Выполнение работ по установке системы контроля доступа

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

2024 г.

Общие сведения.

техническое задание на выполнение работ по установке системы контроля доступа на территорию на основе многофункциональной программной платформы.

|  |  |
| --- | --- |
| Перечень основных данных и требований | Основные характеристики, сведения и требования к проекту |
| Наименование заказчика | АО «ПО «Баррикада» |
| Наименование объекта проектирования | КПП «Юг» |
| Адрес объекта проектирования ЛО, г. Гатчина, проезд Энергетиков д. 2 |
| Подрядчик | Определяется по итогам конкурса, проводимого Заказчиком |
| Основание для работ | 1. Постановление Правительства РФ от 18.12.2014 № 1413 «Об утверждениитребований к антитеррористической защищенности объектов (территорий)промышленности и формы паспорта безопасности объекта (территории)промышленности».2. Приказ от 29.02.2016г. №19 «Об утверждении Единой технической политики пообеспечению инженерно-технической и специальной защиты объектовГосударственной корпорации «Ростех» и ее организаций».3. Планы техперевооружения предприятия. |
| Стадии и срок выполнения работ | • Монтажные работы: 2024-2024 год, в соответствии с договором• Пусконаладочные работы: 2024-2024 год, в соответствии с договором |
| Виды и объёмы работ | • Выполнение работ по установке системы контроля доступ; |
| Исходные данные | 1. Технические условия на применяемые материалы и оборудование. |
| Система сбора, обработки и отображения информации | Система сбора, обработки и отображения информации должна представлять собой совокупность централизованного оборудования, программных и технических средств охраны объекта и позволять:• Реализовать текущий информационный обмен с периферийными элементами.• Реализовать прием, обработку и передачу поступающих информационных потоков.• Реализовать текущее визуальное отображение на мониторах и запись в архив всех событий.• Обеспечить конфиденциальность сис1емы сбора, обработки, передачи и отображения информации с ограничением доступа паролями, сетевую защиту информации. |
| Система контроля и управления доступом | СКУД должна быть выполнена на базе оборудования обеспечивающего интеграцию с RusGuard Soft.Технические средства системы должны обеспечивать реализацию следующих основных функций:воспрепятствование несанкционированного прохода/проезда на территорию предприятия и проходу в помещения ограниченного доступа лиц и транспортных средств, не имеющих пропуска установленной формы (идентификационной карты);обеспечение дистанционного (с КПП) управления и контроль за турникетами;регистрация, документирование и отображение событий в СКУД (запросы на проход);подготовка отчётов о событиях в системе СКУД за интересующий период времени, и их распечатка (в том числе учет рабочего времени сотрудников);протоколирование событий по проходу сотрудников через проходные предприятия или другие локальные зоны;разработка произвольных отчётов операторами/администраторами СКУД по данным протокола событий с группировкой по определенным условиям (функционал определяется на этапе реализации проекта);выгрузка отчетов в форматах Excel, Word, PDF;оформление постоянных, временных и разовых пропусков сотрудникам; автоматизированная идентификация доступа по электронным картам; отображение на мониторе охраны фотографии и личных данных владельцакарты (фото-верификация); сохранение идентификационных признаков в энергонезависимой памятиконтроллера при отключении электропитания; аварийное автоматическое и ручное открывание исполнительных и управляемых преграждающих устройств СКУД (в точках прохода) при возникновении нештатных ситуаций на предприятии, а также при срабатывании АПС; разблокировки дверей при чрезвычайных ситуациях с использованием кнопок экстренной разблокировки, устанавливаемых внутри помещений у выходов из них. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | Предусмотреть возможность: |
|  | включения режима визуальной верификации владельца карты, проходящего |
|  | через точку доступа. Данная функция СКУД должна позволять охраннику |
|  | вручную разрешать или запрещать доступ на основании решения о |
|  | визуальном соответствии лица предъявителя карты фотографии из базы |
