

**ПРОГРАММА УПРАВЛЕНИЯ КЛЮЧНИЦЕЙ  
И ДОСТУПОМ ПОЛЬЗОВАТЕЛЕЙ KEY1CONTROL**

**РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ**

Санкт-Петербург

2025

## СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ.....	3
2. АРХИТЕКТУРА И СИСТЕМНЫЕ ТРЕБОВАНИЯ .....	4
3. УСТАНОВКА И АКТИВАЦИЯ.....	4
4. АВТОРИЗАЦИЯ И БЕЗОПАСНОСТЬ .....	6
5. АДМИНИСТРИРОВАНИЕ СТРУКТУРЫ ОРГАНИЗАЦИИ .....	6
6. УПРАВЛЕНИЕ КЛЮЧАМИ И ОБОРУДОВАНИЕМ .....	7
7. КОНТРОЛЬ ДОСТУПА И РАСПИСАНИЯ.....	9
8. МОНИТОРИНГ, АУДИТ И ОТЧЕТНОСТЬ .....	9
9. ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ИХ РЕШЕНИЕ .....	10
10. СЛУЖБА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ .....	10

## 1. ВВЕДЕНИЕ

### 1.1. Назначение программы

Программа управления ключницей и доступом пользователей Key1Control предназначена для автоматизированного управления доступом к ключам (штекерам) и администрирования пользователей в системе «умной» ключницы.

### 1.2. Область применения

ПО может использоваться в госучреждениях, научных центрах и коммерческих организациях, где требуется строгий контроль доступа.

### 1.3. Основные возможности

ПО обеспечивает централизованное управление правами, мониторинг операций, аудит событий, поддержку многофакторной аутентификации, а также интеграцию с RFID и биометрией.

Функциональные возможности программы включают:

- управление организациями, отделами и пользователями;
- настройку ролей и расписаний;
- визуализацию ключницы;
- двустороннюю репликацию данных;
- модуль бронирования;
- диагностику штекеров;
- ведение журналов событий с фильтрацией и экспортом;
- уведомления;
- API-интеграцию.

### 1.4. Условные обозначения

В данном руководстве используются следующие выделения:

1. **Жирный шрифт** – названия кнопок, меню, полей ввода.
2. *Курсив* – важные примечания и предупреждения.
3. Моноширинный шрифт – пути к файлам, системные сообщения.

## 2. АРХИТЕКТУРА И СИСТЕМНЫЕ ТРЕБОВАНИЯ

### 2.1. Архитектура системы

ПО реализовано как клиент-серверное веб-решение, обеспечивает надёжность, масштабируемость и соответствие требованиям информационной безопасности.

### 2.2. Системные требования

Для корректной работы ПО Key1Control необходимо соответствие следующим минимальным требованиям:

Параметр	Минимальные требования	Рекомендуемые требования
ОС	Linux, Debian 12	Linux, Debian 12
Процессор	4, 3.2 ГГц	4, 3.2 ГГц
ОЗУ	8 Гб	16 Гб
Свободное место	SSD, 100 Гб	SSD, 256 Гб
Подключение	> 100 Мбит/с	1 Гбит/с
Дополнительное ПО	Docker	Docker

### 2.3. Синхронизация данных

Синхронизация позволяет автоматически переносить создаваемые и изменяемые данные между сервером и ключницами.

## 3. УСТАНОВКА И АКТИВАЦИЯ

### 3.1. Установка

1. Подключите установочный носитель (USB-накопитель) к вычислительному модулю ключницы.
2. Запустите установочный скрипт `install.sh` с правами администратора.
3. Дождитесь завершения процесса установки.
4. Программное обеспечение будет автоматически запущено после успешной установки.

*Для корректной установки убедитесь, что на устройстве установлена поддерживаемая версия операционной системы и имеются необходимые права доступа.*

### 3.2. Подключение оборудования

Перед запуском программного обеспечения проверьте подключение аппаратных компонентов:

#### 1. Плата-преобразователь:

- убедитесь, что плата-преобразователь ключницы подключена к USB-порту вычислительного модуля.

#### 2. Сетевое подключение:

- подключите кабель Ethernet к сетевому разъему вычислительного модуля.
- убедитесь, что установлено соединение с локальной сетью организации (при работе в клиент-серверном режиме).

#### 3. Дополнительные интерфейсы (опционально):

- при использовании RFID-считывателя или биометрического модуля проверьте их подключение к соответствующим портам.

