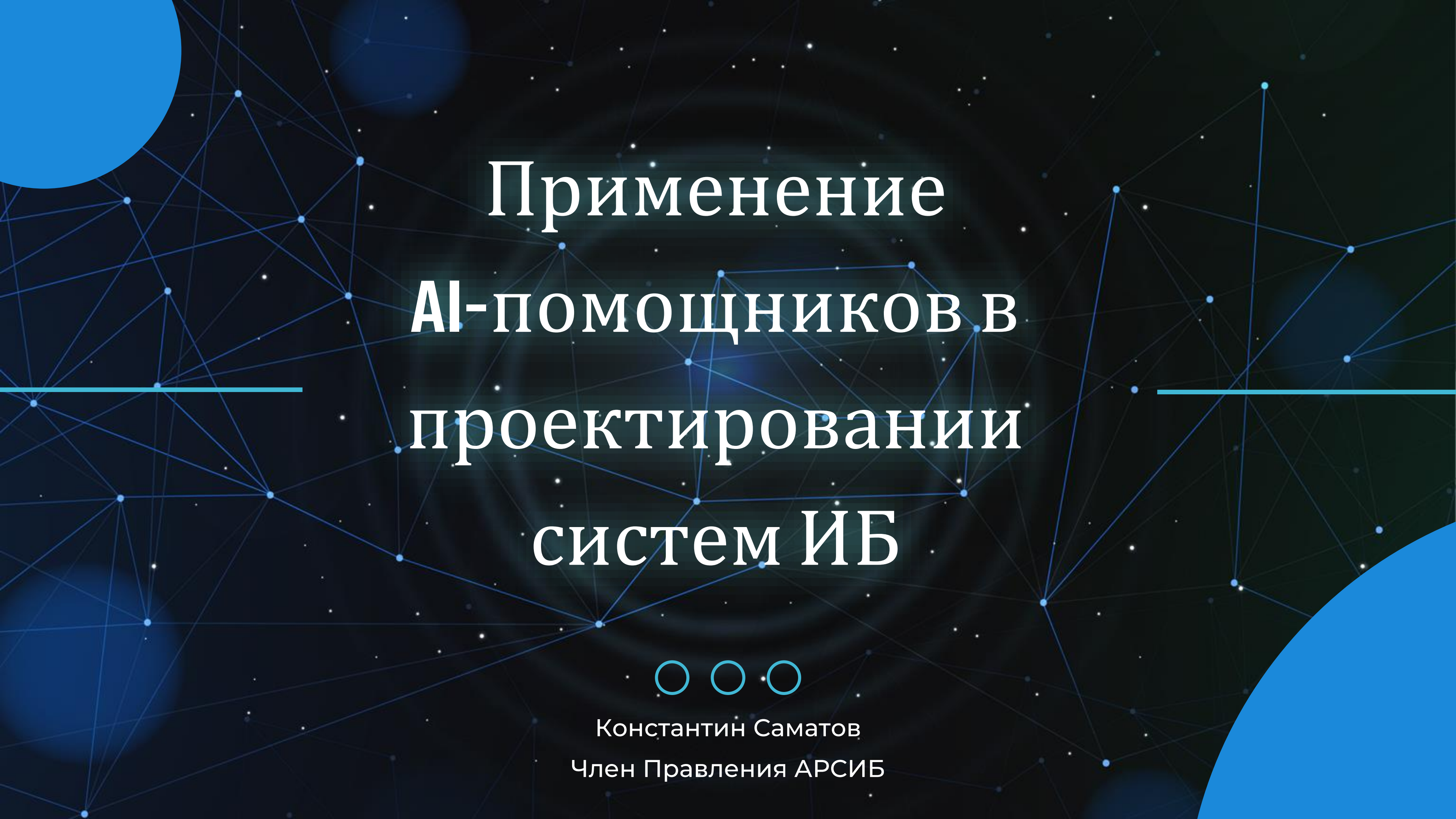




Применение AI-помощников в проектировании систем ИБ



Константин Саматов
Член Правления АРСИБ

Что такое AI-помощник?

Определение:

AI-помощник — это программа, использующая технологии искусственного интеллекта (машинное обучение, NLP, аналитика данных) для автоматизации задач, генерации идей и поддержки принятия решений

Ключевые возможности:

- обработка больших объемов информации для выявления паттернов и аномалий;
- **создание текстов, схем, кода и документации;**
- моделирование рисков и сценариев на основе исторических данных;
- выполнение рутинных задач.

Создание AI помощника для проектирования

Действуй как промпт-инженер экспертного уровня. Создай мне системный промпт для AI-помощника для проектирования. Он должен уметь помогать мне проектировать в соответствии с ГОСТ 34.601-90



✖ Deep Research



✖ Answer

Системный промпт для AI-помощника по проектированию автоматизированных систем по ГОСТ 34.601-90

