом виде на языках FBD/LD;
- описание технологической задачи в текстовом виде на языке ST;
- использование встроенной библиотеки функций;
- проверка синтаксиса и компиляции технологической программы;
- эмуляция выполнения технологического приложения;
- загрузка технологического проекта в контроллер;
- отладка технологического приложения в реальном времени;
- создание конфигурации контроллера и OPC-сервера;
- диагностика и калибровка аппаратных средств контроллера;
- аутентификация и разграничение доступа к возможностям системы;
- сбор статистики о работе системы;
- экспорт и импорт данных;
- сохранение и редактирование технологического проекта;
- использование защищенных каналов связи.

Документ предназначен для ознакомления потребителей с технической информацией о инструментальной системе «**Unimod PRO версии 2**» (далее по тексту – ОО (объект оценки)) и содержит общие сведения об ОО, организационно-распорядительные меры, сведения о структуре ОО и описание настроек ОО.

**1. Организационно-распорядительные меры****1.1 Процедуры поставки****1.1.1 Общий порядок поставки**

При поставке ОО заказчику от среды производства до среды установки АО «ТРЭИ» (далее Разработчик) выполняет следующие действия:

- расчет контрольных сумм файлов программного обеспечения ОО;
- упаковка комплекта поставки;
- передача упакованного комплекта поставки на склад готовой продукции;
- выдача упакованного комплекта поставки уполномоченному представителю заказчика.

**1.1.2 Комплектность упаковки**

Упаковка в общем случае содержит следующие комплектующие:

1. носитель с образом программного обеспечения;
2. формуляр на ОО;
3. руководство администратора.

**1.1.3 Процедуры и меры безопасности при распространении ОО к месту назначения**

Процедуры и меры безопасности при распространении ОО к месту назначения решают следующие задачи:

- обеспечивают идентификацию и целостность ОО во время пересылки;
- обеспечивают обнаружение несанкционированных модификаций ОО;
- препятствуют попыткам подмены ОО от имени разработчика.

**1.1.3.1 Контроль целостности программного обеспечения компонентов ОО**

Расчет эталонных контрольных сумм файлов программного обеспечения компонентов ОО осуществляется на этапе сборки и выполняется сторонним ПО (ФИКС-UNIX 1.0 Программа фиксации и контроля целостности информации сертификат ФСТЭК № 680, действительный до 26 февраля 2026 г).

**1.1.3.2 Контроль целостности файлов установочного диска**

Перечень файлов, записанных на установочный компакт-диск, а также их контрольные суммы содержатся в формуляре на ОО, входящего в комплект поставки.

### **1.1.3.3 Контроль сохранности упакованного комплекта**

Комплект ОО упаковывают в пластиковый пакет, помещают в картонную коробку и заклеивают коробку скотчем с символикой АО «ТРЭИ». Упакованный комплект хранится на складе готовой продукции, оснащенном охранной сигнализацией.

### **1.1.3.4 Поддержка безопасности доставки**

Доставка готовой продукции к месту назначения осуществляется силами разработчика. Выдача ОО уполномоченному представителю заказчика осуществляется на основании документов, удостоверяющих полномочия представителя. Передача ОО заказчику подтверждается актом сдачи-приемки ОО, на котором проставляются подписи и печати сторон.

## **1.2 Требования безопасности к среде ИТ**

ОО обеспечивает функциональное назначение при реализации пользователем следующих предварительных организационно-распорядительных мер:

- обеспечение сохранности оборудования и физической целостности системных блоков компьютеров;
- ведение журнала учета работы компьютеров, проведения регламентных мероприятий и внесения изменений в конфигурацию технических и программных средств;
- реализация мероприятий по антивирусной защите и обеспечение свободной от вирусов программной среды компьютеров.

К среде ИТ, в которой функционирует ОО, предъявляются следующие требования безопасности, относящиеся к пользователю:

- обеспечение регламентация запрета доступа непривилегированных пользователей из внешней сети в защищаемые сети по всем типам протоколов, за исключением специально созданной для такого доступа сети;
- обеспечение установки, конфигурирования и управления ОО в соответствии с эксплуатационной документацией;
- обеспечение поддержки средств аудита, используемых в ОО.

## 2. Структура программы

Программа **Unimod PRO** имеет событийно-ориентированную архитектуру. Спецификой является то, что запуск в работу основных компонентов системы выполняется при инициации человеком-пользователем управляющих элементов графического интерфейса GUI. Программа состоит из функциональных компонентов, описанных в следующих разделах. Компонент программы может реализовать одно или несколько функциональных требований к программе.

### 2.1 Компонент конфигурации контроллера

Компонент реализует:

- возможность задания параметров связи с контроллером;
- возможность задания параметров линий Ethernet;
- возможность задания параметров последовательных линий;
- возможность задания параметров связи с модулями ввода-вывода;
- возможность задания параметров компонентов исполнительной системы;
- блокировку ввода недопустимых значений параметров.

### 2.2 Компонент загрузки конфигурации OPC сервера

Компонент реализует:

- блокировке загрузки при наличии ошибок в технологическом приложении;
- возможность задания параметров связи с OPC сервером;
- возможность считывания и отображения текущего состояния OPC сервера:
  - атрибуты загруженного приложения (имя проекта, дата, версия, контрольная сумма);
  - состояние выполнения (выполняется, остановлено, причина остановки);
- возможность обнаружения и показа различий в словаре проектов: текущего и загруженного.

### 2.3 Графический пользовательский интерфейс (GUI)

Компонент реализует:

- многооконный режим работы;
- система меню и иконок быстрого доступа;
- табличное и древовидное представление данных;
- возможность селекции отображаемой информации;
- возможность создания, удаления, копирования данных;



- возможность отмены и повтора изменений;
- элементы управления поддерживают работу с мышью и клавиатурой;
- предупредительные сообщения о выполнении ответственных операций (удаление, загрузка изменений и т.п.).

