	Спецификация требований к программному обеспечению для Проекта СКБ	Автор: TEAM15 № документа: TEAM15-v0.1 Дата: 2023-10-10 Страниц: x

Содержание

История изменений

Дата	Версия	Описание	Автор(ы)
2023-10-10	0.1	Начальная ревизия	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 обеспечения контроля безопасности предприятия (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.

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.

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

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 и реагирования на аварийные ситуации.

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 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

Подлежат выяснению.

2.1.4 Интерфейсы программного обеспечения

Подлежат выяснению.

2.1.5 Интерфейсы коммуникаций

Подлежат выяснению.

2.1.6 Ограничения памяти

Нет строгого ограничения памяти.

2.1.7 Действия

Подлежат выяснению.

2.1.8 Требования настройки рабочих мест

Подлежат выяснению.

2.2 Функции изделия

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

Подлежат выяснению.

2.5 Предположения и зависимости

Подлежат выяснению.

2.6 Распределение требований

3 Детальные требования

This section of the **SRS** should contain all the software requirements to a level of detail sufficient to enable designers to design a system to satisfy those requirements, and testers to test that the system satisfies those requirements. When using use-case modelling, these requirements are captured in the Use-Cases and the applicable supplementary specifications.]

3.1 Функциональные требования

[This section describes the functional requirements of the system for those requirements which are expressed in the natural language style. For many applications, this may constitute the bulk of the **SRS** Package and thought should be given to the structure of this section. This section is typically structured by feature, but alternative structures may also be appropriate, for example, structure by user or by subsystem. Functional requirements may include feature sets, capabilities, and security.

Where application development tools, such as requirements tools, modelling tools, etc., are employed to capture the functionality, this section will refer to the availability of that data, indicating the location and name of the tool that is used to capture the data.]

3.1.1 <Functional Requirement One>

[The requirement description.]

3.2 Надежность

[Requirements for reliability of the system should be specified here. Some suggestions follow:

• Availability—specify the percentage of time available (xx.xx%), hours of use, maintenance access, degraded mode operations, etc.

• Mean Time Between Failures (MTBF) — this is usually specified in hours, but it could also be specified in terms of days, months or years.

• Mean Time To Repair (MTTR)—how long is the system allowed to be out of operation after it has failed?

• Accuracy—specify precision (resolution) and accuracy (by some known standard) that is required in the system’s output.

• Maximum Bugs or Defect Rate—usually expressed in terms of bugs per thousand of lines of code (bugs/KLOC) or bugs per function-point(bugs/function-point).

• Bugs or Defect Rate—categorized in terms of minor, significant, and critical bugs: the requirement(s) must define what is meant by a “critical” bug; for example, complete loss of data or a complete inability to use certain parts of the system’s functionality.]

3.2.1 <Reliability Requirement One>

[The requirement description.]

3.3 Производительность

[The system’s performance characteristics should be outlined in this section. Include specific response times. Where applicable, reference related Use Cases by name.

• response time for a transaction (average, maximum)

• throughput, for example, transactions per second

• capacity, for example, the number of customers or transactions the system can accommodate

• degradation modes (what is the acceptable mode of operation when the system has been degraded in some manner)

• resource utilization, such as memory, disk, communications, etc.

3.3.1 <Performance Requirement One>

[The requirement description goes here.]

3.4 Ремонтопригодность

[This section indicates any requirements that will enhance the maintainability of the system being built, including coding standards, naming conventions, class libraries, maintenance access, maintenance utilities.]

3.4.1 <Maintainability Requirement One>

[The requirement description goes here.]

3.5 Ограничения проекта

[This section should indicate any design constraints on the system being built. Design constraints represent design decisions that have been mandated and must be adhered to. Examples include software languages, software process requirements, prescribed use of developmental tools, architectural and design constraints, purchased components, class libraries, etc.]

3.5.1 <Design Constraint One>

[The requirement description goes here.]

3.6 Требования к пользовательской документации

[Describes the requirements, if any, for on-line user documentation, help systems, help about notices, etc.]

3.7 Используемые приобретаемые компоненты

[This section describes any purchased components to be used with the system, any applicable licensing or usage restrictions, and any associated compatibility and interoperability or interface standards.]

3.8 Интерфейсы

[This section defines the interfaces that must be supported by the application. It should contain adequate specificity, protocols, ports and logical addresses, etc. so that the software can be developed and verified against the interface requirements.]

3.8.1 Интерфейс пользователя

[Describe the user interfaces that are to be implemented by the software.]

3.8.2 Аппаратные интерфейсы

[This section defines any hardware interfaces that are to be supported by the software, including logical structure, physical addresses, expected behaviour, etc.]

3.8.3 Программные интерфейсы

[This section describes software interfaces to other components of the software system. These may be purchased components, components reused from another application or components being developed for subsystems outside of the scope of this **SRS** but with which this software application must interact.]

3.8.4 Интерфейсы коммуникаций

[Describe any communications interfaces to other systems or devices such as local area networks, remote serial devices, etc.]

3.9 Требования лицензирования

[Defines any licensing enforcement requirements or other usage restriction requirements that are to be exhibited by the software.]

3.10 Применимые стандарты

[This section describes by reference any applicable standard and the specific sections of any such standards which apply to the system being described. For example, this could include legal, quality and regulatory standards, industry standards for usability, interoperability, internationalization, operating system compliance, safety, security, etc.]

Индекс