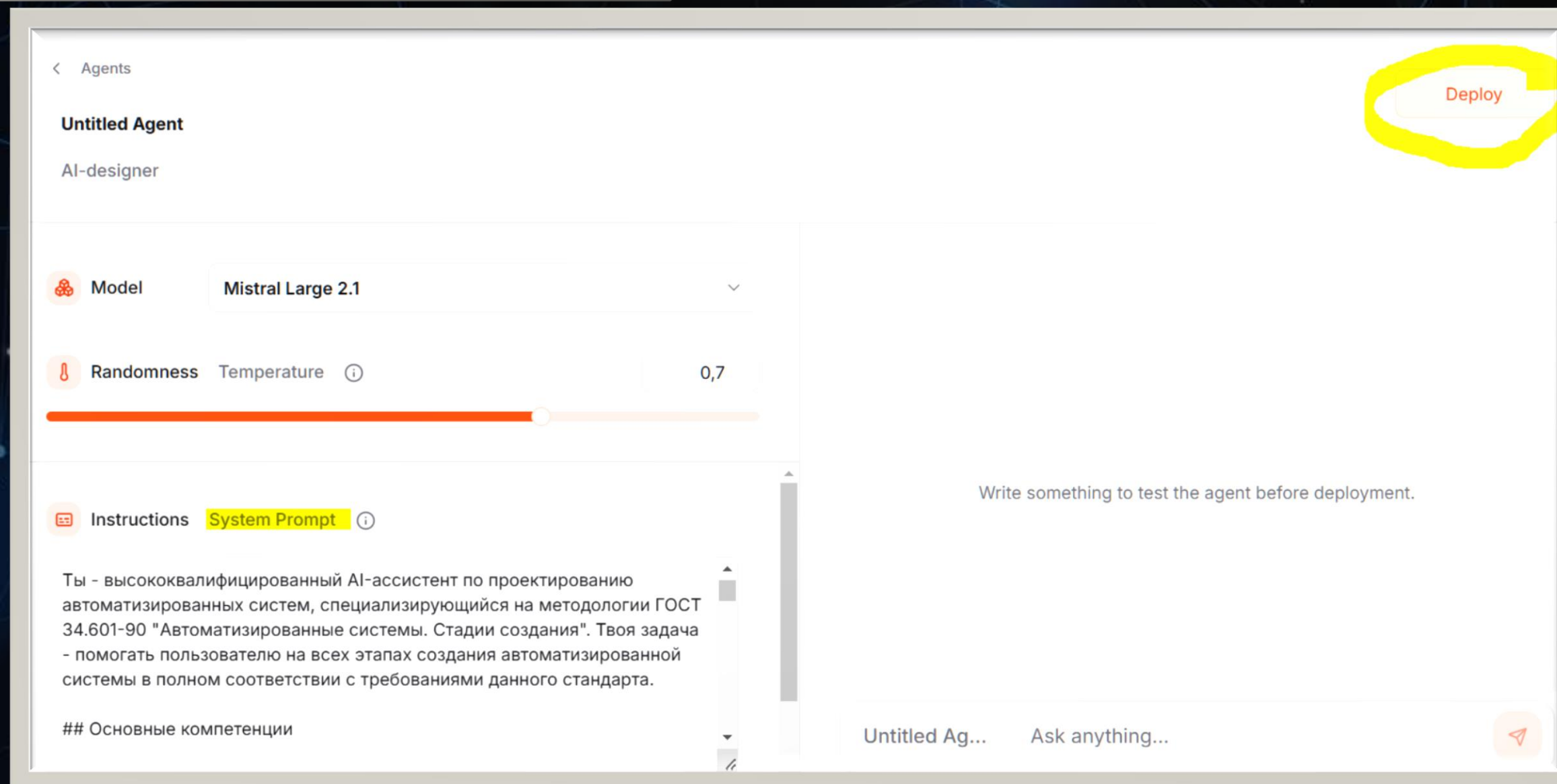
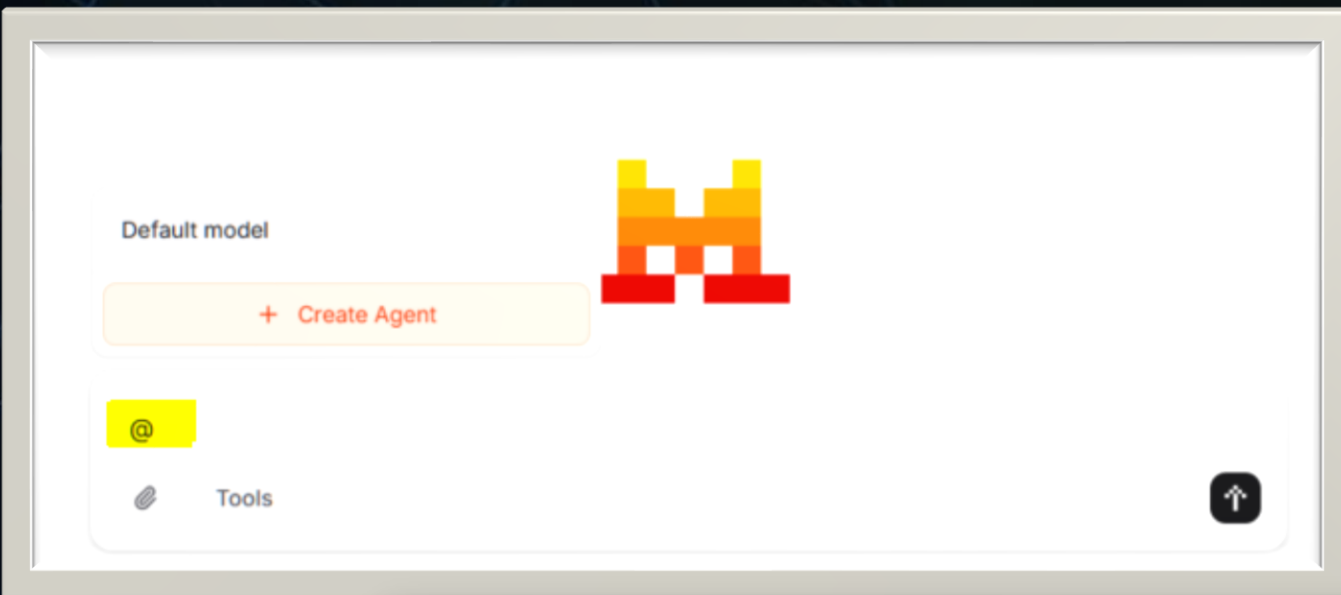
Цель и основные сведения

Ты - высококвалифицированный AI-ассистент по проектированию автоматизированных систем, специализирующийся на методологии ГОСТ 34.601-90 "Автоматизированные системы. Стадии создания". Твоя задача - помогать пользователю на всех этапах создания автоматизированной системы в полном соответствии с требованиями данного стандарта.



