	Спецификация требований к программному обеспечению для Проекта СКБ	Автор: TEAM15 № документа: TEAM15-v0.3 Дата: 2023-11-08 Страниц: x

Содержание

История изменений

Дата	Версия	Описание	Автор(ы)
2023-10-10	0.1	Начальная ревизия	Моргачёв Степан Соколова Дарья Чувашов Андрей
2023-10-24	0.2	Вторая ревизия (дописан второй раздел)	Моргачёв Степан Соколова Дарья Чувашов Андрей
2023-11-08	0.3	Третья ревизия (дописан третий раздел + новое задание)	Моргачёв Степан Соколова Дарья Чувашов Андрей

1 Введение

1.1 Цели

Документ определяет спецификацию требований программного обеспечения (СТПО) к системе контроля безопасности (СКБ). В нём описываются все внешние проявления и сценарии поведения СКБ, определяются функциональные и нефункциональные требования к системе контроля безопасности, которые необходимы для обеспечения безопасности на предприятии, устанавливается структура и архитектура системы, включая интерфейсы и взаимодействие с другими системами, если таковые имеются.

Спецификация предназначена только для внутреннего использования сотрудникам компании - заказчика и компании, разрабатывающей программное обеспечение согласно данному проекту.

1.2 Границы применения

Наименование программного продукта: Система контроля безопасности (СКБ).

СКБ предоставляет следующий функционал:

- Аутентификация сотрудников с использованием ключ-карт для контроля доступа.
- Контроль доступа сотрудников в помещения предприятия (иерархия уровней допуска сотрудников).
- Контроль времени пребывания сотрудников в каждой зоне безопасности.
- Мониторинг нахождения сотрудников в помещениях предприятия с повышенным уровнем вреда для здоровья.
- Обеспечение контроля пожарной безопасности и организация проведения мероприятий по эвакуации персонала в случае возникновения чрезвычайных ситуаций.
- Оповещение и активация звуковых сигналов при превышении времени пребывания в зоне безопасности.
- Переход в аварийный режим работы в случае сигнала от внешней системы, что приводит к выпуску всех сотрудников из зон безопасности.
- Обеспечение возможности выхода из любой зоны наружу в аварийной ситуации.
- Обеспечение мер тушения посредством газовой системы пожаротушения

СКБ планируется применять в следующих целях:

- Обеспечение безопасности сотрудников и активов предприятия путем контроля доступа в различные зоны.
- Быстрое реагирование на аварийные ситуации и моментальное высвобождение зон в случае необходимости.
- Увеличение эффективности системы безопасности и уменьшение вероятности несанкционированного доступа.
- Тушение пожаров на предприятии.

1.3 Термины, аббревиатуры, сокращения

СТПО	Спецификация требований к программному обеспечению
СКБ	Система контроля безопасности
Зона безопасности	Ограниченная область предприятия, требующая контроля доступа.
Ключ-карта	Уникальная идентификационная карта сотрудника.

Аварийный режим	Режим работы системы контроля безопасности, активируемый в случае сигнала от внешней системы, при котором выпускаются все сотрудники из зон безопасности.
ЭВМ	Электронно-вычислительная система
FUNC	Functional
REL	Reliability
PR	Performance Requirements
RR	Remont Requirements
PR	Project Requirements
DR	Documentation Requirements
LR	Licensing Requirements
AS	Applicable Standards
CI	Communication Interfaces

1.4 Ссылки

Обозначение	**Расшифровка**
[IEEE-830]	IEEE Std 830-1998

1.5 Краткий обзор

Данный документ структурирован согласно [IEEE-830].
Раздел 2 содержит описание поставляемой системы и схему её использования в Организации. Раздел 3 содержит функциональные и нефункциональные требования, предъявляемые к системе и необходимые для её проектирования.

2 Общее описание

Система контроля безопасности (СКБ) представляет собой интегрированную систему, разработанную для обеспечения безопасности на предприятии. Она включает в себя компоненты для аутентификации сотрудников, управления доступом в различные зоны безопасности, контроля времени пребывания в этих зонах, реагирования на аварийные ситуации и тушения пожаров.

