ООО «АтомиСофт»

РУКОВОДСТВО АДМИНИСТРАТОРА ПО РАБОТЕ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ «ПРИМА РВ»

2024

СОДЕРЖАНИЕ

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Сокращение (обозначение)	Расшифровка (пояснение)
ОС	Операционная система
ПО	Программное обеспечение
СУБД	Система управления базами данных
УЕ	Учетная единица
РВ	Радиоактивные вещества
УУП	Универсальная учетная платформа

1. ОБЩИЕ ПОЛОЖЕНИЯ

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

В данном ПО функционал администратор разделен на две роли:

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

1.1. Область применения

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

1.2. Уровень подготовки администратора.

Администратор обязан знать:

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

соответствующую терминологию настоящего документа;

основные принципы работы сайтов.

Администратор ПО должен обладать следующими знаниями и навыками:

настройка и диагностирование работы ПО;

обслуживание технического и системного программного обеспечения ПО;

администрирование баз данных;

резервное копирование и восстановление данных;

обеспечение регламентных работ и анализ результатов регламентных операций.

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

настройка рабочих станций локальной вычислительной сети;

инсталляция, общесистемное сопровождение и администрирование;

администрирование СУБД.

2. ОСНОВНОЕ ОПИСАНИЕ АРХИТЕКТУРЫ ПО

2.1. Построение архитектуры.

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

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

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

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

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

2.2. Техническое и программное обеспечение.

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

Функционирование ПО обеспечивается следующим программным обеспечением:

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

Веб-обозреватель Chrome (105 и выше);

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.

В ПО реализованы меры защиты для Системы, в соответствии с Приложением № 1.

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 Системы, 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 приложений;

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.
- Файрволл ОС должен осуществлять логирование всех входящих http/https запросов на порт, на котором развернуто ПО.

Полное описание принятых мер по информационной 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 главе 3.
Администратор ИБ	Выполнение функций администрирования ПО описанных в главе 4.
Настройщик	Назначается пользователю для создания и редактирования конфигурации ПО.

Учетчик	Назначается пользователю для выполнения основного функционала учета необходимых 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.

1.1. Для входа на страницу администрирования ПО необходимо:

