Контур безопсности

16/10/2019

1. Введение

1.1. Цели

Этот документ определяет спецификацию требований к программному обеспечению (SRS) для системы обеспечения контура безопасности. В нем описываются область действия системы, как функциональные, так и нефункциональные требования к программному обеспечению, конструктивные ограничения и системные интерфейсы. Продукт должен обеспечить корректное функционирование для любого коммерческого предприятия.

1.2. Границы применения

Система обеспечения контура безопасности -система, представляющая собой комплекс программных и технических средств, необходимых для поддержания санкционированного доступа в помещения в охраняемых зонах. СОКБ должна предоставить доступ лицу, имеющему соответствующий пропуск. Лица, не имеющие пропуска, не должны иметь возможности доступа к объекту. Программное обеспечение должно функционировать на двух уровнях безопасности. Первый уровень безопасности представляет собой установленный при входе в помещение турникет, считывающий с пропуска информацию о прошедшем лице. Вторым уровнем безопасности являются доступ к рабочему отделу организации. Также как и на первом уровне считывается информация о лице. При наличии соответствующих прав должен предоставиться доступ к отделу.

Информация о доступах на обоих уровнях безопасности должна заноситься в базы данных. Использование данной системы должно значительно снизить риск несанкционированного доступа, способного нанести серьезный материальный ущерб.

1.3. Определения, сокращения, термины

Аббривиатура	Расшифровка
СОКБ	Система обеспечения контура безопасности
АРМ	Автоматизированное рабочее место
ЗПБ	Зона повышенной безопасности
УД	Уровень доступа
КСБ	Комплекс системы безопасности
СУРВ	Система учета рабочего времени
СКУД	Система контроля и управления доступом

1.4. Ссылки

1.5. Краткий обзор

2. Общее описание

2.1. Описание изделия

2.1.1. Интерфейсы системы

2.1.2. Интерфейсы пользователя

2.1.3. Интерфейсы аппаратных средств ЭВМ

2.1.4. Интерфейсы программного обеспечения

2.1.5. Интерфейсы коммуникаций

2.1.6. Ограничения памяти

2.1.7. Действия

2.1.8. Требования настройки рабочих мест

2.2. Функции изделия

2.3. Характеристики пользователей

2.4. Ограничения

2.5. Предложения и зависимости

2.6. Поднаборы требований(распределение требований)

3. Детальные требования

3.1. Внешние интерфейсы

На первом уровне имеется 2 картоприемника, каждый из которых соединен посредством канала связи с турникетом. На вход картоприемник должен получить карту, с которой считывает необходимую информацию, а также заносит новые данные в базу данных. На выходе формируется ответ о наличии прав доступа и отсылает его турникету. Турникет должен быть связан с двумя картоприемниками. Картоприемник №1,расположенный на входе, при наличии прав доступа должен разрешить вход 1 человека. Картоприемник №2, расположенный на выходе, при наличии прав должен разрешить выход 1 человека. В обычном ситуации турникет должен находиться в одном из 3х состояний:

- вход и выход запрещен.
- Вход разрешен, выход запрещен
- Вход запрещен, выход запрещен

В аварийном ситуации турникет должен находиться в состоянии:

- вход и выход Разрешен.

Турникет имеет 3 индикатора:

Индикатор №1 имеет форму стрелочки влево и сообщает о том, что разрещен выход.

Индикатор №2 имеет форму креста и сообщает о том, что запрещены вход и выход

Индикатор №3 имеет форму стрелочки вправо и сообщает о том, что разрешен вход

В Аварийной ситуации активны индикаторы №1 и №3.

На втором уровне на входе в отдел имеется 1 картоприемник, который соединен каналом связи с дверью. При считывании данных с карты информация заносится в базу данных. При наличии прав доступа дверь открывается. При выходе из отдела имеется выключатель, открывающий дверь.