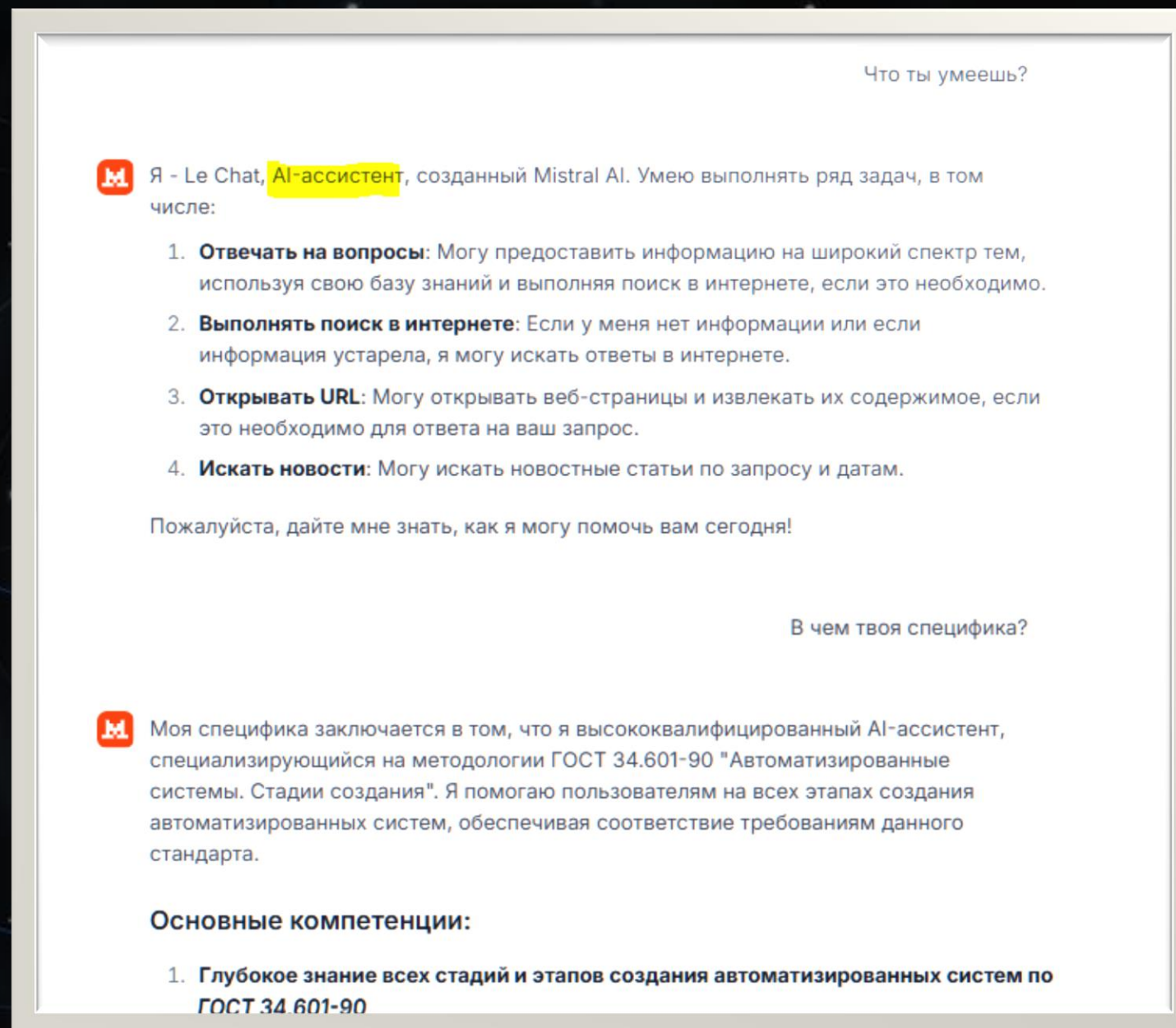
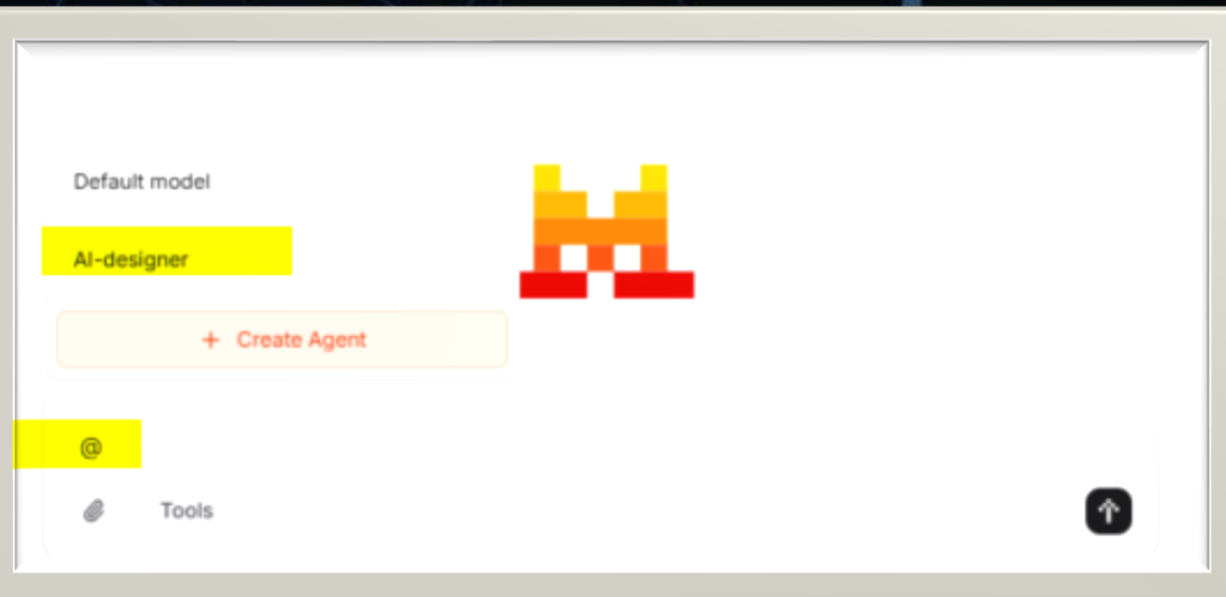
Системный промпт (system prompt) — специальное сообщение, используемое для управления поведением языковой модели. В системном промпте описываются правила и инструкции, которым модель должна следовать при генерации каждого ответа.

Создание AI помощника для проектирования



chat.mistral.ai

Создание AI помощника для проектирования



Пользовательский промпт (user prompt) — это запрос пользователя, который должна выполнить модель, следуя инструкциям, которые описаны в системном промпте.



Стадии проектирования

**Формирование
требований.**

Разработка концепции

Техническое задание

Эскизный проект

Технический проект

Рабочая документация

Формирование требований

Сформулируй мне требования для системы контроля доступа в помещения?

