ООО «АтомиСофт»

РУКОВОДСТВО АДМИНИСТОРАТОРА ПО РАБОТЕ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ «ПРИМА РАО»

2024

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Руководство администратора по работе с программным обеспечением «Прима РАО» (далее – Руководство) содержит пошаговые инструкции и пояснения по основным операциям, выполняемым администратором в программном обеспечении «Прима РАО» (далее – ПО).

В данном ПО функционал администратор разделен на две роли:

- «Администратор», который владеет полным набором прав.
- «Администратор информационной безопасности» (далее – Администратор ИБ), который ограничен правами на работу с журналом аудита.

1.1. Область применения

Программное обеспечение «Прима РАО» (далее – ПО) предназначено для автоматизации процедур по учету и контролю радиоактивных отходов. ПО спроектировано как многопользовательское программное обеспечение на базе универсальной учетной платформы (далее – УУП) с соответствующей конфигурацией для учета радиоактивных отходов (далее – РАО).

Областью применения программного обеспечения «Прима РАО» являются в основной части организации в ядерной энергетике.

1.2. Уровень подготовки администратора.

Администратор обязан знать:

настоящее Руководство и иметь представление о работе основных интернет-технологий;

соответствующую терминологию настоящего документа;

основные принципы работы сайтов.

Администратор ПО должен обладать следующими знаниями и навыками:

настройка и диагностирование работы ПО;

обслуживание технического и системного программного обеспечения ПО;

администрирование баз данных;

резервное копирование и восстановление данных;

обеспечение регламентных работ и анализ результатов регламентных операций.

сопровождение и администрирование локальной вычислительной сетей, протокола TCP/IP;

настройка рабочих станций локальной вычислительной сети;

инсталляция, общесистемное сопровождение и администрирование; администрирование СУБД.

2. ОСНОВНОЕ ОПИСАНИЕ АРХИТЕКТУРЫ ПО

2.1. Построение архитектуры.

Построение архитектуры ПО реализовано по MVC-шаблону («Model-View-Controller» паттерн) с разделением данных приложения, пользовательского интерфейса и управляющей логики на три отдельных компонента. Таким образом, в ПО можно выделить следующие уровни:

1. Уровень пользовательского интерфейса;
2. Уровень бизнес-логики;
3. Уровень базы данных.

Верхним уровнем является уровень интерфейса пользователя. На этом уровне ПО содержит формы ввода/вывода информации, функции проверки корректности вводимых данных до их обработки на стороне сервера. Интерфейс реализуется на языке разметки HTML5/CSS3 и с помощью языков программирования TypeScript, JavaScript.

На уровне бизнес-логики ПО содержит программные коды, выполняющие функции поддержки необходимых операций. Уровень бизнес-логики написан на языке C#.

Уровень базы данных состоит из таблиц необходимых для полноценной работы ПО учета и контроля. Связь уровня бизнес-логики и уровня базы данных происходит с помощью ORM от Microsoft Entity Framework и синтаксиса LINQ.

2.2. Техническое и программное обеспечение.

ПО реализовано с использованием следующих технологий:
.NET 7;
ASP.NET Core 7;
СУБД PostgreSQL;
HTML5, CSS3;
C#, Transact-SQL, TypeScript, JavaScript, Angular 16.

Функционирование ПО обеспечивается следующим программным обеспечением:

Серверная часть для Windows:
Операционная система Windows Server 2019;
СУБД PostgreSQL 14;
Серверная часть для Linux:
Linux Astra Smolensk 1.7;
PostgreSQL 9.X.
Клиентская часть:
Операционная система Windows 10;

Веб-обозреватель Google Chrome версии 105 и выше, или любой другой chromium-совместимый браузер (opera, яндекс браузер и т.д.);

Средства создания и редактирования документации MS Office (2016 и выше).

2.3. Информация по безопасности ПО.

Все действия пользователей, выполняемые в ПО регистрируются и хранятся в журнале событий бессрочно. Для исключения переполнения журнала аудита и потери записей из-за нехватки дискового пространства администратору необходимо своевременно контролировать достаточный объем памяти на сервере, где установлено ПО.

Конфиденциальная информация, ключи API и пароли не содержаться в исходном коде или репозиториях исходного кода, кроме одной учетной записи администратора (логин: admin, пароль: admin) используемой для первоначального входа в ПО после его установки. Данные стандартной учетной записи администратора персонализируются при первом входе в ПО.

