**План действий по созданию и настройке GPT-агента для поддержки ролей и бизнес-процессов в области информационной безопасности**

**I. Анализ требований и целей**

1. **Определение задач**:
   * Выявить ключевые функции и задачи для каждой роли в организации.
   * Определить бизнес-процессы, которые нужно автоматизировать (например, реагирование на инциденты, подготовка отчетов, управление доступом).
   * Установить требования к информационной базе (БЗ) и формату взаимодействия.
2. **Определение источников данных**:
   * Законодательные акты: ФЗ-152, ФЗ-187, ГОСТы, международные стандарты (ISO/IEC 27001).
   * Внутренние политики и инструкции.
   * Актуальная база знаний о угрозах и уязвимостях (например, CVE, SOC отчеты).
3. **Формирование технических требований**:
   * Интеграция с существующими системами (1С, SIEM, CRM, Jira).
   * Формат вывода данных (чек-листы, отчеты, пошаговые инструкции).
   * Уровни доступа для пользователей.

**II. Проектирование GPT-агента**

1. **Разработка архитектуры**:
   * Создать модули для каждой роли (CISO, аналитик SOC, пентестер и др.).
   * Настроить БЗ для поддержки различных бизнес-процессов.
2. **Разделение функционала**:
   * **Для специалистов**: Интерактивные ответы на запросы, генерация отчетов, помощь в реагировании на инциденты.
   * **Для руководства**: Дашборды с метриками, стратегические рекомендации.
   * **Для обучения**: Проведение тестирования, предоставление материалов.
3. **Определение форматов взаимодействия**:
   * Чат-бот для оперативных запросов.
   * Веб-интерфейс для генерации сложных отчетов.
   * API для интеграции с другими системами.

**III. Разработка базы знаний**

1. **Структурирование данных**:
   * Законы и стандарты (разделение на категории: персональные данные, КИИ, управление рисками).
   * Внутренние документы (политики, инструкции).
   * Список угроз и уязвимостей (систематизация по типам).
2. **Автоматизация обновлений**:
   * Настроить парсинг данных из открытых источников (например, RSS-ленты правовых новостей).
   * Создать механизм проверки и обновления БЗ через API или скрипты.
3. **Формат хранения данных**:
   * Использовать базы данных (PostgreSQL, MongoDB) для масштабируемости.
   * JSON для структурированных данных.

**IV. Разработка и настройка GPT-агента**

1. **Тренировка модели**:
   * Подготовить набор данных для обучения модели на основе БЗ.
   * Использовать сценарии взаимодействия для каждой роли.
2. **Настройка алгоритмов**:
   * Добавить контекстное понимание запросов.
   * Настроить выдачу результатов в зависимости от роли пользователя.
3. **Реализация функционала**:
   * **Генерация чек-листов**: Автоматическое формирование по запросу (например, для аудита или категорирования объектов).
   * **Пошаговые инструкции**: Подготовка планов действий в случае инцидентов.
   * **Аналитика и рекомендации**: Анализ данных и предоставление рекомендаций для устранения рисков.

**V. Интеграция с бизнес-системами**

1. **API для взаимодействия**:
   * Настроить API для связи GPT-агента с 1С, SIEM и другими системами.
   * Разработать веб-интерфейс для взаимодействия сотрудников с агентом.
2. **Интеграция с 1С**:
   * Автоматизация документооборота (генерация отчетов, актов проверок).
   * Управление задачами для ролей.
3. **Подключение к SIEM**:
   * Получение логов и данных об инцидентах.
   * Предоставление рекомендаций по реагированию.

**VI. Тестирование и оптимизация**

1. **Тестирование функционала**:
   * Проверка работы с разными ролями (CISO, пентестер, аналитик SOC).
   * Тестирование корректности выдачи данных.
2. **Обратная связь**:
   * Получение отзывов от сотрудников, использующих агента.
   * Корректировка алгоритмов и интерфейса на основе обратной связи.
3. **Оптимизация производительности**:
   * Ускорение времени обработки запросов.
   * Оптимизация работы с большими объемами данных.

**VII. Внедрение и обучение**

1. **Обучение сотрудников**:
   * Проведение тренингов по работе с GPT-агентом.
   * Разработка инструкций и видеоматериалов.
2. **Пилотное внедрение**:
   * Запуск агента в ограниченном масштабе для тестирования в реальных условиях.
   * Исправление выявленных ошибок.
3. **Полное развертывание**:
   * Интеграция во все отделы.
   * Настройка регулярного мониторинга работы агента.

**VIII. Поддержка и развитие**

1. **Регулярное обновление БЗ**:
   * Внесение новых законов, стандартов и угроз.
2. **Анализ эффективности**:
   * Мониторинг использования и полезности агента.
3. **Развитие функционала**:
   * Добавление новых ролей и сценариев взаимодействия.
   * Улучшение интеграции с другими системами.