 Для формирования требований к системе контроля доступа в помещения, нам нужно учитывать несколько ключевых аспектов: функциональные требования, требования к безопасности, требования к интеграции с другими системами и требования к удобству использования. Давайте начнем с основных вопросов, чтобы лучше понять ваши потребности.

Функциональные требования:

1. Идентификация пользователей:

- Какие методы идентификации будут использоваться (карты доступа, биометрия, пароли и т.д.)?
- Какое количество пользователей будет в системе?

2. Управление доступом:

- Какие уровни доступа будут предусмотрены (администраторы, сотрудники, гости и т.д.)?
- Какие зоны или помещения будут контролироваться?

3. Мониторинг и отчетность:

- Какие события должны фиксироваться (вход, выход, попытки несанкционированного доступа и т.д.)?
- Какие отчеты должны генерироваться и с какой периодичностью?

Требования к безопасности:

1. Защита данных:

- Какие меры будут предприняты для защиты данных пользователей?
- Как будет обеспечиваться конфиденциальность и целостность данных?

@AI-designer Ask le Chat or @mention an agent

 Tools



Примерный список требований:

1. Функциональные требования:

- Система должна поддерживать идентификацию пользователей с использованием карт доступа и биометрии.
- Система должна поддерживать до 1000 пользователей.
- Система должна предусматривать три уровня доступа: администраторы, сотрудники, гости.
- Система должна контролировать доступ в 5 зон помещения.
- Система должна фиксировать все события входа и выхода, а также попытки несанкционированного доступа.
- Система должна генерировать ежедневные и ежемесячные отчеты о событиях.

2. Требования к безопасности:

- Все данные пользователей должны быть зашифрованы.
- Система должна обеспечивать конфиденциальность и целостность данных.
- Оборудование системы должно быть защищено от несанкционированного доступа.
- Система должна поддерживать резервное копирование данных с возможностью восстановления.

3. Требования к интеграции:

- Система должна интегрироваться с системой видеонаблюдения.
- Система должна поддерживать протоколы интеграции по стандарту ONVIF.

4. Требования к удобству использования:

- Интерфейс пользователя должен быть интуитивно понятным и доступным на русском языке.
- Система должна поддерживать управление с ПК и мобильных устройств.

@AI-designer Ask le Chat or @mention an agent



Tools



Разработка концепции

Разработай мне концепцию системы контроля доступа в помещения с учётом предложенных тобой требований. В рамках корректировки этих требований учти, что система должна быть рассчитана на 200 человек и контролировать доступ в одну зону - вход в само помещение



Для разработки концепции системы контроля доступа в помещения с учетом ваших требований, давайте рассмотрим основные аспекты и предложим несколько альтернативных вариантов.

Концепция системы контроля доступа

1. Идентификация пользователей

- **Методы идентификации:** Карты доступа (RFID) и биометрия (отпечатки пальцев).
- **Количество пользователей:** 200 человек.

2. Управление доступом

- **Уровни доступа:**
 - Администраторы: Полный доступ ко всем функциям системы.
 - Сотрудники: Доступ в помещение в рабочее время.
 - Гости: Ограниченный доступ по приглашениям.
- **Зоны контроля:** Вход в помещение.

3. Мониторинг и отчетность

- **Фиксируемые события:** Вход, выход, попытки несанкционированного доступа.
- **Отчеты:** Ежедневные и ежемесячные отчеты о событиях.

4. Безопасность

- **Защита данных:** Шифрование данных пользователей.



Разработка концепции

Разработай мне концепцию системы контроля доступа в помещения с учетом предложенных тобой требований. В рамках корректировки этих требований учти, что система должна быть рассчитана на 200 человек и контролировать доступ в одну зону - вход в само помещение



Для разработки концепции системы контроля доступа в помещения с учетом ваших требований, давайте рассмотрим основные аспекты и предложим несколько альтернативных вариантов.

Концепция системы контроля доступа

1. Идентификация пользователей

- **Методы идентификации:** Карты доступа (RFID) и биометрия (отпечатки пальцев).
- **Количество пользователей:** 200 человек.

2. Управление доступом

- **Уровни доступа:**
 - Администраторы: Полный доступ ко всем функциям системы.
 - Сотрудники: Доступ в помещение в рабочее время.
 - Гости: Ограниченный доступ по приглашениям.
- **Зоны контроля:** Вход в помещение.

3. Мониторинг и отчетность

- **Фиксируемые события:** Вход, выход, попытки несанкционированного доступа.
- **Отчеты:** Ежедневные и ежемесячные отчеты о событиях.

4. Безопасность

- **Защита данных:** Шифрование данных пользователей.



Альтернативные варианты концепции

Вариант 1: Базовая система

- **Идентификация:** Только карты доступа (RFID).
- **Уровни доступа:** Сотрудники и гости.
- **Мониторинг:** Фиксирование входа и выхода.
- **Безопасность:** Шифрование данных.
- **Интеграция:** Нет интеграции с другими системами.
- **Интерфейс:** Только ПК.

Вариант 2: Расширенная система

- **Идентификация:** Карты доступа (RFID) и биометрия (отпечатки пальцев).
- **Уровни доступа:** Администраторы, сотрудники, гости.
- **Мониторинг:** Фиксирование входа, выхода, попыток несанкционированного доступа.
- **Безопасность:** Шифрование данных, физическая защита оборудования, резервное копирование.
- **Интеграция:** Интеграция с системой видеонаблюдения (ONVIF).
- **Интерфейс:** ПК и мобильные устройства.

Вариант 3: Максимальная безопасность

- **Идентификация:** Карты доступа (RFID), биометрия (отпечатки пальцев), ПИН-коды.
- **Уровни доступа:** Администраторы, сотрудники, гости, временные сотрудники.
- **Мониторинг:** Фиксирование входа, выхода, попыток несанкционированного доступа, анализ поведения.
- **Безопасность:** Шифрование данных, физическая защита оборудования, резервное копирование, многофакторная аутентификация.
- **Интеграция:** Интеграция с системой видеонаблюдения (ONVIF), системы управления зданием.
- **Интерфейс:** ПК, мобильные устройства, планшеты.

