ООО «АтомиСофт»

РУКОВОДСТВО АДМИНИСТОРАТОРА ПО РАБОТЕ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ «ПРИМА ИДК»

2026

СОДЕРЖАНИЕ

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Сокращение (обозначение)	Расшифровка (пояснение)
АЭС	Атомная электростанция
ИБ	Информационная безопасность
ИДК	Индивидуальный дозиметрический контроль
ОС	Операционная система
ПО	Программное обеспечение
СУБД	Система управления базами данных
УЕ	Учетная единица
УУП	Универсальная учетная платформа

1. ОБЩИЕ ПОЛОЖЕНИЯ

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

В данном ПО функционал администратор разделен на две роли:

– «Администратор», который владеет полным набором прав.

– «Администратор информационной безопасности» (далее – Администратор ИБ), который функционально наделен правами на работу только с журналом аудита (см. п.3.11).

1.1. Область применения

ПО применяется для обеспечения радиационной безопасности, ведения персонифицированного учета доз, контроля за соблюдением норм радиационной безопасности и основных санитарных правил.

ПО спроектировано как многопользовательское программное обеспечение на базе универсальной учетной платформы (далее – УУП).

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 должен обладать следующими знаниями и навыками:

– настройки и диагностирования работы ПО;

– резервного копирования и восстановления данных;

– сопровождения и администрирования локальной вычислительной сети, протокола TCP/IP;

– настройки рабочих станций локальной вычислительной сети;

– инсталляции, общесистемное сопровождения и администрирование;

– администрирования СУБД.

2. ОСНОВНОЕ ОПИСАНИЕ АРХИТЕКТУРЫ ПО

2.1. Построение архитектуры.

Построение архитектуры ПО реализовано по MVC-шаблону («Model-View-Controller») 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 O/RM от Microsoft Entity Framework и синтаксиса LINQ.

2.2. Техническое и программное обеспечение.

ПО реализовано с использованием следующих технологий:
.NET 9;
ASP.NET Core 9;
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 1.6;
PostgreSQL не ниже версии 9.X.
Клиентская часть:
Операционная система Windows 10;

Веб-обозреватель Chrome (не ниже версии 105);

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.

Лог-файл работы ПО лежит по пути: C:\ProgramData\AtomiSoft\{папка с названием ПО}.

Информационная безопасность ПО обеспечивается комплексом мер, направленным на предотвращение несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

Комплекс мер включает в себя следующее:

1. Защита передачи данных в сети, передача данных в зашифрованном виде, использование протоколов SSL/TLS;

2. Ведение и мониторинг записей отслеживания и аудита действий пользователей в системе, в том числе неуспешных действий;

3. Ограничение доступа к ресурсам ПО, авторизация пользователей;

4. Разделение ролей пользователей, управление правами пользователей и использование управляющих аккаунтов;

5. Меры предосторожности против известных атак на уязвимости аутентификации, внедрения SQL или командного кода, межсайтовой подделки запроса (CSRF), переполнения памяти;

6. Отсутствие кэширования чувствительных данных как на стороне клиента, так и на сервере;

7. В средах разработки и тестирования не используются реальные данные;

8. Использование последних стабильных версий зависимых технологий;

9. Использование сертификата безопасности, проведение аудита сертификата.

Часть мер безопасности должна быть обеспечена организационными мерами и мерами безопасности IT- инфраструктуры эксплуатирующей организации. Это такие меры как:

- Безопасная настройка базы данных: отсутствие простого доступа из интернета;
- Применение конфигураций безопасности, чтобы только приложение и авторизованные пользователи могли получить доступ к серверам и рабочим средам (базе данных, файловой системе, службам);
- Для запуска и эксплуатации СУБД не должны применяться учетные записи и пароли по умолчанию;
- Программное обеспечение веб-сервера должно запускаться с учетной записи, специально созданной для этой цели, а не с учетной записи администратора;
- Необходимо указать каталоги с разрешениями на запись, права записи должны быть предоставлены только каталогам, которым требуется загрузка файлов. Необходимо удалить разрешение на запуск в каталогах файлов, загруженных через приложение.
- Неиспользуемые порты на серверах должны быть закрыты.

Полное описание принятых мер по безопасности ПО описано в Приложении 1 настоящего Руководства.

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 разделе 3.
Администратор ИБ	Пользователь выполняющий мониторинг информационной безопасности в ПО. Доступна только функциональность описанная в п.3.11 и 3.18. раздела 3.
Настройщик	Пользователь, который выполняет создание, наладку и редактирование конфигурации ПО.
Учетчик	Назначается пользователю для выполнения основного функционала учета необходимых учетных единиц.

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 и описание интерфейса

Для входа на страницу администрирования ПО необходимо:

Шаг 1. В адресную строку браузера введите url-адрес ПО и нажмите на клавишу «Enter».

Шаг 2. После перехода по соответствующему адресу, пользователь попадает на страницу авторизации.

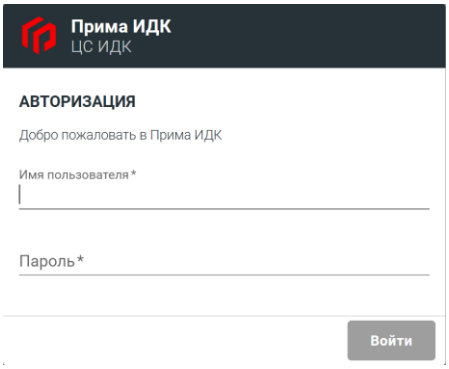

Рисунок 3.1. Страница авторизации пользователя

Шаг 3. Введите логин и пароль администратора в соответствующие поля для входа в ПО.

Шаг 4. Нажмите кнопку «Войти» или «Enter».

Шаг 5. После успешной аутентификации произойдет переход на страницу администрирования ПО.

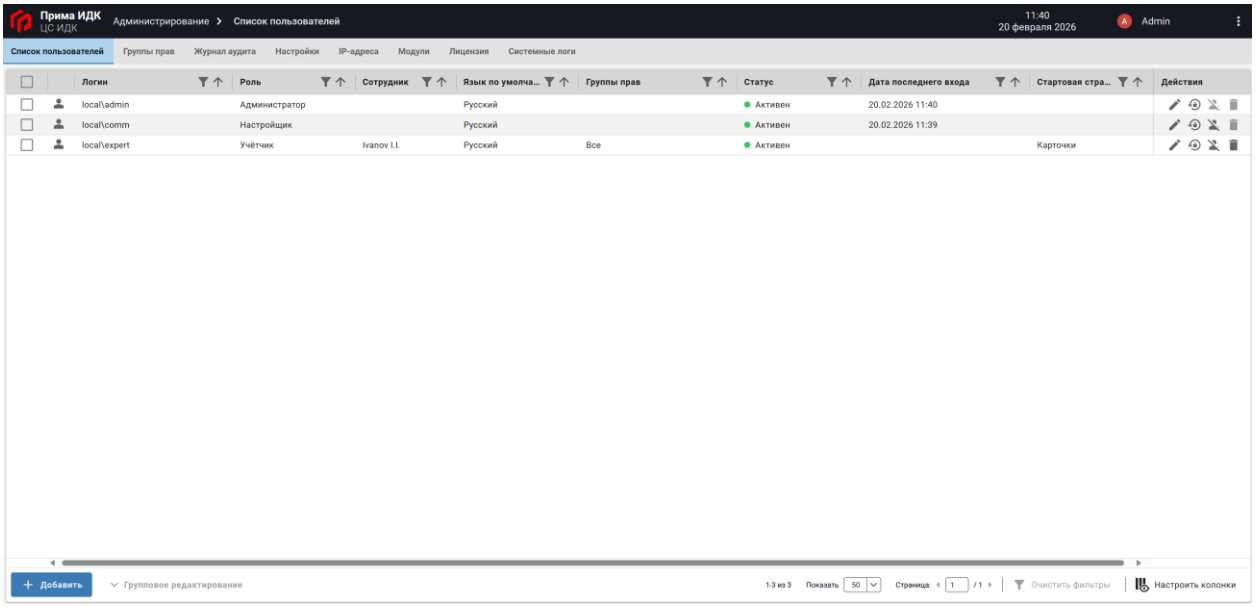

Рисунок 3.2. Пример интерфейса пользователя с ролью «Администратор»

Интерфейс пользователя с ролью «Администратор» состоит из следующих элементов:

– строка заголовка (верхняя часть окна) содержит название продукта и конфигурации, текущую дату и время, а также информационная панель пользователя и кнопку ;

– набор навигационных вкладок, при переключении которых пользователь переходит на необходимую часть функционала администрирования;

– рабочая область (центральная часть страницы), в которой отображается рабочая информация, которая меняется в зависимости от активной вкладки.

Информационная панель пользователя по нажатию которой появляется функциональное подменю со следующим функционалом:

– отображение логина текущего пользователя;

– отображение сведений о сотруднике, привязанном к пользователю (в формате: Фамилия И.О.);

– переключение языка ПО;

– завершение текущей сессии работы с ПО кнопкой «Выход».

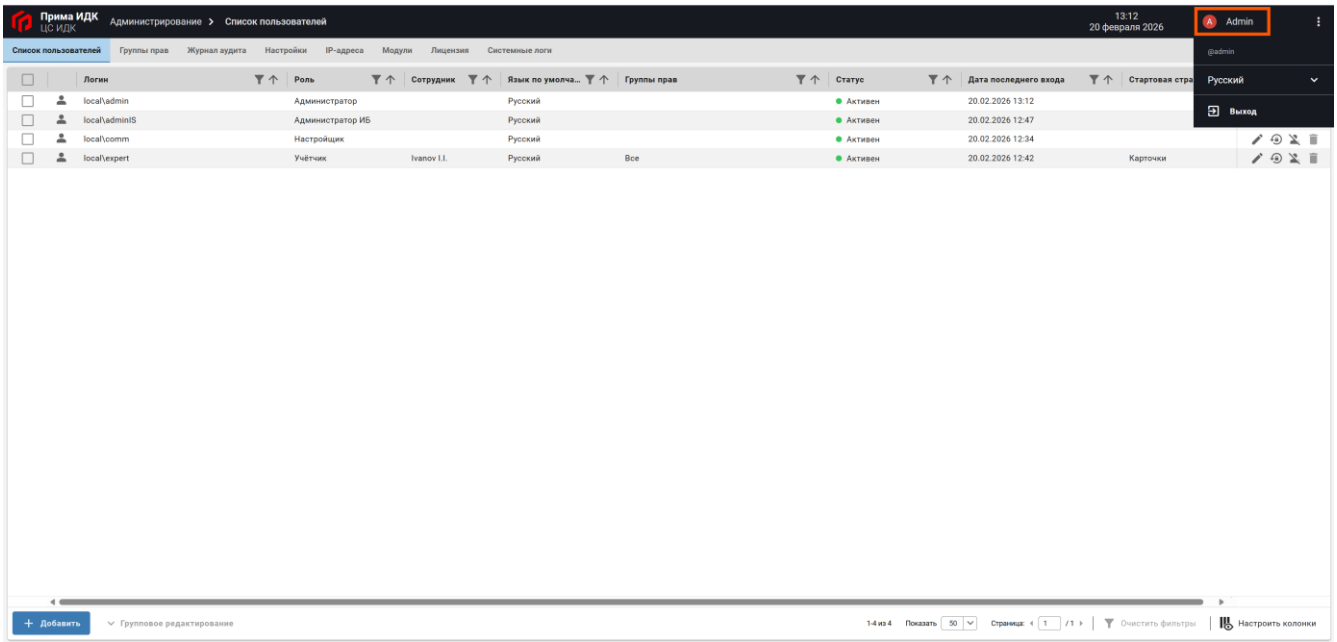

Рисунок 3.3. Пример подменю информационной панели пользователя

Кнопка , нажатие которой откроет выпадающий список с кнопками «О программе» и «Помощь».

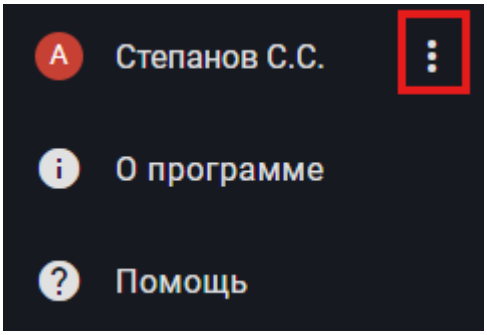

Рисунок 3.4. Подменю после нажатия кнопки ⋮

Нажатие кнопки «Помощь» приводит к открытию страницы с Руководством в формате .pdf.

Кнопка «О программе» ведет к диалоговому окну, которое содержит:

– версию ПО;
– дату выпуска;
– полное наименование ПО;
– информацию об изготовителе ПО;
– информацию об установленных моделях и их версия.

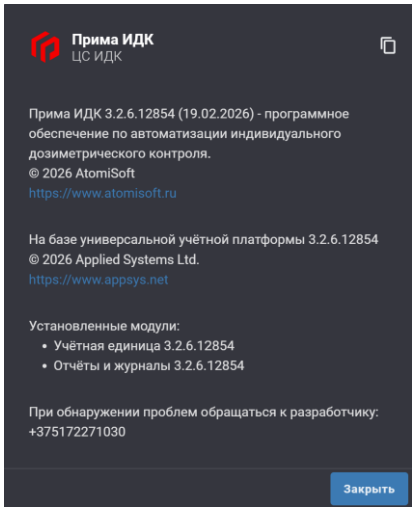

Рисунок 3.5. Пример диалогового окна «О программе»

3.2. 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/системными логами;
– настройка параметров аутентификации;

– работа с IP-адресами;

– просмотр установленных или подключенных модулей категорий и/или категорий;

– работа с лицензией.

Для регистрации пользователя с ролью «Администратор ИБ» необходимо:

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. Перейти на вкладку «Список пользователей» и нажать кнопку Добавить.

Шаг 3. Зарегистрировать нового пользователя с ролью «Администратор»:

– В полях «Логин» и «Временный пароль» введите необходимые данные для аутентификации регистрируемого пользователя;

– В поле «Сотрудник» при необходимости выбрать сотрудника, к которому будет привязана новая учетная запись с ролью «Администратор». Список сотрудников формируется из учетных единиц объекта конфигурации с присвоенной категорией «Сотрудники» (например, из учётных единиц справочника «Сотрудники», на который присвоена категория «Сотрудники»);

– Добавить IP адрес компьютера пользователя.

Шаг 4. Нажать кнопку «Сохранить».