3.2. Функции

Система должна обеспечить:

- контроль над датой и временем прохода сотрудников в помещения.
- учет рабочего времени.
- идентификацию сотрудника с помощью визуального срав-

нения лица, воспользовавшегося картой, и оригинальной фотографии владельца данной карты.

○ возможность оформления бесконтактных карт доступа в виде пропусков.

○ постоянный поименный учет нахождения сотрудников и посетителей в контролируемых зонах, учет времени входа и выхода сотрудников и посетителей, сдачи разовых пропусков, ведение протокола событий.

○ ведение базы данных, обеспечивающей регистрацию всех фактов посещения объекта сотрудниками и посетителями, с указанием даты и времени посещения, их фотографий и иных данных, с возможностью хранения и использования данных в течение не менее 5 лет.

○ организацию контроля и управления системой с учетом авторизованных прав доступа операторов к функциям системы и протоколированием действий операторов.

○ возможность работы системы в аварийном режиме.

○ В случае возникновения каких-либо ошибок запретить вход, разрешить выход, сообщить об ошибке в организацию контроля и управления системой.

○ При работе не в аварийном режиме резрешить вход или выход для неболее чем 1 человеку в очереди.

○ При попытке одновременного считывая информации с пропуска на вход и выход приоритет отдавать на выход.

3.3. Требования исполнения

Система должна поддерживать работоспособность 2х и более турникетов, а также 5ти и более отделов. Система в 90 % случаем должна считывать информацию, заносить её в базу данных и предоставлять доступ в случае наличия прав не более чем за 1 секунду

3.4. Требования логики базы данных

В базе данных должны храниться следующие данные: ○ Информация о выдаче пропуска:ID,Дата выдачи, ФИО, фотография.

○ Информация о наличии прав:ID, наличие прав доступа в каждый из отделов.

○ Информация о посещениях:ID, время входа и выхода в рабочее помещение, время входа в отделы организации.

Информация в базе данных должна храниться в течении 5 лет с момента увольнения работника.

3.5. Ограничения проекта Никаких особых конструктивных ограничений не налагается, за исключением целевой платформы системы. Целевая платформа должна быть стандартной средой LAMP (PHP 5 или новее, MySQL 4 или новее, Perl 5 или новее, Apache 2.1 или новее), поддерживаемые операционные системы должны быть Windows XP (SP 2 или более поздняя версия), Windows Vista, Linux (ядро 2.2.26 или позже), Mac OS X (10.4.1 или позже).

3.6. Характеристики программного обеспечения системы

3.6.1. Надежность
В этом подразделе мы обсудим все потребности в надежности. Поскольку термин надежность не всегда понятен, мы определяем это как вероятность безотказной системы, рассматривающей отказ в широком смысле (неожиданно поведение).

3.6.2. Защита данных. Должна быть предусмотрена возможность настройки системы таким образом, чтобы все сохраненные данные автоматически сохранялись на нескольких серверах.

3.6.3. Одновременный доступ. Система не должна учитывать одновременный доступ к защищенным ресурсам. В случае одновременного доступа последнее изменение должно быть принято.

3.6.4. Безопасность

Сессии. В случае наличия прав доступа разрешить проход 1 человека. Если человек прошел, или по истечению 20 секунд, запретить доступ. Внешний интерфейс Открытый API внешнего интерфейса должен позволять только те операции, которые доступны пользователям.

3.6.5. Ремонтопригодность

Смена разработчиков В случае, если команда разработчиков или компания должны измениться после первого выпуска системы, новые разработчики смогут начать работу над системой менее чем за 5 дней, если это предписано старой командой. Небольшие изменения Должно быть возможно выполнить все незначительные изменения (включая обновление всех документов) менее чем за 16 человеко-часов работы.

3.7. Структурирование детальных требований

3.7.1. Режим системы

3.7.2. Классы пользователей

3.7.3. Объекты

3.7.4. Особенности

3.7.5. Воздействие

3.7.6. Реакция

3.7.7. Функциональные иерархии

3.7.8. Дополнительные комментарии