Оглавление

[**Цель проекта**: 2](#_Toc182262063)

[**Шаг 1: Детализация функциональных модулей и интерфейсов** 2](#_Toc182262064)

[**Шаг 2: Предложение стека технологий для** 2](#_Toc182262065)

[**Предлагаемое решение по шифрованию документов** 3](#_Toc182262066)

[**Резюме** 4](#_Toc182262067)

[**Шаг 3: План разработки (разделим на этапы)** 4](#_Toc182262068)

[**Этап 1: Подготовка и проектирование** 5](#_Toc182262069)

[**Этап 2: Разработка backend и базы данных** 5](#_Toc182262070)

[**Этап 3: Разработка frontend** 5](#_Toc182262071)

[**Этап 4: Безопасность и шифрование** 6](#_Toc182262072)

[**Этап 5: Тестирование и развертывание** 6](#_Toc182262073)

[**Итого: Общий срок выполнения проекта** 6](#_Toc182262074)

[**Возможные факторы, влияющие на сроки:** 6](#_Toc182262075)

[**Референсы:** 7](#_Toc182262076)

# **Цель проекта**:

Создать современный и безопасный веб-портал для автоматизации обмена электронными документами между организациями и их контрагентами. Портал должен обеспечить:

1. **Оптимизацию документооборота**: упрощение процесса отправки, подписания и хранения юридически значимых документов, что позволит снизить затраты на бумажный документооборот и ускорить рабочие процессы.
2. **Безопасность и надежность**: интеграция с сертифицированными центрами ключей Украины для использования электронных подписей, шифрование данных, поддержка двухфакторной аутентификации и защита от несанкционированного доступа.
3. **Удобство взаимодействия**: предоставление контрагентам и сотрудникам личных кабинетов для управления документами, а также возможности общения через встроенный чат.
4. **Гибкость и масштабируемость**: поддержка интеграции с внешними ERP и бухгалтерскими системами (например, 1С) и сервисами электронного документооборота (М.E.Doc, Вчасно), что позволит в будущем расширять функциональность платформы по мере роста потребностей бизнеса.
5. **Цифровизацию и автоматизацию бизнес-процессов**: переход на электронные форматы обмена документами для повышения эффективности и минимизации ошибок при ручной обработке данных.

**Шаг 1: Детализация функциональных модулей и интерфейсов**

**Основные модули портала и их функции**

1. **Авторизация и регистрация**
   * Авторизация через логин/пароль или e-mail. (опционально, подключается в кабинете контрагента)
   * Регистрация контрагентов с возможностью акцепта заявки сотрудником.
   * Самостоятельная регистрация контрагентов с прикреплением уставных документов.
   * Логика подтверждения регистрации и отправка данных для входа на e-mail контрагента.
2. **Личный кабинет контрагента**
   * Разделы:
     + **Панель управления**: общий обзор загруженных документов и уведомлений. Возможность добавить договор.
     + **Мои документы**: загрузка, просмотр и подписание документов.
     + **Чат**: Выбор отдела при начале общения общение с менеджерами, бухгалтерией и юристами.
     + **Профиль**: управление реквизитами и контактными данными.
     + **История действий**: лог всех операций контрагента на портале.
   * Возможность настроить уведомления (e-mail, SMS, Telegram).
3. **Описание процесса регистрации**

Сам процесс, необходимыми поля и т д. приведено в приложении 1.1 (Регистрация на портале данные и поля.docx)

1. **Управление документооборотом**
   * Загрузка документов (счета, накладные, договоры и ТТН).
   * Загружая счет под него, загружаются товарные накладные и ТТН
   * Возможность подписания документов с использованием электронного ключа (поддержка PAdES, XAdES, CAdES).
   * Возможность пометить документы на удаление.
   * Отслеживание статусов документов: «Ожидает подписи», «Подписан», «На доработку».
   * Запросы на удаление документов с подтверждением всех сторон.
2. Полный перечень необходимых документов для загрузки на портал

Перечень всех необходимых документов длязагрузки на портал контрагентом приведен в приложении 1.2 (1.2 Перечень документов для заключения договоров поставки.docx)