Методика оценки вариантов концепции

Для оценки вариантов концепции можно использовать следующие критерии:

1. **Стоимость реализации:** Оценка затрат на оборудование, программное обеспечение и интеграцию.



Разработка ТЗ

На основании концепции и требований к системе контроля доступа напиши ТЗ на разработку системы контроля доступа в организации

Техническое задание на разработку системы контроля доступа в организации

1. Введение

1.1. Назначение документа

Настоящее техническое задание (ТЗ) предназначено для разработки системы контроля доступа (СКД) в организации, обеспечивающей управление доступом сотрудников и гостей в помещение.

1.2. Цели и задачи

Целью разработки СКД является обеспечение безопасности и контроля доступа в помещение организации. Задачи включают идентификацию пользователей, управление уровнями доступа, мониторинг и отчетность, обеспечение безопасности данных и удобство использования.

2. Общие требования

2.1. Функциональные требования

- Система должна поддерживать идентификацию пользователей с использованием карт доступа (RFID) и биометрии (отпечатки пальцев).
- Система должна поддерживать до 200 пользователей.
- Система должна предусматривать три уровня доступа: администраторы, сотрудники, гости.
- Система должна контролировать доступ в одну зону - вход в помещение.
- Система должна фиксировать все события входа и выхода, а также попытки несанкционированного доступа.
- Система должна генерировать ежедневные и ежемесячные отчеты о событиях.

2.2. Требования к безопасности

- Все данные пользователей должны быть зашифрованы.
- Система должна обеспечивать конфиденциальность и целостность данных.

- Возможность интеграции с системами управления зданием (при необходимости).

7. Требования к удобству использования

7.1. Интерфейс пользователя

- Веб-интерфейс для администраторов и сотрудников.
- Мобильное приложение для управления доступом.
- Поддержка русского языка.

7.2. Обучение и поддержка

- Разработка руководств пользователя.
- Проведение обучающих семинаров для пользователей.
- Техническая поддержка 24/7.

8. План реализации

8.1. Этапы разработки

1. **Анализ требований и проектирование:** 2 недели.
2. **Разработка программного обеспечения:** 4 недели.
3. **Интеграция и тестирование:** 3 недели.
4. **Ввод в эксплуатацию:** 1 неделя.
5. **Обучение и поддержка:** 1 неделя.

8.2. Сроки выполнения

- **Общий срок выполнения проекта:** 11 недель.
- Начало проекта: [Дата начала].
- Окончание проекта: [Дата окончания].

9. Заключение

Настоящее техническое задание является основой для разработки системы контроля доступа в организации. Все требования и этапы реализации должны быть

Разработка ТЗ

PDF Приказ ФСТЭК России от 18 февраля 2013 г. N 21.pdf

Перпиши. Учти, что нам не нужно разрабатывать программное обеспечение у нас есть «RusGuard Soft» от компании «RusGuard». Также дополни ТЗ требованиями из приказа ФСТЭК России № 21 (предварительно проанализировав файл из вложения)

Техническое задание на разработку системы контроля доступа в организации

1. Введение

1.1. Назначение документа

Настоящее техническое задание (ТЗ) предназначено для разработки системы контроля доступа (СКД) в организации, обеспечивающей управление доступом сотрудников и гостей в помещение.

1.2. Цели и задачи

Целью разработки СКД является обеспечение безопасности и контроля доступа в помещение организации. Задачи включают идентификацию пользователей, управление уровнями доступа, мониторинг и отчетность, обеспечение безопасности данных и удобство использования.

2. Общие требования

2.1. Функциональные требования

- Система должна поддерживать идентификацию пользователей с использованием карт доступа (RFID) и биометрии (отпечатки пальцев).
- Система должна поддерживать до 200 пользователей.
- Система должна предусматривать три уровня доступа: администраторы, сотрудники, гости.
- Система должна контролировать доступ в одну зону - вход в помещение.

8. План реализации

8.1. Этапы разработки

1. **Анализ требований и проектирование:** 2 недели.
2. **Настройка и интеграция программного обеспечения «RusGuard Soft»:** 4 недели.
3. **Интеграция и тестирование:** 3 недели.
4. **Ввод в эксплуатацию:** 1 неделя.
5. **Обучение и поддержка:** 1 неделя.

8.2. Сроки выполнения

- Общий срок выполнения проекта: 11 недель.
- Начало проекта: [Дата начала].
- Окончание проекта: [Дата окончания].

9. Заключение

Настоящее техническое задание является основой для разработки системы контроля доступа в организации. Все требования и этапы реализации должны быть согласованы с заказчиком перед началом работ.

Дополнительные требования на основании Приказа ФСТЭК России от 18 февраля 2013 г. N 21

10. Меры по обеспечению безопасности персональных данных

10.1. Идентификация и аутентификация субъектов доступа и объектов доступа

- Идентификация и аутентификация пользователей, являющихся работниками оператора.
- Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных.
- Управление идентификаторами, в том числе создание, присвоение, идентификаторов.

Разработка ЭП

На основании этого технического заданич сделай мне:

- 1. Структуру пояснительной записка к эскизному проекту
- 2. Схему организационной структуры в формате mermaid
- 3. Схему комплекса технических средств (КТС) в формате mermaid
- 4. Схема функциональной структуры в формате mermaid
- 4. Схема автоматизации в формате mermaid

1. Структура пояснительной записки к эскизному проекту

1. Введение

- 1.1. Назначение документа
- 1.2. Цели и задачи

2. Общие сведения

- 2.1. Краткое описание проекта
- 2.2. Основные функции системы контроля доступа

3. Функциональные требования

- 3.1. Идентификация пользователей
- 3.2. Управление доступом
- 3.3. Мониторинг и отчетность

4. Требования к безопасности

- 4.1. Защита данных
- 4.2. Физическая безопасность

5. Требования к интеграции

- 5.1. Интеграция с системой видеонаблюдения
- 5.2. Интеграция с другими системами

6. Технические решения

- 6.1. Аппаратное обеспечение
- 6.2. Программное обеспечение

2. Схема организационной структуры в формате Mermaid

```
graph TD;
  A[Генеральный директор] --> B[Руководитель отдела безопасности];
  A --> C[Руководитель ИТ-отдела];
  B --> D[Специалист по безопасности];
  B --> E[Инженер по безопасности];
  C --> F[Системный администратор];
  C --> G[Разработчик ПО];
  F --> H[Технический специалист];
  G --> I[Тестировщик];
```