## 2.4 Графический редактор для языков FBD/LD

Компонент реализует:

- возможность произвольной расстановки графических элементов LD и FBD по выбору пользователя в едином графическом поле;
- соединительные линии проводятся автоматически после выбора оператором элемента-источника и элемента-приемника линии:
  - выбор графического элемента-источника и элемента-приемника соединительной линии может выполняться как отдельными кликами мыши, так и в режиме "нажал-переместил";
  - отмеченные источник и приемник еще не построенной линии, должны отображаться специальным графическим элементом;
  - в режиме проводки соединительных линий, при движении мыши, элементы схемы, для которых допустимо быть либо источником или приемником линии, должны отображаться специальным графическим элементом;
  - соединительные линии должны проводиться только по линиям "сетки";
  - в соединительной линии должно быть не более 5 звеньев;
- возможность автоматической адаптации размеров графических элементов под длину текстовых надписей (имена контактов, переменных и т.п.). Допускается ограничение количества отображаемых символов до некоего предела, задаваемого опционально;
- в режиме эмуляции (отладки) должны показываться как имена элементов, так и текущие значения;
- возможность вставки элементов (операций) языков FBD/LD;
- возможность вставки элементов из глобального и локального словаря;
- возможность автоматического создания экземпляров библиотечных типов;
- возможность отмены и повтора изменений;
- поддержка всех допустимых типов данных.

## 2.5 Графический редактор для языка ST

Компонент реализует:

- возможность вставки элементов (операций) языка ST;
- возможность вставки элементов из глобального и локального словаря;
- возможность автоматического создания экземпляров библиотечных типов;
- возможность отмены и повтора изменений.

## 2.6 Компонент модели данных проекта и системной библиотеки

Компонент реализует:

- возможность сохранения проекта в виде набора файлов;
- возможность сохранения проекта в виде архива;
- автоматический контроль целостности проекта;
- автоматическое настраиваемое сохранение копий во время работы;
- возможность отмены изменений;
- библиотеку математических функций;
- библиотеку тригонометрических функций;
- библиотеку логических функций;
- библиотеку функций преобразования данных;
- библиотеку функций работы с файлами (портами);
- библиотеку функций работы со временем;
- библиотеку функций автоматического регулирования;
- библиотеку функций реализации протоколов обмена (modbus, и т.п.)
- библиотеку функций расчета свойств газа, жидкости.

## 2.7 Менеджер взаимодействия между программными компонентами

Менеджер отвечает за взаимодействие между всеми компонентами для корректного выполнения всех функциональных требований системой в целом.

## 2.8 Компонент аутентификации и разграничения доступа

Компонент реализует:

- возможность задания пользователя, его пароля и прав доступа:
  - для просмотра технологического приложения;
  - для изменения технологического приложения;
  - для просмотра конкретной программы или библиотечной функции;
  - для изменения конкретной программы или библиотечной функции;
  - для компиляции и загрузки приложения в контроллер;
  - для диагностики контроллера;

- для изменения значений выходов контроллера;
- для калибровки измерительных каналов контроллера;
- для изменения параметров сбора статистики;
- блокировку недопустимых действий пользователя;
- запись в журнал о фактах аутентификации пользователя в системе.

## 2.9 Компонент эмуляции выполнения технологического приложения

Компонент реализует:

- возможность эмуляции выполнения технологического приложения программными средствами (кроме обмена с модулями ввода-вывода);
- возможность перевода графического интерфейса пользователя в режим эмуляции:
  - показ текущих значений переменных в словаре;
  - показ текущих значений переменных в редакторе FBD/LD;
  - показ текущих значений переменных в редакторе ST;
- возможность отладки приложения:
  - перевод в поцикловый режим эмуляции;
  - перевод в режим эмуляции реального времени;
  - изменение текущих значений переменных;
  - задание точек останова;
  - просмотр значений избранных переменных в отдельном окне;
- запрет редактирования кода приложения.

## 2.10 Компонент связи с контроллером и отладки технологического приложения в реальном времени

Компонент реализует:

- возможность перевода графического интерфейса пользователя в режим отладки технологического приложения на контроллере:
  - показ текущих значений переменных в словаре;
  - показ текущих значений переменных в редакторе FBD/LD;
  - показ текущих значений переменных в редакторе ST;
- возможность отладки приложения:
  - перевод в поцикловый режим эмуляции;
  - перевод в режим эмуляции реального времени;
  - изменение текущих значений переменных;

- задание точек останова;
- просмотр значений избранных переменных в отдельном окне;
- запрет редактирования кода приложения.
- запись в статистику о факте подключения отладчика к контроллеру.

### 2.11 Компонент графических интерфейсов отладчика

Компонент реализует:

- возможность обнаружения и показа различий в словаре проектов: текущего и загруженного;
- возможность задания начальных значений для переменных загружаемого приложения;
- возможность загрузки только исполняемой части технологического проекта;
- возможность загрузки полного технологического проекта (с исходными текстами программ);
- диагностика процесса загрузки;
- визуализация результата загрузки приложения;
- возможность отката на предыдущую версию приложения в случае сбоя в загрузке.

### 2.12 Компилятор

Компонент реализует:

- возможность компиляции в интерпретируемый код (TIC);
- возможность компиляции в платформно-зависимый код;
- возможность обнаружения обращений к несуществующим данным;
- возможность обнаружения нарушений синтаксиса в программах на ST/FBD/LD;
- возможность показа списка обнаруженных ошибок;
- возможность показа позиции ошибки в редакторах ST/FBD/LD;
- блокировка загрузки в контроллер приложения, имеющего ошибки.

### 2.13 Компонент редактирования настроек

Компонент реализует возможность сохранения и редактирования пользовательских настроек приложения.

### 2.14 Компонент приема конфигурации OPC сервера

Компонент реализует функцию приема от среды разработки и проверки конфигурации OPC сервера.

## 2.15 Компонент OPC UA сервера

Компонент предназначен для сбора и передачи данных по спецификации OPC UA.

