ПРИЛОЖЕНИЕ 1

**УТВЕРЖДЕН**

**ПМ.02 Осуществление интеграции программных модулей**

**Проектирование модулей системы защиты объекта критической информационной инфраструктуры (КИИ) на основе 187-ФЗ «О безопасности КИИ Российской Федерации»**

**Техническое задание**

**Листов 20**

|  |  |
| --- | --- |
| **Инв. № подл** |  |
| **Подпись и дата** |  |
| **Взам. инв. №** |  |
| **Инв. № дубл.** |  |
| **Подпись и дата** |  |

**2024**

**СОДЕРЖАНИЕ**

[**1. ВВЕДЕНИЕ 1**](#_Toc164929231)

[**2. ОСНОВАНИЕ ДЛЯ РАЗРАБОТКИ 2**](#_Toc164929232)

[**3. НАЗНАЧЕНИЕ РАЗРАБОТКИ 3**](#_Toc164929233)

[**4. ТРЕБОВАНИЯ К ПРОГРАММЕ ИЛИ ПРОГРАММНОМУ ИЗДЕЛИЮ 4**](#_Toc164929234)

[**4.1. Требования к функциональным характеристикам 4**](#_Toc164929235)

[**4.2. Требования к надежности 4**](#_Toc164929236)

[**4.3. Условия эксплуатации 4**](#_Toc164929237)

[**4.4. Требования к составу и параметрам технических средств 4**](#_Toc164929238)

[**4.5. Требования к информационной и программной совместимости 4**](#_Toc164929239)

[**4.6. Требования к маркировке и упаковке 4**](#_Toc164929240)

[**4.7. Требования к транспортированию и хранению 4**](#_Toc164929241)

[**4.8. Специальные требования 4**](#_Toc164929242)

[**5. ТРЕБОВАНИЯ К ПРОГРАММНОЙ ДОКУМЕНТАЦИИ 4**](#_Toc164929243)

[**6. ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ 5**](#_Toc164929244)

[**7. СТАДИИ И ЭТАПЫ РАЗРАБОТКИ 7**](#_Toc164929245)

[**8. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ 8**](#_Toc164929246)

# ВВЕДЕНИЕ

В современном мире обеспечение безопасности объектов критической инфраструктуры (КИИ) является одним из ключевых аспектов деятельности. Независимо от характера деятельности и масштабов объекта, пропускной режим остается неотъемлемой частью системы обеспечения безопасности. В этом контексте разработка программного решения, направленного на организацию и управление пропускным режимом, приобретает особую важность.

Представляю вашему вниманию техническое задание на разработку программного решения для модуля "ХранительПРО". Данный модуль рассчитан на объекты критической инфраструктуры и направлен на эффективное организацию пропускного режима. В его функционал входит веб-сервис для заказа пропусков, терминалы для формальной проверки заявок, реализации пропускного режима и учета посещений.

Целью данного технического задания является создание надежного и эффективного программного решения, способного обеспечить безопасность и контроль доступа на объектах критической инфраструктуры. Важными аспектами проектирования и разработки модуля "ХранительПРО" являются его гибкость, надежность и простота использования, а также соответствие современным стандартам безопасности и требованиям заказчика.

Успешная реализация данного проекта позволит повысить уровень безопасности объектов критической инфраструктуры и обеспечить эффективное управление пропускным режимом.

