**Содержание**

[**1.** **ВВЕДЕНИЕ** 2](#_Toc193710548)

[**2.** **ОБЩИЕ СВЕДЕНИЯ** 3](#_Toc193710549)

[**3.** **НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ** 3](#_Toc193710550)

[3.1 Назначение 3](#_Toc193710551)

[3.2 Цели и создание 3](#_Toc193710552)

[**4.** **ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ** 4](#_Toc193710553)

[**5.** **ТРЕБОВАНИЯ К СИСТЕМЕ** 4](#_Toc193710554)

[5.1 Требования к структуре 4](#_Toc193710555)

[5.2 Требования к процедурам доступа в системе 5](#_Toc193710556)

[5.3 Требования к функциональной безопасности 6](#_Toc193710557)

[5.4 Требования к информационной безопасности 7](#_Toc193710558)

[5.5 Требования к патентной чистоте 8](#_Toc193710559)

[**6.** **ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ** 9](#_Toc193710560)

[6.1 Требования к информационному обеспечению 9](#_Toc193710561)

[6.2 Требования к математическому обеспечению 10](#_Toc193710562)

[6.3 Требования к программному обеспечению 11](#_Toc193710563)

[6.4 Требования к техническому обеспечению 12](#_Toc193710564)

[6.5 Требования к организационному обеспечению 13](#_Toc193710565)

[**7.** **СОСТАВ И СОДЕРЖАНИЕ РАБОТ** 14](#_Toc193710566)

[**8.** **ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ** 15](#_Toc193710567)

[**9.** **ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ** 16](#_Toc193710568)

# **ВВЕДЕНИЕ**

Эффективное управление персоналом является ключевым фактором успешной работы любой организации. В условиях растущей конкуренции и необходимости оперативного принятия управленческих решений автоматизация процессов управления кадрами становится важнейшей задачей.

Данный документ представляет собой описание технических требований к автоматизированной системе управления персоналом (АСУП), которая обеспечит поддержку и оптимизацию процессов кадрового администрирования. Система направлена на автоматизацию учёта сотрудников, мониторинг их профессионального роста, управление расписанием и контроль эффективности.

АСУП предназначена для упрощения взаимодействия между кадровыми службами и сотрудниками, минимизации ошибок, связанных с человеческим фактором, и повышения общей эффективности управления персоналом. Система также будет способствовать снижению затрат на кадровое администрирование за счёт автоматизации рутинных процессов.

Основная цель документа — описать функциональные и технические требования к разработке АСУП, а также обеспечить создание системы, соответствующей потребностям организации и современным стандартам информационной безопасности.

# **ОБЩИЕ СВЕДЕНИЯ**

* 1. Наименование работы: Разработка технических требований на автоматизированную систему управления персоналом (АСУП).
  2. Заказчик АС и Ответственный по проекту: Заказчиком автоматизированной системы является Государственное объединение "Управление кадрами". Ответственной стороной по проекту является отдел кадровой политики и автоматизации труда Государственного объединения "Управление кадрами".
  3. Наименование Организации-пользователя АС: Организация, использующая автоматизированную систему — Государственное предприятие "Центр управления кадрами".
  4. Наименование объекта внедрения: Объектом внедрения системы является головной офис и региональные отделения Государственного предприятия "Центр управления кадрами".

# **НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ**

## Назначение

Автоматизированная система управления персоналом (АСУП) предназначена для обеспечения эффективного администрирования процессов управления кадрами, повышения точности учета данных о сотрудниках и автоматизации рутинных задач кадровых служб.

Система предоставит инструменты для управления жизненным циклом сотрудников, включая обработку информации о найме, обучении, оценке эффективности, карьерном росте и увольнении. Кроме того, АСУП позволит минимизировать риски, связанные с человеческим фактором, и обеспечит удобный доступ к данным для принятия управленческих решений.

