

РУКОВОДСТВО АДМИНИСТРАТОРА ПРОГРАММЫ ДЛЯ ЭВМ «ЗАРПЛАТОМИР»

1. Назначение программы для ЭВМ

Программа для ЭВМ «Зарплатомир» (далее — Программа или ПО) предназначена для управления системными пользователями, партнерами, клиентами, продуктами, тарифами и обработкой сообщений клиентов через административную панель.

Административная панель предоставляет веб-интерфейс для выполнения операций настройки и сопровождения системы.

2. Доступ к административной панели

2.1 Вход в систему

Для входа в административную панель необходимо открыть браузер и перейти по адресу:

<http://api.zarplatawant.ru/admin>

После открытия страницы авторизации необходимо ввести:

- адрес электронной почты (Email);
- пароль.

После успешной аутентификации будет открыта главная страница панели управления.

2.2 Разграничение прав доступа

Система использует ролевую модель доступа.

Каждому системному пользователю могут быть назначены одна или несколько ролей.

Права системного пользователя определяют возможность:

- просмотра данных;
- просмотр страниц, виджетов
- создания записей;
- редактирования записей;
- удаления записей;
- управления ролями пользователей.

3. Структура административной панели

Основные разделы панели:

- Статистика
- Системные пользователи (это администраторы);
- Продукты;

- Клиенты (клиенты продуктов);
- Сообщения (сообщения отправленные клиентами в продукты);
- Стоимость продуктов партнеров;
- Документация.

4. Управление системными пользователями

4.1 Создание системного пользователя

Для создания системного пользователя:

1. Перейти в раздел «Пользователи».
2. Нажать кнопку «Создать».
3. Заполнить поля:

Поле	Описание
Name	Имя пользователя
Email address	Адрес электронной почты
Password	Пароль
Roles	Назначаемые роли

4. Сохранить запись.

4.2 Изменение системного пользователя

1. Открыть карточку пользователя.
2. Внести необходимые изменения.
3. Нажать «Сохранить».

4.3 Назначение ролей

Роли назначаются через поле «Roles».

Изменение ролей доступно только пользователям с соответствующими полномочиями.

5. Управление продуктами

5.1 Создание продукта

Для добавления продукта:

1. Перейти в раздел «Продукты».
2. Нажать «Создать».
3. Заполнить поля:

Поле	Описание
Name	Наименование продукта
ID Яндекс Метрики	Идентификатор счетчика Метрики
Agent Access ID	Идентификатор доступа агента из TIMEWEB AGENT
Agent Access Token	Токен доступа агента из TIMEWEB AGENT

4. Сохранить изменения.

5.2 Редактирование продукта

Изменение выполняется через карточку продукта.

6. Формирование и управление ключами доступа

В системе используются следующие виды ключей:

6.1 Agent Access ID

Уникальный идентификатор интеграции внешнего сервиса (TIMEWEB AGENT).

Указывается в карточке продукта.

6.2 Agent Access Token

Секретный токен авторизации (TIMEWEB AGENT).

Требования:

- хранить в защищенном виде;
- не передавать третьим лицам;
- изменять при подозрении на компрометацию.

Порядок замены:

1. Получить новый токен.
2. Открыть карточку продукта.
3. Обновить значение поля «Agent Access Token».
4. Сохранить изменения.

7. Управление клиентами

7.1 Создание клиента

Для регистрации клиента (в крайнем случае, т.к партнеры сами указывают клиентов через API):

1. Открыть раздел «Клиенты».
2. Создать новую запись.
3. Указать один из параметров:
 - номер телефона; или
 - уникальный ключ доступа.
4. Выбрать партнера.
5. Указать срок действия доступа.
6. Сохранить запись.

7.2 Продление доступа

Для продления доступа:

1. Открыть карточку клиента.
2. Изменить дату окончания доступа.
3. Сохранить изменения.

Также продление возможно через API.

7.3 Удаление клиента

Для удаления клиента:

1. Открыть карточку клиента.
2. Нажать «Удалить».
3. Подтвердить операцию.

8. Управление стоимостью продуктов партнеров

Раздел предназначен для хранения тарифов.

Для каждой записи указываются:

Поле	Назначение
Partner	Партнер
Product	Продукт
First Price	Стоимость первого периода(в рублях)
Repeat Price	Стоимость последующих периодов (в рублях)

Порядок создания:

1. Открыть раздел тарифов.
2. Создать новую запись.
3. Заполнить поля.
4. Сохранить данные.

9. Работа с сообщениями клиентов

9.1 Просмотр сообщений

Раздел «Сообщения» содержит обращения клиентов.

Карточка сообщения включает:

- текст сообщения;
- клиента;
- партнера;
- ответ системы;
- идентификатор родительского сообщения.

9.2 Ответ клиенту

1. Открыть сообщение.
2. Заполнить поле «Ответ».
3. Сохранить запись.

10. Типовые ситуации

Ситуация 1. Пользователь не может войти в систему

Возможные причины:

- неверный пароль;
- отсутствует учетная запись;
- пользователь заблокирован;
- истек срок действия учетных данных.

Действия администратора:

1. Проверить наличие пользователя.
2. Сбросить пароль.
3. Проверить назначенные роли.

Ситуация 2. Клиент не имеет доступа к сервису

Проверить:

- дату окончания доступа;
- наличие привязки к партнеру;
- корректность ключа доступа.

Ситуация 3. Не работает интеграция продукта

Проверить:

- Agent Access ID;
- Agent Access Token;
- доступность внешнего сервиса.

Ситуация 4. Сообщения не обрабатываются

Проверить:

- наличие новых сообщений в разделе «Сообщения»;
- состояние очередей обработки;
- журналы приложения.

11. Эксплуатация программного обеспечения

Ежедневный контроль

Рекомендуется ежедневно выполнять:

- проверку доступности панели управления;
- проверку новых сообщений клиентов;
- контроль сроков действия клиентских доступов;
- проверку журналов ошибок.

Резервное копирование

Необходимо регулярно выполнять:

- резервное копирование базы данных;
- резервное копирование файлов конфигурации;
- сохранение токенов интеграций.

Обновление системы

Перед обновлением необходимо:

1. Создать резервную копию.
2. Выполнить обновление программного обеспечения.
3. Выполнить миграции базы данных.
4. Проверить работоспособность административной панели.
5. Проверить работу API.

12. Журналирование и диагностика

При возникновении ошибок рекомендуется анализировать:

- журналы Laravel;
- журналы веб-сервера;
- записи ошибок базы данных;
- сообщения очередей обработки.

Расположение журналов:

storage/logs/

Основной файл:

laravel.log

13. Требования информационной безопасности

Администратор обязан:

- использовать сложные пароли;
- ограничивать доступ к административной панели;
- регулярно изменять учетные данные администраторов;