# ОСНОВАНИЕ ДЛЯ РАЗРАБОТКИ

В современном мире обеспечение безопасности объектов критической инфраструктуры (КИИ) является одним из главных приоритетов. Независимо от характера деятельности и масштабов объекта, пропускной режим остается важной составляющей системы обеспечения безопасности. В этом контексте разработка программного решения, направленного на организацию и управление пропускным режимом, приобретает ключевое значение. Модуль "ХранительПРО" разрабатывается с целью предоставления эффективного инструмента для организации пропускного режима на объектах критической инфраструктуры. Он предназначен для обеспечения безопасности и контроля доступа на таких объектах. Предполагается, что данный модуль будет включать в себя веб-сервис для заказа пропусков, терминалы для формальной проверки заявок, реализации пропускного режима и учета посещений. Целью данного технического задания является создание надежного и эффективного программного решения, способного обеспечить безопасность и контроль доступа на объектах критической инфраструктуры. Ключевыми аспектами проектирования и разработки модуля "ХранительПРО" являются его гибкость, надежность и простота использования, а также соответствие современным стандартам безопасности и требованиям заказчика. Успешная реализация данного проекта позволит повысить уровень безопасности объектов критической инфраструктуры и обеспечить эффективное управление пропускным режимом, что является необходимым условием для надежной защиты таких объектов от потенциальных угроз и инцидентов безопасности.

# НАЗНАЧЕНИЕ РАЗРАБОТКИ

Разработка программного решения "ХранительПРО" предназначена для организации пропускного режима на объектах критической инфраструктуры. Независимо от периметра контролируемой и опасной зоны, каждый объект критической инфраструктуры требует эффективной системы управления доступом. Модуль "ХранительПРО" будет предоставлять средства для контроля, отслеживания и регистрации всех проходящих через него лиц, обеспечивая тем самым надежную защиту и безопасность объектов.

# 4. ТРЕБОВАНИЯ К ПРОГРАММЕ ИЛИ ПРОГРАММНОМУ ИЗДЕЛИЮ

## **4.1. Требования к функциональным характеристикам**

1. **Управление доступом:**
   * Система должна обеспечивать эффективное управление доступом на объекты критической инфраструктуры.
   * Предусмотреть возможность создания и администрирования пользовательских аккаунтов с различными уровнями доступа.
2. **Регистрация посещений:**
   * Система должна регистрировать все проходящие через нее лица с указанием времени и места прохождения.
   * Обеспечить возможность просмотра и анализа данных о посещениях через удобный интерфейс.
3. **Заявки на пропуск:**
   * Предусмотреть веб-интерфейс для подачи заявок на получение пропуска с учетом всех необходимых данных о посетителе.
   * Автоматизировать процесс рассмотрения заявок и выдачи пропусков с учетом установленных правил и ограничений.
4. **Интеграция с внешними системами:**
   * Обеспечить возможность интеграции с существующими системами безопасности и учета на объекте.
   * Гарантировать совместимость с различными видами оборудования, включая считыватели пропусков и видеонаблюдение.
5. **Журналирование и аудит:**
   * Реализовать систему журналирования действий пользователей для обеспечения возможности последующего аудита.
   * Гарантировать сохранность и защищенность журналов от несанкционированного доступа и модификации.
6. **Безопасность данных:**
   * Обеспечить шифрование и защиту конфиденциальных данных пользователей в соответствии с современными стандартами безопасности.
   * Предусмотреть механизмы резервного копирования и восстановления данных для обеспечения их целостности и доступности.
7. **Обучение пользователей:**
   * Предоставить обучающие материалы и руководства по использованию системы для пользователей различного уровня подготовки.
   * Обеспечить техническую поддержку и консультации пользователей в процессе эксплуатации системы.
8. **Гибкость и расширяемость:**
   * Реализовать систему с возможностью дальнейшего расширения функциональности и интеграции новых модулей.
   * Обеспечить простоту конфигурации и настройки системы для адаптации к изменяющимся потребностям заказчика.