АСУП также нацелена на оптимизацию взаимодействия между отделами кадров и сотрудниками, обеспечивая прозрачность процессов и сокращая время, затрачиваемое на выполнение административных задач.

## Цели и создание

Основные цели создания автоматизированной системы управления персоналом (АСУП) включают:

* Автоматизация кадровых процессов: Упрощение и оптимизация рутинных задач, таких как учет персонала, обработка документации, планирование кадрового расписания и управление карьерным ростом сотрудников.
* Повышение эффективности управления персоналом: Сокращение временных и трудовых затрат на обработку данных, минимизация ошибок, связанных с человеческим фактором, и ускорение принятия управленческих решений.
* Обеспечение прозрачности и доступа к данным: Создание единой базы данных, которая предоставляет актуальную информацию о сотрудниках, их должностных обязанностях и результатах работы.
* Повышение безопасности данных: Внедрение современных стандартов информационной безопасности для защиты данных сотрудников от несанкционированного доступа и утечки.
* Гибкость и масштабируемость системы: Обеспечение возможности адаптации системы под нужды различных подразделений и интеграции с другими информационными системами.
* Поддержка профессионального развития сотрудников: Ведение записей о достижениях, обучении и профессиональном росте, что способствует мотивации и удержанию кадров.

# **ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ**

* 1. Учетные записи сотрудников: Каждая учетная запись представляет собой отдельный объект системы, содержащий информацию о сотруднике, включая личные данные, должностные обязанности, квалификацию, результаты аттестаций и профессионального роста.
  2. База данных персонала: Централизованное хранилище информации, обеспечивающее доступ к актуальным данным о сотрудниках. База данных включает в себя разделы для хранения записей о трудовых договорах, учебных курсах, карьерных достижениях и графике работы.
  3. Модули функциональности:
* Модуль управления данными сотрудников: Отвечает за добавление, изменение и удаление информации о сотрудниках.
* Модуль оценки эффективности труда: Поддерживает отслеживание и анализ производительности сотрудников на основе заданных критериев.
* Модуль кадрового планирования: Помогает формировать расписание работы, распределение ресурсов и планирование профессионального роста.
  1. Система безопасности: Включает в себя механизмы защиты данных от несанкционированного доступа, такие как шифрование данных, контроль прав доступа, а также мониторинг подозрительной активности.
  2. Интерфейс пользователя: Интуитивно понятный интерфейс, предоставляющий доступ к функциональным возможностям системы. Интерфейс разработан с учетом потребностей различных категорий пользователей — от кадровых специалистов до руководителей подразделений.
  3. Подсистема интеграции: Механизмы, обеспечивающие взаимодействие АСУП с другими информационными системами, такими как бухгалтерские программы, системы управления проектами и корпоративные мессенджеры.

# **ТРЕБОВАНИЯ К СИСТЕМЕ**

## Требования к структуре

Структура автоматизированной системы управления персоналом (АСУП) должна быть организована таким образом, чтобы обеспечивать эффективность, гибкость и безопасность всех процессов управления кадровыми данными. Основные требования к структуре включают:

5.1.1 Модульная архитектура: Система должна быть построена на основе модулей, каждый из которых отвечает за выполнение отдельных функций. Основные модули:

* Модуль учета персонала;
* Модуль анализа эффективности работы сотрудников;
* Модуль кадрового планирования;
* Модуль обработки документации;
* Модуль безопасности данных.

5.1.2 Централизованная база данных: Все данные о сотрудниках должны храниться в единой защищенной базе данных, которая обеспечивает удобный доступ для пользователей с соответствующими правами.

5.1.3 Гибкость и масштабируемость: Система должна быть адаптируема к изменениям численности персонала и расширению функционала, включая возможность добавления новых модулей.

5.1.4 Интеграция с внешними системами: Структура должна предусматривать возможность интеграции с другими корпоративными системами, такими как бухгалтерские программы, CRM и системы управления проектами.