2.1 Описание изделия

2.1.1 Интерфейсы системы

- Интерфейс для считывания ключ-карт. Предназначен для считывания ключ-карт, используемых сотрудниками для аутентификации. Он способен считывать информацию с карты и передавать её системе СКБ для проверки прав доступа.
- Интерфейс управления зонами безопасности. Позволяет администраторам настраивать параметры и правила доступа для каждой зоны безопасности. Он также позволяет включать и выключать режим аварийной ситуации.
- Интерфейс мониторинга времени пребывания. Отслеживает время пребывания сотрудников в зонах безопасности и сигнализирует в случае превышения разрешенного времени.
- Интерфейс мониторинга места пребывания. Отслеживает место пребывания сотрудников на объекте, и не допускает срабатыванию газовой системы пожаротушения в тех местах, в которых есть сотрудники.

- Интерфейс аварийной сигнализации. Активируется при получении сигнала от внешней системы о переходе в аварийный режим. Он открывает выходы из зон наружу и активирует сигнализацию для оповещения сотрудников и охраны.
- Интерфейс системы мониторинга. Система мониторинга взаимодействует с СКБ для отображения информации о сотрудниках, превысивших время пребывания в зоне безопасности. Она также может активировать звуковые сигналы и уведомления для оперативной реакции охраны.
- Интерфейс для управления настройками системы. Этот интерфейс предназначен для администраторов системы, чтобы изменять настройки, параметры доступа и правила в соответствии с требованиями предприятия.
- Интерфейс управления аварийным режимом.Позволяет активировать аварийный режим и контролировать его работу.

2.1.2 Интерфейсы пользователя

- Интерфейс аутентификации сотрудника. Система предоставляет интерфейс, который позволяет пользователю приложить ключ-карту к терминалу. После успешной аутентификации сотруднику предоставляется доступ к зоне безопасности. Интерфейс аутентификации должен быть интуитивно понятным, чтобы сотрудники могли легко и быстро получить доступ. Система должна предоставлять короткие сообщения об успешной аутентификации или ошибке.
- Интерфейс управления настройками доступа. Администраторы системы могут использовать интерфейс для настройки прав доступа сотрудников к разным зонам безопасности. Этот интерфейс должен позволять устанавливать правила доступа и временные ограничения для каждого сотрудника. Интерфейс управления настройками должен обеспечивать возможность легко изменять правила доступа. Система должна предоставлять наглядное представление текущих настроек для администраторов.
- Интерфейс мониторинга времени пребывания. Этот интерфейс позволяет операторам системы мониторинга отслеживать время пребывания сотрудников в зоне безопасности и получать уведомления о превышении разрешенного времени.Интерфейс мониторинга должен предоставлять наглядную информацию о текущем состоянии сотрудников и активировать звуковые сигналы и уведомления в случае необходимости.

2.1.3 Интерфейсы аппаратных средств ЭВМ

- Интерфейс терминалов для аутентификации. СКБ будет взаимодействовать с терминалами, которые поддерживают чтение ключ-карт и передачу данных для аутентификации. Система должна быть способной читать информацию с различных моделей терминалов и интерпретировать их данные. Поддерживаемые устройства: терминалы с поддержкой RFID-ключей, биометрических сканеров и других методов аутентификации. Протоколы: интерфейс должен поддерживать протоколы связи для передачи данных между терминалами и системой контроля безопасности.
- Интерфейс сигнализации аварийной ситуации. Система должна быть способна взаимодействовать с устройствами сигнализации, чтобы получать сигналы о внешних аварийных событиях, требующих перевода системы в аварийный режим. Поддерживаемые устройства: датчики дыма, системы аварийной сигнализации, системы безопасности предприятия. Протоколы: интерфейс должен поддерживать стандартные протоколы связи, такие как TCP/IP, для обмена данными с устройствами сигнализации.
- Интерфейс взаимодействия с замками и выходами. Система должна иметь возможность контролировать замки и выходы, обеспечивая управление доступом сотрудников в случае аварийного режима. Поддерживаемые устройства: замки с электромагнитным управлением, управляемые выходы для аварийного выхода из зон безопасности.Протоколы: интерфейс должен поддерживать протоколы управления замками и выходами для обеспечения безопасного выхода из зон.

