**Техническое задание**

**Проектирование автоматической системы контроля законодательства для медицинских организаций в сфере защиты информации**

**1. Введение**

В современном мире медицинские организации обязаны соблюдать многочисленные законодательные и нормативные требования в сфере защиты информации, включая персональные данные пациентов. Необходимость своевременного мониторинга изменений в законодательстве и оперативного внедрения соответствующих мер требует автоматизации процессов.

**Цель проекта**: Разработать автоматическую систему, которая будет осуществлять мониторинг законодательства в сфере защиты информации, анализировать изменения, преобразовывать их в конкретные задачи для медицинских организаций и обеспечивать контроль их исполнения.

**2. Цели и задачи проекта**

**2.1. Цели**

* Обеспечить медицинские организации актуальной информацией о законодательных изменениях в сфере защиты информации.
* Автоматизировать процесс анализа законодательных актов и преобразование их в конкретные действия.
* Повысить уровень соответствия медицинских организаций требованиям законодательства и снизить риски нарушений.

**2.2. Задачи**

* Создать систему мониторинга источников законодательства (официальные сайты, базы данных).
* Разработать модуль анализа и интерпретации законодательных изменений.
* Реализовать механизм формирования конкретных задач и рекомендаций для внедрения в организации.
* Обеспечить интеграцию системы с внутренними процессами организации (например, с системами управления документами).
* Разработать интерфейс для пользователей с различными уровнями доступа.

**3. Область применения**

* **Тип организаций**: Государственные и частные медицинские учреждения, клиники, больницы, поликлиники.
* **Сфера деятельности**: Защита информации, обработка персональных данных пациентов, обеспечение информационной безопасности.

**4. Требования к системе**

**4.1. Функциональные требования**

1. **Мониторинг законодательства**
   * Система должна автоматически отслеживать изменения в законодательстве, включая федеральные законы, постановления, приказы, стандарты и методические рекомендации.
   * Источники мониторинга: официальные сайты правовой информации (pravo.gov.ru, consultant.ru), регуляторные органы (Минздрав, Роскомнадзор, ФСТЭК, ФСБ).
2. **Анализ и интерпретация**
   * Модуль семантического анализа для выявления изменений и их влияния на деятельность медицинских организаций.
   * Классификация изменений по степени важности и срочности внедрения.
3. **Преобразование в задачи**
   * Генерация конкретных задач для различных подразделений организации (ИТ-отдел, отдел кадров, юридический отдел и т.д.).
   * Формирование чек-листов и рекомендаций по внедрению изменений.
4. **Уведомления и оповещения**
   * Система должна отправлять уведомления ответственным лицам о новых изменениях и назначенных задачах.
   * Настройка периодичности и каналов оповещения (email, SMS, мессенджеры).
5. **Управление задачами**
   * Возможность отслеживания статуса выполнения задач.
   * Назначение ответственных лиц и контроль сроков исполнения.
   * Журналирование действий пользователей.
6. **Интеграция**
   * Интеграция с внутренними системами организации (СЭД, ERP, CRM).
   * Возможность экспорта и импорта данных в стандартных форматах (XML, JSON, CSV).
7. **Отчётность и аналитика**
   * Формирование отчётов о выполнении задач, степени соответствия требованиям законодательства.
   * Статистический анализ для выявления узких мест и планирования улучшений.

**4.2. Нефункциональные требования**

1. **Безопасность**
   * Соответствие требованиям законодательства по защите информации (ФЗ-152 «О персональных данных», ФЗ-149 «Об информации, информационных технологиях и о защите информации»).
   * Аутентификация и авторизация пользователей с разграничением прав доступа.
   * Шифрование данных в хранилище и при передаче.
2. **Надёжность и отказоустойчивость**
   * Обеспечение бесперебойной работы системы.
   * Резервное копирование и восстановление данных.
3. **Масштабируемость**
   * Возможность расширения функционала и обработки увеличивающегося объёма данных.
4. **Юзабилити**
   * Интуитивно понятный интерфейс для пользователей с различным уровнем технической подготовки.
   * Поддержка русского языка.
5. **Совместимость**
   * Работа на распространённых операционных системах (Windows, Linux).
   * Поддержка современных веб-браузеров для веб-интерфейса.

**5. Архитектура системы**

**5.1. Общая архитектура**

* **Модуль сбора данных**: Отвечает за мониторинг источников законодательства и загрузку новых документов.
* **Модуль анализа**: Проводит семантический анализ текстов, выявляет изменения и их влияние.
* **Модуль управления задачами**: Формирует задачи, назначает ответственных, контролирует выполнение.
* **База данных**: Хранит документы, результаты анализа, задачи, информацию о пользователях.
* **Интерфейс пользователя**: Веб-приложение или десктопное приложение для взаимодействия с системой.
* **Интеграционные модули**: Обеспечивают взаимодействие с внутренними системами организации.