## **4.2. Требования к надежности**

1. **Отказоустойчивость:**
   * Система должна быть способной обнаруживать и устранять сбои в работе, минимизируя временные простои и потерю данных.
   * Обеспечить автоматическое восстановление после сбоев для непрерывной работы системы.
2. **Резервное копирование и восстановление:**
   * Реализовать механизмы регулярного автоматического резервного копирования данных с возможностью их быстрого восстановления в случае потери или повреждения.
   * Гарантировать целостность и доступность резервных копий данных.
3. **Защита от несанкционированного доступа:**
   * Обеспечить многоуровневую защиту системы от несанкционированного доступа, включая защиту от взлома, атак переполнения буфера и других известных угроз.
   * Реализовать механизмы обнаружения и предотвращения вторжений для быстрого реагирования на потенциальные угрозы.
4. **Мониторинг и управление ресурсами:**
   * Обеспечить систему мониторинга производительности и загрузки ресурсов для своевременного выявления и устранения узких мест и проблем с производительностью.
   * Предусмотреть возможность удаленного управления и мониторинга системы для оперативного реагирования на проблемы.
5. **Система резервирования данных:**
   * Реализовать механизмы резервирования данных на нескольких независимых носителях для защиты от потери данных в случае отказа оборудования или человеческого фактора.
   * Гарантировать согласованность и целостность данных при использовании системы резервирования.
6. **Тестирование и верификация:**
   * Провести комплексное тестирование системы на различных этапах разработки для обеспечения ее надежной работы и соответствия требованиям.
   * Предусмотреть процедуры верификации и валидации системы перед ее внедрением для минимизации возможных ошибок и проблем.

## **4.3. Условия эксплуатации**

1. **Требования к аппаратному обеспечению:**
   * Система должна быть совместима с широким спектром аппаратного обеспечения, включая серверы, сетевое оборудование, считыватели пропусков и другие устройства.
   * Предусмотреть минимальные и рекомендуемые характеристики для обеспечения оптимальной производительности и стабильной работы.
2. **Требования к программному обеспечению:**
   * Обеспечить совместимость с различными операционными системами, включая Windows и Linux, для обеспечения гибкости при выборе платформы.
   * Предоставить подробное руководство по установке и настройке программного обеспечения для упрощения процесса развертывания и настройки.
3. **Условия окружающей среды:**
   * Обеспечить работоспособность системы в различных климатических условиях, включая высокую влажность, экстремальные температуры и воздействие агрессивных сред.
   * Учитывать требования по защите от пыли, влаги и электромагнитных помех для обеспечения долговечности и надежности оборудования.
4. **Требования к сетевому оборудованию:**
   * Обеспечить поддержку различных сетевых протоколов и стандартов для совместимости с существующей инфраструктурой заказчика.
   * Гарантировать безопасность передачи данных по сети и защиту от атак на уровне сетевого взаимодействия.
5. **Требования к технической поддержке:**
   * Предусмотреть механизмы технической поддержки и обновлений для обеспечения стабильной работы системы в течение всего периода эксплуатации.
   * Обеспечить доступность специалистов для оперативного реагирования на проблемы и вопросы пользователей.
6. **Требования к безопасности эксплуатации:**
   * Разработать процедуры и рекомендации по обеспечению безопасности при эксплуатации системы, включая управление доступом к административным функциям и защиту от утечек данных.

## **4.4. Требования к составу и параметрам технических средств**

1. **Система пропускного контроля:**
   * Включать считыватели пропусков с поддержкой различных технологий, включая RFID, биометрическую идентификацию и штрихкоды.
   * Обеспечить совместимость с различными типами пропусков и карт доступа для удобства пользователей.
2. **Серверное оборудование:**
   * Предусмотреть использование высокопроизводительных серверов с достаточными вычислительными ресурсами для обработки данных и обеспечения отказоустойчивости системы.
   * Гарантировать возможность масштабирования серверной инфраструктуры для адаптации к изменяющимся потребностям и нагрузкам.
3. **Сетевое оборудование:**
   * Включать сетевые коммутаторы и маршрутизаторы с поддержкой высокоскоростной передачи данных и защитой от сетевых атак.
   * Обеспечить резервирование сетевых каналов и механизмы балансировки нагрузки для обеспечения непрерывной работы системы.
4. **Устройства хранения данных:**
   * Использовать надежные носители данных, такие как жесткие диски или массивы хранения данных, с возможностью горячей замены и резервирования.
   * Обеспечить достаточное пространство для хранения архивных данных и резервных копий.
5. **Система резервного питания:**
   * Включать в состав технических средств системы надежное резервное питание для предотвращения потери данных и обеспечения непрерывной работы в случае отключения основного электропитания.
   * Гарантировать достаточное время автономной работы системы на резервном питании для проведения необходимых мероприятий по восстановлению работы.
6. **Мониторинговые устройства:**
   * Обеспечить возможность мониторинга состояния оборудования и ресурсов системы с помощью специализированных мониторинговых устройств.
   * Предусмотреть систему оповещений и уведомлений о возможных проблемах и сбоях для оперативного реагирования администраторов.

