Автономная некоммерческая организация
Агентство привлечения инвестиций и развития инноваций
Хабаровского края (АНО «АПИРИ ХК»)

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на разработку проекта бесконтактной системы контроля и управления доступом на территории базы ГК «Интерфейс»

наименование технической задачи (конкурсного задания) ежегодного краевого конкурса молодежных инновационных команд «КУБ»

на 16 (шестнадцати) листах

СОГЛАСОВАНО

И.о. министра инвестиционного развития
и предпринимательства Хабаровского
края

_____ М.А. Тарасов
(подпись) (И.О. Фамилия)
"17" августа 2020 г.

г. Хабаровск

Содержание

Используемые термины и сокращения

КПП – контрольно-пропускной пункт.

ДИУ – датчики, контроллеры и исполнительные устройства, которые могут передавать и получать информацию, используя различные протоколы передачи данных.

ЗИП – запасные части, инструменты и принадлежности.

СКУД – система контроля и управления доступом.

API – (*англ. Application Programming Interface*) программный интерфейс для взаимодействия с другими системами.

RFID – (*англ. Radio Frequency Identification*) – радиочастотная идентификация.

ERP – (*англ. Enterprise Resource Planning*) программный продукт, реализующий организационную стратегию интеграции производства и операций, управления трудовыми ресурсами, финансового менеджмента и управления активами.

1С – программный продукт одноименной компании «1С», предназначенный для автоматизации деятельности на предприятии.

НСД – несанкционированный доступ.

ОС – операционная система.

СУБД – система управления базами данных.

1 Наименование технической задачи (конкурсного задания)

Разработка проекта бесконтактной системы контроля и управления доступом территории базы ГК «Интерфейс».

2 Описание компании-кейсодателя

Группа компаний «Интерфейс» – одно из крупнейших предприятий в сфере теплоэнергетики на Дальнем Востоке.

3 Основание для разработки

Предприятие внедряет концепцию бесконтактного контроля и управления доступом на территории базы, а также возможность мониторинга и учета рабочего времени сотрудников и отслеживания их перемещений в том числе при въезде/выезде на автотранспортных средствах.

4 Назначение разработки

Участникам конкурса необходимо разработать проект бесконтактного контроля и управления доступом на территории базы (далее – Система) в соответствии с требованиями настоящего Технического задания.

5 Требования к Системе

5.1 Назначение и цели создания Системы

5.1.1 Назначение Системы

Система предназначена для отметки в СКУД при въезде/выезде сотрудников предприятия с территории базы на автотранспортных средствах, фиксации рабочего времени и фактического маршрута перемещений. Предоставлению доступа на въезде/выезде путём открытия шлагбаума/ворот. Открытия электрозамков в помещениях в зависимости от уровня доступа.

5.1.2 Цели создания Системы

Создание Системы должно обеспечить достижение следующих целей:

- организация процесса бесконтактной отметки в СКУД и открытия шлагбаума/ворот при въезде/выезде с территории базы на личном автотранспорте;
- организация фиксации начала/окончания рабочего дня сотрудников при прохождении КПП/ворот;
- организация предоставления доступа в кабинеты сотрудников в зависимости от уровня доступа;

- контроль перемещения по территории базы/АБК сотрудников.

5.1.3 Общие требования

Для реализации поставленных целей система должна:

- иметь возможность интеграции, с используемыми ГК Интерфейс системами Битрикс и 1С;
- обладать комплексом оборудования для удаленной и бесконтактной идентификации сотрудника компании и его транспортного средства;
- обладать программными инструментами и оснастками для формирования отчетности по полученным данным;
- обладать инструментами ведения базы данных в 1С, выдачи разрешений на въезд/выезд транспортных средств и предоставления доступа в кабинеты.