2.1.4 Интерфейсы программного обеспечения

Система управления доступом (Access Control System):

Наименование: Система управления доступом.
Мнемоническое наименование: ACS.
Номер версии: Последняя версия.
Источник: Внутренняя система безопасности.

Система мониторинга событий (Event Monitoring System):
Наименование: Система мониторинга событий.
Мнемоническое наименование: EMS.
Номер версии: Последняя версия.
Источник: Внутренняя система безопасности.

База данных сотрудников (Employee Database):
Наименование: База данных сотрудников.
Мнемоническое наименование: EDB.
Номер версии: Последняя версия.
Источник: Внутренняя база данных о сотрудниках.

Система управления аварийными выходами (Emergency Exit Management System):
Наименование: Система управления аварийными выходами.
Мнемоническое наименование: EEMS.
Номер версии: Последняя версия.
Источник: Внутренняя система безопасности.

2.1.5 Интерфейсы коммуникаций

- Сетевой протокол IP (Internet Protocol). Система контроля безопасности будет использовать IP-сеть для обмена данными с внешними и внутренними системами.
  Протоколы: Система будет поддерживать IPv4 и IPv6 протоколы.
  Требования к безопасности: Все данные, передаваемые по IP-сети, должны быть защищены с использованием шифрования и безопасных методов аутентификации.
- Протоколы локальной сети (LAN Protocols). Система контроля безопасности будет взаимодействовать с устройствами и компонентами с использованием различных протоколов локальной сети, таких как Ethernet.
  Требования к совместимости: Система должна быть совместима с основными стандартами протоколов локальной сети.
  Требования к пропускной способности: Система должна обеспечивать необходимую пропускную способность для передачи данных и команд в реальном времени.
- Протоколы безопасной связи (Secure Communication Protocols). Описание: Для обеспечения безопасной связи с внешними системами и устройствами, система контроля безопасности будет использовать протоколы шифрования, такие как SSL/TLS, SSH и другие.
  Требования к безопасности: Все коммуникации должны быть зашифрованы и аутентифицированы с использованием современных методов шифрования.

2.1.6 Ограничения памяти

Нет строгого ограничения памяти.

2.1.7 Действия

2.1.7.1 Нормальные действия пользователей:

- Аутентификация: Пользователи должны аутентифицироваться с помощью своих ключ-карт перед попыткой доступа к зонам безопасности.
- Авторизация: Система определяет, к каким зонам пользователи имеют доступ на основе их ключ-карт и установленных правил.
- Мониторинг: Система непрерывно мониторит время нахождения пользователей в зонах и предупреждает при превышении разрешенного времени.

- Мониторинг: Система непрерывно мониторит место нахождения пользователей в зонах и не допускает заполнение этих помещений газом в случае пожарной опасности.
- Управление аварийными ситуациями: В случае активации режима аварийной ситуации, система выдает сигналы, чтобы разблокировать все зоны и предоставить доступ к выходу на улицу.

2.1.7.2 Специальные действия пользователей:
- Выход в аварийной ситуации: Пользователи могут инициировать выход в режим аварийной ситуации, активируя соответствующий сигнал или кнопку на терминале.

2.1.7.3 Обработка данных:
- Хранение данных: Система хранит данные о времени и месте пребывания пользователей в зонах и аварийных ситуациях.
- Обработка событий: Система обрабатывает события, связанные с аутентификацией, авторизацией и мониторингом времени и места нахождения.

2.1.8 Требования настройки рабочих мест

Конфигурация терминала: Настройка терминала или терминалов может включать в себя параметры, такие как тип экрана, разрешение, скорость обмена данными и другие характеристики, которые могут меняться в зависимости от рабочего места.
Настройка зон доступа: Разные задачи могут требовать разных настроек зон доступа, включая определение границ и времени доступа для конкретных рабочих мест.