**5.2. Технологии**

* **Язык программирования**: Python, Java, C# или другой, соответствующий требованиям организации.
* **База данных**: PostgreSQL, MS SQL Server или аналогичная СУБД.
* **Фреймворки**: Django, .NET, Spring или другие для ускорения разработки.
* **Семантический анализ**: Использование NLP-библиотек (NLTK, spaCy) или готовых решений.
* **Безопасность**: SSL/TLS для шифрования, OAuth 2.0 для аутентификации.

**6. Этапы реализации**

**6.1. Этап 1: Анализ и проектирование**

* Сбор требований и уточнение технического задания.
* Проектирование архитектуры системы.
* Определение технологий и инструментов разработки.

**6.2. Этап 2: Разработка прототипа**

* Реализация основных модулей:
  + Модуль сбора данных.
  + База данных.
  + Базовый интерфейс пользователя.
* Тестирование прототипа на небольшом объёме данных.

**6.3. Этап 3: Полноценная разработка**

* Разработка всех функциональных модулей.
* Реализация механизмов безопасности.
* Интеграция с внутренними системами организации.
* Оптимизация и улучшение производительности.

**6.4. Этап 4: Тестирование**

* Функциональное тестирование.
* Нагрузочное тестирование.
* Тестирование безопасности.

**6.5. Этап 5: Внедрение**

* Установка системы на серверы организации.
* Обучение персонала.
* Миграция данных (при необходимости).

**6.6. Этап 6: Сопровождение и поддержка**

* Техническая поддержка пользователей.
* Обновление системы в соответствии с изменениями законодательства.
* Доработка функционала по запросам пользователей.

**7. Требования к ресурсам**

**7.1. Аппаратные ресурсы**

* **Серверная часть**:
  + Процессор: не менее 4 ядер.
  + Оперативная память: не менее 16 ГБ.
  + Место на диске: от 500 ГБ с возможностью расширения.
* **Клиентская часть**:
  + Любой современный компьютер или мобильное устройство с поддержкой веб-браузера.

**7.2. Человеческие ресурсы**

* **Команда разработки**:
  + Системный аналитик.
  + Разработчики (Frontend, Backend).
  + Специалист по информационной безопасности.
  + Тестировщики.
* **Команда внедрения**:
  + Инженеры по поддержке.
  + Тренеры для обучения персонала.

**8. Критерии приёмки**

* Полное соответствие функциональным и нефункциональным требованиям.
* Отсутствие критических ошибок при тестировании.
* Положительные отзывы пилотных пользователей.
* Документация по системе (техническая, пользовательская).

**9. Документация**

* **Техническая документация**:
  + Описание архитектуры.
  + Инструкции по установке и настройке.
  + Описание API и интеграционных модулей.
* **Пользовательская документация**:
  + Руководство пользователя.
  + ЧаВо (FAQ).
  + Обучающие материалы и презентации.

**10. Дополнительные требования**

* **Соблюдение стандартов разработки ПО**.
* **Возможность масштабирования** системы для использования в других сферах (не только медицинских организаций).
* **Гибкость настройки** под специфические требования отдельных организаций.

**11. Сроки реализации**

* **Этап 1 (Анализ и проектирование)**: 1 месяц.
* **Этап 2 (Разработка прототипа)**: 2 месяца.
* **Этап 3 (Полноценная разработка)**: 4 месяца.
* **Этап 4 (Тестирование)**: 1 месяц.
* **Этап 5 (Внедрение)**: 1 месяц.
* **Общий срок проекта**: 9 месяцев.

**12. Бюджет**

* **Разработка**: Оценка затрат на команду разработчиков и необходимое оборудование.
* **Внедрение**: Затраты на установку, обучение и интеграцию.
* **Сопровождение**: Ежегодные затраты на поддержку и обновления.

*Точные цифры бюджета будут определены после детального планирования и оценки трудозатрат.*

**13. Риски и способы их минимизации**

* **Риск**: Изменение законодательства во время разработки.
  + **Митигирование**: Гибкая архитектура, позволяющая быстро вносить изменения.
* **Риск**: Сопротивление пользователей новым технологиям.
  + **Митигирование**: Проведение обучения и демонстрация преимуществ системы.
* **Риск**: Утечка конфиденциальных данных.
  + **Митигирование**: Строгое соблюдение требований безопасности, регулярные аудиты.

**14. Контактные лица**

* **Руководитель проекта**: [Имя, контактная информация]
* **Технический директор**: [Имя, контактная информация]
* **Ответственный за информационную безопасность**: [Имя, контактная информация]

**15. Заключение**

Реализация автоматической системы контроля законодательства в сфере защиты информации позволит медицинским организациям эффективно соблюдать нормативные требования, снизить риски нарушений и повысить уровень безопасности персональных данных пациентов. Тщательное планирование, использование современных технологий и учет специфики отрасли обеспечат успешное внедрение и эксплуатацию системы.