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

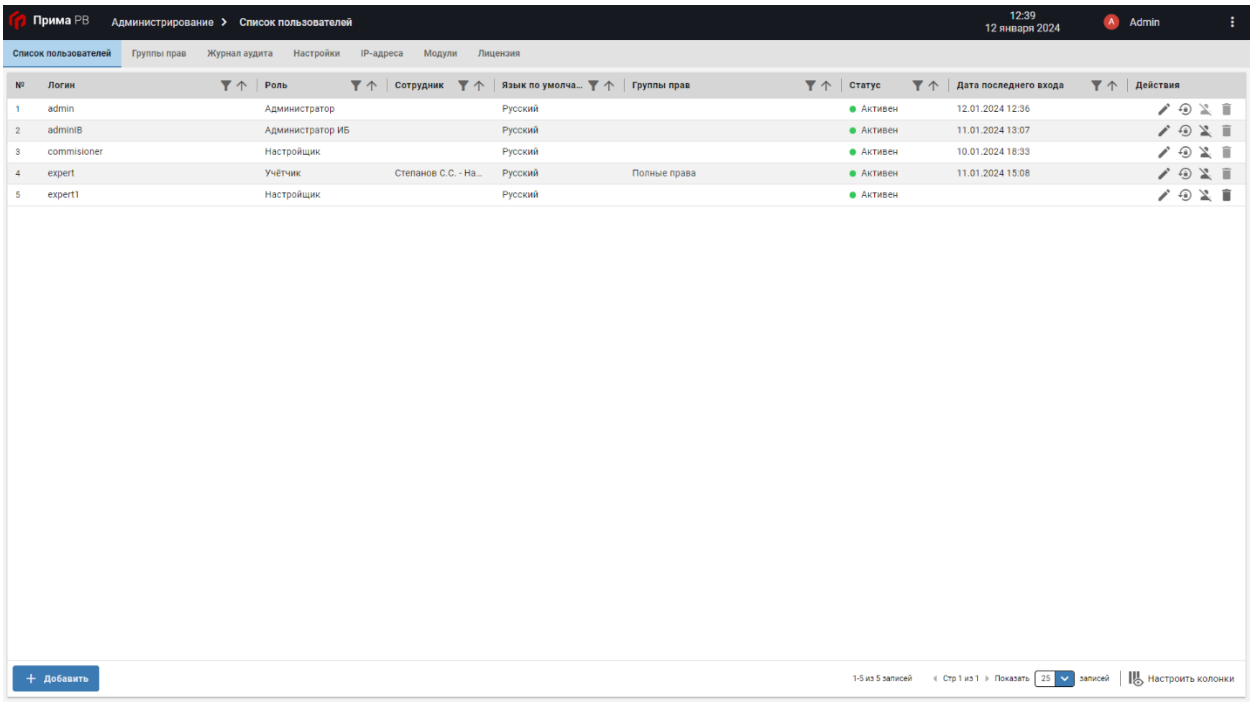


Рисунок 3.1. Пример интерфейса пользователя с ролью «Администратор»

3.2. Создание группы прав для пользователей.

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

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку **«Группы прав»**.
3. Нажать кнопку **«Добавить»** и внести информацию о наименовании созданной группы прав.
4. Выбрать из списка областей, необходимую область которой будут владеть пользователи в созданной группе.

5. В правой части страницы выбрать необходимые права из списка для пользователей созданной группы выбранной области.

6. Нажать кнопку **Сохранить**.