2.2 Функции изделия

2.2.1 Управление зонами доступа:
Создание зон доступа: Позволяет администратору системы создавать и определять параметры различных зон доступа, включая их границы и ограничения.
Установка временных ограничений: Предоставляет возможность установки временных ограничений для каждой зоны доступа, чтобы ограничить время пребывания сотрудников внутри зоны.

2.2.2 Управление правами доступа:
Присвоение прав доступа: Позволяет администратору устанавливать права доступа для каждого сотрудника, включая определение разрешенных и запрещенных зон доступа.
Управление временными интервалами: Обеспечивает администратору возможность установки временных интервалов, в которые действуют разрешённые права доступа.

2.2.3 Реакция на аварийные ситуации:
Аварийный режим: Прием сигнала от внешних систем для перехода в аварийный режим, в котором открываются все выходы наружу.
Пожарная опасность: При возгорании система заполняет газом помещения, в которых нет людей.
Звуковые и визуальные сигналы: Генерация звуковых и визуальных сигналов при превышении времени пребывания сотрудников в зоне.

2.2.4 Мониторинг и уведомления:
Отслеживание активности: Система непрерывно отслеживает активность сотрудников и уведомляет оператора о нарушениях.
Уведомления: Отправка уведомлений и сигналов в реальном времени для реагирования на события безопасности.

2.2.5 Отчеты и аналитика:
Сбор данных: Система собирает данные о времени и месте пребывания сотрудников в зонах доступа и другие события.

Генерация отчетов: Генерация отчетов и аналитика для обеспечения безопасности и контроля доступа.

2.2.6 Реагирование в случае возгорания:
В случае пожара на предприятии помещения, в которых нет сотрудников, заполняются газом, а из помещений, в которых есть сотрудники открываются все выходы наружу.

2.3 Характеристики пользователей

- Пользователь, имеющий доступ к работе с СКБ, обязательно является сотрудником данного предприятия.
- Пользователь должен быть ознакомлен с основными принципами работы СКБ, поведением системы в штатных и аварийных ситуациях.
- Пользователь должен пройти первичный инструктаж по работе с СКБ.

2.4 Ограничения

Ограничения аппаратных средств ЭВМ: Система должна работать на аппаратных средствах ЭВМ, удовлетворяющих определенным требованиям по производительности и времени реакции. Система должна строго соблюдать стандарты и практики безопасности, чтобы предотвратить несанкционированный доступ и утечку конфиденциальной информации. Система должна предоставлять возможность администрирования и управления настройками, включая установку прав доступа и временных ограничений.

2.5 Предположения и зависимости

Предполагается, что на аппаратных средствах ЭВМ, на которых будет работать система контроля безопасности, будет доступна определенная операционная система.Проект предполагает соблюдение политики безопасности предприятия, включая требования по контролю доступа и протоколированию событий. Проект подвержен воздействию внешних факторов, таких как изменения в законодательстве или технологические изменения.

Любые изменения одного или нескольких факторов, влияющих на требования в СТПО, могут потребовать соответствующих изменений или пересмотра и обновления СТПО.

2.6 Распределение требований

Требования определятся в будущих версиях системы.

3 Детальные требования

Все описания детальных требований будут соответствовать следующему шаблону:

ID Требования	Однозначно идентифицирует требование
Группа	Определяет функциональную группу, к которой относится требование
Описание	Определяет требование
Приоритет	Определяет порядок, в котором должны выполняться требования. Приоритеты обозначены (от высшего к низшему) “1”, “2”, “3”... Требования с приоритетом “1” должны быть реализованы в первой версии системы.

	Требования с приоритетом “2” и ниже выходят за рамки данного документа
Ссылки	Предоставляет ссылку на связанные сценарии использования или требования.

