**Анализ требований для проекта по работе с документами и практикой ИБ**

**I. Цель анализа**

* Определить функциональные и нефункциональные требования к продукту.
* Учесть потребности целевой аудитории.
* Оценить технические и юридические ограничения.

**II. Вопросы для анализа**

1. **Целевая аудитория**
   * Кто будет пользоваться продуктом?
     + Сотрудники отделов ИБ?
     + Руководители организаций?
     + Специалисты по аудиту и compliance?
   * Какие задачи они хотят решать с помощью продукта?
2. **Основные функции**
   * Какие задачи должен решать продукт:
     + Автоматизация работы с нормативными документами?
     + Создание отчетов и чек-листов?
     + Управление инцидентами и реагирование?
   * Нужна ли интеграция с существующими системами (1С, SIEM)?
3. **Юридические требования**
   * Какие нормативные акты необходимо учитывать:
     + ФЗ № 152 "О персональных данных"?
     + ФЗ № 149 "Об информации"?
     + ФЗ № 187 "О безопасности КИИ"?
   * Нужно ли соответствие международным стандартам (ISO 27001, GDPR)?
4. **Формат данных**
   * Какие форматы документов будут использоваться (PDF, DOCX, TXT)?
   * Нужно ли преобразование форматов для обработки?
5. **Обновление данных**
   * Как часто требуется обновление нормативных документов?
   * Нужна ли интеграция с внешними источниками для автоматического обновления?
6. **Пользовательский интерфейс**
   * Нужна ли веб-платформа, десктопное или мобильное приложение?
   * Какие функции важны в интерфейсе:
     + Поиск по документам?
     + Фильтрация по категориям?
     + Визуализация данных?
7. **Обучение и поддержка пользователей**
   * Нужны ли встроенные курсы по ИБ?
   * Какой формат поддержки пользователей требуется (чат, FAQ, тикеты)?
8. **Монетизация**
   * Какую модель оплаты выбрать:
     + Подписка?
     + Разовая покупка?
     + Платные модули?
9. **Технические ограничения**
   * Какие системы и технологии будут использоваться:
     + База данных (PostgreSQL, MongoDB)?
     + Язык программирования для разработки?
   * Какой объем данных продукт должен обрабатывать?
10. **Сроки и бюджет**
    * Какие временные рамки для разработки?
    * Какой бюджет выделяется на проект?

**III. Результат анализа**

1. **Документ с функциональными требованиями (FRD)**:
   * Описание всех функций, которые должен выполнять продукт.
   * Сценарии использования (use cases).
2. **Документ с техническими требованиями (TRD)**:
   * Технические ограничения и спецификации.
   * Требования к интеграции и масштабируемости.
3. **Юридический анализ**:
   * Список обязательных нормативных актов и стандартов.
   * Рекомендации по обеспечению соответствия требованиям.

**IV. Пример функциональных требований**

1. **Поиск и фильтрация документов**:
   * Быстрый поиск по ключевым словам.
   * Фильтрация по дате, категории, источнику.
2. **Автоматическое обновление**:
   * Сканирование правовых порталов на новые версии документов.
   * Уведомления об изменениях.
3. **Управление инцидентами**:
   * Ведение журнала событий.
   * Генерация плана реагирования на инциденты.
4. **Обучение сотрудников**:
   * Доступ к курсам и тестам по ИБ.
   * Система сертификации.

**V. Следующий шаг**

* Определите ключевых пользователей и их задачи.
* Составьте приоритетный список функций.
* Разработайте пользовательские сценарии (user stories) для каждой группы пользователей.

Если готовы работать с конкретными функциями или группами пользователей, могу помочь детализировать!

4o

**Вы сказали:**

Кто будет пользоваться продуктом - хочу развися в гос.инф. систему - один на всех подход на всю страну

**ChatGPT сказал:**

ChatGPT

**Анализ требований для создания государственной информационной системы по информационной безопасности**

**I. Цель системы**

Создать государственную информационную систему (ГИС) для автоматизации работы с нормативными документами, сопровождения отделов ИБ и обеспечения соответствия требованиям законодательства во всех организациях РФ.

**Главная идея:**  
Единая платформа, обеспечивающая единообразный подход к управлению информационной безопасностью для государственных и частных организаций.