|  | данных, отображаемой на экране; |
|  | задавать период времени, в течение которого карты должны использоваться в |
|  | системе. Если какая-либо карта не будет использована в системе в |
|  | течение этого временного интервала, то она должна блокироваться; |
|  | реализации функции глобального (в сети из нескольких контроллеров) |
|  | «Запрета двойного прохода» без участия сервера. |
|  | Контроллеры СКУД должно иметь следующие характеристики: |
|  | наличие исполнительных электронных реле с индивидуальными настройками |
|  | и защитой (силовые + слаботочные); |
|  | дополнительные входы (кнопки, датчики и т.д.); |
|  | контроль состояния блока питания: 220/АКБ, АКБ норма/АКБ разряд; |
|  | контроль извещателя вскрытия корпуса; |
|  | климатический диапазон эксплуатации: 0 +50С; |
|  | количество ключей в энергонезависимой памяти: до 64 ООО; |
|  | количество событий в энергонезависимой памяти: до 60 ООО. |
|  | Считыватели СКУД должно иметь следующие характеристики: |
|  | доступ по картам HID Prox II и EM-Marine |
|  | интерфейсы связи: Wiegand (26-58), Touch Memory, RBus, RS-485, USB; |
|  | энергонезависимая память: 1500 шт. ключей / QR/ штрих-кодов; |
|  | извещатель отрыва от стены. |
|  | Тип устройств биометрической идентификации, состав и характеристики |
|  | применяемого оборудования определить на этапе проектирования. |
|  | ПО СКУД должно обеспечивать: |
|  | полную поддержку всех современных операционных систем семейства |
|  | Windows, как х32 так и х64 разрядных версий; |
|  | интерфейс оператора для управления картами пользователей; |
|  | возможность наращивания (дооснащения) без нарушения функционирования |
|  | системы; |
|  | встроенный модуль автоматического распознавания документов; |
|  | возможность ввода фотографий пользователей в базу данных СКУД с |
|  | помощью цифрового фотоаппарата или путем импорта из файлов |
|  | различных графических форматов. |
|  | Необходимо обеспечить хранение протоколов событий в СКУД |
|  | продолжительностью не менее 3 лет. |
|  | В системе должна быть предусмотрена возможность автоматического |
|  | разграничения уровня доступа идентификационной карты, запрещающего проход |
|  | сотрудников в помещения, посещение которых не предусмотрено их служебными |
|  | обязанностями. |
|  | Разрешение на вход на проходных осуществлять по алгоритму двухфакторной |
|  | идентификации (карта + биометрический параметр человека). |
|  | В составе СКУД следует предусмотреть: |
|  | центральное оборудование СКУД; |
|  | контроллеры управления доступом; |
|  | считыватели бесконтактных карт; |
|  | биометрические терминалы; |
|  | Турникет «Скоростной проход»; |
|  | доводчики дверей; |
|  | электромагнитные замки на внутренние двери, оборудуемые СКУД; |
|  | извещатели магнитно-контактные; |
|  | кнопки выхода; |
|  | кнопки аварийной разблокировки дверей (устанавливаются на каждую дверь, |
|  | оборудованную СКУД), факт нажатия аварийной кнопки должен |
|  | фиксироваться в протоколе событий СКУД и/или ООС; |
|  | источники резервного питания с АКБ; |
|  |  |
|  | Рабочее место на КПП 2шт. Контроллеры должны обеспечивать контроль состояния подключённых к ним модулей управления исполнительными устройствами: считывателей бесконтактных карт, замков и осуществлять подачу на них сигналов управления.Контроллеры СКУД должны располагаться в защищаемой зоне (помещении) в недоступном для посторонних лиц мест или в максимально возможной близости от защищаемых помещений и зон. В таком случае, контроллеры СКУД разместить в металлических шкафах, закрывающихся на замок и имеющих сигнализацию на вскрытие. Бюро пропусков должно обеспечивать:автоматизацию процесса заказа, визирования и оформления пропусков всех типов (разовые, временные, материальные, по списку, разовые автомобильные, временные автомобильные и т.д.); возможность указывать при заказе пропуска организацию, объект,корпус/территорию и т.д.; возможность ведения баз данных (посетителей, сотрудников, автомобилей и т.д.);возможность многоуровневого визирования заявок; выдача и контроль возврата карт доступа. В СКУД предусмотреть следующие АРМ: АРМ сотрудника охраны 2 шт.;АРМ бюро пропусков, расположенного в помещении бюро пропусков. Технические характеристики АРМ определяются на этапе проецирования и должны быть не хуже:- процессор AMD Ryzen3 «или эквивалент»;- оперативная память DDR4 8Gb;- системный диск SDD 256Gb;- блок питания АТХ 500Вт;- операционная система Windows 10. |