5.1.5 Механизмы резервного копирования: Для защиты данных структура должна включать системы автоматического резервного копирования информации и возможность восстановления данных.

5.1.6 Распределение прав доступа: Пользователи системы должны иметь доступ только к той информации и функциям, которые соответствуют их должностным обязанностям. Это достигается путем внедрения механизма ролей и групп пользователей.

5.1.7 Программный интерфейс (API): Для обеспечения взаимодействия с другими системами структура должна включать открытый и стандартизированный программный интерфейс.

## Требования к процедурам доступа в системе

5.2.1 Процедура аутентификации:

* Пользователь должен пройти процедуру аутентификации, предоставив уникальный логин и пароль.
* Пароль должен соответствовать установленным требованиям безопасности: не менее 8 символов, использование цифр, символов разного регистра и специальных знаков.
* Проверка пароля на соответствие этим требованиям должна происходить на стороне клиента для повышения уровня безопасности.

5.2.2 Защищённое соединение:

* Все данные, передаваемые во время аутентификации, должны шифроваться с использованием современных криптографических протоколов, например TLS/SSL.
* Процедуры передачи данных между клиентом и сервером должны быть защищены от атак типа "человек посередине".

5.2.3 Разграничение прав доступа:

* Каждому пользователю должны быть предоставлены права доступа, соответствующие его роли в системе (например, кадровый специалист, руководитель подразделения, сотрудник).
* Доступ к данным и функциям системы должен быть строго ограничен в соответствии с назначенными ролями.

5.2.4 Управление сессиями:

* Сессия пользователя должна автоматически завершаться при отсутствии активности в течение 10 минут.
* После завершения сессии повторный доступ к системе возможен только после повторной аутентификации.

5.2.5 Процедура восстановления доступа:

* Система должна предоставлять функционал для сброса и восстановления доступа в случае утери учетных данных.
* Процедура восстановления должна включать подтверждение личности через проверочные данные (например, код, отправляемый на email или телефон).

5.2.6 Журналирование действий:

* Система должна вести журнал действий пользователей, включая операции входа, выхода, изменения данных и другие значимые события.
* Журналы должны быть защищены от несанкционированного доступа и использоваться для мониторинга безопасности.

5.2.7 Блокировка при подозрительной активности:

* Система должна автоматически блокировать учетную запись при обнаружении подозрительных действий, например, при превышении допустимого количества неудачных попыток входа.

## Требования к функциональной безопасности

5.3.1 Защита от несанкционированного доступа: Система должна обеспечивать проверку подлинности учетных данных каждого пользователя для предотвращения доступа к информации лиц, не имеющих соответствующих прав.

5.3.2 Контроль сеансов работы пользователей:

* Автоматическое завершение сеанса пользователя при отсутствии активности более 10 минут.
* Возможность ручного завершения сеанса администратором в случае обнаружения подозрительной активности.

5.3.3 Защита данных от потери или повреждения:

* Реализация механизма резервного копирования данных для предотвращения потери информации при сбоях.
* Система должна быть устойчива к непредвиденным ошибкам и способна восстанавливаться после отказов.

5.3.4 Проверка корректности данных: Все операции, выполняемые в системе (добавление, изменение или удаление данных), должны быть защищены от ошибок, обеспечивая сохранение целостности базы данных.

5.3.5 Мониторинг и журналирование событий:

* Система должна вести подробный журнал событий, включая информацию о входе в систему, изменении данных и доступе к конфиденциальной информации.
* Журналы должны быть защищены от несанкционированного изменения и доступны только для администраторов системы.

5.3.6 Блокировка при попытках взлома:

* Ограничение количества попыток входа в систему с неверными учетными данными.
* При превышении допустимого числа попыток учетная запись пользователя должна автоматически блокироваться.

5.3.7 Интеграция с механизмами безопасности: Система должна поддерживать современные технологии безопасности, включая антивирусные решения и межсетевые экраны, для защиты данных от внешних угроз.