### 3. Настройка программы

#### 3.1 Системные требования

Перед установкой программного обеспечения **Unimod PRO** необходимо обратить внимание на выполнение описанных в Таблице 3.1 требований к аппаратному обеспечению.

Аппаратный компонент	Характеристика (минимальная рекомендуемая конфигурация оборудования для общих задач)
Процессор	Intel Atom Dual Core 1,6 ГГц или аналогичный
ОЗУ	2 Гбайт
Жесткий диск	1 Гбайт свободного пространства
Видеосистема	Разрешение: 1024 x 768
Сетевой адаптер	10/100 Мбит/сек

Таблица 3.1 – Требования к аппаратному обеспечению

Требования к программному обеспечению приведены в Таблице 3.2.

Операционная система	Поддерживаемая редакция
Astra Linux	Special Edition, версии 1.7
Пакет	Установочный диск
libqt5script5	5.11.0-0astra1

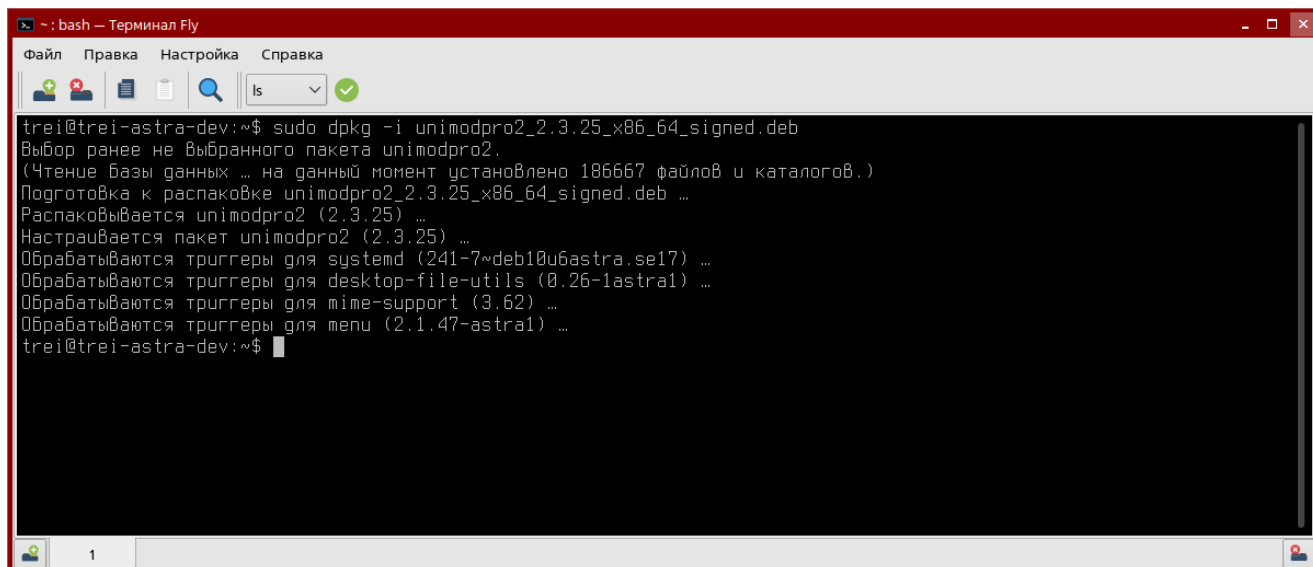
Таблица 3.2 – Требования к программному обеспечению

#### 3.2 Установка и удаление в ОС «ASTRA Linux»

Установка программы **Unimod PRO** под управлением ОС «**Astra Linux**» выполняется в следующем порядке:

1. необходимо запросить ссылку на скачивание дистрибутива через отправку сообщения с указанием организации на почтовый адрес [tr-penza@trei.biz](mailto:tr-penza@trei.biz)
2. перейти по полученной ссылке и скачать установочный пакет **Unimod PRO** в формате «**\*.deb**»
3. перейти в меню приложений и запустить «**Терминал Fly**» (кнопка запуска меню – «**Системные**» – «**Терминал Fly**»)
4. откроется окно эмулятора терминала. Для установки локального пакета в формате «**\*.deb**» введите команду «**sudo dpkg -i**» с указанием установочного пакета «**Unimod**

PRO» в формате «\*.deb», например, «unimodpro2\_2.3.25\_x86\_64\_signed.deb» (рисунок 3.1), и нажмите клавишу «[Enter]». Если в ОС не установлен пакет «libqt5script5», необходимо выполнить его установку до установки основного пакета. Для этого введите команду «**sudo dpkg -i**» с указанием установочного пакета «libqt5script5» в формате «\*.deb»



```
trei@trei-astra-dev:~$ sudo dpkg -i unimodpro2_2.3.25_x86_64_signed.deb
Выбор ранее не выбранного пакета unimodpro2.
(Чтение базы данных ... на данный момент установлено 186667 файлов и каталогов.)
Подготовка к распаковке unimodpro2_2.3.25_x86_64_signed.deb ...
Распаковывается unimodpro2 (2.3.25) ...
Настраивается пакет unimodpro2 (2.3.25) ...
Обрабатываются триггеры для systemd (241-7~deb10u6astra.se17) ...
Обрабатываются триггеры для desktop-file-utils (0.26-1astra1) ...
Обрабатываются триггеры для mime-support (3.62) ...
Обрабатываются триггеры для menu (2.1.47-astra1) ...
trei@trei-astra-dev:~$
```

Рисунок 3.1 – Установка пакета unimodpro2 в ОС «Astra Linux»

5. после ввода команды начнется процесс распаковки и установки пакета. Программный пакет устанавливается в директорию «/opt/TREI/UnimodPRO2», проекты при этом можно создавать в любой директории, например, домашнем каталоге пользователя. Запуск программы выполняется посредством ярлыка на рабочем столе или вводом в терминале команду: «/opt/TREI/UnimodPRO2/run\_unimod».