| КПП охраны - 2 шт. | Оборудование, размещаемое на КПП, должно быть оформлено в виде АРМ на базе ПК с соответствующим ПО.Место расположения КПП уточнить на этапе выполнения работ. |
| Основные требования | 1. В здании на центральной проходной оборудовать 4 биометрические точкипрохода с двухфакторной идентификацией;2. Установить и настроить программное обеспечение на рабочей станции6. Настроить установленное сетевое оборудование. |
| Перечень применяемого оборудования(предпроектный расчёт) | • сервер СКУД-1 шт.;• контроллер доступа - 2 шт.;• источник питания резервированный - 1 шт.;• аккумулятор - 1 шт.;• кнопка аварийной разблокировки - 2 шт.;• считыватель бесконтактный - 4 шт.;• извещатель охранный магнитоконтактный - 2 шт.;• замок электромагнитный - 2 шт.;• организатор кабельный, горизонтальный - 2 шт.;• турникет «Скоростной проход» - 2 шт.;• Секция двухсторонняя турникета -6 шт.;• картоприемник - 1 шт.;• терминал доступа с распознаванием лиц - 4 шт.• веб-камера - 1 шт.;•  |
| Программное обеспечение | ПО должно содержать широкий набор функциональных возможностей по гибкому введению исходной информации, управлению периферийной аппаратурой, по режимам управления доступом и охраны, по алгоритмам прохода через рубежи доступа, накоплению и систематизации информации.Требования к программным средствам:прикладное ПО АРМ должно иметь функционально разные возможности для оператора и администратора;Все сообщения о событиях в системе, тексты меню графического интерфейса пользователя, выводимые на средства отображения информации, должны быть на русском языке. |
| Требования к электробезопасности, пожарной безопасности и соответствия оборудования санитарным нормам эксплуатации | Устанавливаемое оборудование и кабельная сеть системы должны быть безопасны для лиц, соблюдающих правила их эксплуатации.Должны выполняться все требования ПУЭ относящиеся к работам по данному Предприятию.Материалы, применяемые при монтаже комплекса технических средств охраны должны быть безвредны для здоровья, как пользователей, так и лиц, имеющих к ним доступ.Устанавливаемое оборудование должно отвечать требованиям по электробезопасности по ГОСТ Р МЭК 60065-2002 «Аудио-, видео- и аналогичная электронная аппаратура. Требования безопасности (ИУС 5-2002)».Напряжение в кабельной слаботочной сети не должно превышать 24 В постоянного или переменного тока (безопасное для обслуживающего персонала).Электрическая прочность изоляции устанавливаемого оборудования должна соответствовать ГОСТ Р 52931-2008 «Приборы контроля и регулирования технологических процессов. Общие технические условия».Устанавливаемое оборудование должно отвечать требованиям пожарной безопасности по ГОСТ 12.1.004-91; СНиП 21-01-97.Допустимые уровни электромагнитных полей на рабочих местах должны отвечать требованиям ГОСТ 12.1.006-84.Сопротивление защитного заземления должно быть не более 4 Ом.Применяемое оборудование, его расположение и условия эксплуатации должны отвечать требованиям "Санитарных правил и норм". |
|  | Аппаратура ТСО, устанавливаемая в помещениях, должна безотказно функционировать в диапазоне температур от +5°С до +40°С и относительной влажности 80%.ТСО, устанавливаемые на Объектах, должны соответствовать ГОСТ Р 50009-2000.Гарантийный срок эксплуатации оборудования технических средств - не менее 3 года с момента подписания акта приемки в эксплуатацию. |
| Требования к техническим средствам |
|  |
| Дополнительные требования к характеристикам поставляемого оборудования, указываемые участником закупки |  |

Перечень ссылочных и нормативных документов

ГОСТ Р 51241-2008 «Средства и системы контроля управления доступом. Классификация. Общие технические требования. Методы испытаний»;

Р 78.36.018-2011 «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»;

Р 064-2017 Методические рекомендации. Выбор и применение технических средств и систем контроля и

управления доступом;