5.3.8 Минимизация человеческих ошибок: Система должна включать подсказки и предупреждения для пользователей в случае ввода некорректных данных или выполнения потенциально опасных операций.

5.3.9 Обновления безопасности: Поддержка регулярного обновления модулей безопасности для защиты от новых угроз и уязвимостей.

## Требования к информационной безопасности

5.4.1 Шифрование данных:

* Все персональные данные сотрудников, хранящиеся в системе, должны быть зашифрованы с использованием современных криптографических алгоритмов.
* Передача данных между клиентом и сервером должна осуществляться через защищённые соединения, такие как протоколы TLS/SSL.

5.4.2 Управление доступом:

* Реализовать многоуровневую систему контроля доступа на основе ролей (RBAC), чтобы пользователи имели доступ только к информации, необходимой для выполнения их обязанностей.
* Администраторы системы должны иметь возможность задавать и изменять права доступа пользователей.

5.4.3 Аудит и мониторинг:

* Ведение журнала всех операций, связанных с доступом к данным, их изменением или удалением, для последующего аудита.
* Реализация механизма мониторинга активности пользователей для обнаружения подозрительных действий.

5.4.4 Защита от несанкционированного доступа:

* Ограничение числа попыток ввода пароля с последующей временной блокировкой учетной записи при превышении допустимого лимита.
* Использование двухфакторной аутентификации (2FA) для повышения уровня безопасности при входе в систему.

5.4.5 Резервное копирование данных:

* Реализация системы автоматического резервного копирования данных для предотвращения их потери.
* Хранение резервных копий в зашифрованном виде с ограничением доступа.

5.4.6 Обновление системы безопасности:

* Поддержка регулярных обновлений программного обеспечения для устранения уязвимостей и соответствия современным стандартам информационной безопасности.
* Оперативное применение исправлений для устранения новых обнаруженных угроз.

5.4.7 Защита от вредоносного ПО:

* Интеграция системы с антивирусными решениями и межсетевыми экранами для предотвращения атак и защиты данных.

5.4.8 Политика работы с персональными данными:

* Система должна соответствовать нормативным требованиям и законодательству по защите персональных данных, включая GDPR, если применимо.
* Пользователи должны быть уведомлены о правилах сбора, хранения и обработки их данных.

## Требования к патентной чистоте

5.5.1 Отсутствие нарушений патентного законодательства: Все решения, используемые в разработке АСУП, должны быть свободны от нарушений патентов, авторских прав, торговых марок или других интеллектуальных прав третьих лиц.

5.5.2 Использование открытых стандартов и технологий: При разработке системы предпочтение должно быть отдано открытым стандартам, технологиям и инструментам с прозрачной и открытой лицензией.

5.5.3 Проверка применяемых решений: Все используемые программные компоненты, библиотеки и алгоритмы должны быть проверены на предмет наличия ограничений по патентам или лицензиям.

5.5.4 Документация интеллектуальной собственности: Весь программный код, разработанный в рамках проекта, должен сопровождаться документацией, подтверждающей исключительные права разработчиков или законное использование сторонних решений.

5.5.5 Согласование с юридической службой: До внедрения системы следует провести согласование всех используемых технологий и решений с юридической службой организации для подтверждения их патентной чистоты.

5.5.6 Исключение использования запатентованных технологий без лицензии: Запрещается использование решений, защищенных патентами, без соответствующего лицензирования или официального разрешения правообладателя.

5.5.7 Контроль соблюдения лицензий: Все используемые сторонние компоненты и инструменты должны соответствовать условиям лицензий, включая соблюдение ограничений на коммерческое или некоммерческое использование.

# **ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ**

## Требования к информационному обеспечению

6.1.1 Централизованная база данных:

* Система должна использовать централизованное хранилище данных, объединяющее информацию о сотрудниках, их должностных обязанностях, результатах аттестаций, карьерном росте и другой связанной информации.
* База данных должна быть структурирована и оптимизирована для быстрого поиска и обработки данных.