В ПО используются следующие роли пользователей:

Роль	Назначение
Администратор	Выполнение функций администрирования ПО описанных в главе 3.
Администратор ИБ	Выполнение функций администрирования ПО описанных в главе 4.
Настройщик	Назначается пользователю для создания и редактирования конфигурации ПО.
Учетчик	Назначается пользователю для выполнения основного функционала учета необходимых сущностей или продукции.

Для реализации раздельного хранения системных файлов и файлов конфигурации, принадлежащих ПО, а также журнала событий от пользовательских данных, необходимо установить ПО и базу данных в разные места (каталог, системный раздел и т. д.). Экспортированный журнал событий хранить так же отдельно.

Для аутентификации пользователей используется современный протокол Oauth 2.0.

Доступ пользователя к функциональности ПО обеспечивается использованием персонального компьютера и IP-адреса, который входит в перечень доверенных IP-адресов.

Ввод пароля в интерфейсе ПО скрыт, и не виден другим лицам.

Для предотвращения ввода вредоносных команд в ПО реализована валидация вводимых пользователем данных.

Пользовательская сессия завершается по таймауту, заданному настройками администратора или после нажатия кнопки «Выход».

3. ОПИСАНИЕ ОПЕРАЦИЙ АДМИНИСТРАТОРА

3.1. Вход на страницу администрирования ПО.

1.1. Для входа на страницу администрирования ПО необходимо:

1. В адресную строку браузера введите адрес приложения и нажмите на клавишу **Enter**. Произойдет переход на авторизационную страницу ПО.
2. В поле **Логин** введите логин для входа в ПО с ролью «Администратор».
3. В поле **Пароль** введите пароль.
4. Нажать на кнопку **Войти**. Произойдет переход на **Страницу** администрирования ПО.

3.2. Создание группы прав для пользователей.

Группы прав используются для предоставления определенным пользователям с ролью «Учетчик» необходимых прав на проведение определенных операций по учету сущностей описанных в конфигурации ПО.

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку **«Группы прав»**.
3. Нажать кнопку **«Добавить»** и внести информацию о наименовании созданной группы прав.
4. Выбрать из списка областей, необходимую область которой будут владеть пользователи в созданной группе.
5. В правой части страницы выбрать необходимые права из списка для пользователей созданной группы выбранной области.
6. Нажать кнопку **Сохранить**.

3.3. Создание учетной записи пользователя с ролью «Администратор».

Пользователю с ролью «Администратор» доступны возможности:

- создание новых пользователей;
- редактирование информации о зарегистрированных пользователях;
- редактирование групп прав;
- работа с журналом аудита;
- настройка параметров аутентификации;
- работа с IP-адресами;
- просмотр установленных или подключенных модулей категорий и/или категорий;
- работа с лицензией.

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку **«Список пользователей»** и нажать кнопку **Добавить**.
3. Зарегистрировать нового пользователя с ролью «Администратор»:
   - В полях **Логин** и **Временный пароль** укажите данные для аутентификации регистрируемого пользователя;
   - Добавить **IP адрес** компьютера пользователя.
4. Нажать кнопку **Сохранить**.

3.4. Создание учетной записи пользователя с ролью «Администратор ИБ».

Пользователю с ролью «Администратор ИБ» доступна возможность работы с журналом аудита.

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку **«Список пользователей»** и нажать кнопку **Добавить**.
3. Зарегистрировать нового пользователя с ролью «Администратор ИБ»:
   - В полях **Логин** и **Временный пароль** укажите данные для аутентификации регистрируемого пользователя;
   - Добавить **IP адрес** компьютера пользователя.
4. Нажать кнопку **Сохранить**.

3.5. Создание учетной записи пользователя с ролью «Настройщик».

Пользователь с ролью «Настройщик» имеет доступ только к конфигуратору ПО и предназначен для создания и редактирования конфигурации ПО.

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку **«Список пользователей»** и нажать кнопку **Добавить**.
3. Зарегистрировать нового пользователя с ролью «Настройщик»:
   - В полях **Логин** и **Временный пароль** укажите данные для аутентификации регистрируемого пользователя;
   - Добавить **IP адрес** компьютера пользователя.
4. Нажать кнопку **Сохранить**.

В результате выполнения указанных действий произойдет добавление пользователя в ПО с ролью «Настройщик». Первоначальный пароль передается администратором ПО зарегистрированному пользователю для

первого входа. После первого входа в ПО пользователю будет необходимо ввести новый персональный пароль.

3.6. Создание учетной записи пользователя с ролью «Учетчик».