5.2 Характеристика объекта автоматизации

5.2.1 Общее представление

Контрольно-пропускной пункт (КПП), оснащенный шлагбаумами для внешнего проезда автотранспорта и турникетами для внутреннего прохода сотрудников ГК Интерфейс. Идентификация сотрудников проходит через СКУД.

5.2.2 Дополнительные требования к автоматизации объекта

При проектировании системы необходимо принять правила и требования для совместного применения оборудования и создания единого RFID-пространства ГК Интерфейс, а именно:

- унифицированный по информационным системам идентификационный код объекта;
- стандартный набор данных по объекту;
- типы, материал и печатная форма RFID-меток;
- типы, функции и частота работы RFID оборудования и др.

5.3 Требования к структуре, реализации и функционированию

5.3.1 Требования к структуре

В состав Системы должны входить следующие подсистемы:

- подсистема аппаратно-технических средств;
- подсистема программных средств;
- подсистема пользовательских интерфейсов.

5.3.1.1 Подсистема аппаратно-технических средств

Подсистема аппаратно-технических средств включает в себя:

- технически средства – комплекс модульных устройств сбора и передачи данных, установленных на ключевые части оборудования и дальнейшей передачи данных в локальную подсистему обработки данных (далее – Платформа) для определения фактического наличия, месторасположения, состояния, перемещений и инвентаризации объектов. В состав системы должны входить следующие типы RFID оборудование и ДИУ:
  - оборудование для кодирование RFID-меток,
  - RFID считыватели стационарные и мобильные,
  - RFID принтеры,
  - RFID-метки для размещения на разные поверхности (бумага, металл, пластик и др.), соответствующие стандарту GS1.

  Состав оборудования будет уточняться на этапе информационного обследования объекта, при подготовке проекта;
- аппаратные средства – комплекс рабочих станций, устройств бесперебойного питания, сетевого и серверного оборудования, необходимых для хранения данных, установки и работы подсистемы программных средств, в отказоустойчивом режиме 24/7 365 дней в году.
- подсистема предназначена для сбора и преобразование информации в заданный формат, для дальнейшей её передачи в Платформу.

5.3.1.2 Подсистема программных средств

Подсистема, являющаяся специализированным программным обеспечением, которое за счет данных, полученных от ДИУ, позволяет организовать единую среду для хранения, обработки и визуализации информации об управляемом объекте, для мониторинга, управления и координации, с помощью разработанных или объеденных программных модулей.

Подсистема предназначена:

- для хранения и обработки данных объектов, которые к ней подключены, за счет созданных в ней программных сценариев, шаблонов, модулей (далее – Приложения);
- для визуализации всех процессов и операций, происходящих с объектом автоматизации в режиме «реального времени»;
- для анализа и прогнозирования состояния объекта автоматизации, за счет заданных математических методов и алгоритмов.

5.3.1.3 Подсистема пользовательских интерфейсов

Подсистема, которая за счет созданных приложений, позволяет работать с данными датчиков, представленными в графическом виде, на мобильных и десктопных устройствах. Подсистема предназначена для аналитической и управленческой работы с данными и объектами подсистемы технических устройств, для мониторинга и управления объектами автоматизации

5.3.2 Требования к реализации Системы

5.3.2.1 Требования к взаимодействию с другими информационными системами (API)

Система должна обладать интерфейсом прикладного программирования для контролируемого взаимодействия с другими системами.

5.3.2.2 Показатели назначения

Система должна обеспечивать возможность хранения данных с глубиной не менее 10 лет.

Система должна обеспечивать поддержку многопользовательской работы с подсистемой пользовательских интерфейсов при следующих характеристиках времени отклика:

- для операций навигации по экранным формам Системы – не более 5 сек.;
- для операций формирования аналитических отчетов – не более 10 сек.;
- для операций вывода «Цифрового двойника» с отображением работы объекта автоматизации в реальном времени – не более 10 сек.

Время формирования аналитических отчетов определяется их сложностью и может занимать продолжительное время.