*Все подключения оборудования должны выполняться при обесточенном устройстве во избежание повреждения электронных компонентов.*

### 3.3. Активация лицензии

При первом запуске системы требуется активация лицензионного ключа.

1. Нажмите кнопку **Сгенерировать** конфигурацию. Файл конфигурации устройства будет сохранен локально.
2. Направьте файл конфигурации разработчику по электронной почте (см. раздел 10).
3. Получите лицензионный ключ от разработчика.
4. Загрузите ключ в соответствующую форму интерфейса.
5. При успешной активации откроется главное окно системы.

## 4. АВТОРИЗАЦИЯ И БЕЗОПАСНОСТЬ

### 4.1. Вход в систему

1. Веб-интерфейс (Сервер): при запуске введите логин и пароль супер-пользователя. Учетные данные предоставляются производителем.
2. Локальный интерфейс (Ключница): на экране аутентификации нажмите **PIN-код администратора** и введите код, установленный при инициализации устройства.

### 4.2. Интеграция средств идентификации

Система поддерживает следующие методы аутентификации:

- ввод PIN-кода (через сенсорную панель);
- RFID-карты;
- биометрия (распознавание лица или отпечатков пальцев).

### 4.3. Соответствие требованиям безопасности

Для обеспечения сохранности данных рекомендуется регулярно выполнять резервное копирование базы данных (БД):

- используйте ПО администрирования БД (**PgAdmin**).
- создавайте резервные копии БД сервера или ключницы согласно регламенту организации.

## 5. АДМИНИСТРИРОВАНИЕ СТРУКТУРЫ ОРГАНИЗАЦИИ

### 5.1. Управление организацией и отделами

1. Организация: В разделе **Организация** (веб-интерфейс) можно изменить название компании, логотип и часовой пояс.
2. Отделы: В разделе **Организация** (веб-интерфейс) доступен полный цикл управления отделами – создание, редактирование, просмотр, поиск и удаление.

## 5.2. Управление пользователями и ролями

В разделе **Сотрудники** осуществляется управление учетными записями пользователей. Система предусматривает 4 роли уровня доступа:

1. **Superadmin** – полные права на администрирование всех сущностей системы во всех организациях.
2. **Admin** – полные права на администрирование сущностей в рамках своей организации.
3. **Key manager** – управление доступными ключницами, выдача прав другим пользователям, доступ ко всем штекерам закрепленных ключниц.
4. **Employee** – просмотр информации о доступных ключницах, своем отделе и организации, получение доступа к закрепленным штекерам.

## 5.3. Расписания доступа

В разделе **Организация** на вкладке **Расписания** доступна настройка рабочих графиков для отделов и сотрудников:

- указание названия расписания, рабочих часов, рабочих и выходных дней;
- привязка расписания к соответствующим объектам системы.

## 6. УПРАВЛЕНИЕ КЛЮЧАМИ И ОБОРУДОВАНИЕМ

### 6.1. Визуализация ключницы

Система предлагает два режима отображения состояния ключницы:

1. **Табличный** – список штекеров и слотов с подробными атрибутами (имя, привязка, статус).
2. **Графический** – схема, дублирующая физическое расположение слотов и штекеров.

## 6.2. Диагностика оборудования

Система предоставляет следующие инструменты для проведения диагностики оборудования:

1. **Управление дверью:** статус (открыта/закрыта); кнопка **Разблокировать**.
2. **Проверка RFID-считывателя:** индикация обнаружения карты.
3. **Концевик сервисной двери:** статус (открыта/закрыта).
4. **Резервное питание:** статус (активно/не активно).
5. **Контакты «Пожар»:** статус (активно/не активно).
6. **Управление реле:** активация/деактивация реле №1–4.
7. **Разблокировка штекеров:** выбор диапазона (например, 0–80), индивидуальная или групповая разблокировка («змейкой» по 10).
8. **Считывание штекеров:** тест наличия штекеров в слотах посредством кнопки **Считать штекеры** (отчет о считанных/несчитанных номерах).
9. **Оборудование на CAN-шине:** отображение списка обнаруженных плат посредством кнопки **Показать платы** с указанием типа и логического ID (например, Key 1-40, external-electric-circuits).

## 6.3. Инициализация ключницы

Процесс первичной настройки включает следующие этапы:

1. Ввод названия, серийного номера и PIN-кода администратора.
2. Выбор размерности ключницы.
3. Загрузка логотипа (опционально).
4. Настройка подключения к серверу (опционально).