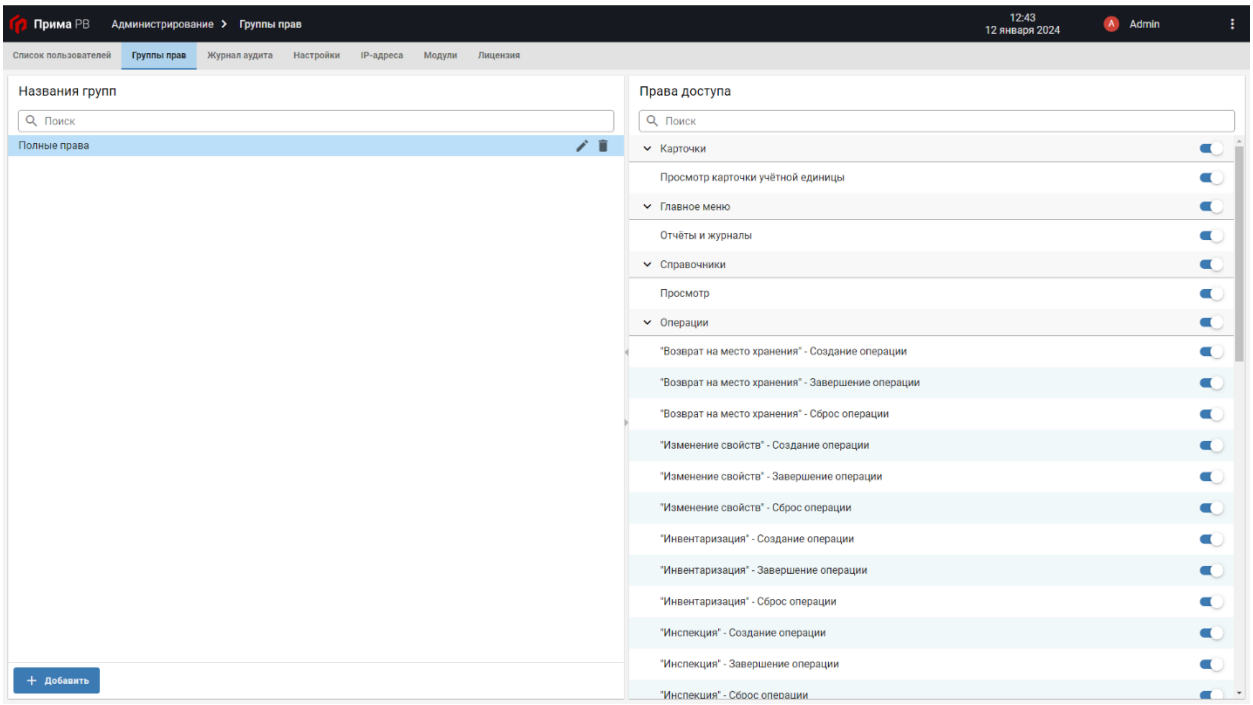


Рисунок 3.2. Пример настройки группы прав для пользователя

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

Пользователю с ролью «Администратор» доступны возможности:

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

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку **«Список пользователей»** и нажать кнопку **Добавить**.
3. Зарегистрировать нового пользователя с ролью «Администратор»:

•В полях **Логин** и **Временный пароль** укажите данные для аутентификации регистрируемого пользователя;

•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.

4. Нажать кнопку **Сохранить**.

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

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

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку **«Список пользователей»** и нажать кнопку **Добавить**.
3. Зарегистрировать нового пользователя с ролью «Администратор ИБ»:

• В полях **Логин** и **Временный пароль** укажите данные для аутентификации регистрируемого пользователя;

• 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.

4. Нажать кнопку **Сохранить**.

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

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

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку **«Список пользователей»** и нажать кнопку **Добавить**.
3. Зарегистрировать нового пользователя с ролью «Настройщик»:

- В полях **Логин** и **Временный пароль** укажите данные для аутентификации регистрируемого пользователя;
- 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.

4. Нажать кнопку **Сохранить**.

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

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

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку **«Список пользователей»** и нажать кнопку **Добавить**.
3. Зарегистрируйте нового пользователя с ролью «Учетчик»:

- В полях **Логин** и **Временный пароль** укажите данные для аутентификации регистрируемого пользователя;
- 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»);
- Добавить **IP адрес** компьютера пользователя.

4. Нажать кнопку **Сохранить**.

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

3.7. Деактивация учетной записи

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

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

3.8. Изменение данных в учетной записи пользователя.

Для изменения информации в учетной записи пользователя выполните следующие действия:

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

3.9. Удаление пользователя (Доступно только для учетных записей, под которыми ни разу не был осуществлен вход в систему)

1. Войти в ПО с ролью «Администратор».
2. Перейти на вкладку «Список пользователей».
3. Выбрать в таблице из списка зарегистрированных пользователей учетную запись, под которой не было совершено ни одного входа в ПО и инициировать ее удаление, путем нажатия на кнопку  (удалить)
4. Подтвердить удаление учетной записи нажатием кнопки  .

3.10. Сброс пароля записи пользователя.

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

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

3.11. Просмотр журнала действий пользователей (логирование).