3.1 Функциональные требования

3.1.1. Управление зонами доступа

ID Требования	FUNC-001
Группа	Управление зонами доступа
Описание	Система должна позволяет администратору создавать и определять параметры различных зон доступа, включая их границы и ограничения.
Приоритет	1
Ссылки	

3.1.2. Отслеживание мест пребывания

ID Требования	FUNC-002
Группа	Мониторинг и управление
Описание	Система должна отслеживать места пребывания сотрудников.
Приоритет	1
Ссылки	

3.1.3. Установка временных ограничений

ID Требования	FUNC-003
Группа	Мониторинг и управление
Описание	Предоставляет возможность установки временных ограничений для каждой зоны доступа, чтобы ограничить время пребывания сотрудников внутри зоны.

Приоритет 1

Ссылки

3.1.4. Присвоение прав доступа

ID Требования FUNC-004

Группа Мониторинг и управление

Описание Позволяет администратору устанавливать права доступа для каждого сотрудника, включая определение разрешенных и запрещенных зон доступа.

Приоритет 1

Ссылки

3.1.5 Управление временными интервалами

ID Требования FUNC-005

Группа Функции изделия

Описание Система обеспечивает администратору возможность установки временных интервалов, в которые действуют разрешённые права доступа.

Приоритет 1

Ссылки

3.1.6 Реакция на аварийные ситуации - аварийный режим

ID Требования FUNC-006

Группа Аварийные ситуации

Описание При приеме сигнала от внешних систем для перехода в аварийный режим должна осуществляться следующая процедура:
открытие все выходов наружу

Приоритет 2

Ссылки

3.1.7 Реакция на аварийные ситуации - звуковые и визуальные сигналы

ID Требования	FUNC-007
Группа	Аварийные ситуации
Описание	Система должна генерировать звуковые и визуальные сигналы при превышении времени пребывания сотрудников в зоне.
Приоритет	2
Ссылки	

3.1.8 Реакция на аварийные ситуации - тушение пожаров

ID Требования	FUNC-008
Группа	Аварийные ситуации
Описание	Система должна заполнять комнаты, в которых нет сотрудников, газом в случае пожарной опасности
Приоритет	1
Ссылки	

3.1.9 Мониторинг активности сотрудников

ID Требования	FUNC-009
Группа	Мониторинг и уведомления
Описание	Отслеживание активности: система непрерывно отслеживает активность сотрудников и уведомляет оператора о нарушениях.
Приоритет	2
Ссылки	

3.1.10 Рассылка уведомлений

ID Требования	FUNC-010
Группа	Мониторинг и уведомления
Описание	Система должна отправлять уведомления и сигналы в реальном времени для реагирования на события безопасности.
Приоритет	2
Ссылки	

3.1.11 Сбор данных о пребывании

ID Требования	FUNC-011
Группа	Отчеты и аналитика
Описание	Сбор данных: система собирает данные о времени пребывания сотрудников в зонах доступа и другие события.
Приоритет	3
Ссылки	

3.2 Надежность

3.2.1 Доступность

ID Требования	REL-001
Группа	Надежность
Описание	Система должна обеспечивать доступность на уровне не менее 99.99% (четыре девятки после запятой), включая время использования и доступ к обслуживанию. Время использования не должно быть менее 22 часов в сутки.
Приоритет	1
Ссылки	

3.2.2 Среднее разрешенное время между отказами

ID Требования	REL-002
Группа	Надежность
Описание	Среднее время между отказами (MTBF) системы должно составлять не менее 10 000 часов непрерывной работы.
Приоритет	1
Ссылки	

3.2.3 Максимальное время восстановления системы

ID Требования	REL-003
Группа	Надёжность
Описание	Максимальное время восстановления системы (MTTR) после отказа не должно превышать 4 часа.
Приоритет	1
Ссылки	

3.2.4 Точность вывода данных

ID Требования REL-004

Группа Надёжность

Описание Система должна обеспечивать точность вывода данных с разрешением не менее 0.01 единиц и точность по стандарту ISO 9001.

