

## **Описание функциональных характеристик и информация, необходимая для установки и эксплуатации ПО «Программа управления ключницей и доступом пользователей Key1Control»**

### **1. Краткое описание ПО**

1.1. Программное обеспечение «Программа управления ключницей и доступом пользователей Key1Control» представляет собой систему, предназначенную для администрирования и управления ключницами, отделами и сотрудниками.

1.2. ПО обеспечивает взаимодействие между сотрудниками организаций, предоставляя инструменты для аутентификации, получения доступа к ключницам и мониторинга.

1.3. Функциональные возможности программного обеспечения включают:

- Управление отделами и пользователями
- Управление ключницами и штекерами
- Выполнение аутентификации и авторизации
- Выдача доступов к штекерам
- Мониторинг
- Бронирование штекеров

### **2. Назначение и задачи ПО**

2.1. Программное обеспечение «Программа управления ключницей и доступом пользователей Key1Control» предназначено для централизованного и автономного управления ключницами и штекерами, включая выдачу, возврат, блокировку/разблокировку, контроль доступов и фиксацию событий в сфере обеспечения физической безопасности и контроля доступа (автоматизации управления инфраструктурой физической безопасности).

2.2. Задачи, которые решает ПО

- автоматизация процессов контроля и управления доступами;
- предоставление пользователям инструментов управления ключницами и организацией;
- управление правами доступа пользователей;
- интеграция с внешними системами электронной почты;
- сбор системных и пользовательских событий;
- формирование отчетов;
- синхронизация данных между ключницами и сервером.

### **3. Вводная информация, ресурсы и выходные данные**

3.1. Вводная информация

3.2. Входными данными для работы программного обеспечения являются:

- Лицензионный ключ;

- Учетные данные пользователей;
- Отделы;
- Введенные факторы аутентификации пользователей (RFID-карты, PIN-коды, биометрия);
- Ключницы с привязанными штекерами;
- Правила аутентификации;
- Данные бронирования.

#### **4. Затрачиваемые ресурсы**

##### 4.1. Для работы программного обеспечения требуется:

- веб-браузер: Google Chrome, Yandex Browser, Mozilla Firefox, и другие;
- доступ к сети Интернет: не требуется; требуется наличие интрасети на объекте размещения ПО;
- серверная инфраструктура: требуется;
- специальные требования к аппаратному обеспечению: не требуются (ПО совместимо с ОС общего назначения и сертифицированными ОС при соответствии аппаратной платформы требованиям регуляторов);
- персонал с навыками администрирования веб-приложений, управления СУБД, настройки сетевых взаимодействий и обеспечения базовых мер информационной безопасности.

#### **5. Выходные данные**

##### 5.1. В результате работы программного обеспечения формируются:

- Данные о сотрудниках и отделах;
- Данные о ключницах на объекте;
- Данные о доступах сотрудников и отделов к ключницам;
- Системные и пользовательские события.

#### **6. Функциональные возможности системы**

##### 6.1. Управление пользователями и ролями

- аутентификация пользователей с использованием логина и пароля, RFID-карт, PIN-кодов, биометрии (лицо/ладонь);
  - поддержка механизмов безопасности многофакторной аутентификации, ролевого разграничения прав доступа, политик паролей и контроля активных сеансов;
  - система ролей: Employee, Key Manager, Admin, Superadmin;
  - настройка прав доступа к функциям и модулям системы.
- ##### 6.2. Управление объектами учета (сайты / проекты / ресурсы)
- добавление объектов пользователями;

- модерация и проверка объектов;
- управление статусами объектов (вставлен, извлечен, неисправен).

### 6.3. Управление функциональными модулями

- создание и настройка ключниц;
- активация и деактивация доступов;
- настройка правил аутентификации;
- автоматическая генерация отчетов.

### 6.4. Статистика и аналитика

- получение статистических данных из внутренних журналов событий и базы данных системы;
- хранение информации о событиях в базе данных PostgreSQL;
- фильтрация и группировка событий по параметрам;
- визуализация данных о событиях в формате таблицы;
- экспорт отчетов о событиях в формате csv.

### 6.5. Финансовые / расчетные модули (при наличии)

- ввод и хранение \_\_\_\_\_;
- автоматический расчет \_\_\_\_\_;
- формирование и подтверждение \_\_\_\_\_;
- ведение истории \_\_\_\_\_.

### 6.6. Интеграция с внешними системами

- интеграция с сервером электронной почты;
- синхронизация данных отсутствует;
- использование API и веб-хуков отсутствует.

## 7. Установка и эксплуатация

7.1. Программное обеспечение «Программа управления ключницей и доступом пользователей Key1Control» является локальным ПО (интернет-сервис / серверное ПО / локальное ПО).

7.2. Специальная установка на стороне пользователя требуется.

7.3. Доступ к программному обеспечению осуществляется через веб-браузер или встроенного планшета с использованием GUI.

7.4. Для различных категорий пользователей не предусмотрены различия в интерфейсах.

7.5. Подробная информация об использовании программного обеспечения содержится в документе «Руководство пользователя», доступном по адресу: <https://ecos-security.ru/company/software/>.

**8. Ответственный за управление доступом**

Регулирование доступа к исходному коду, процессам эксплуатации и функциональным возможностям программного обеспечения осуществляется назначенным должностным лицом – Коско А.В.