5.3.2.3 Требования к защите информации

Система должна обеспечивать защиту от НСД на уровне не ниже установленного требованиями, предъявляемыми к категории 1Д по классификации действующего руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем» 1992 г.

Компоненты подсистемы защиты от НСД должны обеспечивать:

- идентификацию пользователя;
- проверку полномочий пользователя при работе с системой;
- разграничение доступа пользователей на уровне задач и информационных массивов.

Протоколы аудита системы и приложений должны быть защищены от НСД как локально, так и в архиве.

Уровень защищённости от несанкционированного доступа средств вычислительной техники, обрабатывающих конфиденциальную информацию, должен соответствовать требованиям к классу защищённости 6 согласно требованиям действующего руководящего документа Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

Защищённая часть системы должна использовать «слепые» пароли (при наборе пароля его символы не показываются на экране либо заменяются одним типом символов; количество символов не соответствует длине пароля).

Защищённая часть системы должна автоматически блокировать сессии пользователей и приложений по заранее заданным временам отсутствия активности со стороны пользователей и приложений.

Защищённая часть системы должна предотвратить работу с некатегоризированной информацией под сеансом пользователя, авторизованного на доступ к конфиденциальной информации.

Защищённая часть Системы должна использовать многоуровневую систему защиты. Защищённая часть Системы должна быть отделена от незащищённой части системы межсетевым экраном.

5.3.2.4 Требования к надежности

Система должна сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих внештатных ситуаций:

- при сбоях в системе электроснабжения аппаратной части, приводящих к перезагрузке программной платформы, восстановление Системы должно происходить после перезапуска ОС и запуска исполняемого файла системы;
- при ошибках в работе аппаратных средств (кроме носителей данных и программ) восстановление функции системы возлагается на серверную ОС;
- при ошибках, связанных с программным обеспечением (ОС и драйверы устройств), восстановление работоспособности возлагается на серверную ОС;
- при сбоях работы БД, восстановление работоспособности возлагается на сервер базы данных (создание регулярных резервных копий).

Сервер с Платформой Системы должен быть защищен от НСД.

5.3.2.5 Требования к безопасности

Все внешние элементы технических средств Системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь зануление или защитное заземление в соответствии с ГОСТ 12.1.030-81 и ПУЭ.

Система электропитания должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в цепях нагрузки, а также аварийное ручное отключение.

Общие требования пожарной безопасности должны соответствовать нормам на бытовое электрооборудование. В случае возгорания не должно выделяться ядовитых газов и дымов. После снятия электропитания должно быть допустимо применение любых средств пожаротушения.

Факторы, оказывающие вредные воздействия на здоровье со стороны всех элементов системы (в том числе инфракрасное, ультрафиолетовое, рентгеновское и электромагнитное излучения, вибрация, шум, электростатические поля, ультразвук строчной частоты и т.д.), не должны превышать действующих норм (СанПиН 2.2.2./2.4.1340-03 от 03.06.2003 г.).

5.3.2.6 Требования к эргономике и технической эстетике

Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав Системы должно осуществляться посредством визуального графического интерфейса. Интерфейс системы должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм. Навигационные элементы должны быть выполнены в удобной для пользователя форме.

Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть управление системой должно осуществляться с помощью набора экранных меню, кнопок и т. п.

Система должна обеспечивать проверку и корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей или недопустимыми значениями входных данных. В указанных случаях система должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Система должна соответствовать требованиям эргономики и профессиональной медицины при условии комплектования высококачественным оборудованием (ПЭВМ, монитор и прочее оборудование), имеющим необходимые сертификаты соответствия и безопасности Росстандарта.

5.3.2.7 Требования к сохранности информации при авариях

Программное обеспечение Системы должно восстанавливать свое функционирование при корректном перезапуске аппаратных средств. Должна быть предусмотрена возможность организации автоматического и (или) ручного резервного копирования данных системы средствами системного и базового программного обеспечения (СУБД), входящего в состав программно-технического комплекса заказчика.