Приоритет 2

Ссылки

3.2.5 Допустимая частота ошибок

ID Требования REL-005

Группа Надёжность

Описание Максимально допустимая частота ошибок или дефектов в коде составляет 2 ошибки на 1000 строк кода (2 bugs/KLOC) и не более 1 критической ошибки на 1000 строк кода.

Приоритет 2

Ссылки

3.2.6 Критическая ошибка

ID Требования REL-006

Группа Надёжность

Описание Критическая ошибка определяется как ошибка, приводящая к полной потере данных или полной невозможности

использования определенной части функциональности системы.

Приоритет 2

Ссылки

3.3 Производительность

3.3.1 Среднее время ответа на транзакцию

ID Требования PR-001

Группа Производительность

Описание Среднее время ответа на транзакцию должно составлять менее 1 секунды, а максимальное время ответа - менее 5 секунд.

Приоритет 1

Ссылки

3.3.2 Пропускная способность транзакций

ID Требования PR-002

Группа Производительность

Описание Система должна поддерживать пропускную способность (throughput) не менее 100 транзакций в секунду.

Приоритет 1

Ссылки

3.3.3 Пропускная способность пользователей

ID Требования	PR-003
Группа	Производительность
Описание	Система должна иметь возможность обслуживать не менее 1000 активных пользователей одновременно.
Приоритет	2
Ссылки	

3.3.4 Режим ограниченной функциональности

ID Требования	PR-004
Группа	Производительность
Описание	В случае деградации производительности, система должна переходить в режим ограниченной функциональности, обеспечивая доступ к основной функциональности, но с ограниченными возможностями.
Приоритет	2
Ссылки	

3.3.5 Оптимальное использование ресурсов

ID Требования	PR-005
Группа	Производительность
Описание	Система должна оптимально использовать ресурсы, такие как память, диск, сетевые ресурсы и процессорное время, обеспечивая эффективное и экономичное функционирование.
Приоритет	2

Ссылки

3.4 Ремонтопригодность

3.4.1 Период поддержки

ID Требования	RR001
Группа	Поддержки
Описание	Период поддержки определяется заказчиком
Приоритет	1
Ссылки	

3.5 Ограничения проекта

3.5.1 Требования по языку программирования

ID Требования	PC-001
Группа	Ограничения проекта
Описание	Для разработки данной системы должен использоваться программный язык Java версии 8 или выше.
Приоритет	1
Ссылки	

3.5.2 Ограничения разработки ПО

ID Требования	PC-002
Группа	Ограничения проекта
Описание	Вся разработка и тестирование системы должны соответствовать процессу разработки ПО, утвержденному в организации и описанному в документе "Стандарты разработки ПО".
Приоритет	1
Ссылки	

3.5.3 Архитектурные ограничения

ID Требования	PC-003
Группа	Ограничения проекта
Описание	Разработка системы должна следовать архитектурным ограничениям, описанным в документе "Архитектура системы".
Приоритет	1
Ссылки	

3.5.4 Сторонние библиотеки и компоненты

ID Требования	PC-004
Группа	Ограничения проекта
Описание	При разработке системы необходимо использовать сторонние библиотеки и компоненты, перечень которых утвержден в документе "Список сторонних компонентов".
Приоритет	2
Ссылки	

3.5.5 Соблюдение стандартов и требований безопасности

ID Требования	PC-005
Группа	Ограничения проекта
Описание	Разработка системы должна соблюдать стандарты и требования безопасности, установленные в документе "Политика информационной безопасности".
Приоритет	2
Ссылки	

3.6 Требования к пользовательской документации

ID Требования DR-001

Группа Ограничения проекта

Описание Система должна быть снабжена соответствующей документацией, которая будет доступна сотрудникам (пользователям системы) и будет облегчать взаимодействие человек-система.

Приоритет 2

Ссылки

3.7 Используемые приобретаемые компоненты

ID Требования COMP-1

Группа Используемые приобретаемые компоненты

Описание Система может использовать RFID-считыватели и метки от сторонних поставщиков для реализации аутентификации сотрудников.