6. Для удаления программного пакета используется команда «**sudo dpkg -r unimodpro2**» (рисунок 3.2).

```

trei@trei-astra-dev:~$ sudo dpkg -r unimodpro2
(Чтение базы данных ... на данный момент установлено 186955 файлов и каталогов.)
Удаляется unimodpro2 (2.3.25) ...
dpkg: предупреждение: при удалении unimodpro2 каталог «/opt/TREI/OPCUA» не пуст, поэтому не удалён
dpkg: предупреждение: при удалении unimodpro2 каталог «/etc/TREI/OPCUA/uaroot/CertificateStore» не пуст, поэтому не
удалён
Обрабатываются триггеры для desktop-file-utils (0.26-1astra1) ...
Обрабатываются триггеры для mime-support (3.62) ...
Обрабатываются триггеры для systemd (241-7~deb10u6astra.se17) ...
trei@trei-astra-dev:~$

```

Рисунок 3.2 – Удаление пакета unimodpro2 в ОС «Astra Linux»

### 3.3 Описание старта и процедура проверки правильности старта

Запуск программы выполняется посредством ярлыка на рабочем столе или вводом в терминале команды: `#!/opt/UnimodPro2/run_unimod`. После запуска на рабочем столе должно появиться главное окно программы (рисунок 3.3).

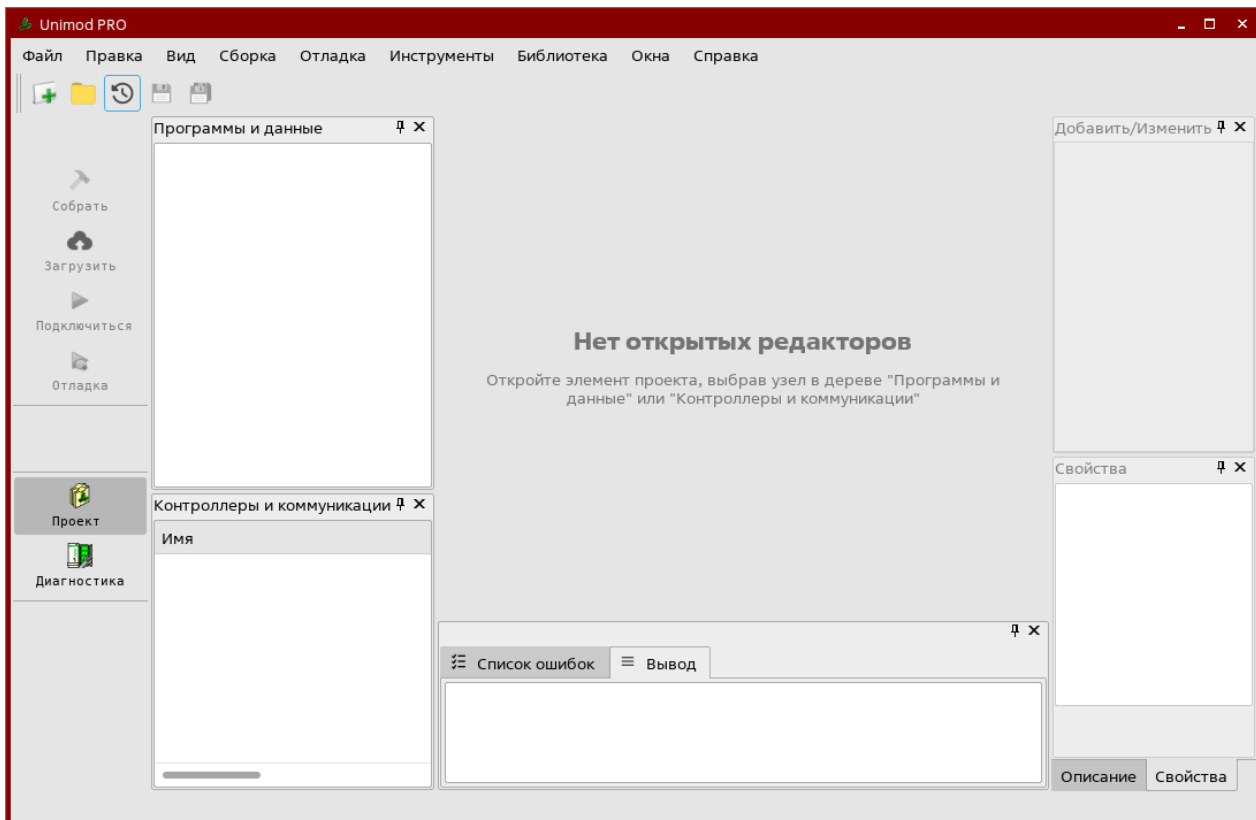


Рисунок 3.3 – Главное окно программы



### 3.4 О программе

После запуска администратор может посмотреть сведения об ОО (версию, производителя и т.п.), перейдя в меню «Справка → О программе» (рисунок 3.4).