6.1.2 Обновляемость данных:

* Обеспечение своевременного обновления информации в системе.
* Создание механизмов проверки и актуализации данных для предотвращения ошибок и дублирования.

6.1.3 Сопровождающая документация:

* Подготовка руководств для пользователей, описывающих порядок работы с системой.
* Создание технической документации, описывающей архитектуру системы, форматы данных и механизмы их обработки.

6.1.4 Интеграция с внешними источниками данных:

* Возможность интеграции системы с другими корпоративными платформами (например, бухгалтерскими системами, CRM и ERP) для обмена данными.
* Автоматический импорт и экспорт данных в стандартных форматах (XML, CSV, JSON).

6.1.5 Обеспечение аналитической информации:

* Поддержка инструментов анализа данных, таких как построение отчетов и статистики.
* Возможность визуализации аналитической информации в виде графиков, таблиц и диаграмм.

6.1.6 Контроль корректности данных:

* Реализация механизмов проверки вводимых данных для предотвращения ошибок, связанных с человеческим фактором.
* Автоматическое уведомление пользователя о некорректных или отсутствующих данных.

6.1.7 Безопасность информационного обеспечения:

* Реализация механизмов защиты информации, включая шифрование данных, резервное копирование и управление доступом.
* Все данные должны обрабатываться в соответствии с нормативными требованиями и политикой конфиденциальности.

6.1.8 Поддержка языковых настроек:

* Возможность использования системы на нескольких языках для удобства работы сотрудников из различных регионов.

6.1.9 Пользовательский интерфейс:

* Разработка интуитивно понятного интерфейса для ввода, обработки и анализа данных.
* Возможность настройки интерфейса в соответствии с потребностями конкретных пользователей.

## Требования к математическому обеспечению

6.2.1 Алгоритмы обработки данных:

* Система должна использовать эффективные алгоритмы для обработки больших объемов данных, связанных с управлением персоналом.
* Применение методов оптимизации для расчета расписаний, нагрузки сотрудников и анализа эффективности.

6.2.2 Методы анализа и прогнозирования:

* Разработка математических моделей для анализа производительности сотрудников на основе заданных метрик.
* Использование прогнозных методов для оценки потребностей в кадрах и планирования трудовых ресурсов.

6.2.3 Распознавание закономерностей:

* Система должна поддерживать алгоритмы машинного обучения для анализа больших массивов данных и выявления закономерностей в работе сотрудников.
* Применение статистических методов для обнаружения отклонений или аномалий.

6.2.4 Автоматизация расчётов:

* Реализация формул и алгоритмов для расчета показателей эффективности, заработной платы, отпускных периодов и других параметров.
* Упрощение проведения массовых расчетов для большого количества сотрудников.

6.2.5 Инструменты обработки времени:

* Использование методов расчета рабочего времени сотрудников, включая учет сверхурочных часов и периодов отпусков.
* Поддержка алгоритмов составления и оптимизации графиков.

6.2.6 Методы визуализации данных:

* Поддержка графических методов отображения аналитической информации, таких как диаграммы, графики и тепловые карты, для удобства интерпретации данных.
* Обеспечение функций построения отчетов с использованием математических результатов.

6.2.7 Надежность вычислений:

* Математическое обеспечение должно гарантировать точность расчетов и стабильность работы системы даже при увеличении объемов данных или нагрузки.
* Реализация механизмов проверки корректности вычислений.

6.2.8 Совместимость с нормативами:

* Все используемые математические методы должны соответствовать актуальным стандартам и нормативным требованиям, связанным с управлением кадров.

## Требования к программному обеспечению

6.3.1 Функциональные требования:

* Программное обеспечение должно обеспечивать выполнение всех заявленных функций системы: учет данных сотрудников, расчет эффективности, управление расписанием и хранение документов.
* Возможность автоматизации рутинных процессов, таких как генерация отчетов, расчет заработной платы и контроль рабочего времени.