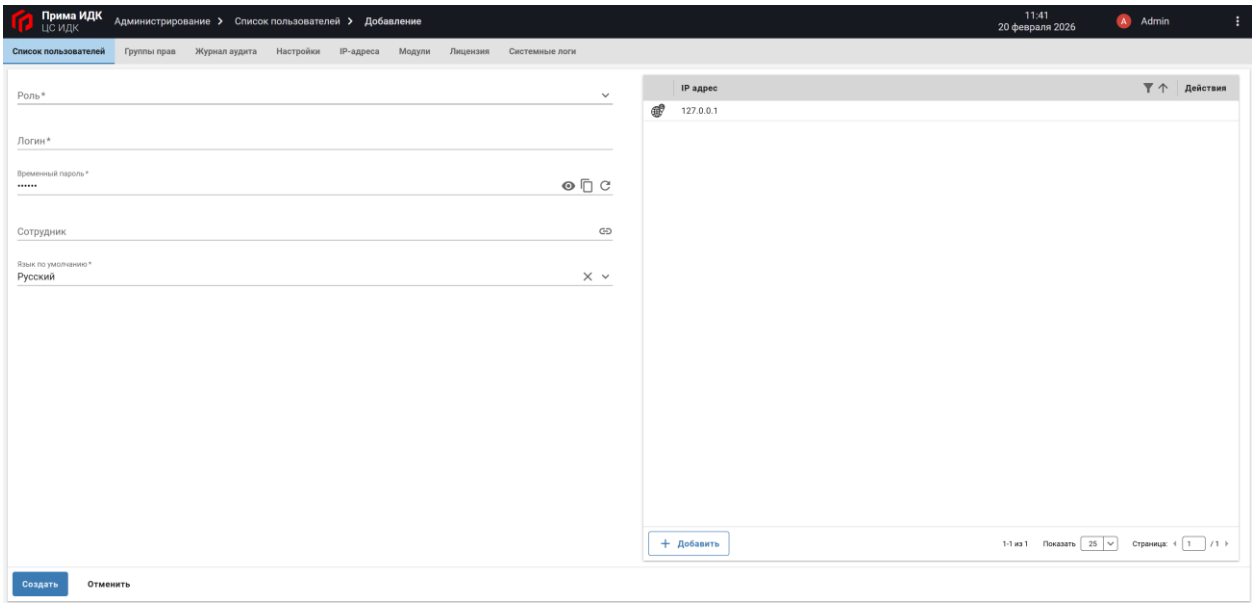

Рисунок 3.6. Форма для создания нового пользователя с ролью «Администратор»

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

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

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

Пользователю с ролью «Администратор ИБ» доступна возможность работы с журналом аудита. Для регистрации пользователя с ролью «Администратор ИБ» необходимо:

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. Перейти на вкладку «Список пользователей» и нажать кнопку «Добавить».

Шаг 3. Зарегистрировать нового пользователя с ролью «Администратор ИБ»:

– В полях «Логин» и «Временный пароль» введите необходимые данные для аутентификации регистрируемого пользователя;

– В поле «Сотрудник» при необходимости выбрать сотрудника, к которому будет привязана новая учетная запись с ролью «Администратор ИБ». Список сотрудников формируется из учетных единиц объекта конфигурации с присвоенной категорией «Сотрудники» (например, из учётных единиц справочника «Сотрудники», на который присвоена категория «Сотрудники»);

– Добавить IP адрес компьютера пользователя.

Шаг 4. Нажать кнопку «Сохранить».

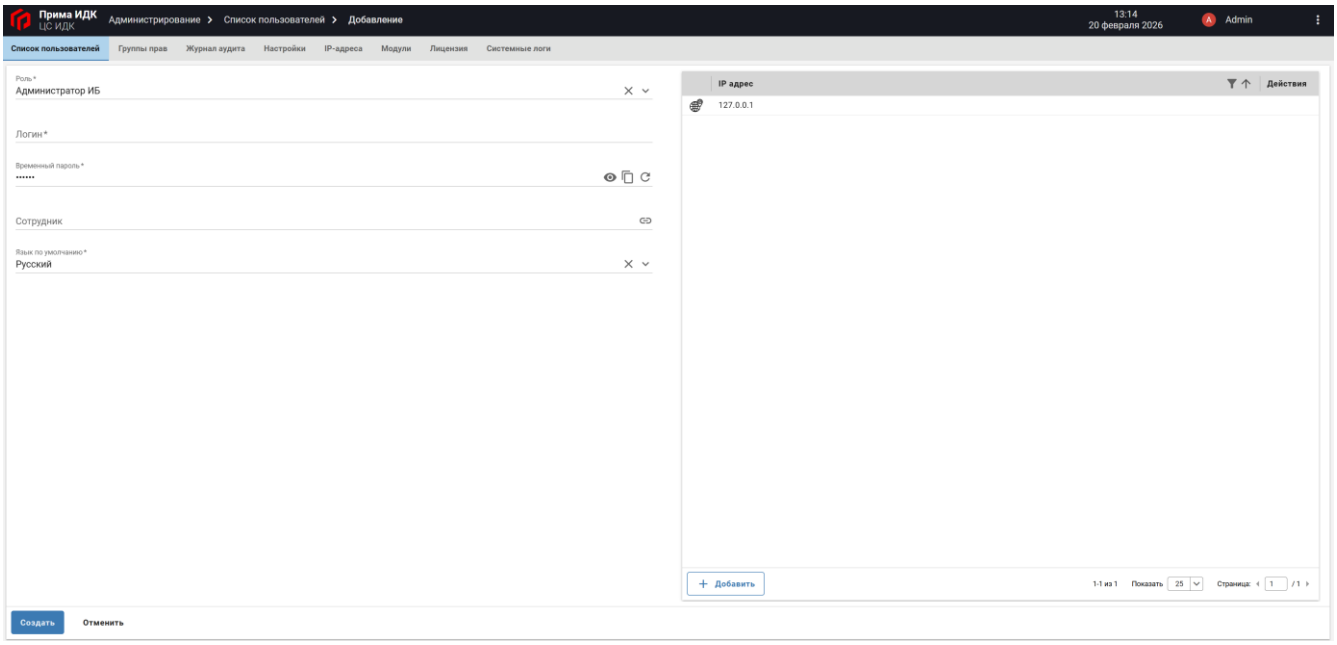

Рисунок 3.7. Форма для создания нового пользователя с ролью «Администратор ИБ»

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

3.4. 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. Для регистрации пользователя с ролью «Настройщик» необходимо:

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. Перейти на вкладку «Список пользователей» и нажать кнопку «Добавить».

Шаг 3. Зарегистрировать нового пользователя с ролью «Настройщик»:

– В полях «Логин» и «Временный пароль» введите необходимые данные для аутентификации регистрируемого пользователя;

– В поле «Сотрудник» при необходимости выбрать сотрудника, к которому будет привязана новая учетная запись с ролью «Настройщик». Список сотрудников формируется из учетных единиц объекта конфигурации с присвоенной категорией «Сотрудники» (например, из учётных единиц справочника «Сотрудники», на который присвоена категория «Сотрудники»);

– Добавить IP адрес компьютера пользователя.

Шаг 4. Нажать кнопку «Сохранить».

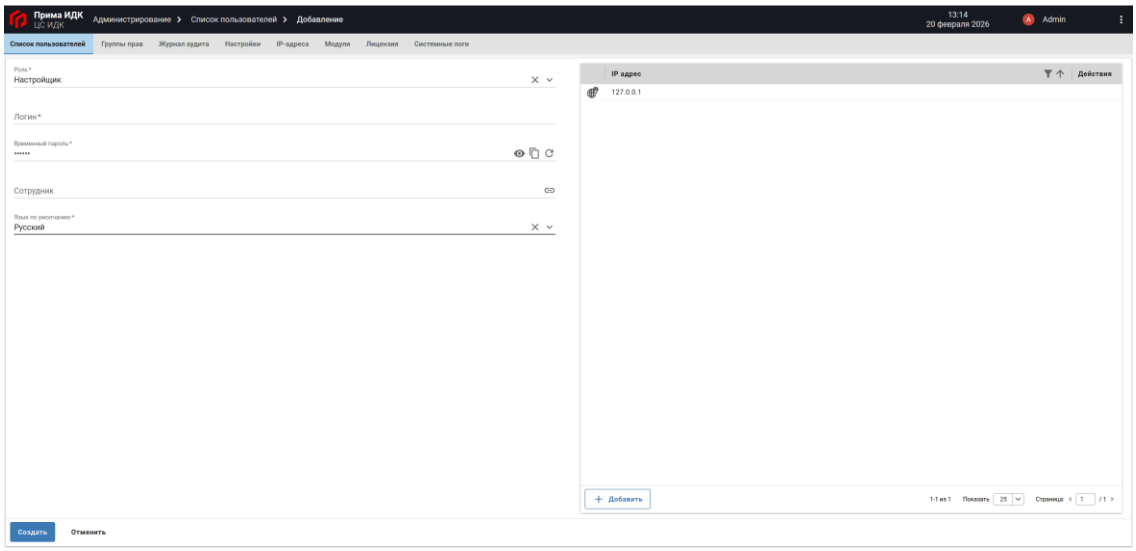

Рисунок 3.8. Форма для создания нового пользователя с ролью «Администратор ИБ»

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.

3.5. 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.

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. Перейти на вкладку «Группы прав».

Шаг 3. Нажать кнопку «Добавить» и введите название для новой группы прав.

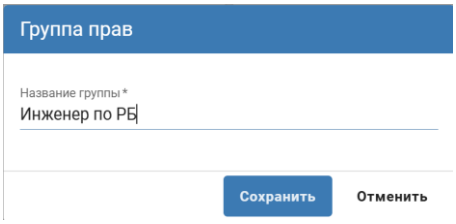

Рисунок 3.9. Окно для ввода названия новой группы прав

Шаг 4. Выбрать из списка областей, необходимую область которой будут владеть пользователи в созданной группе.

Шаг 5. Нажать кнопку «Сохранить».

Шаг 6. В правой части страницы выбрать необходимые права из списка для пользователей созданной группы.

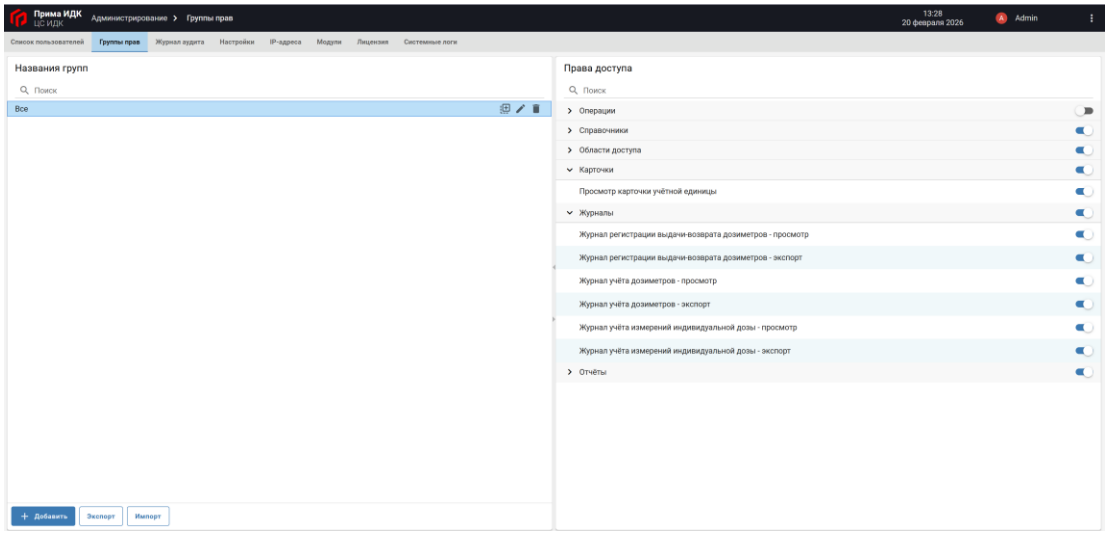

Рисунок 3.10. Пример настройки группы прав

При необходимости существует возможность отредактировать название группы прав с помощью кнопки , а также удалить необходимую группу прав с помощью кнопки .

3.6. Создание учетной записи пользователя с ролью «Учетчик»

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. Перейти на вкладку «Список пользователей» и нажать кнопку «Добавить».

Шаг 3. Зарегистрируйте нового пользователя с ролью «Учетчик»:

– В полях «Логин» и «Временный пароль» введите необходимые данные для аутентификации регистрируемого пользователя;

– Добавить IP адрес компьютера пользователя;

– В поле «Сотрудник» выбрать сотрудника, к которому будет привязана новая учетная запись с ролью «Учетчик». Список сотрудников формируется из учетных единиц объекта конфигурации с присвоенной категорией «Сотрудники» (например, из учётных единиц справочника «Сотрудники», на который присвоена категория «Сотрудники»);

– Выбрать группу прав для пользователя с ролью «Учетчик».

Шаг 4. Нажать кнопку «Сохранить».

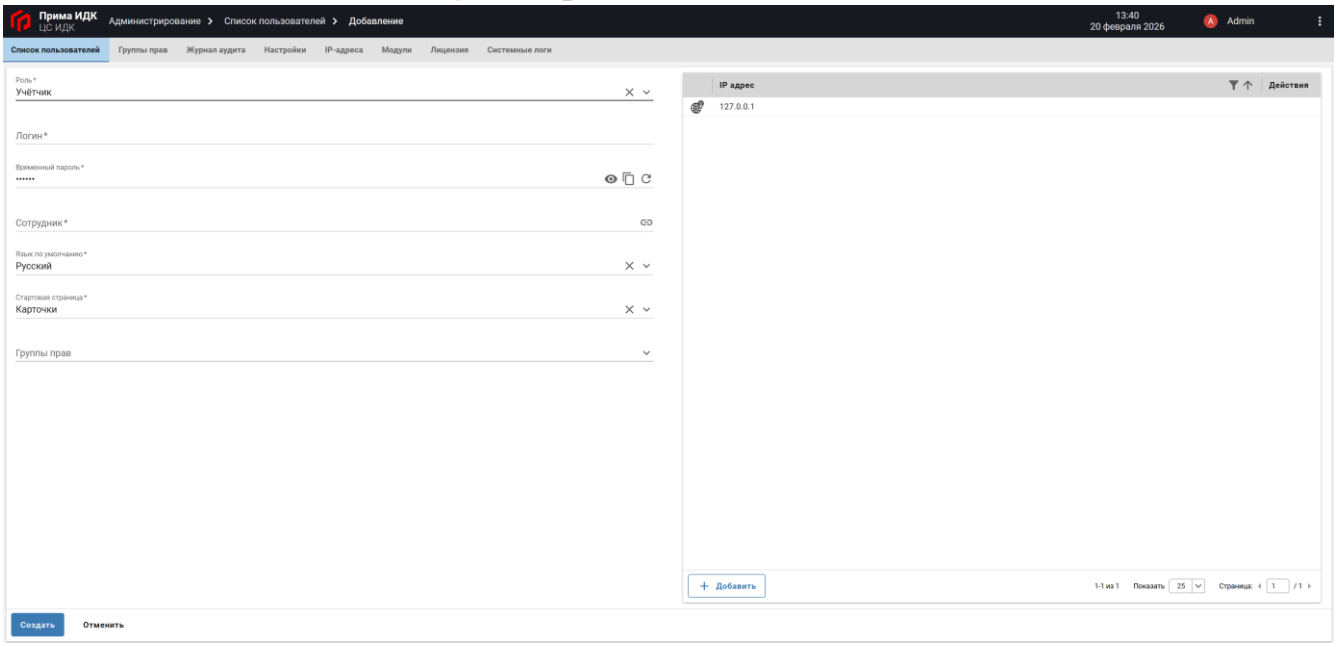

Рисунок 3.11. Форма для создания нового пользователя с ролью «Учетчик»

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. Деактивация учетной записи происходит автоматически в случае нарушения настроек аутентификации (См. п.3.12). Администратор таже имеет возможность деактивировать учетную запись вручную (принудительно) следующими шагами:

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. Перейти на вкладку «Список пользователей».