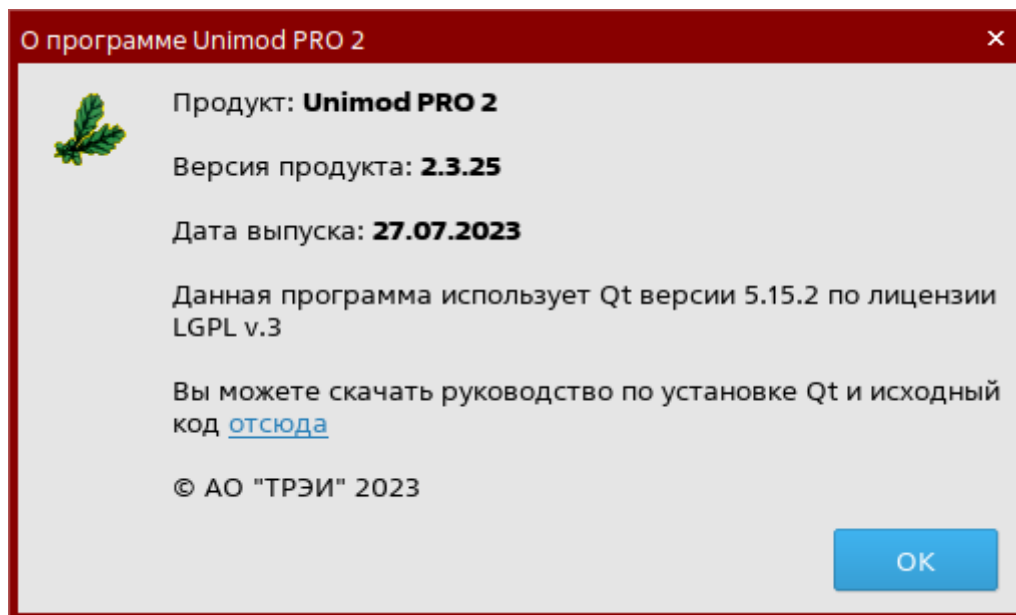


Рисунок 3.4 – Окно просмотра сведений о программе

## 4. Настройка подсистемы безопасности

### 4.1 Общие сведения

Проект технологической программы создается в «открытом режиме», в котором функции безопасности и разграничения доступа не задействованы. Для обеспечения разграничения доступа к функциям **Unimod PRO** предусмотрены следующие режимы:

- защищенный;
- однопользовательский;
- открытый (по умолчанию).

В **защищенном режиме** создается «каркас» проекта с пользователем «**Администратор**», без пароля. Пользователю «**Администратор**», вошедшему в систему первый раз, с момента создания проекта необходимо задать пароль для своей учетной записи, после чего ему будут доступны функции по управлению пользователями и защитой информации.

Администратор создает пользователей, роли, ролям назначает функции и компоненты, закрепляет роли за пользователями.

Администратор настраивает «аудит безопасности» указав способ регистрации событий информационной безопасности и все необходимые настройки (или «не использовать регистрацию событий ИБ»).

Каждый пользователь в первые вошедший в среду разработки с паролем, который ему выдал администратор, создавший учетную запись, должен изменить пароль. Для этого выводится блокирующее диалоговое окно смены пароля учетной записи.

После смены пароля пользователю доступны целевые функции среды соответствующие роли учетной записи, назначенные администратором.

Пользователь имеет возможность сменить пароль своей учетной записи (используя диалоговую оконную форму).

«Администратор» может перевести проект из «защищенного» режима в «открытый» режим.

В **однопользовательском режиме** создается проект с одной учетной записью типа «пользователь», которой доступны все целевые функции среды (кроме функций управления пользователями, защиты информации, редактирование системных компонент среды).

В данном режиме сложность, срок действия пароля и прочие параметры учетной записи не проверяются.

Из «однопользовательского» режима проект можно перевести в «открытый» режим.

В **открытом режиме** функции подсистемы разграничения доступа работают таким образом, чтобы не блокировать действия пользователей – диалоговые окна ввода данных учетной записи не отображаются, функции проверки прав доступа всегда возвращают значения соответствующее «доступ разрешен».

В процессе «жизненного цикла проекта» режим может быть изменен, при этом сменить режим «защищенный» на «открытый» может только администратор. В открытом режиме пользователей фактически не существует (аутентификация не выполняется) поэтому перевести проект в «закрытый» или «однопользовательский» режимы может любой «оператор».

## **4.2 Защищенный режим**

Для того, чтобы перевести проект в «**Защищенный режим**» нужно последовательно выбрать пункты верхнего меню «**Инструменты**» / «**Безопасность**» / «**Выбор режима проекта**» / «**Защищенный**», после чего появится диалоговое окно, в котором нужно ввести учетные данные (имя пользователя и пароль) администратора проекта.

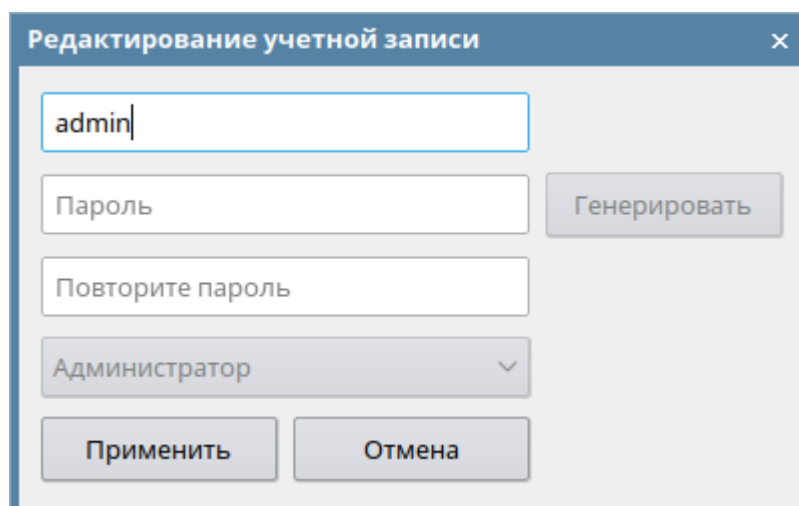


Рисунок 4.1 – Окно создание учетной записи «Администратор»

Нажать кнопку «**Применить**». Для работы проекта с новыми параметрами доступа нужно закрыть и заново открыть проект.

При открытии проекта появится диалоговое окно ввода «**Учетных данных пользователя**».

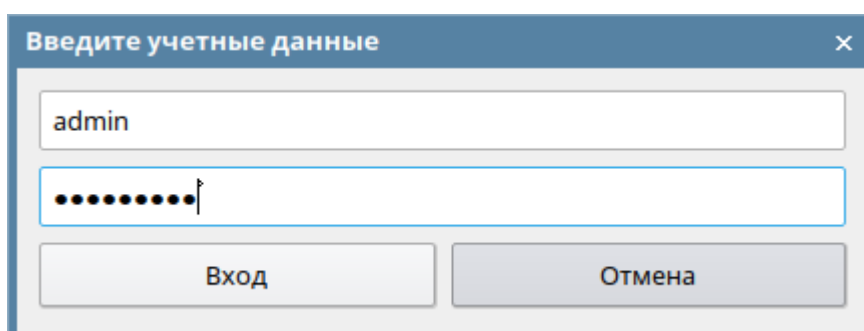


Рисунок 4.2 – Окно ввода учетных данных

Ввести имя пользователя и пароль пользователя «**Администратор проекта**».