6.3.2 Интуитивно понятный интерфейс:

* Интерфейс должен быть доступным для пользователей различных категорий, включая кадровых специалистов, руководителей и сотрудников.
* Обеспечить простую навигацию и удобный доступ к основным функциям системы.

6.3.3 Поддержка многоплатформенности:

* Программное обеспечение должно быть совместимо с основными операционными системами, включая Windows, macOS и Linux.
* Возможность работы на мобильных устройствах (iOS и Android) через мобильные приложения или адаптивный веб-интерфейс.

6.3.4 Обеспечение производительности:

* Программное обеспечение должно быть оптимизировано для обработки больших объемов данных без значительных задержек.
* Поддержка многопользовательского режима работы с высокой степенью одновременной нагрузки.

6.3.5 Интеграция с внешними системами:

* Поддержка интеграции с другими корпоративными системами, такими как ERP, CRM и бухгалтерские приложения, через стандартные API.
* Обеспечение возможности импорта и экспорта данных в стандартных форматах (CSV, XML, JSON).

6.3.6 Безопасность программного обеспечения:

* Внедрение механизмов защиты от несанкционированного доступа, включая шифрование данных и защиту от атак.
* Регулярное обновление и исправление уязвимостей в системе.

6.3.7 Логирование и мониторинг:

* Система должна вести журнал действий пользователей и событий для обеспечения возможности аудита.
* Реализация механизма мониторинга производительности системы и ее компонентов.

6.3.8 Масштабируемость:

* Программное обеспечение должно быть адаптируемым для работы в организациях любого размера, от малых предприятий до крупных корпораций.
* Возможность добавления новых функций и модулей по мере развития потребностей организации.

6.3.9 Поддержка работы в сети:

* Программное обеспечение должно обеспечивать сетевой режим работы для удаленного доступа и взаимодействия между сотрудниками различных подразделений.

6.3.10 Документация:

* В комплект программного обеспечения должна входить подробная документация, включающая руководство пользователя, техническое описание системы и инструкции по установке и эксплуатации.

## Требования к техническому обеспечению

6.4.1 Серверное оборудование:

* Система должна быть развернута на серверном оборудовании, обеспечивающем высокую производительность и отказоустойчивость.
* Серверы должны иметь достаточный объем оперативной памяти (не менее 16 ГБ) и накопителей (SSD, объем не менее 500 ГБ).

6.4.2 Рабочие станции пользователей:

* Клиентские устройства должны поддерживать установку программного обеспечения системы или работу через веб-браузер.
* Минимальные требования: процессор не ниже Intel Core i5, 8 ГБ оперативной памяти, стабильное интернет-соединение (не менее 10 Мбит/с).

6.4.3 Сетевое обеспечение:

* Локальная сеть и интернет-соединение должны обеспечивать стабильную и защищённую передачу данных.
* Использование защищенных протоколов связи (например, HTTPS) для работы системы.

6.4.4 Резервное копирование:

* Система должна быть интегрирована с оборудованием для автоматического резервного копирования данных.
* Устройства хранения резервных копий должны иметь достаточную емкость для хранения копий всех критически важных данных.

6.4.5 Электропитание:

* Использование источников бесперебойного питания (ИБП) для серверов и ключевых рабочих станций для предотвращения потери данных при перебоях в электроснабжении.

6.4.6 Операционная система:

* Серверы и клиентские устройства должны поддерживать современные операционные системы, такие как Windows Server, Linux (Ubuntu, CentOS) или их аналоги.
* Обеспечение регулярного обновления операционных систем для устранения уязвимостей.

6.4.7 Защита технического оборудования:

* Серверное оборудование должно находиться в защищенном помещении, обеспечивающем контроль доступа, климатические условия (температура, влажность) и защиту от внешних угроз (пожар, затопление).