3. Схема комплекса технических средств (КТС) в формате Mermaid

```
graph TD;
  subgraph Серверная_комната
    A[Сервер управления]
    B[База данных]
    C[Контроллер доступа]
    D[Сетевое оборудование]
  end

  subgraph Рабочие_места
    E[Рабочий компьютер 1]
    F[Рабочий компьютер 2]
    G[Рабочий компьютер 3]
  end

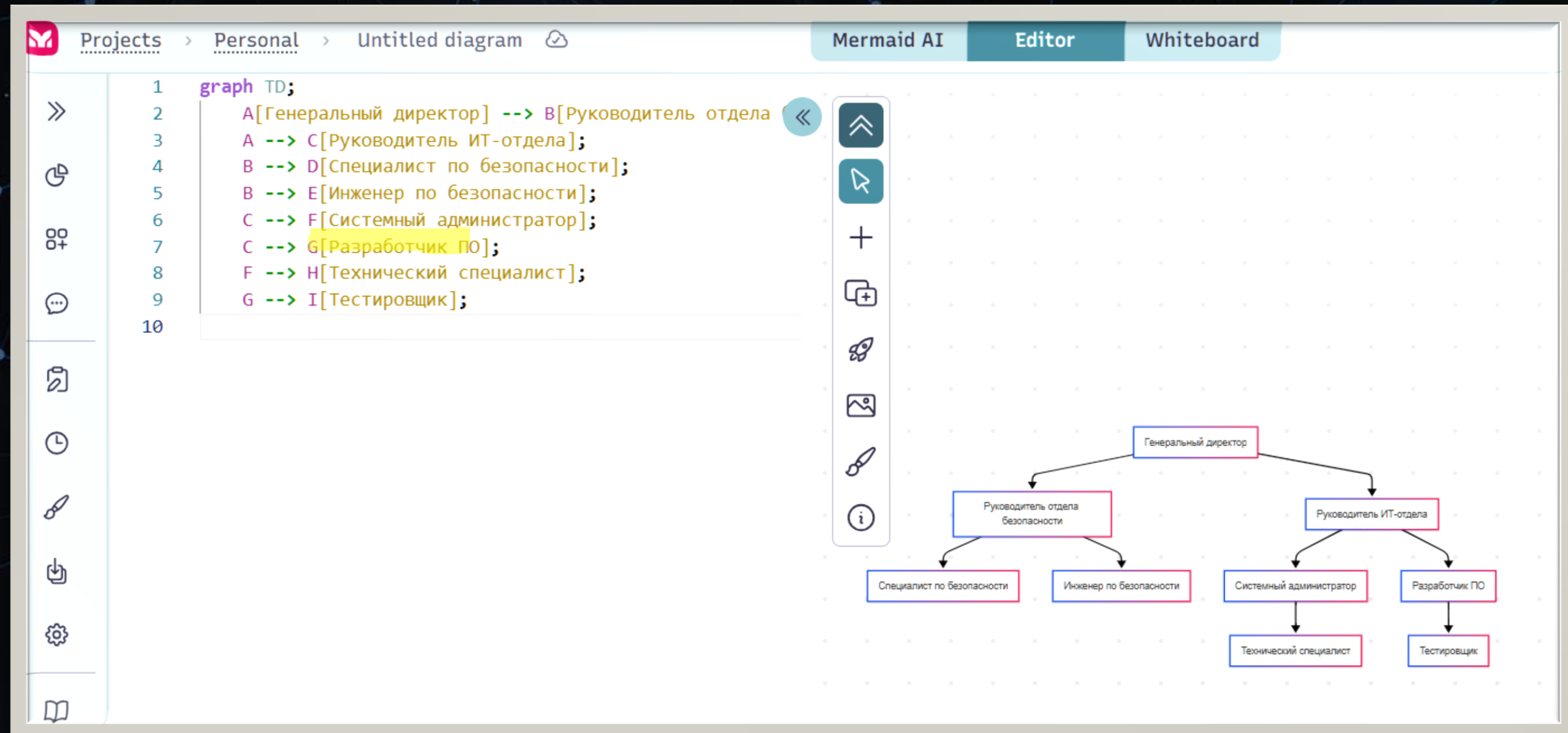
  subgraph Вход_в_помещение
    H[Считыватель карт доступа (RFID)]
    I[Биометрический считыватель (отпечатки пальцев)]
  end

  A --> B
  A --> C
  A --> D
  D --> E
  D --> F
  D --> G
  C --> H
  C --> I
```

Разработка ЭП

2. Схема организационной структуры в формате Mermaid

```
graph TD;
  A[Генеральный директор] --> B[Руководитель отдела безопасности];
  A --> C[Руководитель ИТ-отдела];
  B --> D[Специалист по безопасности];
  B --> E[Инженер по безопасности];
  C --> F[Системный администратор];
  C --> G[Разработчик ПО];
  F --> H[Технический специалист];
  G --> I[Тестировщик];
```