Приведенные выше требования не распространяются на компоненты системы, разработанные третьими сторонами и действительны только при соблюдении правил эксплуатации этих компонентов, включая своевременную установку обновлений, рекомендованных производителями покупного программного обеспечения.

5.3.2.8 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов Системы

Система должна быть рассчитана на эксплуатацию в составе программно-технического комплекса компании-кейсодателя. Техническая и физическая защита аппаратных компонентов системы, носителей данных, бесперебойное энергоснабжение, резервирование ресурсов, текущее обслуживание реализуется техническими и организационными средствами, предусмотренными в инфраструктуре компании-кейсодателя.

Для нормальной эксплуатации разрабатываемой системы должно быть обеспечено бесперебойное питание серверного оборудования. При эксплуатации Система должна быть обеспечена соответствующая стандартам хранения носителей и эксплуатации серверного оборудования температура и влажность воздуха.

Периодическое техническое обслуживание используемых технических средств должно проводиться в соответствии с требованиями технической документации изготовителей, но не реже одного раза в год.

Периодическое техническое обслуживание и тестирование технических средств должны включать в себя обслуживание и тестирование всех используемых средств, включая рабочие станции, серверы, кабельные системы и сетевое оборудование, устройства бесперебойного питания.

В процессе проведения периодического технического обслуживания должны проводиться внешний и внутренний осмотр и чистка технических средств, проверка контактных соединений, проверка параметров настроек работоспособности технических средств и тестирование их взаимодействия. На основании результатов тестирования технических средств должны проводиться анализ причин возникновения обнаруженных дефектов и приниматься меры по их ликвидации.

Восстановление работоспособности технических средств должно проводиться в соответствии с инструкциями разработчика и поставщика технических средств и документами по восстановлению работоспособности технических средств и завершаться проведением их тестирования. При вводе системы в опытную эксплуатацию должен быть разработан план выполнения резервного копирования программного обеспечения и обрабатываемой информации. Во время эксплуатации системы, персонал, ответственный за эксплуатацию системы должен выполнять разработанный план.

Размещение помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и

обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств.

Размещение оборудования, технических средств должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

Все пользователи системы должны соблюдать правила эксплуатации электронной вычислительной техники.

5.3.2.9 Требования к численности и квалификации персонала Системы и режиму его работы

Для эксплуатации Системы определены следующие роли:

- системный администратор;
- администратор баз данных;
- администратор информационной безопасности;
- пользователь.

Основными обязанностями системного администратора являются:

- модернизация, настройка и мониторинг работоспособности комплекса технических средств (сетевого и серверного оборудования, рабочих станций);
- установка, модернизация, настройка и мониторинг работоспособности системного и базового программного обеспечения;
- установка, настройка и мониторинг прикладного программного обеспечения;
- ведение учетных записей пользователей системы.

Системный администратор должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию программных и технических средств, применяемых в Системе.

Основными обязанностями администратора баз данных являются:

- установка, модернизация, настройка параметров программного обеспечения СУБД;
- оптимизация прикладных баз данных по времени отклика, скорости доступа к данным;
- разработка, управление и реализация эффективной политики доступа к информации, хранящейся в прикладных базах данных.

Администратор баз данных должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию используемых в Системе СУБД.

Основными обязанностями администратора информационной безопасности являются:

- разработка, управление и реализация эффективной политики информационной безопасности Системы;

- управление правами доступа пользователей к функциям Системы;
- осуществление мониторинга информационной безопасности.

Администратор информационной безопасности данных должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по обеспечению информационной безопасности.

Основными обязанностями пользователя являются:

- верификация данных (проверка) на основе данных полученных с АИС;
- составления ЗИП на основе данных полученных с АИС.

Пользователи системы должны иметь опыт работы с персональным компьютером на базе операционных систем Microsoft Windows на уровне квалифицированного пользователя и свободно осуществлять базовые операции в операционной системе семейства Windows.