6.4.8 Аппаратное масштабирование:

* Конфигурация серверного и сетевого оборудования должна предусматривать возможность масштабирования при увеличении числа пользователей или данных.

6.4.9 Совместимость с периферийным оборудованием:

* Система должна поддерживать интеграцию с принтерами, сканерами и другими устройствами, необходимыми для работы с документами.

6.4.10 Мониторинг и управление оборудованием:

* Внедрение систем управления и мониторинга оборудования для своевременного выявления и устранения возможных сбоев.

## Требования к организационному обеспечению

6.5.1 Обучение сотрудников:

* Организация обучения пользователей системе, включая кадровых специалистов, руководителей и сотрудников.
* Подготовка обучающих материалов и проведение тренингов, позволяющих эффективно использовать функционал системы.

6.5.2 Административное сопровождение:

* Назначение ответственных сотрудников за эксплуатацию и сопровождение системы в каждом подразделении.
* Формирование команды специалистов для администрирования системы, включая техническое обслуживание и обновление.

6.5.3 Регламентация использования:

* Разработка внутренних регламентов, описывающих порядок работы с системой, включая правила ввода данных, доступа и обработки информации.
* Внедрение политики безопасности данных для соблюдения требований конфиденциальности и защиты информации.

6.5.4 Подготовка инфраструктуры:

* Организация рабочих мест пользователей, оснащённых необходимым оборудованием (компьютеры, периферийные устройства).
* Обеспечение доступа к локальной сети и стабильному интернет-соединению для работы с системой.

6.5.5 Техническая поддержка:

* Создание службы технической поддержки для оперативного решения возникающих вопросов и устранения неполадок.
* Подготовка специалистов, способных проводить диагностику системы и обеспечивать её бесперебойную работу.

6.5.6 Резервное копирование:

* Организация процедур резервного копирования данных и их хранения для предотвращения потери информации.
* Регулярный мониторинг и проверка сохранности резервных копий.

6.5.7 Контроль внедрения:

* Проведение тестирования системы на всех этапах внедрения для выявления и устранения возможных недостатков.
* Постоянный мониторинг работы системы после её запуска, анализ обратной связи от пользователей.

6.5.8 Документационное сопровождение:

* Подготовка инструкций для пользователей и технической документации для администраторов системы.
* Регулярное обновление документации в случае внесения изменений в функционал системы.

6.5.9 Мотивация сотрудников:

* Внедрение системы мотивации для пользователей, активно использующих систему для повышения производительности и достижения целей организации.
* Разработка механизмов стимулирования внедрения новых технологий в рабочий процесс.

# **СОСТАВ И СОДЕРЖАНИЕ РАБОТ**

Этап 1: Анализ и проектирование

* Проведение анализа текущих процессов управления персоналом в организации.
* Определение требований к функционалу системы, включая потребности пользователей и бизнес-процессы.
* Разработка технического задания и согласование с заказчиком.
* Создание архитектурного проекта АСУП, включающего описание модулей, базы данных и пользовательского интерфейса.

Этап 2: Разработка программного обеспечения

* Написание программного кода для каждого модуля системы в соответствии с утвержденным техническим заданием.
* Разработка и настройка базы данных для хранения кадровой информации.
* Создание пользовательского интерфейса, адаптированного под потребности различных категорий пользователей.
* Проведение тестирования программного обеспечения для выявления и устранения ошибок.

Этап 3: Интеграция и настройка системы

* Внедрение разработанной системы в ИТ-инфраструктуру организации.
* Интеграция АСУП с другими корпоративными системами, такими как бухгалтерские и ERP-программы.
* Настройка уровней доступа и распределение ролей между пользователями системы.

Этап 4: Тестирование и запуск

* Проведение всестороннего тестирования системы в рабочих условиях.
* Исправление выявленных ошибок и доработка функционала.
* Постепенный запуск системы, включая пилотное внедрение и последующее развертывание на всех уровнях организации.