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

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

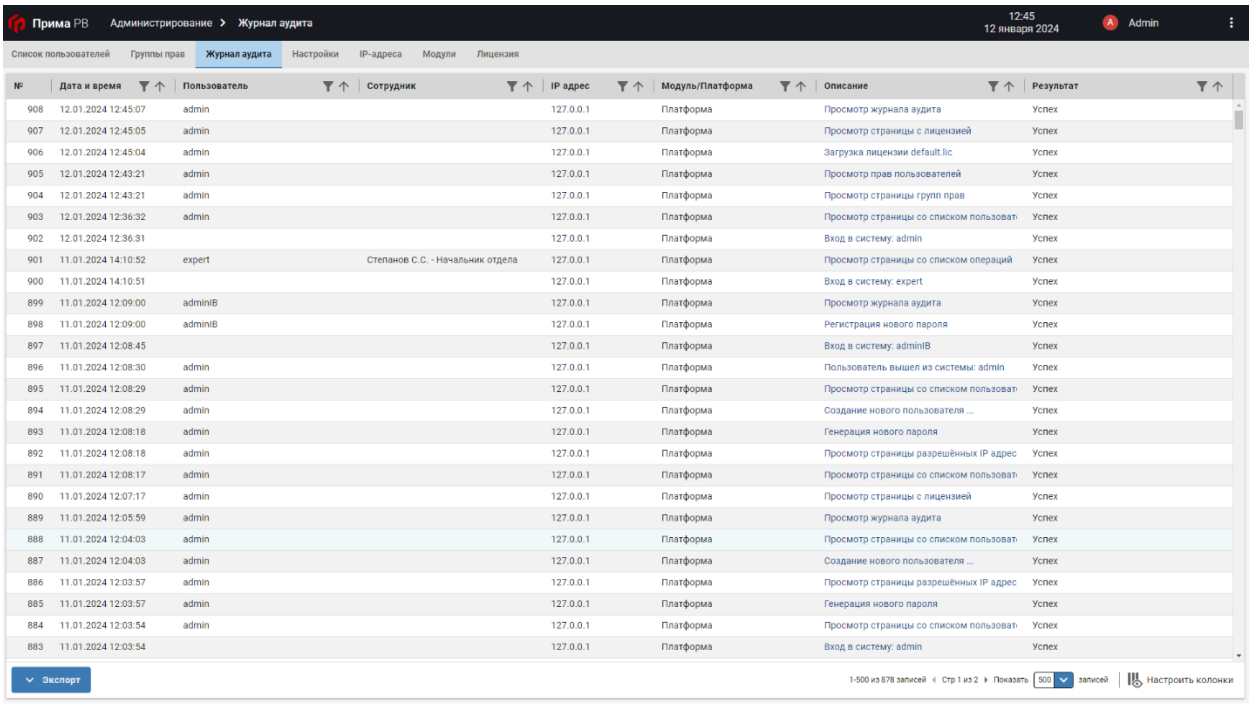


Рисунок 3.3. Пример интерфейса вкладки «Журнал аудита»

3.12. Настройка аутентификации.

1. Войти в ПО с правами администрирования.
2. На странице администрирования открыть вкладку **Настройки**.
3. Задать необходимые параметры для аутентификации:
   - Пароль должен содержать символы верхнего регистра;
   - Пароль должен содержать символы нижнего регистра;

- Пароль должен содержать минимум одну цифру;
- Пароль должен содержать специальные символы;
- Длина пароля;
- Максимальное число попыток входа в систему;
- Время бездействия до приостановки сеанса;
- Срок действия пароля;
- Число предыдущих уникальных паролей;
- Язык по умолчанию.