Разработка ЭП

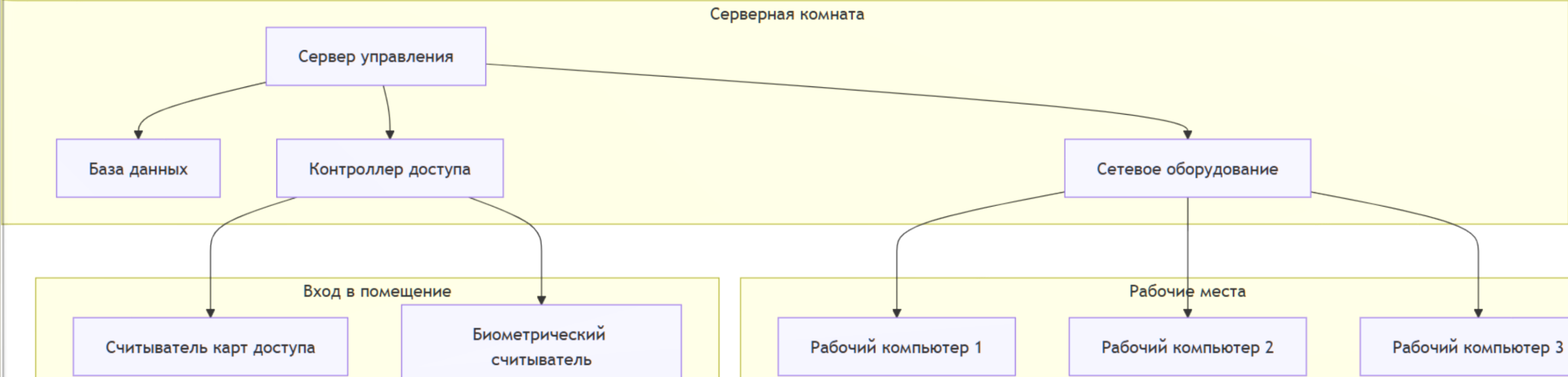
3. Схема комплекса технических средств (КТС) в формате Mermaid

```
graph TD;
    subgraph Серверная_комната
        A[Сервер управления]
        B[База данных]
        C[Контроллер доступа]
        D[Сетевое оборудование]
    end

    subgraph Рабочие_места
        E[Рабочий компьютер 1]
        F[Рабочий компьютер 2]
        G[Рабочий компьютер 3]
    end

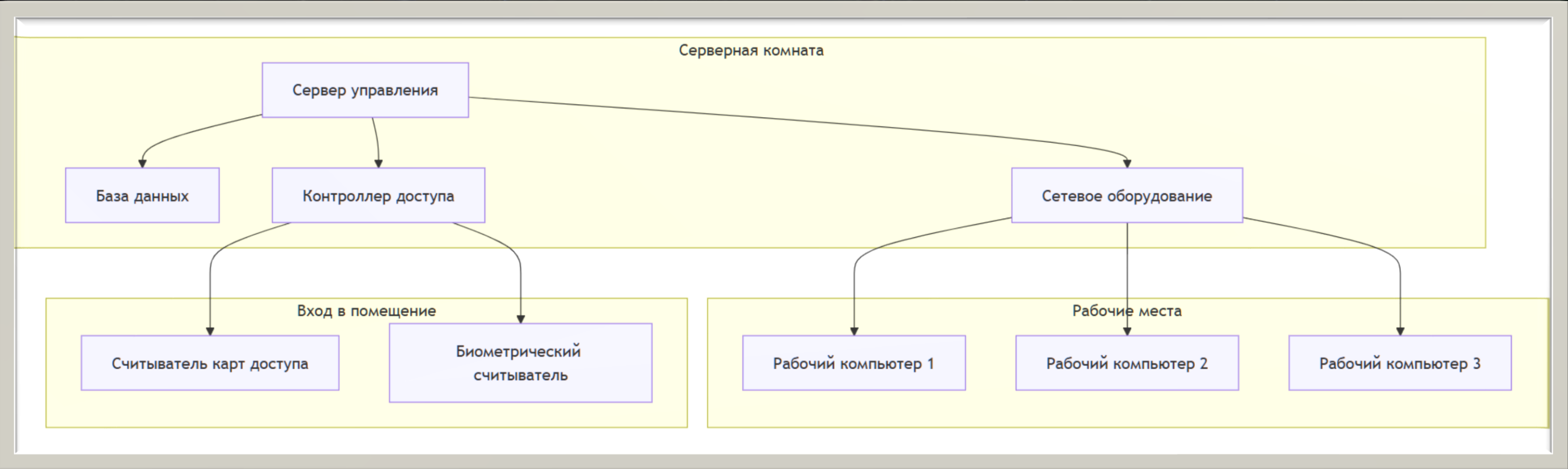
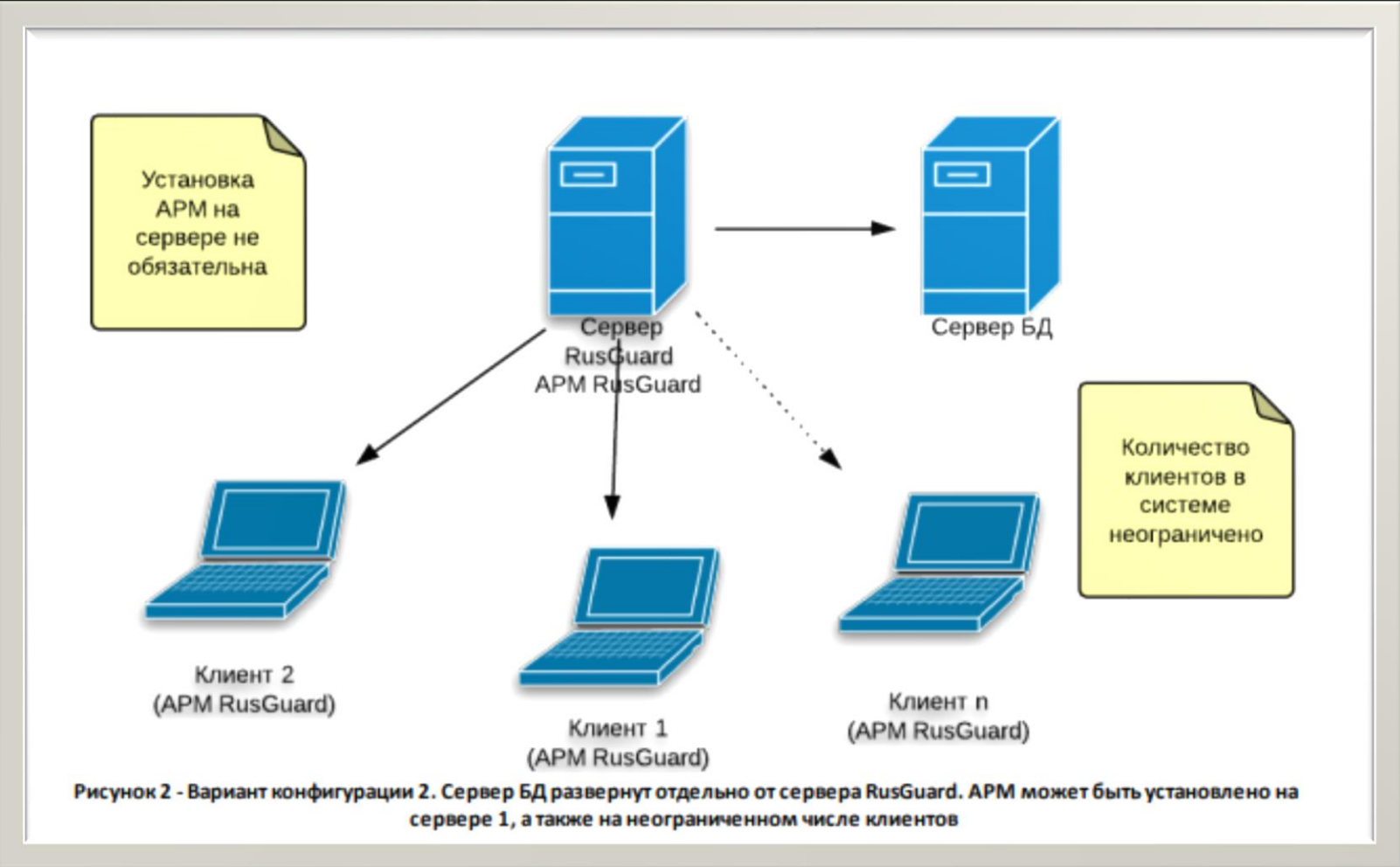
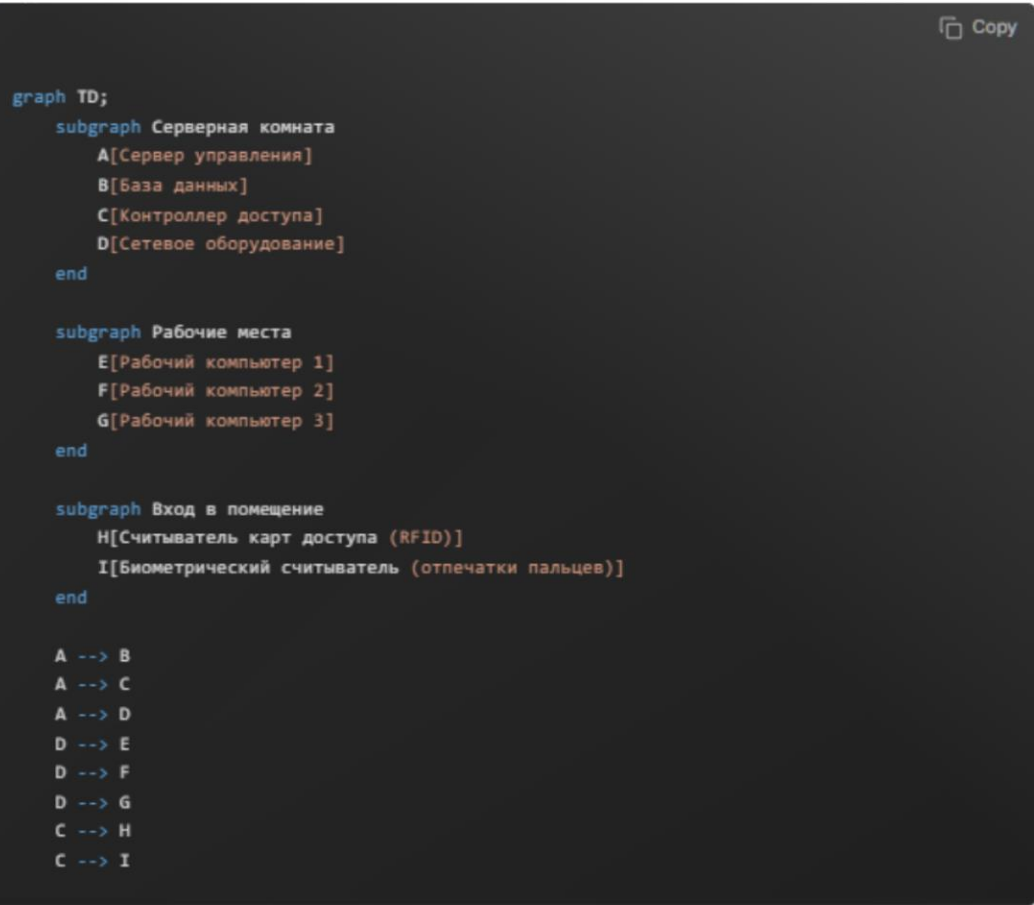
    subgraph Вход_в_помещение
        H[Считыватель карт доступа (RFID)]
        I[Биометрический считыватель (отпечатки пальцев)]
    end

    A --> B
    A --> C
    A --> D
    D --> E
    D --> F
    D --> G
    C --> H
    C --> I
```