## **4.5. Требования к информационной и программной совместимости**

1. **Интеграция с внешними системами:**
   * Обеспечить возможность интеграции с существующими системами безопасности, такими как системы видеонаблюдения, системы контроля доступа и системы управления зданиями.
   * Гарантировать совместимость с популярными стандартами коммуникации для обеспечения удобства интеграции.
2. **Интерфейс пользователя:**
   * Разработать интуитивно понятный пользовательский интерфейс, обеспечивающий простоту и удобство использования для операторов системы.
   * Предусмотреть возможность настройки интерфейса в соответствии с потребностями конкретного пользователя или организации.
3. **Мобильное приложение:**
   * Создать мобильное приложение для управления системой пропускного контроля из любой точки с доступом к интернету.
   * Обеспечить функциональность мобильного приложения, соответствующую основным возможностям веб-интерфейса системы.
4. **Межплатформенная совместимость:**
   * Гарантировать работоспособность программного решения на различных операционных системах, включая Windows, Linux, iOS и Android.
   * Предоставить универсальные средства установки и настройки для обеспечения совместимости с различными платформами.
5. **Обновления и поддержка:**
   * Обеспечить механизмы автоматических обновлений для оперативного внедрения исправлений и улучшений.
   * Предоставить круглосуточную техническую поддержку пользователям программного решения для оперативного реагирования на возникающие проблемы.
6. **Защита данных:**
   * Реализовать механизмы шифрования данных для защиты конфиденциальной информации пользователей и оперативной базы данных.
   * Обеспечить соблюдение требований по защите персональных данных и конфиденциальной информации в соответствии с применимым законодательством.

## **4.6. Требования к маркировке и упаковке**

1. **Маркировка оборудования:**
   * Каждое устройство должно иметь четкую и уникальную маркировку, содержащую информацию о модели, серийном номере, дате изготовления и других релевантных характеристиках.
   * Маркировка должна быть устойчива к внешним воздействиям, чтобы обеспечить ее читаемость в течение всего срока эксплуатации.
2. **Упаковка продукции:**
   * Предоставить надежную упаковку для обеспечения защиты оборудования во время транспортировки и хранения.
   * Упаковка должна соответствовать стандартам безопасности и обеспечивать минимальные риски повреждения при перевозке.
3. **Инструкции по установке и эксплуатации:**
   * Каждое устройство должно поставляться с подробными инструкциями по установке, настройке и эксплуатации на русском языке.
   * Инструкции должны содержать все необходимые сведения о безопасности и технические рекомендации для правильной работы оборудования.
4. **Маркировка упаковки:**
   * Каждая упаковка должна быть помечена ярлыками с информацией о содержимом, включая наименование продукции, количество единиц, вес и размеры упаковки.
   * Предоставить информацию о хранении и транспортировке, включая рекомендации по обращению с упаковкой.
5. **Экологическая маркировка:**
   * При проектировании упаковки уделить внимание использованию экологически чистых материалов и возможности их переработки.
   * Помечать упаковку соответствующими знаками и символами для обозначения экологической безопасности и степени ее перерабатываемости.
6. **Документация и гарантийные обязательства:**
   * Каждое устройство должно поставляться с полным комплектом документов, включая гарантийный талон, сертификаты качества и техническую документацию.
   * Гарантировать соответствие продукции всем действующим нормативным требованиям и стандартам качества.