4. Нажать **Сохранить.**

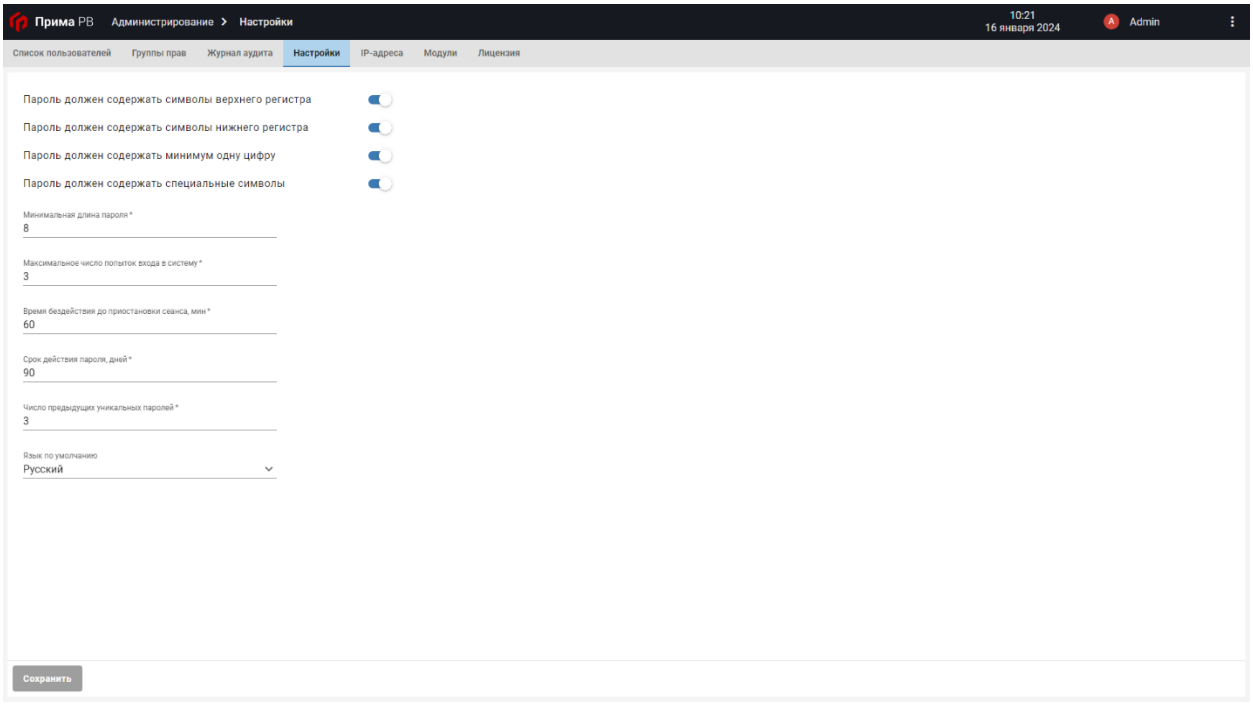


Рисунок 3.3. Пример настройки аутентификации

3.13. Снятие блокировки учётной записи.

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

1. Войти в ПО с ролью «Администратор».
2. На странице администрирования открыть вкладку «IP-адреса» и выбрать Заблокированные.
3. Удалить из списка нужный IP Адрес.

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

5. Нажать кнопку Сохранить.

3.14. Проверка установленных модулей к ПО.

Контроль наличия установленных модулей необходимых версий производится выполнением следующих действий.

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

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

3.15. Работа с лицензией.

Обновление лицензии к ПО производится следующими действиями:

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

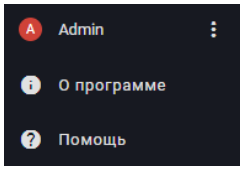
.

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

3.16. Раздел «Помощь».

Раздел «Помощь» даёт доступ к данному Руководству.

Для доступа к разделу «Помощь» необходимо:

1. Войти в ПО пользователем с ролью «Администратор».
2. Нажать на кнопку в правом верхнем углу рядом с логином пользователя.
3. В выпавшем списке 

нажать кнопку **Помощь.**

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

4. ОПИСАНИЕ ОПЕРАЦИЙ АДМИНИСТРАТОРА ИБ

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

Для входа необходимо:

1. В адресную строку браузера введите адрес приложения и нажмите на клавишу Enter. Произойдет переход на авторизационную страницу ПО.

2. В поле **Логин** введите логин для входа в ПО с ролью «Администратор ИБ».

3. В поле **Пароль** введите пароль.

4. Нажать на кнопку **Войти**. Произойдет вход на вкладку **«Журнал аудита»**.

4.2. Работа с журналом аудита.

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

2. На вкладке **«Журнал аудита»** откроется страница со списком всех действий в системе:

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

3. Журнал событий можно отфильтровать с помощью кнопок  .

4.3. Экспорт журнала аудита.

Экспорт журнала производится следующими действиями:

4. Войти в ПО с ролью «Администратор ИБ».

5. На вкладке **«Журнал аудита»** нажать кнопку 

.

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

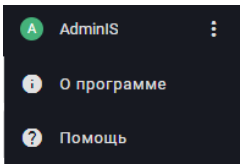
4.4. Раздел «Помощь».

Раздел «Помощь» даёт доступ к данному Руководству.

Для доступа к разделу «Помощь» необходимо:

4. Войти в ПО пользователем с ролью «Администратор ИБ».

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

6. В выпадающем списке 

нажать кнопку **Помощь.**

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

5. ДЕЙСТВИЯ ПРИ АВАРИЙНЫХ СИТУАЦИЯХ

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

Основными признаками аварийной ситуации являются:

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

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

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

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

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

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.