Шаг 3. Выбрать в таблице пользователя, которого необходимо деактивировать и в графе «Действия» нажать кнопку  (деактивировать).

Шаг 4. Подтвердить деактивацию нажатием кнопки  .

Важно: невозможно деактивировать всех администраторов, т.е. в ПО всегда остается один активный пользователь с ролью «Администратор».

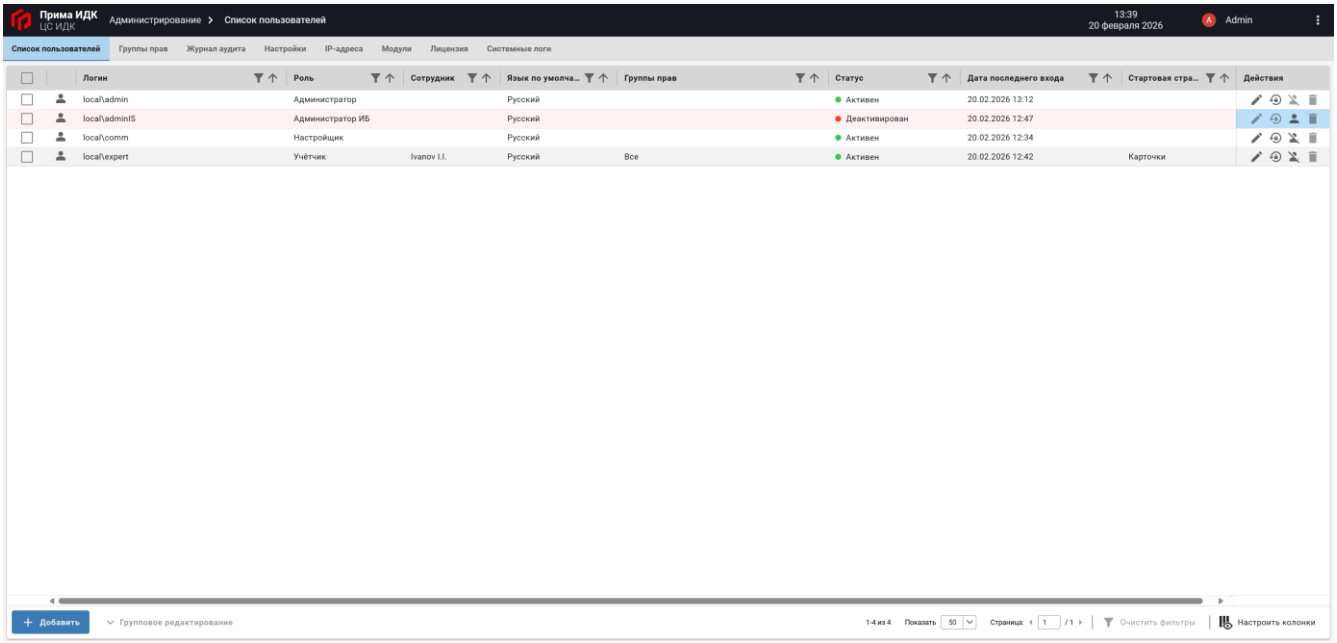

Рисунок 3.12. Пример страницы с деактивированным пользователем «expert_1»

3.8. Изменение данных в учетной записи пользователя

Для изменения информации в учетной записи пользователя выполните следующие действия:

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. Перейти на вкладку «Список пользователей».

Шаг 3. Выбрать в таблице пользователя, у которого необходимо изменить информацию и в графе «Действия» нажать кнопку (изменить).

Шаг 4. Внести необходимые корректировки для выбранного пользователя и нажать кнопку «Сохранить».

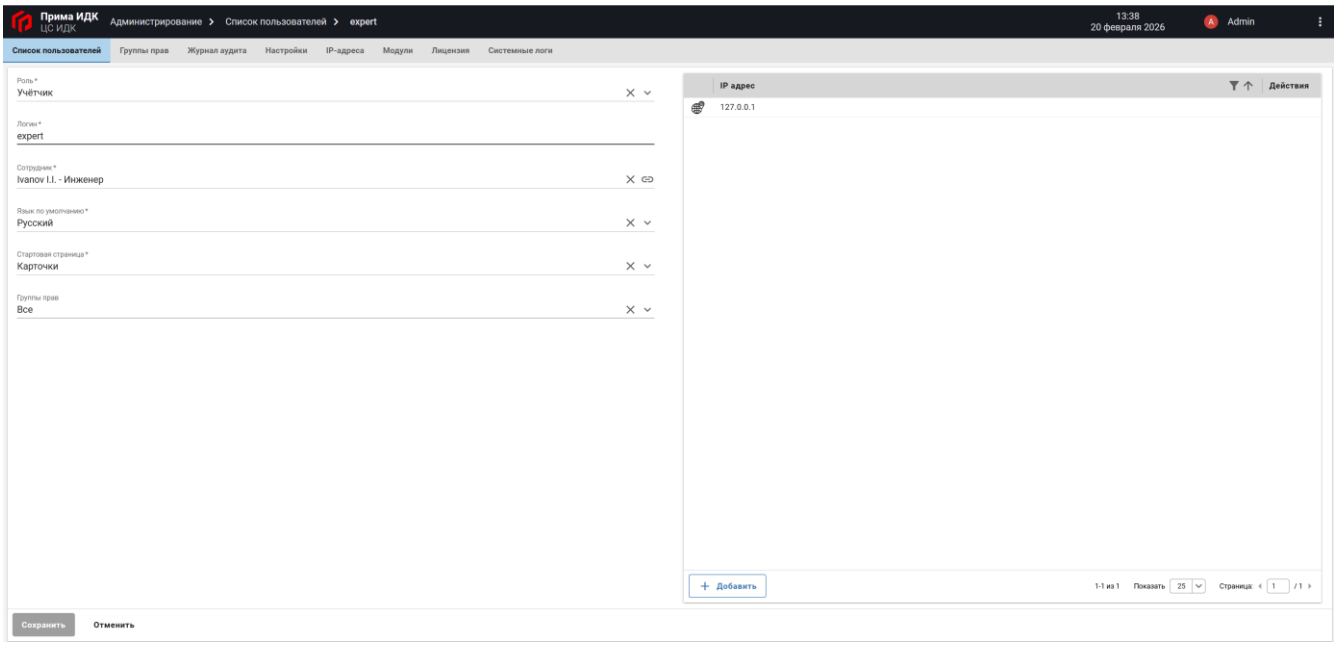

Рисунок 3.13. Пример формы редактирования данных о пользователе

3.9. Удаление пользователя

Удаление пользователей доступно только для учетных записей, под которыми ни разу не осуществлен вход в систему. Для удаления учетной записи пользователя необходимо:

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. Перейти на вкладку «Список пользователей».

Шаг 3. Выбрать в таблице из списка зарегистрированных пользователей учетную запись, под которой не было совершено ни одного входа в ПО и инициировать ее удаление с помощью кнопки .

Шаг 4. Подтвердить удаление учетной записи кнопкой .

3.10. Сброс пароля записи пользователя

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. Перейти на вкладку «Список пользователей».

Шаг 3. Выбрать в таблице пользователя, которому необходимо сбросить пароль и в графе «Действия» нажать кнопку (сбросить пароль).

Шаг 4. В диалоговом окне ввести новый первоначальный пароль для пользователя или выбрать предложенный системой пароль.

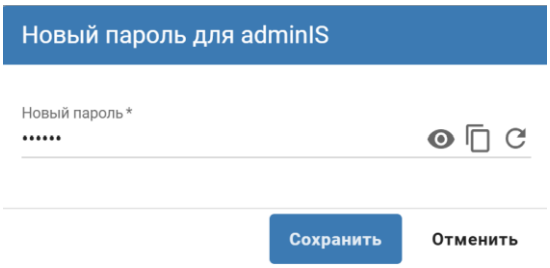

Рисунок 3.14. Пример диалогового окна по сбросу пароля для пользователя «adminIS»

Шаг 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.

3.11. Просмотр и экспорт журнала аудита

Журнал аудита – это журнал, в котором в виде записей фиксируются все действия и события, происходящие в ПО. Он служит для отслеживания действий, выполняемых пользователями и системными процессами. Журнал аудита в общем включает информацию о:

– входах и выходах пользователей: кто и когда входил в систему, а также когда выходил.

– изменениях данных: какие данные были изменены, добавлены или удалены, и кем.

– системных событиях: ошибки, предупреждения и другие важные события, которые могут повлиять на работу системы.

– доступе к ресурсам: какие пользователи имели доступ к определенным ресурсам и когда.

Журнал аудита состоит из следующих граф:

– Номер события;

– Дата и время – дата и время выполнения действия;

– Пользователь – логин пользователя совершившего действия;

– Сотрудник – ФИО и должность пользователя;

– IP адрес – IP адрес с которого произошло действие;

– Модуль/Платформа – Место внесения изменений;

– Результат – результат завершения действия: «Успех» или «Отказ»;

– Описание – описание действий, при нажатии на значение в данной строке открывается дополнительная информация.

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. На странице администрирования открыть вкладку «Журнал аудита» (Пользователю с ролью «Администратор ИБ» доступна только вкладка «Журнал аудита», поэтому для него после авторизации данная вкладка активна сразу).

Шаг 3. Откроется страница со списком всех действий в ПО с указанием данных о времени произведенных изменений и пользователе, вносившем изменения.

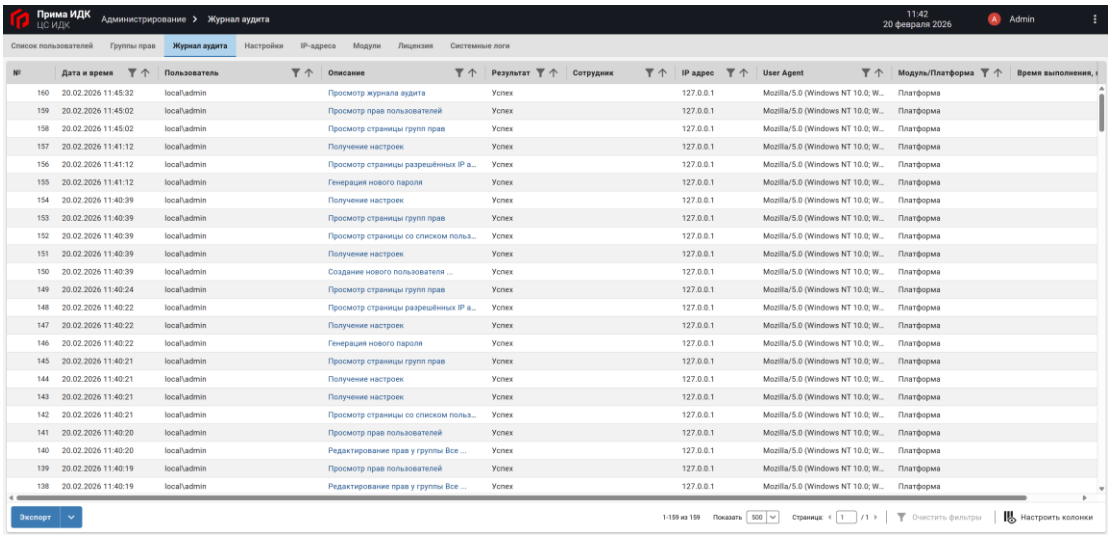

Рисунок 3.15. Интерфейс вкладки «Журнал аудита»

О каждом событии можно открыть подробные сведения, нажав на ссылку в соответствующем событии в графе «Описание».

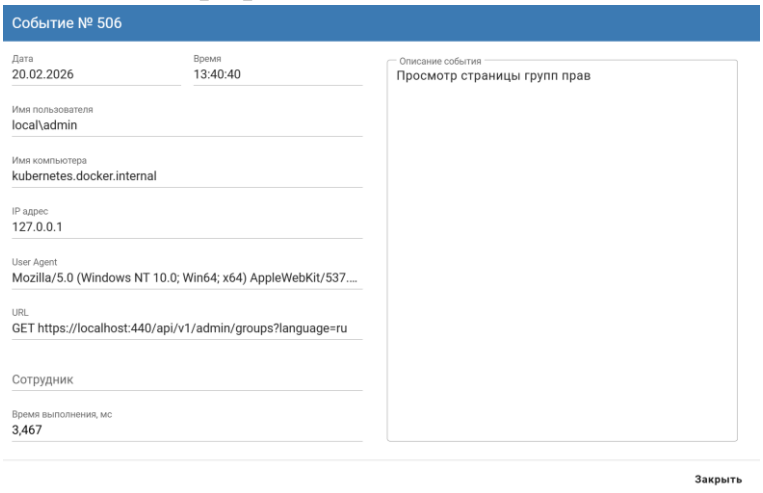

Рисунок 3.16. Диалоговое окно с подробными сведениями о событии

Также журнал событий можно отфильтровать на определённый заданный период, а также имеется возможность экспорта данных журнала в файл *.xlsx, *.csv, *.xml. При нажатии на кнопку «Экспорт», происходит экспорт данных журнала аудита в файл формата xlsx.