Роли системного администратора, администратора баз данных и администратора информационной безопасности могут быть совмещены в единую роль Администратора Системы.

Рекомендуемая численность для эксплуатации Системы:

- администратор Системы – 2 штатных единицы из числа специалистов ДИТ, обучение которых должно быть произведено компаний Разработчиком, а стоимость обучения включено в стоимость работ по развертыванию Системы;
- пользователь – число штатных единиц определяется структурой предприятия.

5.3.2.10 Требования к патентной частоте

Установка системы в целом, как и установка отдельных частей системы не должна предъявлять дополнительных требований к покупке лицензий на программное обеспечение сторонних производителе, кроме программного обеспечения, указанного в разделе 5.4.4.

5.3.2.11 Требования к каналам связи

Информационный обмен между клиентами и сервером осуществляется в пределах внутренней сети КФ. Системная архитектура должна обеспечить комфортный доступ к Системе на скорости не менее 100Мбит/сек. Сетевое взаимодействие должно осуществляться с учетом требований по скорости, надежности и безопасности информационного взаимодействия.

5.3.3 Требования к функционированию (задачам) Системы

5.3.3.1 Требования к обеспечению подсистемы аппаратно-технических средств

Подсистема аппаратно-технических средств должна обеспечивать:

- комплект технических средств:
- комплекс аппаратных средств.

Комплект технических средств должен обеспечивать:

- возможность подключения и обработки полученной информации, по беспроводной и проводной технологии передачи данных, с цифровых и аналоговых Датчиков;
- возможность подключения Датчиками разных производителей;
- световой идентификацией, для возможности определения состояния его работы на расстоянии;
- обладать большим спектром собираемых показателей для получения разного рода данных с узлов автоматизированного объекта (окружающая среда, телеметрия).

Комплекс аппаратных средств должен обеспечивать:

- поддержку работоспособности Системы в режиме 24/7 365 дней в году;
- полную совместимость с существующим сетевым и серверным оборудованием заказчика;
- обеспечивать достаточную вычислительную мощность для получения, обработки и хранения данных.

5.3.3.2 Обеспечение подсистемы программных средств

Подсистема программных средств должна обеспечивать:

- организацию получения, обработки и хранения большого объема данных с подсистемы технических средств;
- создание программных сценариев, шаблонов, модулей (далее Приложения) для мониторинга, анализа и визуализации полученных данных;
- анализ полученных данных, на предмет состояния объекта автоматизации;
- анализ текущего и прогнозирования будущего состояния объекта автоматизации на основе заданных факторов;
- администрирование и разграничение доступа;
- формирование иерархии и управление составом объекта автоматизации (филиал, участок, цех);
- аналитику имеющихся данных и событий, определение и выявление поломок и неисправностей, информирование;
- организацию отправки почтовых и смс-уведомлений;
- создание программных модулей для взаимодействия со сторонними системами.

5.3.3.3 Обеспечение подсистемы пользовательских интерфейсов

Подсистема пользовательских интерфейсов должна обеспечивать:

- создание графического представления объекта автоматизации (2D и 3D-модель) с заданием узлов, с которых собираются данные и выводом полного набора полученных данных;
- изменение свойств объекта автоматизации в режиме реального времени;
- наличия приложения работающего на базе операционных систем типа Windows («толстый» клиент) и web-интерфейсов («тонкий» клиент) для работы с данными хранящимися в подсистеме программных средств.

5.4 Требования к видам обеспечения

5.4.1 Требования к математическому обеспечению

Математические методы и алгоритмы, используемые для шифрования/дешифрования данных, а также программное обеспечение, реализующее их, должны быть сертифицированы уполномоченными организациями для использования в государственных органах Российской Федерации.