Администратор проекта не имеет доступа к целевым функциям **Unimod PRO** таким как редактирование, сборка, загрузка, отладка проекта. Администратору доступны только функции:

- настройка политик безопасности;
- настройка учетных записей пользователей.

Для того, чтобы настроить политики безопасности нужно последовательно выбрать пункты верхнего меню «**Инструменты**» / «**Безопасность**» / «**Настройка политик безопасности**», после чего появится диалоговое окно, в котором нужно ввести данные

согласно требований руководящих документов по информационной безопасности действующих на предприятия (в организации).

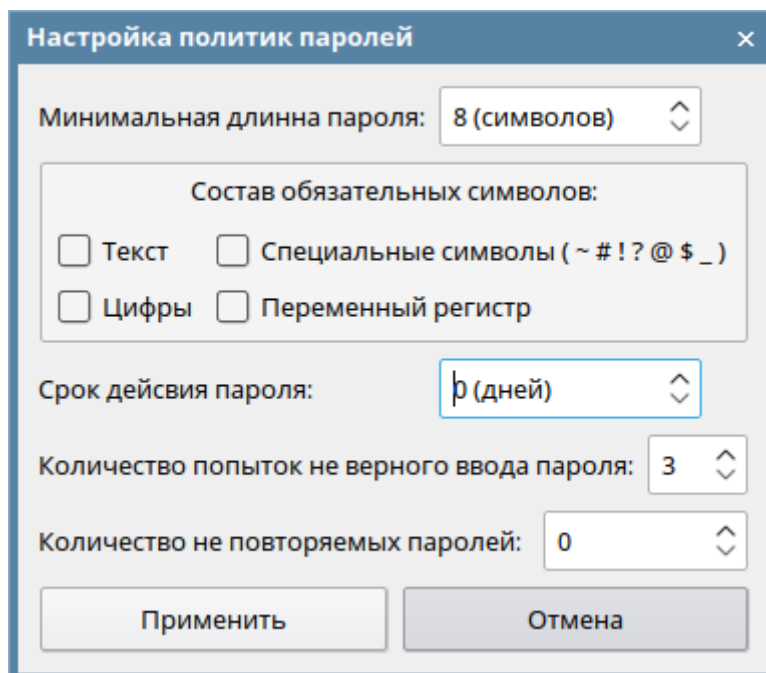


Рисунок 4.3 – Окно настроек политик паролей

Для того, чтобы настроить учетные записи пользователей нужно последовательно выбрать пункты верхнего меню «Инструменты» / «Безопасность» / «Настройка учетных записей».

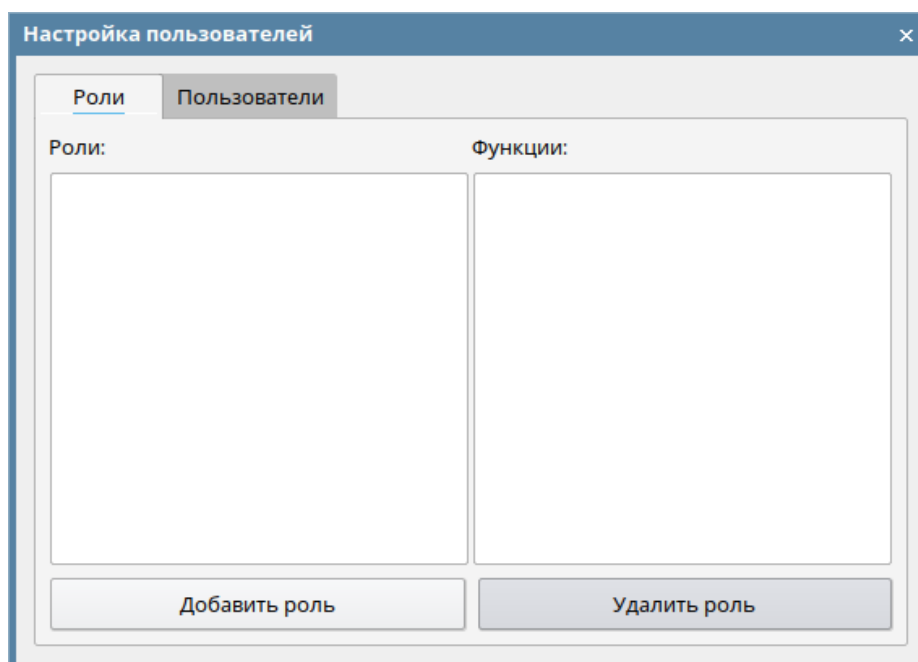


Рисунок 4.4 – Окно настройки пользователей

Настройка учетных записей заключается в создании ролей пользователей с разрешенным перечнем целевых функций **Unimod PRO** и созданием учетных записей с определенными ролями.

Для того, чтобы добавить роль нужно в окне «**Настройка пользователей**» на вкладке «**Роли**» нажать кнопку «**Добавить роль**», в появившемся диалоговом окне ввести «**Название роли**» и нажать кнопку «**Да**».