Выбор формата файла для экспорта журнала аудита происходит при нажатии на стрелочку возле кнопки «Экспорт»

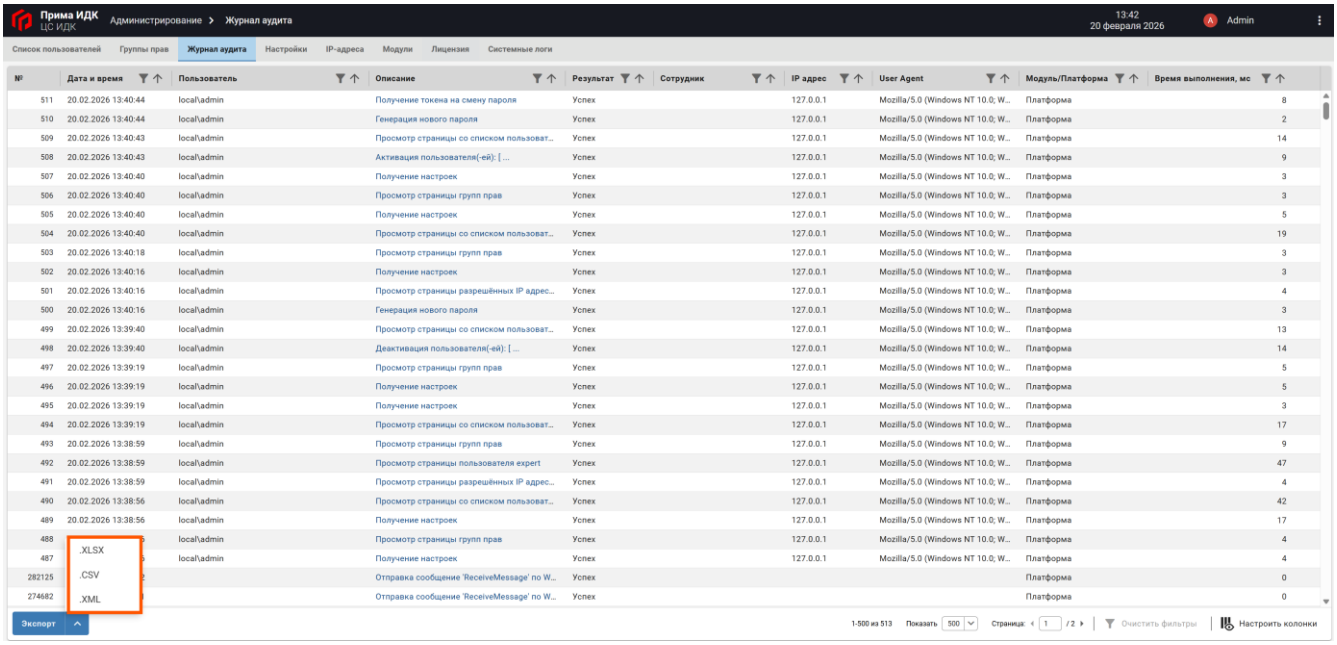

Рисунок 3.17. Выбор формата файла для экспорта журнала аудита

3.12. Настройка аутентификации

Шаг 1. Войти в ПО с правами администрирования.

Шаг 2. На странице администрирования открыть вкладку «Настройки».

Шаг 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.

Шаг 4. Нажать «Сохранить».

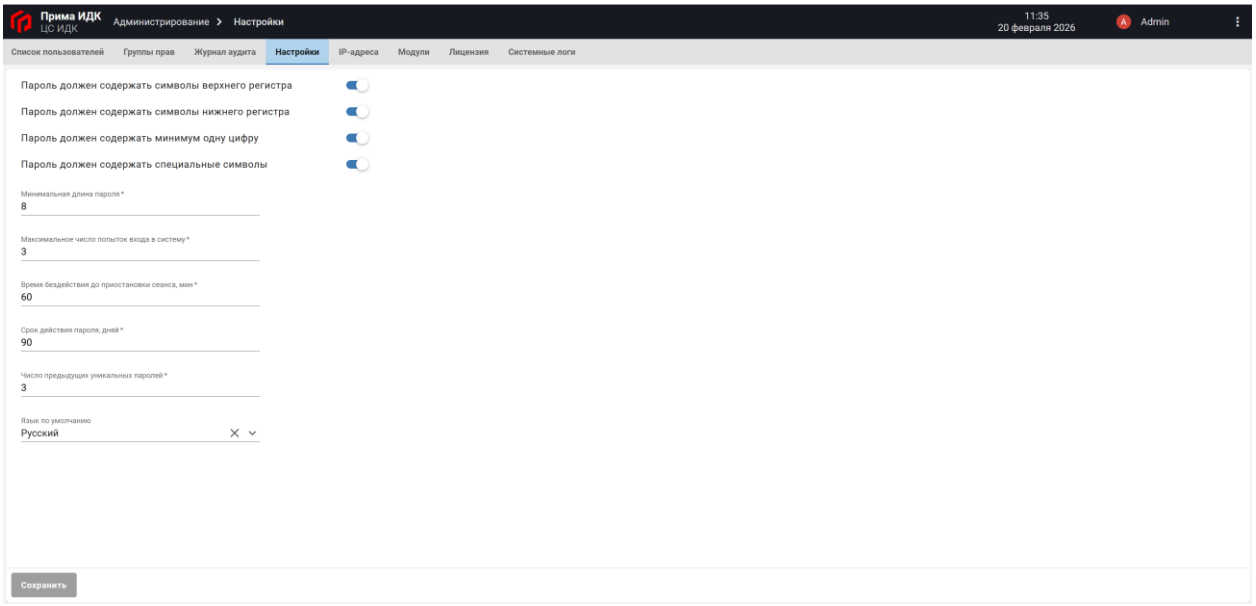

Рисунок 3.18. Пример настройки аутентификации

3.13. Снятие блокировки учётной записи

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

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. На странице администрирования открыть вкладку «IP-адреса» и выбрать «Заблокированные».

Шаг 3. Удалить из списка нужный IP Адрес.

Шаг 4. В главном меню перейти на вкладку «Список пользователей», выбрать в таблице пользователя, которому необходимо активировать доступ, нажать кнопку Активировать в деактивированной учетной записи.

Шаг 5. Нажать кнопку Сохранить.

3.14. Работа с IP-адресами

Для работы всех пользователей в системе необходима их привязка к глобальному (общедоступному) или пользовательскому (частному) IP-адресу. В ПО возможно указать разрешенные IP-адреса, доступ к ПО, с которых разрешен, а также список заблокированных IP-адресов, доступ с которых заблокирован. К IP-адресу также можно добавить маску сети, для поддержки конкретно необходимого списка IP-адресов.

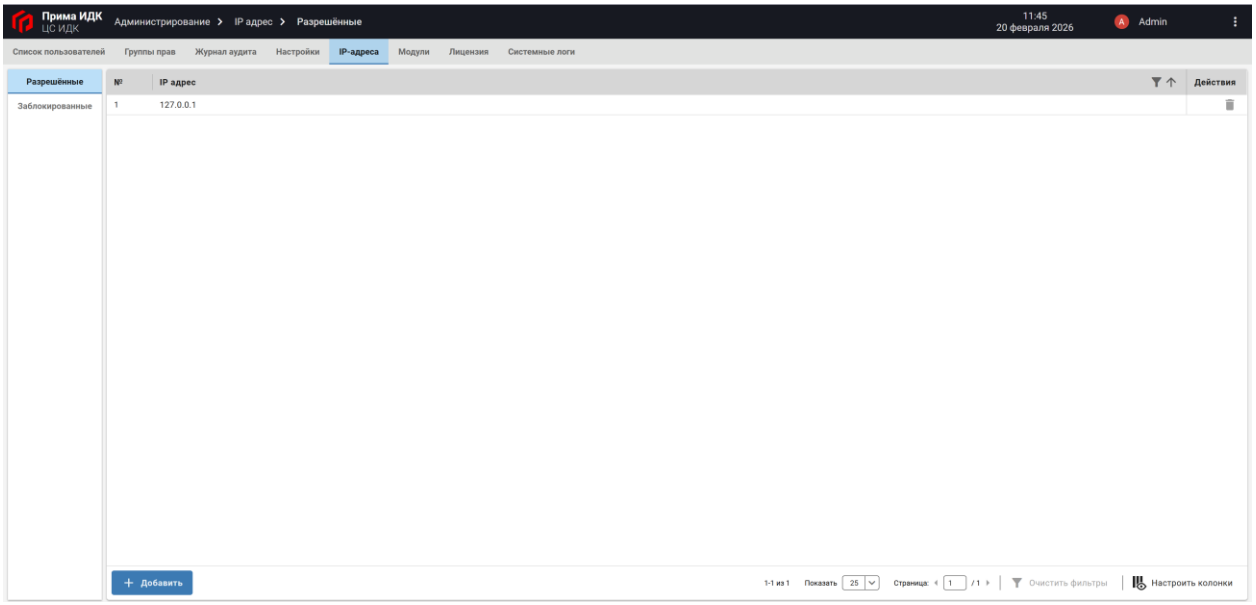

Рисунок 3.19. Интерфейс вкладки «IP-адреса»

Добавление IP-адреса в выбранный раздел выполняется следующим образом:

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. Перейти на вкладку «IP-адреса».

Шаг 3. Выбрать необходимый раздел куда добавляется IP-адрес: «Разрешенные» или «Заблокированные».

Шаг 4. Нажать кнопку «Добавить».

Шаг 5. В диалоговом окне ввести необходимый IP-адрес.

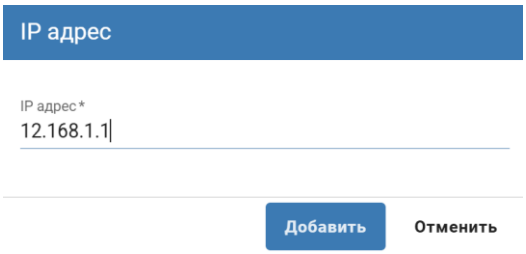

Рисунок 3.20. Диалоговое окно добавления IP-адреса

Шаг 6. Нажать кнопку «Сохранить».

3.15. Проверка установленных модулей к ПО

Контроль наличия установленных модулей необходимых версий производится выполнением следующих действий:

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. На странице администрирования открыть вкладку «Модули».

Данная страница содержит сформированный список доступных (установленных) модулей к ПО и информацию о них. Для каждого модуля также отображаются категории, добавленные в ПО после его установки.

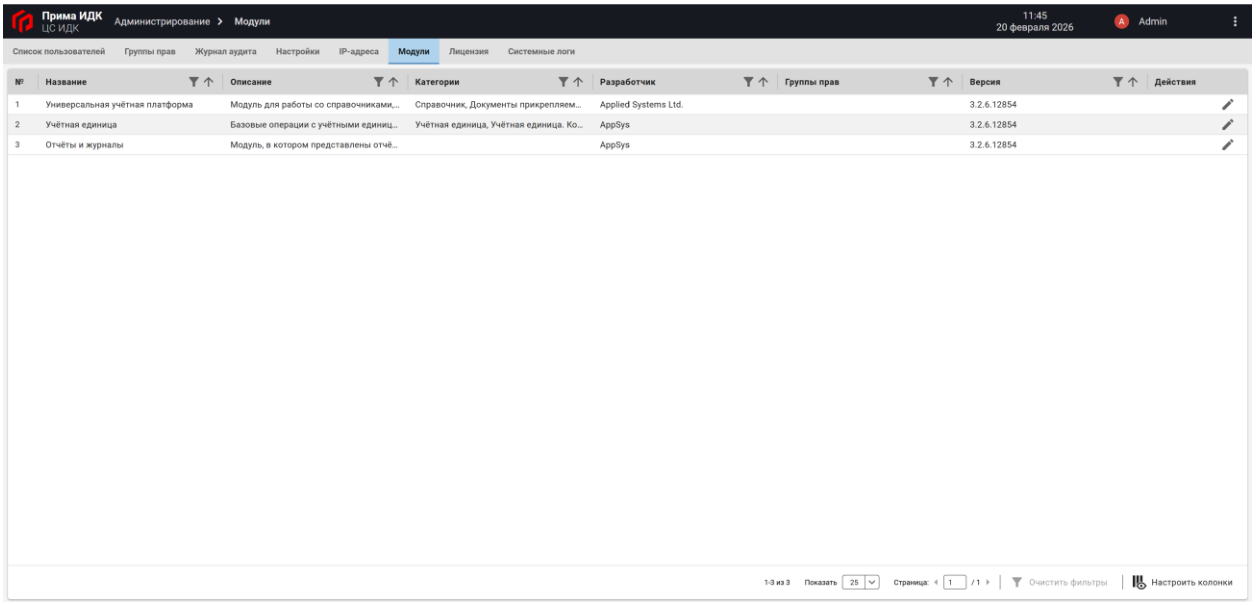

Рисунок 3.21. Пример формы на вкладке «Модули»

3.16. Работа с лицензией

Добавление лицензии в ПО производится следующими действиями:

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. На странице администрирования открыть вкладку **«Лицензия»**.

Шаг 3. На открывшейся странице нажать кнопку 

.

Шаг 4. В открывшемся всплывающем окне, нажать «Загрузить».

Шаг 5. В открывшемся окне выбрать необходимый файл с лицензией формата *.lic и нажать кнопку «Открыть».

Шаг 6. В всплывающем окне из шага 4 нажать «Сохранить». Добавленная лицензия становится активной. (Если в ПО уже были ранее добавленные лицензии, то предыдущая активная лицензия переводится в статус недействительной и сохраняется в истории лицензий. По делает запись в журнал аудита о загрузке новой лицензии.)