Математические методы и алгоритмы, необходимые для анализа состояния и прогнозирования объекта автоматизации по заданным критериям, должны быть разработаны и согласованны со специалистами рабочей группы, на стадии Информационного обследования.

5.4.2 Требования к информационному обеспечению

Состав, структура и способы организации данных в Системе должны быть определены на этапе технического проектирования.

Уровень хранения данных в системе должен быть построен на основе современных реляционных или объектно-реляционных СУБД. Для обеспечения целостности данных должны использоваться встроенные механизмы СУБД.

Средства СУБД, а также средства используемых операционных систем должны обеспечивать документирование и протоколирование обрабатываемой в системе информации.

Структура базы данных должна поддерживать кодирование хранимой и обрабатываемой информации в соответствии с общероссийскими классификаторами (там, где они применимы).

Доступ к данным должен быть предоставлен только авторизованным пользователям с учетом их служебных полномочий, а также с учетом категории запрашиваемой информации.

Структура базы данных должна быть организована рациональным способом, исключающим единовременную полную выгрузку информации, содержащейся в базе данных системы.

Аппаратно-технические средства, обеспечивающие хранение информации, должны использовать современные технологии, позволяющие обеспечить повышенную надежность хранения данных и оперативную замену оборудования (распределенная избыточная запись/считывание данных, зеркалирование, независимые дисковые массивы, кластеризация).

В состав Системы должна входить специализированная подсистема резервного копирования и восстановления данных.

При проектировании и развертывании Системы необходимо рассмотреть возможность использования накопленной информации из уже функционирующих информационных систем.

5.4.3 Требования к лингвистическому обеспечению

Все прикладное программное обеспечение Системы для организации взаимодействия с пользователем должно использовать русский язык.

5.4.4 Требования к программному обеспечению

При проектировании и разработке Системы, необходимо максимально эффективным образом использовать существующее программное обеспечение и АИС.

Используемое при разработке программное обеспечение и библиотеки программных кодов должны иметь широкое распространение, быть общедоступными и использоваться в промышленных масштабах. Базовой программной платформой должна являться операционная система MS Windows.

5.4.5 Требования к аппаратно-техническому обеспечению

Определение состава и требования к оборудованию, необходимого для создания АИС, выполняется на этапе Технического проектирования АИС на основе:

- информационного обследования;
- анализа плана помещений Склада с габаритными размерами;
- разработки и анализа схемы ПСЛ.

Аппаратно-техническое обеспечение Системы должно максимально и наиболее эффективным образом использовать существующие в аппаратные и технические средства.

В состав комплекса должны следующие технические средства:

- сервер базы данных;
- сервер приложений;
- веб-сервер;
- сервер БД, сервер приложений и веб-сервер Системы должны быть объединены одной локальной сетью, с пропускной способностью не

менее 100 Мбит и построены на базе существующей среды виртуализации.

5.5 Перспективы развития и модернизации Системы

При создании Системы должны быть предусмотрены перспективы развития и возможности последующей модернизации в ходе появления новых задач по автоматизации рабочих процессов структурных подразделений, а также появления новых тенденций прогрессивных новаций в сфере информационных технологий.

Должны быть предусмотрены следующие направления развития:

- расширение функциональности системы в процессе ее сопровождения (изменение функциональности эксплуатируемых подсистем и внедрение новых подсистем) без перепрограммирования Системы;
- Система должна быть масштабируемой, с возможностью адаптации к новым требованиям компании-кейсодателя;
- возможность перспектив интеграции Системы со смежными информационными системами;
- обновление и модернизация инфраструктурного программного обеспечения:
  - операционная система;
  - сервер приложений;
  - СУБД;

6 Требования к результату работ

Ожидаемым результатом является разработанный проект бесконтактной системы контроля и управления доступом территории базы ГК «Интерфейс», соответствующий требованиям настоящего Технического задания.

Директор АНО «Агентство привлечения инвестиций и развития инноваций Хабаровского края» Д.А. Хвостиков