1. **Модуль чата и комментариев**
   * Встроенный чат для общения контрагента с сотрудниками (менеджеры, бухгалтерия, юристы).
   * Возможность оставлять комментарии к документам для обсуждения правок.
   * Уведомления о новых сообщениях и комментариях.
2. **Административная панель**
   * Управление пользователями (создание, блокировка, изменение прав доступа).
   * Модерация заявок на регистрацию контрагентов и их аккредитация.
   * Управление IP-адресами (ограничения доступа, черный список).
   * Настройка интеграций ( ЦСК, Telegram, SMS, Email).
3. **Отчеты и аналитика**
   * Формирование отчетов по документообороту, активности пользователей и финансовым операциям.
   * Выгрузка отчетов в формате Excel.
   * Настройка автоматических отчетов и их отправка на e-mail.
4. **Права и доступы на портале**

Необходимые роли, а также права с полным описанием функционала приведены в приложении 1.3 (1.3 Права доступа к порталу.docx)

**Шаг 2: Предложение стека технологий для**

**Фронтенд**

* **React.js**: для создания интерактивного и динамичного пользовательского интерфейса.
* **Bootstrap** или **Tailwind CSS**: для адаптивного и быстрого оформления.
* **Axios**: для работы с API и асинхронных запросов.
* **Redux**: для управления состоянием приложения.

**Бэкенд**

* **Node.js** (NestJS): для построения масштабируемого и гибкого API.
* **PostgreSQL**: как основная база данных (или **MongoDB** для гибкой работы с документами).
* **Redis**: для кеширования и ускорения обработки данных.
* **Nginx**: для балансировки нагрузки и защиты от DDoS-атак.
* **Docker**: для контейнеризации и удобного развертывания.

**Интеграции и безопасность**

* **OpenSSL** и **Let's Encrypt**: для шифрования данных и установки SSL-сертификатов.
* **OAuth2** и **JWT**: для аутентификации и защиты API.
* **TurboSMS API**: для отправки SMS.
* **Telegram Bot API**: для интеграции с Telegram.

**Предлагаемое решение по шифрованию документов**

**1. Выбор метода шифрования**

Для шифрования документов на сервере можно использовать **алгоритм AES (Advanced Encryption Standard)** с длиной ключа 256 бит (AES-256). Это один из наиболее надежных и современных методов шифрования, который широко используется для защиты конфиденциальных данных.

* **Преимущества AES-256**:
  + Высокая безопасность и стойкость к взлому.
  + Быстрая работа даже при больших объемах данных.
  + Стандартизированный алгоритм, поддерживаемый большинством библиотек и платформ.

**2. Процесс шифрования и дешифрования**

**2.1. Шифрование документа перед сохранением:**

* При загрузке документа на портал система автоматически шифрует его перед сохранением на сервере.
* Для шифрования используется уникальный **ключ шифрования**, который генерируется для каждого документа.
* После шифрования оригинальный документ удаляется из временного хранилища, и на сервере сохраняется только зашифрованная версия.

**2.2. Дешифрование документа при доступе:**

* Когда пользователю требуется скачать или просмотреть документ, система выполняет дешифрование на сервере.
* Пользователь может получить доступ к документу только при наличии соответствующих прав.

**3. Хранение и управление ключами**

Для безопасного хранения ключей шифрования можно использовать следующие подходы:

* **Использование KMS (Key Management Service)**:
  + Хранение ключей шифрования в специализированных сервисах, таких как AWS KMS, Google Cloud KMS или Azure Key Vault.
  + Это обеспечивает дополнительную защиту и контроль доступа к ключам.
* **Локальное шифрование с использованием HSM (Hardware Security Module)**:
  + Ключи шифрования могут храниться на локальном сервере в модуле HSM, что повышает безопасность и защищает от компрометации.

**4. Архитектура шифрования**

1. **Генерация ключа**:
   * При загрузке документа генерируется случайный ключ шифрования (AES-256) и вектор инициализации (IV).
   * Ключ и IV используются для шифрования файла.
2. **Шифрование документа**:
   * Документ шифруется с использованием алгоритма AES-256 и сохраняется в зашифрованном виде на сервере.
   * Ключ шифрования сам по себе также шифруется с использованием мастер-ключа и хранится в базе данных.
3. **Доступ к документу**:
   * При запросе на скачивание или просмотр документа система расшифровывает его с использованием ранее сохраненного ключа.
   * Процесс дешифрования выполняется на сервере и предоставляется пользователю только временная ссылка для скачивания.