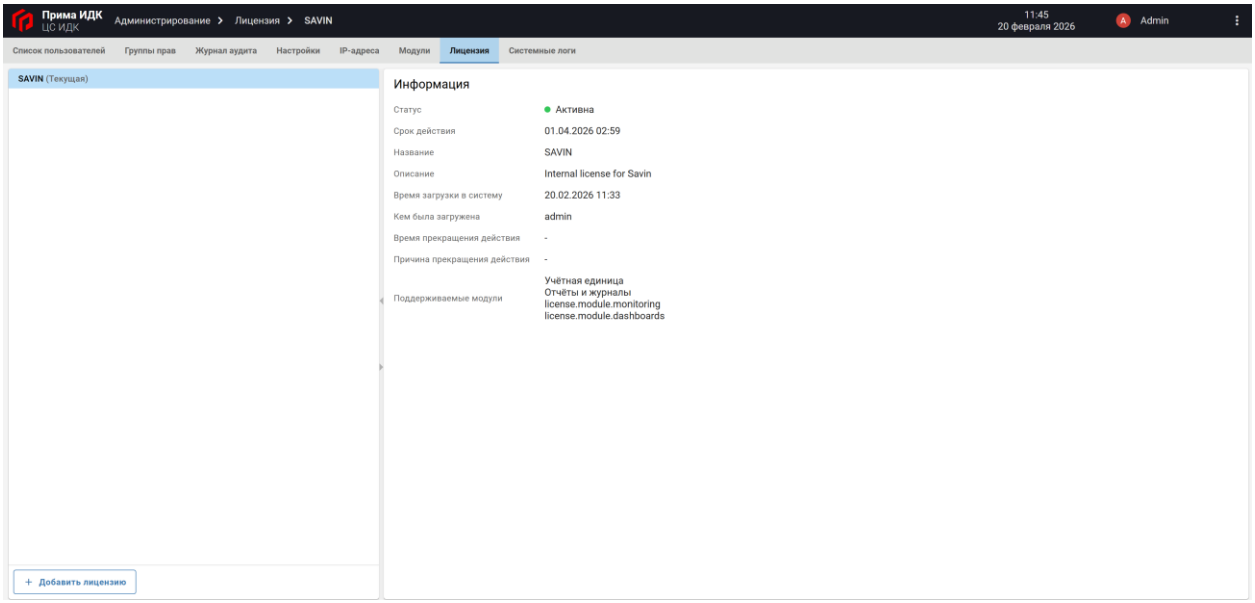

Рисунок 3.22. Пример загруженной лицензии и информации о ней для ПО «Прима ИДК»

При выполнении загрузки лицензии, ПО проверяется следующие условия лицензии:

- совпадение списка лицензируемых функций (модулей);
- серийного номера жесткого диска (Volume Serial Number) либо уникального идентификатора ПК, для которого была выдана лицензия
- срока действия лицензии.

Также вышеуказанные условия проверки лицензии ПО проверяет при:

- каждой авторизации пользователей;
- раз в час.

Если при загрузке лицензии было обнаружено, что лицензия не соответствует условиям, которые указаны выше, выводится сообщение об ошибке с информацией о причине отклонения загрузки. Данное событие фиксируется в журнале аудита.

При просмотре лицензии (как активной, так и лицензий из списка «История») для выбранной лицензии отображается:

- статус (активная, истекла, недействительна);
- срок действия;
- название;
- описание;
- время загрузки;
- имя пользователя, загрузившего лицензию;

- время прекращения действия (в случае, если срок действия лицензии истек либо она стала недействительной);
- причину прекращения действия (в случае, если срок действия лицензии истек либо она стала недействительной);
- список лицензируемых функций (модулей).

Для удаления лицензии необходимо нажать на соответствующую иконку рядом с лицензией, которую необходимо удалить. При удалении производится проверка, что лицензия не является активной. После удаления лицензия исчезает из списка «История», а также в журнал аудита делается запись об удалении лицензии.

При истечении срока лицензии либо при неудачной проверке условий лицензии, статус лицензии меняется на «Истекла» либо «Недействительна», делается соответствующая запись в журнале аудита, и к ПО применяются следующие ограничения:

- возможна авторизация только пользователей с ролью «Администратор»;
- остальные пользователи принудительно деавторизируются.

3.17. Интеграция с Microsoft Active Directory (MS AD) или openLDAP

Интеграция ПО с корпоративной службой каталогов Microsoft Active Directory или с openLDAP по протоколу LDAP дает возможность аутентификации в ПО пользователей зарегистрированных в MS AD/openLDAP.

Интеграция имеет следующие функциональные особенности:

1. ПО не сохраняет пароли пользователей MS AD/openLDAP.

2. Для пользователя ПО с ролью «Администратор» недоступны следующие действия в отношении учетных записей пользователей синхронизированных с MS AD/openLDAP:

– сброс пароля;

– ручное изменение синхронизированных данных;

– удаление учетной записи пользователя.

3. Обновление записей пользователей происходит при изменении данных в MS AD/openLDAP в следующих случаях:

– добавлен новый пользователь MS AD/openLDAP;

– пользователь MS AD/openLDAP удален;

– пользователь MS AD/openLDAP деактивирован, либо у пользователя пропали необходимые атрибуты для синхронизации;

– пользователь MS AD/openLDAP активирован после деактивации;

– произошли изменения в полях, которые отражены в списке пользователей либо в справочнике сотрудников конфигурации ПО.

4. Аутентификация выполняется в реальном времени с проверкой активности пользователя в MS AD/openLDAP.

5. ПО проверяет наличие и активность MS AD/openLDAP пользователя каждый раз при:

– аутентификации пользователя;

– при обновлении refresh токена пользователя.

6. Аутентификация пользователя проходит по следующему сценарию:

Шаг 1. пользователь вводит логин или email, и пароль согласно его учетным данным MS AD/openLDAP;

Шаг 2. ПО проверяет наличие пользователя MS AD/openLDAP в локальной базе данных;

Шаг 3. пользователь успешно аутентифицирован.

7. Синхронизированные пользователи MS AD/openLDAP на вкладке «Список пользователей» страницы администрирования ПО помечаются соответствующей иконкой - 

.

Для настройки интеграции пользователь ПО с ролью «Администратор» должен обладать правами доступа и учетными данными для подключения к MS AD/openLDAP. В конфигурации ПО должен быть создан (если таковой отсутствует) справочник сотрудников, который имеет присвоенную категорию «Сотрудник» (добавление справочника и назначение категории описано в «Руководстве настройщика ПО Прима ИДК»).

Интеграция MS AD/openLDAP по протоколу LDAP выполняется следующим образом:

Шаг 1. Пользователь ПО с ролью «Администратор» открывает файл **appsettings.customization.json** расположенный по пути *{корневая папка ПО}/customization/platform/bin/*.

Шаг 2. Указывает параметры подключения и учётные данные для подключения к MS AD/openLDAP. Подробное описание кастомизации настроек описано в таблице ниже.

Шаг 3. Определяет фильтры для синхронизации пользователей и сотрудников. Подробное описание кастомизации фильтров кастомизации описано в таблице ниже.

Описание настроек интеграции ПО с MS AD/openLDAP

Название поля	Тип данных / возможные значения	Описание	Пример
LDAP	object	Тип внешнего источника пользователей. Данные интеграции LDAP	см. ниже
vendor	string, enum	Сервис службы каталогов	- Active Directory - openLDAP
connection	object	Данные о подключении к LDAP серверу	см. ниже
connection.server	string	IP-адрес/URI сервера	- example.com - 192.168.1.1
connection.port	int	Порт	- 389 - 636
connection.username	string	DN пользователя для подключения. Для MS AD используется значение параметра distinguishedName пользователя	CN=Admin,CN=Users,DC=example,DC=example,DC=com
connection.password	string	Пароль	123456
connection.useSsl	bool	Использовать SSL при подключении по протоколу LDAP	- true - false
synchronization.enabled	bool	вкл/выкл синхронизацию	- true - false
synchronization.period	string, timespa	периодичность синхронизации	12:34:56

	n (HH:mm:ss)		
synchronization.delay	string, timespan (HH:mm:ss)	пауза перед стартом синхронизации	00:00:00
users	object	Объект описывает правила маппинга атрибутов пользователя LDAP в свойства пользователя ПО. Если объект пропущен - не выполняется синхронизация	см. ниже
users.uid	string	Атрибут пользователя LDAP, который будет использоваться в качестве внешнего идентификатора пользователя УУП и отсечки того, что пользователь внешний	- uidnumber (используется для openLDAP) - objectSID (используется для MS AD)
users.name	string	Атрибут пользователя LDAP, который будет использоваться в качестве именем пользователя для отображения в левом верхнем	- cn (используется для openLDAP/ MS AD) - SamAccountName (используется для openLDAP/ MS AD)

		углу, аудите и пр.	
users.mail	string	Атрибут пользователя LDAP, который используется как Email пользователя	example@example.com
users.objectClass	string	objectClass объекта LDAP, который будет использоваться для поиска пользователей	- user (используется для MS AD) - person или inetOrgPerson (используется для openLDAP)
users.path	string	Поддерево, в котором будет происходить поиск пользователей	CN=Users,DC= example,DC= example,DC=com
users.membership	string	Атрибут пользователя LDAP, использующийся для проверки членства пользователя в группе	- DistinguishedName (используется для MS AD) - uid (используется для openLDAP)
groups	object	Объект описывает поиска групп и определения принадлежности пользователя группе Если объект пропущен - не выполняется синхронизация	см. ниже
groups.membership	string	Атрибут группы LDAP, использующийся для проверки членства	- member (используется для MS AD) - memberUid (используется для openLDAP)

		пользователя в группе	
groups.objectClass	string	objectClass объекта LDAP, который будет использоваться для поиска групп пользователей	- group (используется для MS AD) - posixGroup (используется для openLDAP)
groups.path	string	Поддерево, в котором будет происходить поиск групп пользователей	CN=Users,DC= example,DC= example,DC=net
roles	array	Массив объектов. Описывает правила присвоения ролей ПО пользователям из LDAP	см. ниже
roles[].name	string, enum	Название одной из существующих ролей ПО. Невалидные роли игнорируются. Если все роли невалидны или массив пуст - синхронизация не выполняется	- uap.role.accounting.expert - uap.role.administrator - uap.role.commissioner - uap.role.info.security.officer
roles[].filter	object	Объект, в котором хранятся правила фильтрации пользователей LDAP. Логика поиска и фильтрации, следующая: 1. Получить всех	см. ниже

		пользователей 2. Выполнить фильтрацию по свойствам пользователя 3. Выполнить фильтрацию по группе, к которой принадлежит пользователь. ○ Найти группу ○ Взять в группе массив member/ memberUid. Оставить в выборке только тех пользователей, которые принадлежат этой группе ○ Если в фильтре указано несколько групп - пользователь должен состоять во всех Если правил несколько - пользователь должен удовлетворять всем.	
roles[].filter.users	array	Массив объектов, в которых	см. ниже

		указаны правила фильтрации пользователей LDAP по их атрибутам.	
roles[].filter.users[].attribute	string	Имя атрибута пользователя, по которому производится фильтрация	- cn - uid
roles[].filter.users[].operator	string, enum	Оператор сравнения для фильтрации. Поддерживается 6 операторов.	- eq - ne - gt - ge - lt - le
roles[].filter.users[].expression	string	Значение, по которому выполняется фильтрация: строка или шаблон поиска (wildcard) (например: Petrov*).	- user - group - *@mail.com
roles[].filter.groups	array	Массив объектов, в которых указаны правила фильтрации пользователей LDAP по атрибутам групп, к которым данные пользователи принадлежат. Синтаксис аналогичен полю roles[].filter.users	см. ниже
permissions	array	Массив объектов. Описывает	см. ниже

		правила присвоения групп прав ПО пользователям из LDAP. Формат описания объекта такой же, как и для массива roles	
employees	array	Объект описывает правила поиска и добавления элементов в справочник сотрудников Если объект пропущен - не выполняется синхронизация справочника сотрудников, остальные синхронизации по-прежнему выполняются	см. ниже
employees.entityDefinitionId	int	entityDefinitionId справочника сотрудников в конфигурации ПО. Для справочника сотрудников обязательно наличие категории «Сотрудник»	- 166 - 31
employees.filter	object	Формат описания объекта такой же, как и для объекта roles[].filter	см. ниже

employees.fields	array	Правила маппинга полей в учетной единице (УЕ) (с категорией «Сотрудник») значениями полей пользователя из LDAP. Если указаны не все обязательные поля - синхронизация не выполняется. Обязательные поля - поле externalId и все обязательные поля категории «Сотрудник», за исключением поля status	см. ниже
employees.fields[].name	string	Название поля УЕ в ПО (ее системное имя)	- externalId
employees.fields[].attribute	string	Название атрибута пользователя из LDAP. Применяется для не ссылочных полей в ПО	- objectsid
employees.fields[].selector	array	Правила выбора УЕ для заполнения ссылочных полей сотрудника	см. ниже

		Логика работы: 1. Поиск всех пользователей, удовлетворяющих фильтру 2. Для найденных пользователей найти тех, кто есть в результатах фильтра employees.filter 3. В ссылочное поле записать ссылку на соответствующую УЕ	
employees.fields[].selector[].entityId	int	entityId УЕ, которая будет записана в ссылочное поле сотрудника.	- 17 - 18
employees.fields[].selector[].filter	object	Формат описания объекта такой же, как и для объекта roles[].filter	см. ниже

Пример настройки интеграции для MS AD:

```
{
"externalUserSource": {
 "LDAP": {
  "connection": {
      "server": "examp.examp.com",
      "port": 389,
      "username": "CN=Admin,DC=examp,DC=examp,DC=com",
```

```
    "password": "Admin",
    "useSsl": false
},
"synchronization": {
    "enabled": true,
    "period": "24:00:00",
    "delay": "00:00:00"
},
"users": {
    "uid": "objectSid",
    "name": "SamAccountName",
    "mail": "mail",
    "objectClass": "user",
    "path": "CN=Users,DC=examp,DC=examp,DC=com",
    "membership": "DistinguishedName"
},
"groups": {
    "membership": "member",
    "objectClass": "group",
    "path": "CN=Users,DC=examp,DC=examp,DC=net"
},
"roles": [
    {
    "name": "uap.role.administrator",
    "filter": {
        "users": [
            { "attribute": "cn", "operator": "eq", "expression":
"Petrov*" }
            ]
        }
    },
    {
    "name": "uap.role.info.security.officer",
    "filter": {
        "groups": []
        }
    },
    {
    "name": "uap.role.commissioner",
    "filter": {
        "groups": []
        }
```

```
    },
    {
    "name": "uap.role.accounting.expert",
    "filter": {
        "users": [
            { "attribute": "cn", "operator": "eq", "expression":
"Petrov*" }
            ]
        }
    }
 ],
 "employees": {
    "entityDefinitionId": 35,
    "filter": {
        "groups": [
            { "attribute": "cn", "operator": "eq", "expression":
"Petrov*" }
        ]
    },
    "fields": [
        { "name": "externalId",            "attribute": "objectSid"
},
        { "name": "firstName",             "attribute": "givenName"
},
        { "name": "lastName",              "attribute": "sn" },
        { "name": "name",                  "attribute": "cn" },
        { "name": "individualNumber", "attribute": "sAMAccountType"
},
        {
            "name": "position",
            "selector": [
                { "entityId": 60, "filter": { "users": [{
"attribute": "sn", "operator": "eq", "expression": "Petrov*" }] } },
                { "entityId": 61, "filter": { "users": [{
"attribute": "sn", "operator": "eq", "expression": "Sidorov*" }] } },
                { "entityId": 62, "filter": { "users": [{
"attribute": "sn", "operator": "eq", "expression": "Ivanov*" }] } }
            ]
        },
        {
            "name": "department",
            "selector": [
```

```
                    {  "entityId":  80,  "filter":  {  "users":  [{
"attribute": "sn", "operator": "eq", "expression": " Petrov*" }] } },
                    {  "entityId":  81,  "filter":  {  "users":  [{
"attribute": "sn", "operator": "eq", "expression": "Sidorov*" }] } },
                    {  "entityId":  82,  "filter":  {  "users":  [{
"attribute": "sn", "operator": "eq", "expression": "Petrov*" }] } }
                ]
          }
     ]
 }
}
}
}
```