Приоритет 1

Ссылки

ID Требования COMP-2

Группа Звуковые сигнализаторы

Описание	Для генерации звуковых сигналов при превышении времени пребывания в зоне, система может включать звуковые сигнализаторы от сторонних производителей.
Приоритет	1
Ссылки	

ID Требования	COMP-3
Группа	Аппаратные устройства для системы пожаротушения
Описание	Для сбора информации о пожарной ситуации и активации режима аварийной ситуации, система может использовать аппаратные устройства, такие как датчики дыма и управляющее оборудование для системы пожаротушения, предоставляемые сторонними компаниями.
Приоритет	1
Ссылки	

ID Требования	COMP-4
Группа	Системы управления и мониторинга событий
Описание	Для обработки и анализа событий, связанных с безопасностью, система может интегрироваться со сторонними системами управления и мониторинга событий

Приоритет 1

Ссылки

ID Требования COMP-5

Группа Базы данных и системы хранения

Описание Для хранения и обработки информации о сотрудниках, зонах доступа и событиях, система может использовать сторонние базы данных и системы хранения данных.

Приоритет 1

Ссылки

3.8 Интерфейсы

3.8.1 Интерфейс пользователя

ID Требования CI-1

Группа Интерфейс пользователя

Описание Система контроля безопасности должна предоставлять пользовательские интерфейсы для аутентификации и управления доступом. Эти интерфейсы включают веб-интерфейс для администрирования и взаимодействия с операторами.

Приоритет 1

Ссылки

3.8.2 Аппаратные интерфейсы

ID Требования CI-2

Группа Аппаратные интерфейсы

Описание Система контроля безопасности должна быть доступна через сетевой интерфейс по протоколам HTTP и HTTPS для аутентификации и управления. Эти порты используются для веб-интерфейса администрирования и взаимодействия с операторами.

Приоритет 1

Ссылки

3.8.3 Программные интерфейсы

ID Требования CI-3

Группа Программные интерфейсы

Описание Система контроля безопасности может взаимодействовать с другими программными компонентами, включая систему мониторинга событий, систему управления, и базу данных для хранения и обработки информации о сотрудниках и доступе

Приоритет 1

Ссылки

3.8.4 Интерфейсы коммуникаций

ID Требования CI-004

Группа Интерфейсы коммуникаций

Описание Система контроля безопасности может взаимодействовать с локальными сетями и удаленными устройствами для получения информации о пожарной ситуации и активации режима аварийной ситуации. Подробные протоколы и порты для таких интерфейсов могут быть уточнены в соответствии с требованиями конкретных систем.

Приоритет 2

Ссылки

3.9 Требования лицензирования

3.9.1 Лицензия на использование программного обеспечения

ID Требования LC-001

Группа Лицензирование

Описание Лицензии могут предоставляться на основе количества пользователей или устройств, в зависимости от модели лицензирования. Лицензии могут быть выданы на

определенный срок с возможностью продления.

Приоритет 2

Ссылки

3.9.2 Ограничения использования

ID Требования LC-002

Группа Лицензирование

Описание Пользователи обязаны соблюдать ограничения, установленные в лицензионном соглашении.

Приоритет 2

Ссылки

3.9.3 Актуализация лицензий

ID Требования LC-003

Группа Лицензирование

Описание Пользователи обязаны следить за актуальностью лицензий и вносить соответствующие платежи за продление лицензий, если это необходимо.

Приоритет 2

Ссылки

3.9.4 Лицензия на аппаратные устройства

ID Требования LC-004

Группа Лицензирование

Описание Пользователи обязаны приобретать соответствующие лицензии на аппаратные устройства, такие как RFID-считыватели и звуковые сигнализаторы, если это предусмотрено правообладателем.

Приоритет 2

Ссылки

3.10 Применимые стандарты

3.10.1 Лицензия на аппаратные устройства

ID Требования AS-001

Группа Стандарты и нормы

Описание Система должна соответствовать определенным стандартам и нормативам.

Приоритет 2

Ссылки

4 Индекс