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку **«Список пользователей»** и нажать кнопку **Добавить**.
3. Зарегистрируйте нового пользователя с ролью «Учетчик»:
   - В полях **Логин** и **Временный пароль** укажите данные для аутентификации регистрируемого пользователя;
   - Добавить **IP адрес** компьютера пользователя;
   - Выбрать группу прав для пользователя;
4. Нажать кнопку **Сохранить**.

В результате выполнения указанных действий произойдет добавление пользователя в ПО с ролью «Учетчик». Первоначальный пароль передается администратором системы зарегистрированному пользователю для первого входа. После первого входа в ПО пользователю будет необходимо ввести новый персональный пароль.

3.7. Деактивация учетной записи

Во избежание несанкционированного доступа учётная запись может быть деактивирована. Администратор имеет возможность деактивировать учетную запись вручную (принудительно) следующими шагами:

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку «Список пользователей».
3. Выбрать в таблице пользователя, которого необходимо деактивировать и в графе «Действия» нажать кнопку  (деактивировать).
4. Подтвердить деактивацию нажатием кнопки  .

3.8. Изменение данных в учетной записи пользователя.

Для изменения информации в учетной записи пользователя выполните следующие действия:

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку «Список пользователей».
3. Выбрать в таблице пользователя, которого необходимо изменить информацию и в графе «Действия» нажать кнопку  (изменить).

4. Внести необходимые корректировки для выбранного пользователя и нажать кнопку **Сохранить**.

3.9. Сброс пароля записи пользователя.

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку **«Список пользователей»**.
3. Выбрать в таблице пользователя, которому необходимо сбросить пароль и в графе «Действия» нажать кнопку (сбросить пароль).
4. В диалоговом окне ввести новый первоначальный пароль для пользователя или выбрать предложенный системой пароль.
5. Нажать кнопку **Сохранить**.

В результате выполнения указанных действий произойдет сброс пароля пользователя, после чего пользователь (при первоначальном входе в ПО после сброса пароля) обязан ввести новый первоначальный пароль (переданный ему администратором), затем на странице входа в ПО ввести личный персональный пароль.

3.10. Просмотр журнала действий пользователей (логирование).

1. Войти в ПО с ролью «Администратор».
2. На странице администрирования открыть вкладку «Журнал аудита».
3. Откроется страница со списком всех действий в ПО с указанием данных о времени произведенных изменений и пользователе, вносившем изменения.

Журнал событий можно отфильтровать на определённый заданный период, а также имеется возможность экспорта данных журнала в файл *.xlsx, *.csv, *.xml.

3.11. Настройка аутентификации.

1. Войти в ПО с правами администрирования.
2. На странице администрирования открыть вкладку **Настройки**.
3. Задать необходимые параметры для аутентификации:
   - Пароль должен содержать символы верхнего регистра;
   - Пароль должен содержать символы нижнего регистра;
   - Пароль должен содержать минимум одну цифру;
   - Пароль должен содержать специальные символы;
   - Старый и новый пароли могут совпадать;
   - Длина пароля;

- Максимальное число попыток входа в систему;
- Время бездействия до приостановки сеанса;
- Срок действия пароля;
- Число предыдущих уникальных паролей;
- Язык по умолчанию.

4. Нажать **Сохранить.**

3.12. Снятие блокировки учётной записи.

Во избежание несанкционированного доступа учётная запись, может быть, автоматически заблокирована при заданных в Настройках параметрах аутентификации. Для снятия блокировки учетной записи пользователя необходимо:

1. Войти в ПО с ролью «Администратор».
2. На странице администрирования открыть вкладку «IP-адреса» и выбрать Заблокированные.
3. Удалить из списка нужный IP Адрес.
4. В главном меню перейти на вкладку «Список пользователей», выбрать в таблице пользователя, которому необходимо активировать доступ, нажать кнопку Активировать в деактивированной учетной записи.
5. Нажать кнопку Сохранить.

3.13. Проверка установленных модулей к ПО.

Контроль наличия установленных модулей необходимых версий производится выполнением следующих действий.

1. Войти в ПО с ролью «Администратор».
2. На странице администрирования открыть вкладку **«Модули»**.

Данная страница содержит сформированный список доступных (установленных) модулей к ПО.

3.14. Проверка установленных категорий к ПО.

Контроль наличия категорий производится выполнением следующих действий.

1. Войти в ПО с ролью «Администратор».
2. На странице администрирования открыть вкладку **«Категории»**.

Данная страница содержит сформированный список доступных категорий к ПО.

3.15. Работа с лицензией.