№	Наименование меры	Мера
1	2	3
8.	Использование управляющих аккаунтов	Для внесения изменений в конфигурацию, режимы работы, прав доступа и т.п. должны использоваться отдельные привилегированные учетные записи пользователей. Должна 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.

№	Наименование меры	Мера
1	2	3
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.). 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.).

№	Наименование меры	Мера
1	2	3
		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 процессов аутентификации	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. 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.

№	Наименование меры	Мера
1	2	3
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. Нехранение информации в том же месте, что и пользовательские данные	Системные файлы и файлы конфигурации, принадлежащие приложению, а также информация, такая как записи аудита и записи отслеживания, не должны храниться в том же месте (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.

№	Наименование меры	Мера
1	2	3
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. 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.

№	Наименование меры	Мера
1	2	3
37.	Поддержка турецкого языка в интерфейсе	Поддержка турецкого языка должна быть обеспечена для того, чтобы интерфейс, предлагаемый в рамках приложения / системы, был ясно понятен пользователям
38.	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.
39.	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.
40.	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 Турецкой Республики.
41.	Доступ только авторизованных пользователей к базам данных и носителям, в которых хранятся данные	Доступ к базам данных и носителям приложения, в которых хранятся данные, должны выполняться только авторизованными пользователями, на соответствующих источниках должны выполняться авторизация и настройки.
42.	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.
43.	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
44.	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).

№	Наименование меры	Мера
1	2	3
		В приложении должны быть предусмотрены механизмы экспорта журнала событий в машиночитаемых форматах или передача в системы сбора событий.
45.	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.
46.	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.
47.	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
48.	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.
49.	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.)
50.	Отсутствие сообщения об ошибке или записи отслеживания,	Приложение не должно создавать сообщения об ошибках или записи отслеживания, содержащие персональные данные особого характера.

№	Наименование меры	Мера
1	2	3
	включающей персональные данные особого характера	
51.	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.
52.	Обеспечение безопасности записей отслеживания	Приложение не должно позволять изменять или удалять записи отслеживания, чтобы обезопасить их при взломе сервера приложений. См. меру № 2
53.	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
54.	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.
55.	Проведение аудитов сертификата	Для каждого сертификата сервера Transport Layer Security (TLS) от доверенного центра сертификации необходимо 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).
56.	Выполнение аудита проверки вводимых данных на стороне сервера	Приложение должно выполнять проверку вводимых данных на стороне сервера для каждого принятого типа данных.
57.	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.

№	Наименование меры	Мера
1	2	3
		См. меру № 2
58.	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.
59.	Не хранить важную информацию в конфиденциальных полях форм	Приложения, использующие структуру формы, не должны хранить важную информацию в конфиденциальных полях форм.
60.	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).
61.	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.
62.	Предотвращение уязвимостей, связанные с внедрением команд в операционную систему	Необходимо принять меры безопасности приложения против уязвимостей внедрения команд операционной системы.
63.	Предотвращение атак переполнения памяти	Необходимо принять меры против атак переполнения памяти в приложении и рабочей среде приложения.
64.	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.
65.	Предотвращение атак на основе XML	Приложение должно выполнять превентивные проверки безопасности на наличие уязвимостей XML (атаки на

№	Наименование меры	Мера
1	2	3
		запросы XPath, атаки на внешние элементы XML, внедрение XML и т.д.).
66.	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.
67.	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.
68.	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
69.	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.
70.	Контроль аутентификации и авторизации в вызовах веб-сервиса	Контроль аутентификации и авторизации должен выполняться при каждом вызове веб-сервиса приложения.
71.	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.
72.	Операции настройки и управления веб-сервисами	Приложение должно гарантировать, что только авторизованные пользователи могут получить доступ к функциям настройки и управления веб-сервисом.
73.	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.
74.	Экспорт базы данных	Функция экспорта (сохранение в виде папки, передача на локальные или удаленные приложения и т.д.) в