## **4.7. Требования к транспортированию и хранению**

1. **Транспортирование оборудования:**
   * Обеспечить надежную упаковку для оборудования во время транспортировки, чтобы предотвратить повреждения или потерю.
   * Предусмотреть специальные меры для защиты от статических разрядов и электромагнитных полей во время транспортировки.
2. **Хранение оборудования:**
   * Разработать рекомендации по условиям хранения оборудования, включая температурные и влажностные условия.
   * Обеспечить возможность длительного хранения оборудования без ущерба для его характеристик и функциональности.
3. **Условия транспортирования:**
   * Учитывать особенности транспортировки при больших расстояниях или через различные климатические зоны.
   * Предусмотреть защитные меры от воздействия вибрации, ударов и других механических воздействий во время транспортировки.
4. **Безопасность транспортирования:**
   * Обеспечить соблюдение всех требований безопасности в процессе транспортировки, включая правила перевозки опасных грузов (если применимо).
   * Предусмотреть меры по защите от кражи и несанкционированного доступа к оборудованию во время транспортировки.

## **4.8. Специальные требования**

1. **Интеграция с существующими системами безопасности:**
   * Обеспечить возможность интеграции программного решения "ХранительПРО" с уже установленными системами безопасности на предприятии.
   * Гарантировать совместимость и эффективное взаимодействие с системами контроля доступа, видеонаблюдения и сигнализации.
2. **Гибкая настройка и расширяемость:**
   * Предусмотреть возможность гибкой настройки функций программного решения в соответствии с требованиями конкретного предприятия.
   * Обеспечить легкую расширяемость функционала программы для возможности внесения изменений и дополнений в будущем.
3. **Защита от кибератак и утечек данных:**
   * Разработать механизмы защиты программного решения от внешних киберугроз, включая атаки хакеров и вирусы.
   * Гарантировать безопасное хранение и передачу конфиденциальной информации, такой как данные о доступе и персональные данные сотрудников.
4. **Поддержка мобильных устройств:**
   * Обеспечить возможность доступа к программному решению "ХранительПРО" с мобильных устройств (смартфоны, планшеты) для управления пропускным режимом в реальном времени.
5. **Обновления и поддержка:**
   * Обеспечить регулярные обновления программного решения для исправления уязвимостей безопасности и внесения улучшений.
   * Предоставить техническую поддержку и консультации пользователям по вопросам установки, настройки и эксплуатации программы.

# 5. ТРЕБОВАНИЯ К ПРОГРАММНОЙ ДОКУМЕНТАЦИИ

1. **Руководство пользователя:**
   * Предоставить подробное руководство пользователя, описывающее процесс установки, настройки и использования программного решения "ХранительПРО".
   * Включить инструкции по доступу к основным функциям программы, управлению пользователями, настройкам безопасности и мониторингу активности.
2. **Техническое описание:**
   * Предоставить техническое описание программного решения, включая его архитектуру, основные компоненты, протоколы взаимодействия и используемые технологии.
   * Обеспечить описание всех внутренних и внешних интерфейсов для возможности интеграции с другими системами.
3. **Справочная документация:**
   * Подготовить справочные материалы, содержащие описание всех функций, настроек и параметров программы.
   * Включить информацию о возможных ошибочных ситуациях, их причинах и способах их устранения.
4. **Документация по безопасности:**
   * Предоставить подробное описание мер безопасности, реализованных в программном решении, включая механизмы аутентификации, авторизации, шифрования данных и аудита действий пользователей.
   * Включить рекомендации по обеспечению безопасности при установке, настройке и эксплуатации программы.
5. **Руководство по обновлению и поддержке:**
   * Предоставить инструкции по процедуре обновления программного решения, включая загрузку и установку обновлений.
   * Включить контактные данные для получения технической поддержки, а также информацию о доступных каналах обратной связи и сервисных пакетах поддержки.
6. **Документация по API (при наличии):**
   * Если предусмотрено API для взаимодействия с программным решением, предоставить подробное описание его функций, методов, параметров и примеров использования.
   * Обеспечить актуализированную документацию API для обеспечения удобства интеграции с другими приложениями и системами.