**5. Безопасность и аудит доступа**

* Вся работа с документами (загрузка, шифрование, дешифрование) будет логироваться для аудита.
* Логирование действий пользователей и администраторов, включая попытки доступа к документам, с сохранением IP-адресов и меток времени

**Резюме**

* **Алгоритм шифрования**: AES-256 (симметричное шифрование).
* **Хранение ключей**: KMS (облачное решение) или HSM (локально).
* **Процесс шифрования/дешифрования**: автоматическое шифрование при загрузке и дешифрование при доступе.
* **Безопасность**: логирование всех операций для аудита.

Этот подход обеспечивает надежное шифрование и защиту документов на портале, минимизируя риски утечки данных.

**Шаг 3: План разработки (разделим на этапы)**

1. **Проектирование и прототипирование**:
   * Создание прототипа интерфейса (Figma).
   * Разработка детализированных макетов страниц.
2. **Разработка и настройка инфраструктуры**:
   * Настройка VPS сервера, базы данных и Docker-окружения.
   * Разработка API и базы данных.
3. **Реализация фронтенда**:
   * Создание интерфейса личного кабинета и административной панели.
   * Разработка модуля чата и загрузки документов.
4. **Интеграция с внешними сервисами**:
   * Интеграция с ЦСК, TurboSMS, Telegram и ERP.
   * Настройка двухфакторной аутентификации.
5. **Тестирование и запуск**:
   * Тестирование функциональности и безопасности.
   * Оптимизация производительности.
   * Развертывание на VPS и запуск в эксплуатацию.

**Этап 1: Подготовка и проектирование**

1. **Анализ требований и проектирование системы** (1-неделя)
   * Сбор всех уточнений и окончательное формирование технического задания (ТЗ).
   * Создание прототипов интерфейса и архитектуры базы данных.
   * Планирование структуры проекта и определение стеков технологий.
2. **Настройка серверной инфраструктуры и окружения** (1-2 недели)
   * Настройка VPS сервера, установка и конфигурация необходимых инструментов (Docker, Nginx, SSL-сертификаты).
   * Подготовка базы данных (PostgreSQL) и резервного копирования.

**Итого на этап 1** 1-2 недели

**Этап 2: Разработка backend и базы данных**

1. **Создание базовой архитектуры и API** (2 недели)
   * Разработка модулей для авторизации и регистрации пользователей.
   * Реализация системы управления ролями и правами доступа.
   * Создание модулей для работы с документами и чатом.
2. **Интеграция с внешними сервисами** (1 неделя)
   * Подключение к ЦСК для поддержки электронной подписи (PAdES, XAdES, CAdES).
   * Telegram Bot для уведомлений.

**Итого на этап** : 2-3 недель

**Этап 3: Разработка frontend**

1. **Создание интерфейсов личного кабинета и админки** (1-2 недели)
   * Реализация страниц регистрации и авторизации.
   * Разработка личного кабинета контрагента (загрузка документов, чат, профиль).
   * Создание административной панели (управление пользователями, модерация заявок, настройка интеграций).
2. **Интеграция frontend и backend** (1-2 недели)
   * Настройка взаимодействия между фронтендом и бэкендом через API.
   * Тестирование функциональности и отладка.

**Этап 4: Безопасность и шифрование**

1. **Реализация шифрования документов** (1 недели)
   * Реализация шифрования документов на основе алгоритма AES-256.
   * Настройка хранения и управления ключами (KMS или HSM).
2. **Реализация двухфакторной аутентификации (2FA)** (1 неделя)
   * Настройка отправки кодов подтверждения на e-mail и телефон.

**Этап 5: Тестирование и развертывание**

1. **Тестирование функциональности и безопасности** (1 неделя)
   * Тестирование работы всех модулей и интеграций.
   * Тестирование безопасности (шифрование, защита от несанкционированного доступа).
2. **Развертывание и настройка системы на боевом сервере** (1 неделя)
   * Перенос на VPS сервер.
   * Финальная настройка и проверка работы системы.

**Итого: Общий срок выполнения проекта**

**Общая оценка**: 35 дней

**Возможные факторы, влияющие на сроки:**

* **Сложность интеграции** с внешними сервисами, проблемы получения API и необходимой документации (ЦСК, TurboSMS).
* Время, необходимое на тестирование и исправление багов может быть увеличено в связи с регулярным отключением света у заказчика.
* Возможные изменения требований на этапе разработки.

# **Референсы:**

Сайт:

<https://connect.dealssign.com/>

Доступ: *Засекречен*