Пример настройки интеграции для openLDAP:

```
{
"externalUserSource": {
 "LDAP": {
     "connection": {
          "server": "192.168.1.1",
          "port": 389,
          "username": "CN=admin,DC=examp,DC=examp,DC=com",
          "password": "Admin"
     },
     "synchronization": {
          "enabled": true,
          "period": "00:01:00"
     },
     "users": {
          "uid": "uidnumber",
          "name": "cn",
          "mail": "mail",
          "objectClass": "person",
          "path": "dc=examp,dc=examp,dc=com",
          "membership": "uid"
     },
     "groups": {
          "membership": "memberuid",
          "objectClass": "posixGroup",
          "path": "DC=examp,DC=examp,DC=com"
     },
     "roles": [
```

```
{
     "name": "uap.role.administrator",
     "filter": {
          "groups": [
               {
                    "attribute": "cn",
                    "operator": "eq",
                    "expression": "uap_admins"
               }
          ]
     }
},
{
     "name": "uap.role.info.security.officer",
     "filter": {
          "groups": [
               {
                    "attribute": "cn",
                    "operator": "eq",
                    "expression": "uap_sec"
               }
          ]
     }
},
{
     "name": "uap.role.commissioner",
     "filter": {
          "groups": [
               {
                    "attribute": "cn",
                    "operator": "eq",
                    "expression": "uap_comm"
               }
          ]
     }
},
{
     "name": "uap.role.accounting.expert",
     "filter": {
          "groups": [
               {
                    "attribute": "cn",
```

```
                    "operator": "eq",
                    "expression": "uap_experts"
               }
          ]
     }
}
],
"employees": {
     "entityDefinitionId": 35,
     "filter": {
          "groups": [
               {
                    "attribute": "cn",
                    "operator": "eq",
                    "expression": "mcas_employees"
               }
          ]
     },
     "fields": [
          {
               "name": "externalId",
               "attribute": "uidnumber"
          },
          {
               "name": "firstName",
               "attribute": "givenName"
          },
          {
               "name": "lastName",
               "attribute": "sn"
          },
          {
               "name": "name",
               "attribute": "cn"
          },
          {
               "name": "individualNumber",
               "attribute": "employeeNumber"
          },
          {
               "name": "position",
               "selector": [
```

```
                {
                    "entityId": 60,
                    "filter": {
                        "users": [
                            {
                                "attribute": "sn",
                                "operator": "eq",
                                "expression": "Petrov*"
                            }
                        ]
                    }
                },
                {
                    "entityId": 61,
                    "filter": {
                        "users": [
                            {
                                "attribute": "sn",
                                "operator": "eq",
                                "expression": "Sidorov*"
                            }
                        ]
                    }
                },
                {
                    "entityId": 62,
                    "filter": {
                        "users": [
                            {
                                "attribute": "sn",
                                "operator": "eq",
                                "expression": "Ivanov*"
                            }
                        ]
                    }
                }
            ]
        },
        {
            "name": "department",
            "selector": [
                {
```

```
                    "entityId": 80,
                    "filter": {
                        "users": [
                            {
                                "attribute": "sn",
                                "operator": "eq",
                                "expression": "Petrov*"
                            }
                        ]
                    }
                },
                {
                    "entityId": 81,
                    "filter": {
                        "users": [
                            {
                                "attribute": "sn",
                                "operator": "eq",
                                "expression": "Sidorov*"
                            }
                        ]
                    }
                },
                {
                    "entityId": 82,
                    "filter": {
                        "users": [
                            {
                                "attribute": "sn",
                                "operator": "eq",
                                "expression": "Ivanov*"
                            }
                        ]
                    }
                }
            ]
        }
    ]
}
}
}
```

Синхронизация данных проходит по следующему сценарию:

Шаг 1. ПО запускает процесс синхронизации сотрудников и пользователей по таймеру.

Шаг 2. В журнал аудита ПО добавляется запись о начале синхронизации − «Начало синхронизации сотрудников по протоколу LDAP».

Шаг 3. Пользователи MS AD/openLDAP синхронизируются со справочником сотрудников. ПО создает для каждого нового пользователя MS AD/openLDAP запись в справочнике сотрудников либо обновляет данные в записях справочника уже имеющихся пользователей MS AD/openLDAP.

Шаг 4. В журнал аудита ПО добавляется запись с перечислением успешно синхронизированных записей сотрудников − «Перечисленные записи успешно синхронизированы …».

Шаг 5. В журнал аудита ПО добавляется запись об окончании синхронизации сотрудников – «Успешное завершение синхронизации».

Шаг 6. В журнал аудита ПО добавляется запись о начале синхронизации − «Начало синхронизации пользователей по протоколу LDAP».

Шаг 7. Новые пользователи MS AD/openLDAP синхронизируются со списком пользователей ПО. ПО создает для каждого нового пользователя MS AD/openLDAP учетную запись пользователя ПО либо обновляет данные в записях учетных записей пользователей ПО уже имеющихся пользователей MS AD/openLDAP.

Шаг 8. В журнал аудита ПО добавляется запись с перечислением успешно синхронизированных учетных записей пользователей − «Перечисленные записи успешно синхронизированы …».

Шаг 9. В журнале аудита ПО делает запись об окончании синхронизации пользователей − «Успешное завершение синхронизации».

При отсутствии описания интеграции ПО с MS AD/openLDAP, ПО продолжает работать только с локальными учетными записями. Пользователь с ролью «Администратор» создает локальные учетные записи пользователей вручную (см. п.п. 3.2 – 3.4.).

В случае отсутствия описания синхронизации сотрудников (объект *employees*) либо описания синхронизации пользователей (объект *users/groups* и массив *roles*) при синхронизации ПО пропускает шаг 3 (пропущен либо не заполнен блок *employees*) либо пропускает шаг 4 (пропущен либо не заполнены объект *users/groups* и массив *roles*)

При возникновении ошибок синхронизации вместо шагов 3-5 и/или шагов 7-9 синхронизации (в зависимости от того при какой синхронизации сотрудников и/или учетных записей пользователей произошли ошибки), делается запись об ошибке синхронизации − «Завершение синхронизации с ошибками».

Пользователю с ролью «Администратор» при изменении данных в учетных записях синхронизированных пользователей (подробнее см. п.3.8 «Изменение данных в учетной записи пользователя») доступно только добавление разрешенных IP адресов пользователей и изменение групп прав пользователей.

Пользователю с ролью «Администратор» доступна деактивация, а также повторная активация синхронизированных пользователей в ПО, если пользователь был деактивирован вручную внутри ПО (подробнее см. 3.7 «Деактивация учетной записи»).

При деактивации или удаления пользователя в MS AD/openLDAP, а также в случае, если был сменен сервер MS AD/openLDAP и в результате этого пользователи MS AD/openLDAP стали неактуальны, после шага 2 синхронизации данных, ПО получит данные о том, что пользователь MS AD/openLDAP удален или деактивирован. В справочнике сотрудников конфигурации ПО, в записи сотрудника соответствующему пользователю MS AD/openLDAP будет изменено поле «Статус» на значение «Снят с учёта». Затем ПО деактивирует учетную запись пользователя, соответствующую пользователю MS AD/openLDAP. В данном случае пользователю ПО с ролью «Администратор» недоступна повторная активация учетной записи пользователя.

3.18. Настройка экспорта журнала аудита во внешнюю систему Eventlog.

ПО позволяет экспортировать события журнала аудита в Eventlog ОС Windows.

Сообщения аудита экспортируются, при наличии соответствующей конфигурации в файлах appsettings.json (расположенный по пути *{корневая папка ПО}/bin/)* и appsettings.customization.json (расположенный по пути *{корневая папка ПО}/customization/platform/bin/).*

В файле appsettings.json задаются базовые параметры экспорта.

В файле appsettings.customization.json задаются специфичные параметры в зависимости от конфигурации ПО.

3.18.1 Описание конфигурации appsettings.json

Секция Audit.Export:

Параметр	Тип	Описание	Обязательный параметр	Значение по умолчанию

MaxBatchSize	int	Максимальное количество сообщений в одной пачке для отправки.	Да	512
MaxQueueSize	int	Максимальный размер очереди сообщений. При переполнении старые записи удаляются.	Да	2048
ScheduledDelay	int	Задержка между попытками отправки (в миллисекундах).	Да	500

Секция Audit.Database

Параметр	Тип	Описание	Обязательный	Значение по умолчанию
HostNameTtl	string	Время жизни кэшированных DNS-имен хостов в формате "чч:мм:сс"	Нет	"24:00:00"
CaptureHostName	boolean	Флаг, определяющий нужно ли записывать имя хоста в записях аудита	Нет	true

Секция Audit.EventLog:

Параметр	Тип	Описание	Обязательный параметр	Значение по умолчанию
LogName	string	Имя журнала Windows Event Log (Application, Security, System)	Да	Application

Пример законфигурированного файла appsettings.json:

```
"Audit": {
  "Export": {
    "MaxBatchSize": 512,
    "MaxQueueSize": 2048,
    "ScheduledDelay": 500
  },
  "Database": {
    "HostNameTtl": "24:00:00",
    "CaptureHostName": true
  },
  "EventLog": {
    "LogName": "Application"
  }
}
```

3.18.2 Описание конфигурации appsettings.customization.json

Секция Audit.Database:

Параметр	Тип	Описание	Обязательный параметр	Значение по умолчанию
CaptureHostName	bool	Записывать ли имя хоста в аудит-записи	Нет	true

Секция Audit.EventLog:

Параметр	Тип	Описание	Обязательный параметр	Значение по умолчанию
Language	string	Язык сообщений (ru, en и др.)	Да	ru
SourceName	string	Идентификатор источника событий в Windows Event Log	Да	В зависимости от конфигурации. Например, для конфигурации ИДК значение: PrimaIDK.

Пример законфигурированного файла appsettings.customization.json:

```
"Audit": {
  "Database": {
    "CaptureHostName": false
  },
  "EventLog": {
    "Language": "ru",
    "SourceName": "PrimaIDK"
  }
}
```

3.19. Раздел «Помощь»

Раздел «Помощь» даёт доступ к данному Руководству прямо из ПО пользователям с ролью «Администратор» и «Администратор ИБ». Для доступа к разделу «Помощь» необходимо:

Шаг 1. Войти в ПО с ролью «Администратор».

Шаг 2. Нажать на кнопку  в правом верхнем углу рядом с логином пользователя.

Шаг 3. В выпавшем списке нажать кнопку «Помощь».

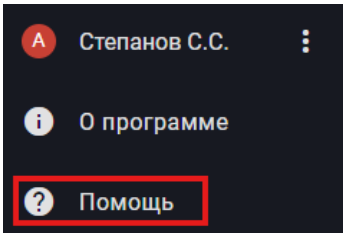

Рисунок 3.23. Кнопка «Помощь» в выпадающем списке

Шаг 4. После выполнения данных действий откроется Руководство в формате ***.pdf**.

4. 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**
Сбой операционной системы сервера	Вся информация, поступившая в ПО с момента окончания последнего резервного копирования данных.	Восстановление данных из резервных копий
Выход из строя жесткого диска	Вся информация, поступившая в ПО с момента окончания последнего резервного копирования данных.	Восстановление данных из резервных копий
Отсутствие на экране необходимой страницы в	Несохраненные администратором данные	Перезагрузка страницы кнопкой «Обновить» интернет-браузера; возврат на предыдущую страницу и

подсистеме администрирования		повторный клик по ссылке на необходимую страницу
Окна с сообщениями об ошибках в веденных данных подсистемы администрирования	Несохраненные администратором данные	Выполнить рекомендации, указанные в сообщении.
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
Долгая загрузка страниц ПО	Отсутствуют	Совместно с сотрудниками информационной безопасности организации произвести настройку антивируса «Kaspersky Security для Windows Server»

Приложение 1

Меры информационной и коммуникационной безопасности

№	Наименование меры	Мера
1	2	3
1.	Защита передачи данных в сети	Для передачи данных в сети необходимо использовать протоколы безопасной передачи данных (технологии VPN, TLS и т.д). Важные данные (чувствительная информация) должны передаваться в зашифрованном виде.
2.	Ведение и мониторинг записей отслеживания и аудита	Механизм записи должен быть активен во всех системах и сетевых устройствах. Записи должны храниться на устройстве или во внешних системах в течение приемлемого периода времени в соответствии с требованиями информационной безопасности и соответствующим законодательством, и должны быть защищены от несанкционированного доступа и изменений. Записи должны быть безопасно уничтожены по истечении приемлемого периода, определенного для их хранения.
3.	Управление записями аудита	Действия системного администратора, операторов и пользователей должны регистрироваться в приложении, записи должны храниться должным образом.
4.	Использование сервера времени	Для всех систем, подключенных к сети (серверов, рабочих станций, продукций безопасности, сетевых устройств и т.д.), должны быть предусмотрены механизмы синхронизации времени. В качестве источника надежных меток времени должны применяться основной и резервный сервер точного времени. См. меру № 91
5.	Подробное ведение записей	Записи отслеживания операционной системы и приложений необходимо хранить, включая описание события, источник события, время события, информация о пользователе / системе, адреса источника, адреса назначения и детали операции, а также их целостность должны быть защищены меткой времени.
6.	Управление неудачными попытками входа в систему	Должны быть приняты меры для предотвращения атак на механизмы входа в систему с использованием методов грубой силы (перебора паролей), такие как: ограничение запросов, увеличение таймаута между запросами, блокировка IP, блокировка пользователей, CAPTCHA и т.д. Должна быть функция регистрации неудачных попыток входа.
7.	Изменение пользователей и паролей по умолчанию	Все пользователи и пароли по умолчанию, используемые в тестовых средах, должны быть удалены или изменены перед запуском.
8.	Использование управляющих аккаунтов	Для внесения изменений в конфигурацию, режимы работы, прав доступа и т.п. должны использоваться отдельные привилегированные учетные записи пользователей. Должна

№	Наименование меры	Мера
1	2	3
		осуществляться регистрация событий (действий) совершаемых привилегированными учетными записями.
9.	Завершение необработанных системных доступов	Бездействующие системные доступы должны быть завершены через определенный период времени.
10.	Аутентификация	Доступ к корпоративным ресурсам должен обеспечиваться только после аутентификации пользователя.
11.	Создание записей отслеживания для операций резервного копирования	Операции резервного копирования должны регистрироваться в журналах системы. Записи должны храниться в течении определенного периода времени с учетом требований информационной безопасности и соответствующего законодательства и защищены меткой времени. См. меру № 2
12.	Осуществление управления пользователями	Приложения должны иметь интерфейсы для управления учетными записями пользователей, и эти интерфейсы должны быть доступны только авторизованным пользователям. В приложении должен быть функционал блокировки учетных записей пользователей на некоторый промежуток времени (на определенный период, условие и т.д.) или на длительное время (навсегда, если не указано иное).
13.	Создание записей отслеживания для операций аутентификации	Должна осуществляться регистрация событий успешных и неуспешных попыток аутентификации. См. меру № 2
14.	Безопасность аутентификационной информации	Когда пользователь осуществляет вход в систему, в поле ввода пароль пользователя по умолчанию должен быть скрыт и не должен быть видимым. Функция забытого пароля и другие средства восстановления не должны раскрывать текущий пароль, а новый пароль не должен отправляться пользователю в виде открытого текста. Учетные данные для аутентификации следует передавать только по безопасным каналам. Пароль или другая аутентификационная информация не должна храниться в виде открытого текста. Для защиты этой информации следует использовать сильные криптографические методы (шифрование, «соление», хеш), устойчивые к атакам грубой силы.
15.	Установка первого пароля	Приложение должно обладать функционалом установить безопасный механизм генерации пароля и механизма пересылки для безопасной передачи сгенерированных паролей. Должен быть функционал принудительной смены паролей при первом использовании.
16.	Не использовать имя пользователя и пароли по умолчанию	В системах должна быть обеспечена возможность смены пароля для всех служебных (сервисных) учетных записей (базы данных, веб-серверы, выполнение скриптов и пакетных заданий и т.д.).