# 6. ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ

1. **Смета затрат:**
   * Подготовить подробную смету затрат на разработку программного решения "ХранительПРО", включая расходы на персонал, аппаратное и программное обеспечение, а также другие операционные издержки.
2. **Оценка трудозатрат:**
   * Произвести оценку общего объема трудозатрат, необходимых для разработки и внедрения программного решения, с учетом всех этапов разработки, тестирования, настройки и поддержки.
3. **Экономическая эффективность:**
   * Провести анализ экономической эффективности проекта, включая оценку ожидаемых экономических выгод от внедрения программного решения, таких как сокращение затрат на безопасность, оптимизация процессов и увеличение производительности.
4. **Анализ рисков и неопределенностей:**
   * Провести анализ возможных рисков и неопределенностей, связанных с реализацией проекта, и предложить меры по их снижению или управлению.
5. **Стратегия масштабирования:**
   * Разработать стратегию масштабирования программного решения, включая планы по расширению функционала, привлечению новых клиентов и развитию партнерских отношений.
6. **Финансовый прогноз:**
   * Подготовить финансовый прогноз на период внедрения и эксплуатации программного решения, включая прогнозируемые доходы, затраты и прибыль.
7. **Оценка социальных и экологических эффектов:**
   * Провести оценку потенциальных социальных и экологических эффектов от внедрения программного решения, таких как улучшение безопасности труда, снижение риска преступности и оптимизация использования ресурсов.
8. **Стратегия маркетинга и продвижения:**

* Разработать стратегию маркетинга и продвижения программного решения на рынке, включая определение целевой аудитории, позиционирование продукта и каналы распространения информации.

# 7. СТАДИИ И ЭТАПЫ РАЗРАБОТКИ

1. **Планирование проекта:**
   * Определение целей и требований проекта.
   * Составление бюджета и графика работ.
   * Назначение ответственных лиц и формирование команды разработки.
2. **Анализ требований:**
   * Изучение и уточнение требований заказчика.
   * Подготовка технического задания и спецификаций к проекту.
3. **Проектирование:**
   * Разработка архитектуры программного решения.
   * Проектирование пользовательского интерфейса.
   * Определение основных компонентов и модулей.
4. **Разработка:**
   * Написание и тестирование кода.
   * Создание баз данных и других необходимых ресурсов.
   * Интеграция различных компонентов системы.
5. **Тестирование и отладка:**
   * Проведение функционального тестирования для проверки работоспособности программного решения.
   * Выявление и устранение ошибок и недочётов.
6. **Внедрение и интеграция:**
   * Установка программного обеспечения на серверы заказчика или в облако.
   * Интеграция с существующими информационными системами заказчика, если необходимо.
7. **Обучение пользователей:**
   * Проведение обучающих семинаров и тренингов для персонала заказчика.
   * Подготовка руководств пользователя и справочных материалов.
8. **Поддержка и сопровождение:**
   * Оказание технической поддержки и консультаций по эксплуатации программного решения.
   * Внесение изменений и выпуск обновлений в соответствии с потребностями заказчика и обнаруженными ошибками.

# 8. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ

1. **Подготовка к контролю:**
   * Определение критериев приемки и контроля.
   * Назначение ответственных лиц со стороны заказчика и исполнителя.
2. **Технический аудит:**
   * Проверка соответствия разработанного программного решения техническим требованиям и спецификациям.
   * Оценка архитектуры, безопасности и производительности системы.
3. **Функциональное тестирование:**
   * Проведение тестирования функциональных возможностей программного решения.
   * Проверка работы основных модулей и компонентов системы.
4. **Тестирование безопасности:**
   * Анализ уровня защиты и безопасности программного решения.
   * Проверка на уязвимости и возможные угрозы.
5. **Тестирование производительности:**
   * Оценка скорости работы программного решения при различных нагрузках.
   * Проверка на оптимизацию и эффективное использование ресурсов.
6. **Приемка и утверждение:**
   * Проведение процедуры приемки разработанного программного решения со стороны заказчика.
   * Формирование отчёта о результатах контроля и приемки.
   * Утверждение программного решения для внедрения и эксплуатации.
7. **Документирование результатов:**
   * Составление документации о процессе контроля и приемки.
   * Фиксация всех выявленных проблем и их решений.
8. **Завершение контроля:**
   * Подписание акта приемки и контроля разработанного программного решения.
   * Организация передачи программного обеспечения заказчику.