**II. Целевая аудитория**

1. **Государственные органы и учреждения**:
   * ФСТЭК России, ФСБ России, Роскомнадзор.
   * Органы исполнительной власти на всех уровнях.
2. **Критическая информационная инфраструктура (КИИ)**:
   * Энергетика, транспорт, здравоохранение, оборона, связь и другие отрасли.
3. **Коммерческие организации**:
   * Компании, работающие с персональными данными.
   * Подрядчики и партнеры государственных учреждений.
4. **Пользователи внутри организаций**:
   * Руководители по ИБ (CISO).
   * Специалисты отделов ИБ.
   * Руководители среднего звена, отвечающие за соответствие законодательству.

**III. Функциональные требования**

1. **Автоматизация работы с нормативными документами**:
   * Центральный реестр нормативных актов, стандартов и методических рекомендаций.
   * Автоматическое обновление и уведомления об изменениях законодательства.
   * Быстрый поиск и фильтрация документов.
2. **Инструменты для compliance**:
   * Чек-листы и шаблоны для выполнения требований ФЗ № 152, № 187, № 149 и других.
   * Автоматический анализ соответствия текущей практики требованиям.
   * Формирование отчетности для ФСТЭК, ФСБ, Роскомнадзора.
3. **Поддержка управления инцидентами**:
   * Ведение журнала инцидентов ИБ.
   * Интеграция с ГосСОПКА для обмена данными об угрозах.
   * Генерация планов реагирования на инциденты.
4. **Обучение и сертификация сотрудников**:
   * Встроенные модули обучения по ИБ.
   * Тесты для проверки знаний и система сертификации.
5. **Мониторинг и аналитика**:
   * Визуализация текущего состояния ИБ в организациях.
   * Метрики эффективности защиты информации.
   * Анализ уязвимостей и рисков.

**IV. Технические требования**

1. **Инфраструктура**:
   * Размещение в защищённых дата-центрах России.
   * Поддержка отечественного оборудования и программного обеспечения.
2. **Интеграция**:
   * Взаимодействие с системами ГосСОПКА, 1С, SIEM и другими.
   * Поддержка API для подключения внешних систем.
3. **Масштабируемость**:
   * Возможность одновременной работы тысяч пользователей.
   * Хранение большого объема данных (нормативных актов, журналов, отчетов).
4. **Безопасность**:
   * Соответствие требованиям ФСТЭК и ФСБ.
   * Шифрование данных при передаче и хранении.
   * Аутентификация пользователей с использованием СКЗИ.

**V. Юридические требования**

1. Обеспечение соответствия:
   * ФЗ № 149 "Об информации, информационных технологиях и защите информации".
   * ФЗ № 152 "О персональных данных".
   * ФЗ № 187 "О безопасности критической информационной инфраструктуры".
2. Регулярное обновление нормативной базы на основе изменений законодательства.
3. Создание единой платформы с учётом национальных стандартов (ГОСТ Р, ISO).

**VI. Основные вызовы**

1. **Согласование требований**:
   * Учет специфики работы разных отраслей и организаций.
2. **Государственные проверки и сертификация**:
   * Подготовка системы к прохождению сертификации ФСТЭК и ФСБ.
3. **Масштабность проекта**:
   * Разработка архитектуры, которая сможет охватить все организации в стране.
4. **Обучение пользователей**:
   * Создание курсов для быстрой адаптации сотрудников к новой системе.

**VII. Этапы реализации**

1. **Анализ требований**:
   * Сбор данных о потребностях организаций и регуляторов (1–2 месяца).
2. **Разработка MVP**:
   * Создание минимальной версии платформы с базовым функционалом (6–12 месяцев).
3. **Тестирование**:
   * Внедрение в пилотных организациях для проверки функционала и нагрузки (3–6 месяцев).
4. **Масштабирование**:
   * Развертывание системы на региональном и федеральном уровнях (1–2 года).
5. **Поддержка и обновление**:
   * Регулярное обновление нормативной базы и улучшение системы.

**VIII. Ожидаемый результат**

* Единая система, позволяющая организациям автоматически соответствовать требованиям законодательства.
* Упрощение работы отделов ИБ и повышение эффективности управления информационной безопасностью.
* Минимизация рисков для организаций и государства за счет централизованного подхода.