№	Наименование меры	Мера
1	2	3
		В системе должна быть обеспечена возможность смены учетной записи «по умолчанию» для служебных учетных записей. Порядок смены служебных учетных записей и паролей к ним должен быть отражен в эксплуатационной документации на систему. Смена пароля служебной учетной записи не должна приводить к нарушению работы системы.
17.	Отсутствие аутентификационной информации в исходном коде	Конфиденциальная информация, ключи API и пароли не должны содержаться в исходном коде и/или репозиториях исходного кода. Вся используемая аутентификационная информация должна быть зашифрована и храниться в защищенном месте. Если используется аутентификация на основе инфраструктуры открытого ключа, должны быть предусмотрены механизмы, разрешающие доступ к закрытому ключу только авторизованному пользователю.
18.	Управление паролями	Поля ввода пароля не должны препятствовать вводу длинных и сложных паролей (не менее 16 символов), включая цифры и специальные знаки. В системе должен быть реализован функционал настройки требований к сложности, длине, минимальному и максимальному сроку действия пароля. Функция изменения пароля должна охватывать старый пароль, новый пароль и подтверждение пароля. Вопросы в виде информационного допроса (секретные вопросы) не должны использоваться для аутентификации.
19.	Меры предосторожности против атак на функции аутентификации	Функции восстановления и сбора пароля учетной записи, не должны раскрывать сведения о наличии (отсутствии) учетной записи, а также присутствия учетной записи, но неверном пароле. Возвращаемые сведения не должны содержать детализированной причины отказа авторизации. Для аутентификации должны применяться механизмы устойчивые к атакам воспроизведения. Должен быть функционал применения методов безопасности для предотвращения атак грубой силы (ограничение запросов, блокировка IP, CAPTCHA и т.д.). Успех процесса аутентификации не считается успешным через такие значения, как размер пакета. Для доступа к учетным записям необходимо использовать механизм аутентификации, устойчивый к атакам воспроизведения.
20.	Создание нового доступа и нового идентификатора доступа после	В результате аутентификации и всех процессов повторной аутентификации должны создаваться новые сессии доступа к системе и новые идентификаторы доступа. Идентификаторы доступа должны быть достаточно длинными, случайными и уникальными среди действующих системных доступов.

№	Наименование меры	Мера
1	2	3
	процессов аутентификации	Созданный идентификатор доступа необходимо использовать только один раз (в рамках установленной сессии доступа).
21.	Проверка подлинности доступа и обеспечение его безопасности	Идентификаторы доступа, созданные приложением, должны использоваться в качестве идентификаторов активного доступа в приложении. Необходимо обеспечить, чтобы идентификатор доступа не отображался URL-адресе, сообщениях об ошибках и журналах регистрации событий. Необходимо предотвратить перезапись идентификатора доступа в URL-адресе.
22.	Завершение пользовательских доступов	Функция выхода из системы должна быть доступна со всех страниц, доступ к которым осуществляется с помощью аутентификации. Кроме того, необходимо определить срок действия созданного идентификатора доступа. Доступ должен стать недействительным по истечении определенного времени, после определенного периода бездействия или после выхода пользователя из системы. Механизм авторизации необходимо использовать в процессе обновления соответствующих периодов. Кроме того, в ситуации, когда информация приводит к тому, что доступ становится недействительным (обновление пароля пользователя, обновление авторизации и т.д.), необходимо обеспечить завершение активных доступов. При системном выходе все области временного хранения и файлы cookie, связанные с доступом на клиенте и сервере, должны быть удалены приложением.
23.	Использование механизмов безопасности доступа	Необходимо использовать механизмы безопасности доступа, обеспечиваемые платформой, языком программирования и протоколом связи. В cookie файлах веб-приложений необходимо использовать флаги HTTPOnly, Secure, SameSite и т.д. Карта идентификаторов доступа, хранящихся в файлах cookie, должна иметь ограничительное значение, подходящее для приложения.
24.	Управление авторизацией	Приложение должно обладать функционалом настройки ролей. Пользователь должен иметь доступ и использовать только те компоненты и ресурсы приложения, для которых он авторизован. Контрольная проверка авторизации должна применяться для каждого запроса к приложению.
25.	Регистрация доступа к важным данным и ресурсам	Приложение должно иметь возможность создавать записи аудита для регистрации доступа к данным и ресурсам, которыми оно управляет. См. меру № 2
26.	Файлы конфигурации, записи аудита, записи отслеживания и т.д.	Системные файлы и файлы конфигурации, принадлежащие приложению, а также информация, такая как записи аудита и записи отслеживания, не должны храниться в том же месте

№	Наименование меры	Мера
1	2	3
	Нехранение информации в том же месте, что и пользовательские данные	(каталог, системный раздел и т.д.), где имеются пользовательские данные. См. меру № 2
27.	Отключить кеширование клиента для критических данных	В системе (ПО) должна быть предусмотрена функция отключения возможности кэширования данных на стороне клиента.
28.	Не хранить ресурсы, используемые приложением, в небезопасных средах	Приложение не должно хранить записи, которые оно использует или создает (изображения, офисные файлы, записи отслеживания и т.д.) в небезопасных средах (общий каталог, USB-диск и т.д.).
29.	Проверка файлов, полученных из ненадежных источников	Приложение должно проверять тип и содержимое файлов, полученных из ненадежных источников, и удостоверяться, не содержат ли они содержимое, которое может привести к уязвимости безопасности. Эти файлы должны храниться с ограниченными разрешениями вне основного каталога приложения. Эти файлы нельзя запускать и включать в запускающий код (как параметры, расширение и т.д.).
30.	Ограничение доступа к ресурсам	При совместном использование ресурсов между разными источниками (CORS) следует предотвратить доступ ненадежных ресурсов к данным приложения. Перенаправления URL-адресов должны выполняться только на известные адреса из белого списка, и, если требуется перенаправление на неизвестные адреса, необходимо предупредить и получить подтверждение пользователя.
31.	Использование в приложении компонентов обновленных мер безопасности и исправлений	Для приложений должны быть использованы обновленные и стабильные версии компонентов, баз данных, веб-серверов и т.д. не содержащие известных уязвимостей и поддерживаемые производителем. Разработчиком ПО должна быть обеспечена возможность обновления программного обеспечения (в том числе операционной системы и заимствованного ПО) без нарушения работоспособности приложения. См. меру № 97
32.	Ужесточение защиты совместного использования ресурсов и безопасности контента	Необходимо использовать безопасные заголовки HTTP (X-Frame-Options, Content-Security-Policy и т.д.) для приложения и обеспечения безопасности ресурсов на стороне клиента. Контроль доступа необходимо проводить для файлов, данных или ресурсов, которые приложение использует совместно с другими системами, приложениями или людьми.
33.	Защищенная и раздельная установка	Должна быть предоставлена эксплуатационная документация, содержащая в том числе инструкции и рекомендации по безопасной установке и настройке продуктов.

№	Наименование меры	Мера
1	2	3
		Приложение должно быть разработано с использованием многоуровневой архитектуры (multitier architecture), и для каждого уровня должны быть созданы механизмы безопасности. Базы данных и записи, используемые приложением, должны быть настроены так, чтобы к ним нельзя было получить доступ напрямую из Интернета.
34.	Доступ к серверам и рабочим средам только для приложений и авторизованных пользователей	Необходимо применить необходимые конфигурации безопасности, чтобы только приложение и авторизованные пользователи могли получить доступ к серверам и рабочим средам (базе данных, файловой системе, службам и т.д.).
35.	Использование учетных записей с минимальной авторизацией, необходимых для связи между серверами	Для обеспечения взаимодействия между компонентами приложения и серверами (например, сервер приложений – сервер базы данных) должны использоваться учетные записи с минимальными привилегиями необходимыми для обеспечения такого взаимодействия.
36.	Не использование реальных данных в среде тестирования и разработки	Данные, которые будут использоваться в среде разработки и / или тестирования, не должны быть реальными данными. Поэтому данные, подходящие для этой цели, должны быть созданы для использования в соответствующих средах.
37.	Использование текущих клиентских и серверных технологий	Серверные или клиентские технологии, для которых истек срок технической поддержки от производителя, с уязвимыми мерами безопасности или технологии, срок действия которых истек, не должны использоваться.
38.	Выполнение тестов безопасности приложений	Должен быть выполнен внешний анализ приложения на предмет выявления уязвимостей программного обеспечения, а также практический тест на проникновение, с предоставлением отчета по результатам тестирования приложения. При выявлении уязвимостей приложения и (или) возможности несанкционированного доступа к серверу, приложению, данным – недостатки должны быть устранены до передачи приложения заказчику.
39.	Отсутствие корпоративных данных в облачных хранилищах	Услуги облачного хранения не должны использоваться для сбережения / хранения важных корпоративных данных, за исключением частных систем компании или местных поставщиков услуг, контролируемых организацией внутри Республики Беларусь.
40.	Доступ только авторизованных пользователей к базам данных и носителям,	Доступ к базам данных и носителям приложения, в которых хранятся данные, должны выполняться только авторизованными пользователями, на соответствующих источниках должны выполняться авторизация и настройки.

№	Наименование меры	Мера
1	2	3
	в которых хранятся данные	
41.	Экспорт базы данных авторизованным пользователем	Экспорт базы данных приложения (сохранение в виде файлов, передача в локальные или удаленные приложения и т.д.) должен выполняться только авторизованными учетными записями.
42.	Отсутствие реальных данных в базе данных, используемой в среде тестирования и разработки	Фактические данные не должны использоваться в качестве тестовых данных. База данных в средах разработки и / или тестирования не должна содержать реальных данных. Вместо этого для соответствующих операций следует использовать специально сгенерированные данные. См. меру № 36
43.	Запрещение пользователям вносить изменения в записи аудита	В приложении должен быть реализован механизм ограничения доступа к журналам регистрации событий. Доступ к журналам регистрации событий в том числе на просмотр, удаление, резервное копирование и т.д. должен предоставляться, только учетным записям с соответствующими привилегиями (аудитор). В приложении должны быть предусмотрены механизмы экспорта журнала событий в машиночитаемых форматах или передача в системы сбора событий.
44.	Не хранить личные данные особого характера в виде открытого текста в базе данных	Персональные данные особого характера запрещено хранить в виде открытого текста в базе данных. Соответствующая информация должна храниться с использованием криптографических методов, принятых национальными и / или международными стандартами.
45.	Предоставление привилегий через роли и / или профили	Приложение должно определять привилегии для ролей и / или профилей, а не для пользователей, в соответствии с принципом минимальной авторизации в рамках возможностей, предлагаемых базой данных.
46.	Не использовать конфигурации по умолчанию	Небезопасные конфигурации по умолчанию (протокол связи, ненужные функции базы данных, небезопасные настроенные параметры по умолчанию и т.д.) не должны использоваться в базах данных. См. меру № 93
47.	Выявление ошибок и переход в безопасное состояние по умолчанию	Приложения должны быть спроектированы таким образом, чтобы обнаруживать любые ошибки, которые могут возникнуть, и по умолчанию переходить в безопасные состояния в ситуациях выявления ошибки. Например, в случае ошибки во время авторизации, приложение должно остановить соответствующий процесс, а пользователь не должен быть авторизован. Если в процессе аутентификации обнаруживается ошибка, следует запретить пользователю входить в приложение. Подробная информация о состоянии ошибки не должна отображаться пользователю.