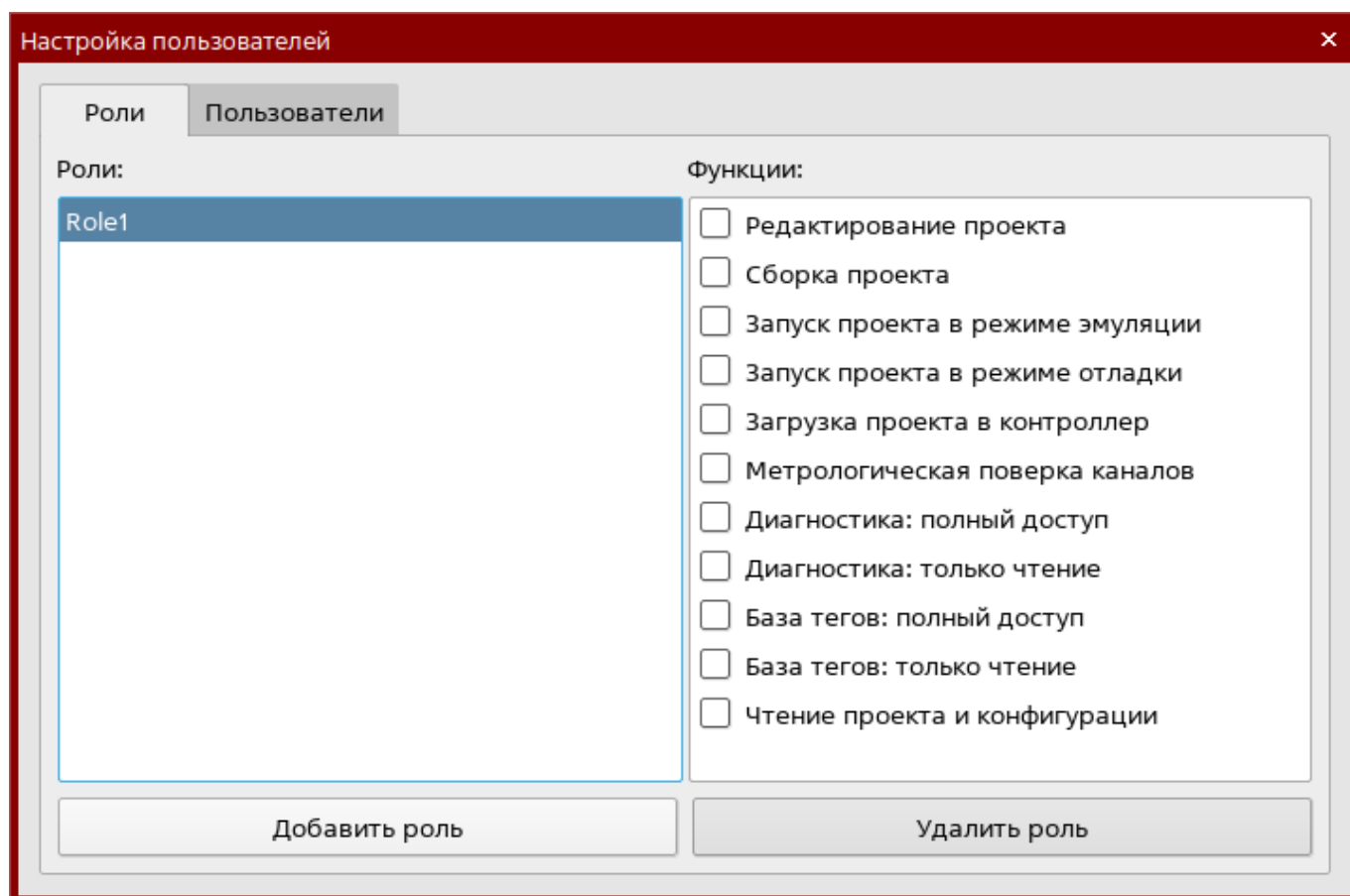


Рисунок 4.5 – Окно список ролей и функций

В список ролей добавится запись. В списке «**Функции**» нужно отметить те функции **Unimod PRO** которые разрешены учетным записям с настраиваемой ролью.

Для того, чтобы добавить пользователя нужно в окне «**Настройка пользователей**» на вкладке «**Пользователи**» нажать кнопку «**Добавить**».

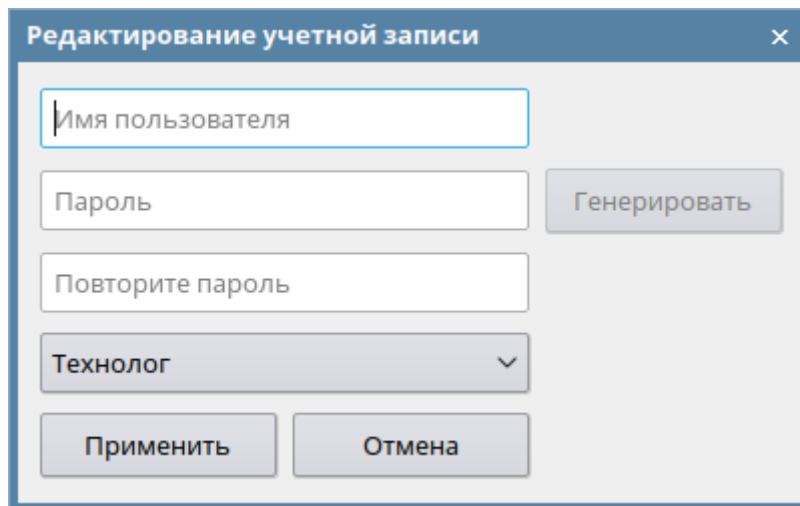


Рисунок 4.6 – Окно редактирования учетной записи

В появившемся диалоговом окне ввести имя пользователя и пароль в выпадающем списке выбрать роль пользователя. Нажать кнопку применить.

В список пользователей добавится запись.