*Если на этапе инициализации сервер отсутствует, или необходимости в подключении ключницы к серверу нет, данный шаг можно пропустить.*

#### 6.4. Регистрация штекеров

1. Выполните аутентификацию на ключнице или сервере.
2. Перейдите в раздел управления ключницей.
3. Нажмите кнопку **Запись** для регистрации неизвестных штекеров, установленных в слоты.

#### 6.5. Выдача и возврат штекера

1. Пройдите аутентификацию.
2. После разблокировки двери извлеките доступный штекер или верните его в слот.
3. Закройте дверь ключницы для фиксации операции.

### 7. КОНТРОЛЬ ДОСТУПА И РАСПИСАНИЯ

#### 7.1. Настройка прав доступа

Права доступа настраиваются в разделах **Организация** (для отделов) и **Сотрудники** (для пользователей). Имеется возможность назначения доступных штекеров конкретных ключниц для сотрудников или отделов.

Разблокировка штекеров происходит автоматически при успешной аутентификации пользователя с соответствующими правами.

#### 7.2. Временные ограничения

Доступ регулируется рабочими расписаниями и глобальными настройками прав. При попытке доступа вне утвержденного временного интервала система блокирует возможность получения штекера.

### 8. МОНИТОРИНГ, АУДИТ И ОТЧЕТНОСТЬ

#### 8.1. Журнал событий

В разделе **Мониторинг** доступен просмотр системных и пользовательских событий. Предусмотрена фильтрация, комментирование записей и экспорт данных.

## 8.2. Уведомления

Система поддерживает отправку уведомлений:

1. **E-mail:** настройка производится в соответствующем разделе настроек.
2. **Pop-up:** всплывающие сообщения в графическом интерфейсе.

## 9. ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ИХ РЕШЕНИЕ

Проблема	Возможная причина	Решение
Сервер не видит ключницу	Адрес сервера на ключнице указан некорректно	Проверьте корректность адреса сервера на ключнице
Медленная работа	Нагрузка на вычислитель повышена	Проверьте соответствие вычислителя рекомендуемым системным требованиям
Медленная синхронизация	Большое количество операций передаваемых по сети	Проверьте скорость передачи данных по локальной сети предприятия и соответствие рекомендуемым системным требованиям

## 10. СЛУЖБА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

### 10.1. Контакты службы поддержки

По вопросам установки, настройки и эксплуатации программного обеспечения «Key1Control» обращайтесь в службу технической поддержки разработчика:

Способ связи	Контактные данные
Телефон	88005555108
E-mail	support@ecos-security.ru

## 10.2. Режим работы

- Понедельник – Пятница: 09:00 – 18:00 (МСК, UTC+3)
- Суббота, Воскресенье: выходные дни
- Обед: 13:00 – 14:00

## 10.3. Порядок обращения в службу поддержки

Для оперативного решения проблемы подготовьте следующую информацию перед обращением:

### 1. Данные о системе:

- Версия ПО «KeyControl» (меню Справка → О программе);
- Серийный номер ключницы;
- Версия операционной системы вычислительного модуля.

### 2. Описание проблемы:

- Текст сообщения об ошибке (скриншот);
- Последовательность действий, приведших к сбою;
- Частота воспроизведения проблемы (единичный случай или воспроизводится постоянно).

### 3. Диагностические данные (при наличии):

- Файлы журналов событий;
- Результаты диагностики оборудования.

## 10.4. Отправка диагностических данных

1. Экспортируйте необходимые файлы через интерфейс программы.
2. Создайте письмо на адрес [support@ecos-security.ru](mailto:support@ecos-security.ru)
3. В теме письма укажите:

*KeyControl | Серийный номер: [X] | Краткое описание проблемы.*

4. Прикрепите файлы.

*При обращении в службу поддержки обязательно указывайте контактные данные ответственного лица (ФИО, должность, телефон для обратной связи). Это ускорит обработку вашего запроса.*

## 10.5. Гарантийные обязательства

Техническая поддержка осуществляется в рамках действующего лицензионного соглашения. Бесплатное обновление ПО предоставляется в течение срока действия лицензии.

Разработчик не несет ответственности за сбои, вызванные несанкционированным изменением кода программы или использованием неоригинальных компонентов оборудования.