

Описание процессов, обеспечивающих поддержание жизненного цикла программного обеспечения ProstoCRM, и информация о персонале

1. Назначение

Документ описывает процессы поддержания жизненного цикла программного обеспечения ProstoCRM (далее — ПО) от ввода в эксплуатацию до вывода из эксплуатации: техническую поддержку и устранение неисправностей, совершенствование ПО, а также состав персонала, необходимого для такой поддержки.

2. Организация поддержки

Правообладатель ПО — индивидуальный предприниматель Анедченко Александр Сергеевич (далее — Правообладатель). Работы по разработке, технической поддержке и эксплуатации ПО выполняются по договору с ООО «Студии Реклама» (далее — Исполнитель) под руководством и контролем Правообладателя.

Роль	Ответственность	Кто выполняет
Руководитель проекта	Стратегия развития, управление требованиями, взаимодействие с пользователями и регуляторами, приёмка работ	ИП Анедченко А.С.
Технический руководитель	Архитектура, управление разработкой, контроль качества кода, безопасность	ООО «Студии Реклама»
Разработчики (backend/frontend)	Новый функционал, исправление ошибок, оптимизация, интеграции	ООО «Студии Реклама»
Специалист по базам данных	Администрирование БД, оптимизация, миграции	ООО «Студии Реклама»
Инженер по эксплуатации (DevOps)	Администрирование серверов, мониторинг, доступность и безопасность инфраструктуры	ООО «Студии Реклама»

3. Техническая поддержка и устранение неисправностей

3.1. Каналы обращений

- чат-бот ProstoCRM в мессенджере MAX;
- e-mail: support@lookmy.info;
- телефон: +7 (999) 691-65-22;
- форма заявки на сайте: <https://prostocrm.shop/forma-zayavka>.

Поддержка оказывается в рабочие дни.

3.2. Уровни поддержки

- **1-я линия** — регистрация обращений, консультации по работе с ПО, решение типовых вопросов (настройка бота, доступ, работа интерфейса), эскалация. Срок реакции — не более 1 рабочего дня.
- **2-я линия** — анализ ошибок логики, интеграций, производительности; воспроизведение ошибок и сбор журналов; изменение конфигурации серверов и БД; взаимодействие с внешними сервисами (MAX, банки, DaData). Срок реакции — не более 2 рабочих дней.
- **3-я линия** — исправление ошибок в коде, тестирование и выпуск исправлений. Срок реакции на критические ошибки — не более 3 рабочих часов.

3.3. Учёт инцидентов

Каждое обращение регистрируется в системе учёта с присвоением номера, приоритета (критический, высокий, средний, низкий), статуса (новый, в работе, на тестировании, закрыт), описания, шагов воспроизведения и ответственного исполнителя. Правообладатель имеет доступ ко всем обращениям и утверждает приоритеты исправлений.

3.4. Сроки устранения

Приоритет	Описание	Целевой срок устранения
Критический	ПО недоступно, потеря данных, остановка работы пользователей	до 4 часов
Высокий	Ошибка в ключевой функции при работающей системе	до 24 часов
Средний	Ошибка в неосновной функции, есть обходной путь	до 72 часов
Низкий	Косметические дефекты, пожелания	в ближайшем релизе (до 2 недель)

3.5. Эскалация

Нерешённое на 1-й линии в течение 2 часов обращение передаётся на 2-ю линию; нерешённое на 2-й линии в течение 8 часов — на 3-ю линию. О критических инцидентах Правообладатель уведомляется немедленно.

3.6. Мониторинг

- мониторинг серверов (процессор, память, диск, сеть) — Zabbix / Prometheus + Grafana;
- сбор и анализ журналов с оповещением об ошибках;
- автоматическая проверка доступности API и обработчиков бота с уведомлением администраторов;
- еженедельный отчёт Правообладателю о состоянии инфраструктуры и инцидентах.

4. Совершенствование ПО

4.1. Управление требованиями

Источники требований: обратная связь пользователей, аналитика, изменения законодательства, инициативы Правообладателя. Требования фиксируются в виде задач с приоритетом и сроком; бэклог утверждает Правообладатель.

4.2. Релизы

- плановый релизный цикл — ежемесячный;

- критические исправления — внеплановые выпуски по решению Правообладателя;
- каждый релиз сопровождается тестированием на тестовом стенде, обновлением документации и автоматизированным развёртыванием (CI/CD).

4.3. Разработка и тестирование

- гибкая методология (Scrum/Kanban);
- система контроля версий Git; репозиторий размещён на защищённом сервере в Российской Федерации, доступ — только у уполномоченных лиц;
- обязательное рецензирование кода (code review);
- автоматические тесты критической логики (PHPUnit, Jest), статический анализ (PHPStan, ESLint);
- интеграционное тестирование с внешними API перед каждым релизом.

4.4. Внедрение изменений

Изменения развёртываются на тестовой (staging) среде, проходят приёмку Правообладателем и затем выпускаются в эксплуатацию с уведомлением пользователей о плановых работах. При обнаружении критических ошибок выполняется откат к предыдущей стабильной версии.

4.5. Версии

Нумерация версий — X.Y.Z (мажорная, минорная, исправления). Предыдущая мажорная версия поддерживается 6 месяцев после выхода новой.

4.6. Вывод из эксплуатации

Пользователи уведомляются о прекращении поддержки версии не менее чем за 3 месяца через бот и e-mail; обеспечивается перенос данных в новую версию.

5. Персонал, необходимый для поддержки

Минимальный состав:

- руководитель проекта (Правообладатель) — 1 чел.;
- технический руководитель — 1 чел.;
- backend-разработчик (PHP, MySQL, интеграции) — 1–2 чел.;
- frontend-разработчик (JavaScript, HTML/CSS, WebApp) — 1 чел.;
- DevOps-инженер (Linux, Apache/nginx, PHP-FPM, MySQL, мониторинг, CI/CD) — 1 чел.

Квалификационные требования: разработчики — PHP 8+, MySQL, JavaScript, HTML/CSS, REST API, Git; DevOps — Linux, веб-серверы, СУБД, системы мониторинга. Все специалисты, имеющие доступ к коду и данным, подписывают соглашение о неразглашении. Для обеспечения непрерывности поддержки Правообладатель вправе привлекать дополнительных специалистов.

6. Инфраструктура

- серверы сервиса и базы данных размещены у хостинг-провайдера АО «ЮНИКО» в центрах обработки данных на территории Российской Федерации (Московская область, г. Химки; г. Москва);
- контроль версий — Git (с резервным копированием);
- CI/CD — GitLab CI / Jenkins;

- мониторинг — Zabbix / Prometheus + Grafana;
- документация ведётся в репозитории и обновляется вместе с релизами.

7. Информационная безопасность

- доступ к серверам — по SSH-ключам с ограничением по IP-адресам;
- журналирование действий с кодом и развёртываний;
- шифрование чувствительных данных (AES-256), передача данных по HTTPS;
- ежедневное резервное копирование с шифрованием.

Правообладатель: ИП Анедченко Александр Сергеевич
Редакция от 17.09.2026