№	Наименование меры	Мера
1	2	3
	авторизованным пользователем	приложении должна осуществляться исключительно уполномоченными пользователями. См. меру № 41
75.	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.
76.	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.
77.	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.
78.	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
79.	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.).
80.	Регистрация доступа	Успешный и неудачный доступ к носителям, содержащим персональные данные, должны регистрироваться.
81.	Обеспечение защиты записей доступа	Приложение должно блокировать несанкционированное чтение, изменение или удаление записей доступа к персональным данным. См. меру № 2

№	Наименование меры	Мера
1	2	3
82.	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.
83.	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
84.	Использование механизма аутентификации	Для доступа ко всем средам приложения, содержащим личные данные (веб-страница, файл и т.д.), должна выполниться аутентификация.
85.	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.).
86.	Шифрование связи	Связь при обмене данными между системами (корпоративные приложения, внешние веб-службы) должна быть зашифрована. См. меру № 53
87.	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
88.	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
89.	Поддержка турецкого языка в интерфейсе	В приложении должна быть реализована поддержка турецкого языка для того, чтобы интерфейс, предлагаемый в рамках приложения / системы, был ясно понятен пользователям.

№	Наименование меры	Мера
1	2	3
90.	Безопасность сервиса	На серверах приложений и БД должны быть запущены и доступны только те сервисы, приложения, программные компоненты, которые необходимы для работы. 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.
91.	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.
92.	Обеспечение синхронизации времени на серверах	Синхронизация времени должна быть обеспечена на всех серверах путем внесения соответствующих настроек NTP.
Требования к базе данных		
93.	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.
94.	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).
95.	Не использовать учетные записи и пароли по умолчанию	Для запуска и эксплуатации СУБД не должны применяться учетные записи и пароли «по умолчанию».
96.	Защита записей истории команд / запросов	В случае, если история выполненных команд / запросов записывается в базе данных, должна быть обеспечена безопасность соответствующих записей / файлов.

№	Наименование меры	Мера
1	2	3
97.	Удаление образцов данных	Образцы данных (образцы таблиц, записей, пользователей и т.д.), поступающие с установкой, должны быть удалены из базы данных.
Требования к серверу		
98.	Использование текущего программного обеспечения веб-сервера	Следует использовать обновленные стабильные версии программного обеспечения веб-сервера, свободные от уязвимостей и поддерживаемые производителем. Кроме того, следует регулярно проверять наличие исправлений безопасности для всех инструментов / пакетов программного обеспечения, используемых на сервере.
99.	Удаление поддержки WebDAV	Поддержка WebDAV (Web Distributed Authoring and Versioning) веб-сервера должна быть удалена. Модули, связанные с WebDAV, должны быть деактивированы или удалены.
100.	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.
101.	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.
102.	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.
103.	Отключение листинга каталогов	Листинг каталогов веб-сервера должен быть отключен, если его использование не является необходимым для функционирования веб-приложения.
104.	Отключение режима отладки	Программное обеспечение веб-сервера не должно запускаться в режиме отладки.
105.	Определение пределов запросов	Для запросов должны быть установлены ограничения в объеме, поддерживаемом программным обеспечением веб-сервера.
106.	Ведение записей отслеживания	Должна осуществляться регистрация событий веб-сервера.
107.	Ограничение каталогов с	Необходимо указать каталоги с разрешениями на запись, права записи должны быть предоставлены только каталогам, которым требуется загрузка файлов.

№	Наименование меры	Мера
1	2	3
	разрешениями на запись	Необходимо удалить разрешение на запуск в каталогах файлов, загруженных через приложение.
108.	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.
109.	Перенаправление запросов с HTTP на HTTPS	Любой порт HTTP на веб-сервере должен направляться на порт сервера с использованием шифрования.
110.	Удаление неиспользуемых модулей	Только модули, используемые на сервере, должны быть активными.
111.	Ограничение открытых портов	Веб-сервер должен прослушивать сетевые подключения только на авторизованных портах. Неиспользуемые порты необходимо закрыть.