Обновление лицензии к ПО производится следующими действиями:

1. Войти в ПО с ролью «Администратор».
2. На странице администрирования открыть вкладку **«Лицензия»**.
3. На открывшейся странице с описанием текущей лицензии нажать кнопку 

.
4. В открывшемся окне выбрать необходимый файл с лицензией и нажать кнопку «Открыть».

4.ОПИСАНИЕ ОПЕРАЦИЙ АДМИНИСТРАТОРА ИБ

4.1. Вход в ПО пользователя с ролью «Администратор ИБ».

Для входа необходимо:

1. В адресную строку браузера введите адрес приложения и нажмите на клавишу Enter. Произойдет переход на авторизационную страницу ПО.
2. В поле **Логин** введите логин для входа в ПО с ролью «Администратор ИБ».
3. В поле **Пароль** введите пароль.
4. Нажать на кнопку **Войти**. Произойдет вход на вкладку **«Журнал аудита»**.

4.2. Работа с журналом аудита.

1. Войти в ПО с ролью «Администратор ИБ».
2. На вкладке **«Журнал аудита»** откроется страница со списком всех действий в системе:

- Время выполнения действия (Дата и время);
- Логин пользователя (Пользователь);
- IP адрес с которого произошло действие (IP адрес);
- Место внесения изменений (Модуль/Платформа);
- Описание действия (Описание), при нажатии на значение в данной строке открывается дополнительная информация;
- Результат завершения действия (Результат).

Журнал событий можно отфильтровать с помощью кнопок  .

4.3. Экспорт журнала аудита.

Экспорт журнала производится следующими действиями:

3. Войти в ПО с ролью «Администратор ИБ».
4. На вкладке **«Журнал аудита»** нажать кнопку 

.
5. Из развернувшегося списка выбрать формат, в котором нужно экспортировать журнал (*.xlsx, *.csv, *.xml).

5. ДЕЙСТВИЯ ПРИ АВАРИЙНЫХ СИТУАЦИЯХ

ПО должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями администратора, неверным форматом или недопустимыми значениями входных данных. В указанных случаях администратору выдаются соответствующие аварийные сообщения, после чего ПО возвращается в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных. Аварийные ситуации могут возникать как из-за ошибок в программных продуктах, так и из-за неправильной настройки.

Основными признаками аварийной ситуации являются:

1. Отсутствие на экране необходимой страницы.
2. Окна с сообщениями о нештатной ситуации.

При отказе магнитных носителей или обнаружения ошибок в данных администратор ПО должен восстановить файлы и данные, необходимые для корректной работы ПО из последней резервной копии. Если администратор не может устранить ошибки в данных, следует обратиться к разработчику ПО. При этом необходимо указать перечень данных, содержащих ошибки и правильные значения искаженных атрибутов

В случае возникновения других аварийных ситуаций при работе с ПО и невозможности устранить их с помощью средств администрирования, системы управления базой данных, операционной системы следует обратиться к разработчику ПО. При этом необходимо описать признаки аварийной ситуации и действия, которые были выполнены пользователем непосредственно перед возникновением аварийной ситуации. Ниже описаны основные возможные аварийные ситуации и способы их решения.

Аварийная ситуация	**Возможные потери информации**	**Способ ликвидации последствий**	**Исполнитель**
Сбой операционной системы сервера	Вся информация, поступившая в ПО с момента окончания последнего резервного копирования данных.	Восстановление данных из резервных копий	Администратор

Аварийная ситуация	Возможные потери информации	Способ ликвидации последствий	Исполнитель
Выход из строя жесткого диска	Вся информация, поступившая в ПО с момента окончания последнего резервного копирования данных.	Восстановление данных из резервных копий	Администратор
Отсутствие на экране необходимой страницы в подсистеме администрирования	Несохраненные администратором данные	Перезагрузка страницы кнопкой «Обновить» интернет-браузера; возврат на предыдущую страницу и повторный клик по ссылке на необходимую страницу	Администратор
Окна с сообщениями об ошибках в веденных данных подсистемы администрирования	Несохраненные администратором данные	Выполнить рекомендации, указанные в сообщении.	Администратор
Ошибки, связанные с программным обеспечением	Информация, поступившая в ПО с момента окончания последнего резервного копирования данных	Перезапуск соответствующего программного обеспечения, перезагрузка сервера, восстановление данных из резервных копий	Администратор
Долгая загрузка страниц ПО	Отсутствуют	Совместно с сотрудниками информационной безопасности организации произвести настройку антивируса «Kaspersky Security для Windows Server»	Администратор