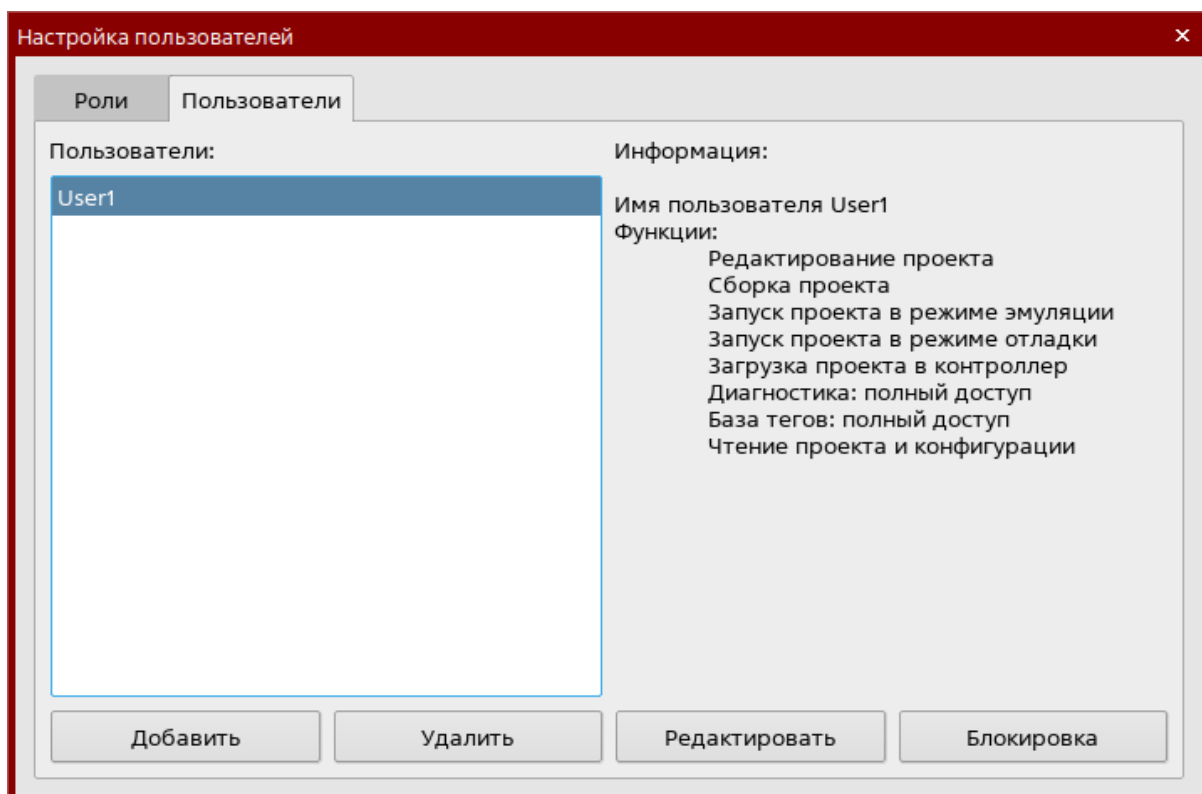


Рисунок 4.7 – Окно список пользователей

Для того чтобы изменить пароль или роль учетной записи нужно её выделить в списке и нажать кнопку «**Редактировать**». В появившемся диалоговом окне нужно изменить требуемые значения и нажать кнопку «**Применить**».

Для того чтобы заблокировать/разблокировать учетную запись нужно её выделить в списке и нажать кнопку **«Блокировка»**. В поле статического текста **«Информация»** добавится соответствующая строка.

После настройки учетных записей, закрытии и последующем открытии проекта будет появляться диалоговое окно ввода учетных данных пользователя, по которым будет определяться роль пользователя и будет отрываться доступ к разрешенным (для текущей роли) функциям **Unimod PRO**.

### 4.3 Смена пароля

Для смены пароля текущей учетной записи нужно последовательно выбрать пункты главного меню **«Инструменты» / «Безопасность» / «Смена пароля»**. В появившемся диалоговом окне ввести текущий пароль, ввести новый пароль и для проверки ввести новый пароль в поле **«Повторите новый пароль»** и нажать кнопку **«Применить»**.

### 4.4 Регистрация событий безопасности

В защищенном режиме в проекте доступен функционал журналирования событий безопасности.

К таким событиям относятся:

- добавление учетной записи пользователя;
- редактирование учетной записи пользователя;
- удаление учетной записи пользователя;
- успешная (не успешная) аутентификация пользователя;
- выход пользователя из проекта.

Для активации функции регистрации событий необходимо выбрать в главном меню пункт **«Инструменты» / «Безопасность» / «Настройка журналирования»**. В открывшемся диалоговом окне выбрать способ журналирования (запись в файл и/или запись на сервер syslog), задать необходимые параметры связи с сервером syslog и нажать кнопку **«Применить»**. При последующем открытии проекта события безопасности будут записаны в журнал выбранным способом.

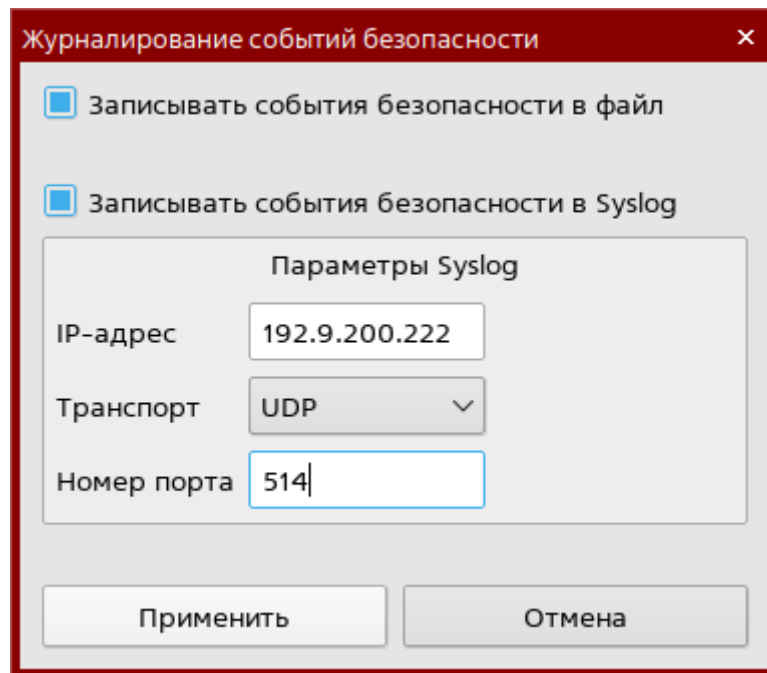


Рисунок 4.8 – Окно настроек журналирования событий безопасности