Этап 5: Обучение пользователей и сопровождение

* Разработка обучающих материалов и проведение тренингов для сотрудников.
* Обеспечение технической поддержки пользователей на этапе освоения системы.
* Подготовка команды для сопровождения и дальнейшего обновления системы.

Этап 6: Обслуживание и развитие системы

* Регулярное обновление системы для повышения её функциональности и безопасности.
* Проведение работ по оптимизации производительности и добавлению новых модулей.
* Постоянный мониторинг работы системы и адаптация к изменяющимся требованиям.

# **ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ**

Предварительная подготовка:

* Разработка технической документации, включающей подробное описание структуры и функционала системы.
* Проведение обучения сотрудников, которые будут участвовать в тестировании и эксплуатации системы.
* Проверка готовности инфраструктуры, необходимой для запуска АСУП.

Тестирование системы:

* Выполнение функционального тестирования для проверки всех модулей системы на соответствие техническому заданию.
* Проведение нагрузочного тестирования для оценки производительности системы в условиях реальных рабочих нагрузок.
* Выявление и устранение ошибок или недостатков, обнаруженных в процессе тестирования.

Пилотный запуск:

* Внедрение системы на ограниченном участке или в отдельном подразделении для тестирования её работы в реальных условиях.
* Оценка эффективности работы системы в пилотном режиме, сбор отзывов пользователей и корректировка параметров.

Финальная приемка:

* Проведение заключительных испытаний для подтверждения полного соответствия системы заявленным требованиям и задачам.
* Согласование результатов тестирования с заказчиком и утверждение готовности системы к эксплуатации.

Оформление документов:

* Подготовка актов приемки, включающих итоги тестирования и согласование введённых в эксплуатацию функций.
* Передача системы заказчику с оформлением всех необходимых сопровождающих документов.

Запуск и сопровождение:

* Ввод системы в эксплуатацию на уровне всей организации.
* Организация технической поддержки пользователей, включая помощь в первых этапах работы с системой.
* Мониторинг работы системы после запуска, с последующим внесением необходимых доработок и обновлений.

# **ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ**

Общая документация:

* Документация должна включать полный перечень всех этапов разработки, внедрения и эксплуатации системы.
* Структура документации должна быть логичной и последовательной, обеспечивать удобство поиска необходимой информации.

Техническое задание:

* Описание функциональных и нефункциональных требований к системе.
* Разработка детального технического задания с указанием целей, задач и особенностей реализации АСУП.

Проектная документация:

* Архитектурный проект системы, включая схему модулей и базы данных.
* Описание интеграции с другими корпоративными системами.
* Спецификации используемого оборудования и программного обеспечения.

Руководства пользователя:

* Подробные инструкции для различных категорий пользователей (кадровые специалисты, администраторы, руководители).
* Описание работы с интерфейсом системы, включая примеры выполнения основных операций.
* Инструкции по настройке параметров системы, доступных пользователю.

Административная документация:

* Руководство для администраторов системы, включая настройку безопасности, управление базой данных и мониторинг работоспособности.
* Описание процедур резервного копирования и восстановления данных.

Сопровождающая документация:

* Акт приемки системы в эксплуатацию с подтверждением её соответствия техническому заданию.
* Отчёт о результатах тестирования системы.
* Регламент обновления и технической поддержки, включая сроки выполнения работ.

Обновление документации:

* Документация должна регулярно обновляться в случае внесения изменений в функционал системы.
* Хранение предыдущих версий документации для исторической справки и анализа.

НАСТОЯЩИЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ МОГУТ УТОЧНЯТЬСЯ И КОРРЕКТИРОВАТЬСЯ ПО ВЗАИМНОЙ ДОГОВОРЕННОСТИ МЕЖДУ ЗАКАЗЧИКОМ И ИСПОЛНИТЕЛЕМ В РАБОЧЕМ ПОРЯДКЕ.