№	Наименование меры	Мера
1	2	3
48.	Создание записей отслеживания ошибок и идентифицированных событий	Приложение должно иметь возможность создавать записи об успехе и неудаче определенных событий безопасности / операций (изменения авторизации, изменения пользователей, процессы аутентификации). В записи отслеживания должна быть как минимум следующая информация: • Информация о пользователе, совершившем операцию (физическое лицо или пользователь, определенный для программного процесса) • Время обработки • Идентификаторы исходной и целевой системы (IP, наименование сервера и т.д.) • Сводка операций (успешная операция, неуспешная операция и т.д.)
49.	Отсутствие сообщения об ошибке или записи отслеживания, включающей персональные данные особого характера	Приложение не должно создавать сообщения об ошибках или записи отслеживания, содержащие персональные данные особого характера.
50.	Включение информации о времени событий в записях отслеживания	Информация о времени должна быть включена в записи приложения, чтобы можно было провести исследование временной последовательности событий.
51.	Обеспечение безопасности записей отслеживания	Приложение не должно позволять изменять или удалять записи отслеживания, чтобы обезопасить их при взломе сервера приложений. См. меру № 2
52.	Предотвращение использования записей отслеживания в качестве вектора атаки	Чтобы гарантировать точность и целостность записей (не допуская подделку логов), приложение должно осуществлять контроль вводимых данных для записей, используемых при создании записей отслеживания. Такие меры, как кодирование символов и фильтрация, должны быть реализованы против уязвимостей (XSS и т.д.), которые могут возникнуть при просмотре записей. См. меру № 66
53.	Безопасное использование протокола SSL / TLS	Все аутентифицированные соединения в приложении, содержащие критические данные или функции, должны выполняться с использованием доверенной версии протокола SSL / TLS, не содержащей определенных уязвимостей. В сертификатах и во всей иерархии сертификата следует использовать надежные алгоритмы и протоколы, которые национальные и / или международные органы считают безопасными.
54.	Проведение аудитов сертификата	Для каждого сертификата сервера Transport Layer Security (TLS) от доверенного центра сертификации необходимо

№	Наименование меры	Мера
1	2	3
		создать цепочку доверия, и каждый доступный в Интернет сертификат сервера, должен быть действительным. Приложение должно быть настроено таким образом, чтобы оно могло проверять отзыв сертификата с помощью таких методов, как сшивание протокола статуса сертификата в сети (сшивание OCSP).
55.	Выполнение аудита проверки вводимых данных на стороне сервера	Приложение должно выполнять проверку вводимых данных на стороне сервера для каждого принятого типа данных.
56.	Создание записи отслеживания для ошибок проверки вводимых данных	В приложении должны создаваться записи отслеживания для ошибок, которые возникают во время процесса проверки вводимых данных в системах (сервере, приложении и т.д.), и соответствующий запрос должен быть отклонен. См. меру № 2
57.	Предотвращение несанкционированного запуска программы приложения	При разработке приложений должен соблюдаться принцип минимальной достаточности. В состав приложения должны включаться только необходимые для его функционирования компоненты, программное обеспечение, плагин и т.п. Все неиспользуемые для функционирования приложения компоненты должны быть удалены или отключены. Должен быть реализован механизм, запрещающий компонентам приложения осуществлять запуск сторонних программ и приложений. В приложениях должен соблюдаться принцип минимальной достаточности. Все неиспользуемые для работы компонентов приложения модули, программное обеспечение, плагины и т.п. должны быть деактивированы либо удалены. Необходимо обеспечить запрет программным модулям приложения запуска сторонних программ, приложений, компонентов, плагинов отличных от перечня необходимых.
58.	Не хранить важную информацию в конфиденциальных полях форм	Приложения, использующие структуру формы, не должны хранить важную информацию в конфиденциальных полях форм.
59.	Принятие мер предосторожности против атак CSRF	Необходимые меры безопасности приложения (токен CSRF, флаг SameSite и т.д.) должны быть приняты против уязвимости межсайтовой подделки запроса (CSRF).
60.	Предотвращение инъекционных атак на язык, используемый при доступе к базе данных	Все запросы к базе данных приложения должны выполняться параметрически, и должны быть приняты меры безопасности для предотвращения инъекционных атак против языка (SQL, NoSQL и т.д.), используемого для доступа к базе данных.
61.	Предотвращение уязвимостей,	Необходимо принять меры безопасности приложения против уязвимостей внедрения команд операционной системы.

№	Наименование меры	Мера
1	2	3
	связанные с внедрением команд в операционную систему	
62.	Предотвращение атак переполнения памяти	Необходимо принять меры против атак переполнения памяти в приложении и рабочей среде приложения.
63.	Предотвращение уязвимостей, связанных с включением файлов	Если приложение принимает путь к файлу в качестве входных данных, оно должно выполнить аудит безопасности, чтобы предотвратить уязвимости удаленного или локального хранения файлов.
64.	Предотвращение атак на основе XML	Приложение должно выполнять превентивные проверки безопасности на наличие уязвимостей XML (атаки на запросы XPath, атаки на внешние элементы XML, внедрение XML и т.д.).
65.	Проверка символов для неструктурированных данных	Допустимые символы и длина для неструктурированных данных в приложении должны быть определены, а контроль вводимых данных должен быть сделан в отношении возможных вредоносных символов, которые могут быть в содержании данных.
66.	Выполнение аудита вводимых данных	Аудит верификации следует выполнять для вводимых данных, таких как ввод данных в поля HTML-формы, вызовы REST, заголовки HTTP, файлы cookie, командные файлы.
67.	Представление веб-сервисов по защищенному протоколу	Представленные веб-сервисы приложения должны быть разработаны для работы с хорошо структурированным протоколом без уязвимостей, который поддерживает текущие версии SSL / TLS. См. меру № 53
68.	Создание и управление конфигурациями веб-сервисов авторизованными пользователями	Конфигурации веб-сервисов приложения (расположение, выделение сервисных портов для открытия, конфигурация сети и т.д.) должны выполняться и управляться авторизованными пользователями. По умолчанию конфигурации приложения должны быть настроены для обеспечения наивысшего уровня безопасности.
69.	Контроль аутентификации и авторизации в вызовах веб-сервиса	Контроль аутентификации и авторизации должен выполняться при каждом вызове веб-сервиса приложения.
70.	Аудит вводимых-исходных данных предлагаемых веб-сервисов	Предлагаемые веб-сервисы приложения должны быть разработаны и позиционированы таким образом, чтобы принимать меры предосторожности против разновидностей атак (XSS, удаленное выполнение кода и т.д.), вызванных отсутствием элементов аудита вводимых-исходных данных. Компоненты с известными уязвимостями (фреймворк, библиотека, программные модули и т.д.) не должны использоваться на этапе разработки веб-сервиса. См. меры 55-66.

№	Наименование меры	Мера
1	2	3
71.	Операции настройки и управления веб-сервисами	Приложение должно гарантировать, что только авторизованные пользователи могут получить доступ к функциям настройки и управления веб-сервисом.
72.	Не использовать персональные данные в качестве первичного ключа в базе данных	Персональные данные (идентификационный номер ТР, номер паспорта и т.д.) не должны использоваться в качестве первичных ключей при разработке таблиц базы данных.
73.	Экспорт базы данных авторизованным пользователем	Функция экспорта (сохранение в виде папки, передача на локальные или удаленные приложения и т.д.) в приложении должна осуществляться исключительно уполномоченными пользователями. См. меру № 41
74.	Запрет хранения персональных данных в небезопасных средах	Записи, содержащие личные данные (изображения, офисные файлы и т.д.), не должны храниться в небезопасных средах (неавторизованный публичный каталог, внешняя память, диск и т.д.). В случаях, когда обязательно нужно сохранить записи, необходимо использовать безопасные методы, принятые национальными / международными стандартами / органами.
75.	Контроль вводимых / исходящих персональных данных	В приложении должны быть реализованы меры безопасности против уязвимостей, вызванных отсутствием проверки вводимых / исходящих личных данных, используемых приложением в качестве входных. См. меры 55-66.
76.	Запрет хранения персональных данных в конфиденциальных зонах	Персональные данные не должны храниться в конфиденциальных областях веб-страниц приложения без согласия субъекта данных. Персональные данные не должны храниться в кеше браузера. Если файлы cookie, используемые в приложении, должны содержать личные данные, следует использовать безопасный флаг (secure flag). Кроме того, личные данные не должны записываться с помощью функции веб-хранилища на стороне клиента.
77.	Хранение персональных данных особого характера	Записи, содержащие персональные данные особого характера, должны храниться с использованием национальных / международно признанных методов безопасности (зашифрованный текст, использование надежных алгоритмов шифрования, шифрование на уровне файлов и т.д.). См. меру № 44
78.	Уничтожение временно хранимых персональных данных	Персональные данные, временно хранящиеся в клиентских и серверных приложениях, файлах и файлах cookie, должны быть уничтожены таким образом по истечении обработки или законного срока хранения, чтобы не было нарушения безопасности (невозможно получить, восстановить и т.д.).
79.	Регистрация доступа	Успешный и неудачный доступ к носителям, содержащим персональные данные, должны регистрироваться.

№	Наименование меры	Мера
1	2	3
80.	Обеспечение защиты записей доступа	Приложение должно блокировать несанкционированное чтение, изменение или удаление записей доступа к персональным данным. См. меру № 2
81.	Передача записей доступа	Записи доступа к персональным данным в приложении должны быть передаваемыми внутрь/извне. Импорт записей в работающую систему не должен уничтожать или изменять существующие записи.
82.	Использование механизма авторизации	Приложение должно обеспечивать, чтобы пользователи получали доступ только к персональным данным, для которых они авторизованы в матрицах авторизации доступа. Доступ к персональным данным должен быть заблокирован по умолчанию в случае несанкционированного доступа или непредвиденной ситуации. См. меру № 24 См. меру № 47
83.	Использование механизма аутентификации	Для доступа ко всем средам приложения, содержащим личные данные (веб-страница, файл и т.д.), должна выполниться аутентификация.
84.	Ограничение доступа	Доступ к средам, содержащим персональные данные (сервер базы данных, файловый сервер и т.д.), должен осуществляться только из приложения, и несанкционированный доступ к этим средам альтернативными и небезопасными методами должен блокироваться (прямой доступ с клиентами базы данных, доступ с использованием небезопасных протоколов и т.д.).
85.	Шифрование связи	Связь при обмене данными между системами (корпоративные приложения, внешние веб-службы) должна быть зашифрована. См. меру № 53
86.	Резервные копии системы, сделанные авторизованными пользователями	Следует обеспечить, чтобы резервные копии приложения, содержащие персональные данные, создавались только авторизованными пользователями. Приложение должно вести записи отслеживания для операций резервного копирования. См. меру № 2
87.	Создание записей отслеживания	Все операции в приложении, такие как авторизация, изменение авторизации, аннулирование, удаление, резервное копирование и т.д., выполняемые с ключами, должны регистрироваться для выполнения юридических обязательств, выявления подозрительных действий и предоставления возможностей судебного расследования в случае нарушений безопасности. См. меру № 2
88.	Безопасность сервиса	На серверах приложений и БД должны быть запущены и доступны только те сервисы, приложения, программные компоненты, которые необходимы для работы.

№	Наименование меры	Мера
1	2	3
		Неиспользуемые сервисы должны быть отключены. Запуск программных продуктов (сервисов, служб и т.п.) должен осуществляться с использованием сервисных учетных записей с минимально необходимыми привилегиями. Информация сетевых заголовков (banner) доступная при сетевом обращении к сервису должна быть (при возможности) изменена, для уменьшения уровня раскрываемой информации. Например, при обращении к веб-серверу не возвращаются сведения о версии и наименовании веб-сервера.
89.	Использование сервисов зашифрованной связи	Сервисы, использующие аутентификацию и связь без ввода пароля (Telnet, FTP, rlogin, HTTP, SMTP и т.д.), следует заменить на аналоги (SSH, SFTP, HTTPS, SMTPS и т.д.), которые обеспечивают шифрованную связь, если таковые имеются.
90.	Обеспечение синхронизации времени на серверах	Синхронизация времени должна быть обеспечена на всех серверах путем внесения соответствующих настроек NTP.
Требования к базе данных		
91.	Управление обновлениями и исправлениями	Должны использоваться системы управления данных поддерживаемые производителем с установленными обновлениями безопасности и не содержащие известных уязвимостей. При разработке/внедрении программного обеспечения должна быть предусмотрена возможность обновления программного обеспечения систем управления баз данных.
92.	Безопасная настройка параметров базы данных	Параметры, представленные для базы данных, должны быть структурированы с использованием методов, признанных безопасными национальными и / или международными органами (при их наличии). Кроме того, следует соблюдать рекомендации по безопасному использованию, опубликованные производителем системы управления базами данных (при их наличии).
93.	Не использовать учетные записи и пароли по умолчанию	Для запуска и эксплуатации СУБД не должны применяться учетные записи и пароли «по умолчанию».
94.	Защита записей истории команд / запросов	В случае, если история выполненных команд / запросов записывается в базе данных, должна быть обеспечена безопасность соответствующих записей / файлов.
95.	Удаление образцов данных	Образцы данных (образцы таблиц, записей, пользователей и т.д.), поступающие с установкой, должны быть удалены из базы данных.
Требования к серверу		
96.	Использование текущего программного	Следует использовать обновленные стабильные версии программного обеспечения веб-сервера, свободные от уязвимостей и поддерживаемые производителем. Кроме того, следует регулярно проверять наличие исправлений

№	Наименование меры	Мера
1	2	3
	обеспечения веб-сервера	безопасности для всех инструментов / пакетов программного обеспечения, используемых на сервере.
97.	Удаление поддержки WebDAV	Поддержка WebDAV (Web Distributed Authoring and Versioning) веб-сервера должна быть удалена. Модули, связанные с WebDAV, должны быть деактивированы или удалены.
98.	Управление пользователями веб-сервера	Программное обеспечение веб-сервера должно запускаться с учетной записи, специально созданной для этой цели, а не с учетной записи администратора. Учетные записи / пароли по умолчанию на веб-сервере должны быть отключены.
99.	Настройка веб-сервера для предотвращения раскрытия информации	Веб-сервер должен быть настроен для предотвращения раскрытия информации. Страницы ошибок и настроек по умолчанию должны быть удалены. Заголовки HTTP, которые вызывают раскрытие информации о технологии веб-сервера, должны быть удалены. Не должно допускаться раскрытие информации в ответах на неправильные HTTP-запросы.
100.	Ограничение поддерживаемых методов HTTP	Для работы веб-приложений должны использоваться методы POST POST, GET, OPTIONS и HEAD. При необходимости использования иных методов должны быть введены ограничения на возможность их использования только в потребностях веб-сервиса. Методы PUT: DELETE не должны использоваться для таких целей как загрузка или удаление файлов.
101.	Отключение листинга каталогов	Листинг каталогов веб-сервера должен быть отключен, если его использование не является необходимым для функционирования веб-приложения.
102.	Отключение режима отладки	Программное обеспечение веб-сервера не должно запускаться в режиме отладки.
103.	Определение пределов запросов	Для запросов должны быть установлены ограничения в объеме, поддерживаемом программным обеспечением веб-сервера.
104.	Ведение записей отслеживания	Должна осуществляться регистрация событий веб-сервера.
105.	Ограничение каталогов с разрешениями на запись	Необходимо указать каталоги с разрешениями на запись, права записи должны быть предоставлены только каталогам, которым требуется загрузка файлов. Необходимо удалить разрешение на запуск в каталогах файлов, загруженных через приложение.
106.	Использование SSL / TLS	Сервер должен быть настроен для использования SSL / TLS. В этом контексте на сервере следует использовать только версии SSL / TLS с надежной версией без известных уязвимостей.
107.	Перенаправление запросов с HTTP на HTTPS	Любой порт HTTP на веб-сервере должен направляться на порт сервера с использованием шифрования.

№	Наименование меры	Мера
1	2	3
108.	Удаление неиспользуемых модулей	Только модули, используемые на сервере, должны быть активными.
109.	Ограничение открытых портов	Веб-сервер должен прослушивать сетевые подключения только на авторизованных портах. Неиспользуемые порты необходимо закрыть.