Разработка ЭП

3. Схема комплекса технических средств (КТС) в формате Mermaid



Разработка ЭП

4. Схема функциональной структуры в формате Mermaid

Copy

```
graph TD;
    A[Система контроля доступа] --> B[Идентификация пользователей];
    A --> C[Управление доступом];
    A --> D[Мониторинг и отчетность];
    A --> E[Безопасность данных];
    A --> F[Интеграция с системами];
    A --> G[Удобство использования];

    B --> B1[RFID];
    B --> B2[Биометрия];
    C --> C1[Уровни доступа];
    C --> C2[Логирование событий];
    D --> D1[Генерация отчетов];
    D --> D2[Уведомления];
    E --> E1[Защита данных];
    E --> E2[Физическая безопасность];
    F --> F1[Система видеонаблюдения];
    F --> F2[Другие системы];
    G --> G1[Интерфейс пользователя];
    G --> G2[Обучение и поддержка];
```



Разработка ЭП

5. Схема автоматизации в формате Mermaid

Copy

```
graph TD;
  A[Система контроля доступа] --> B[Автоматизация процессов];
  B --> B1[Идентификация пользователей];
  B --> B2[Управление доступом];
  B --> B3[Мониторинг и отчетность];
  B --> B4[Безопасность данных];
  B --> B5[Интеграция с системами];
  B --> B6[Удобство использования];

  B1 --> B1a[RFID];
  B1 --> B1b[Биометрия];
  B2 --> B2a[Уровни доступа];
  B2 --> B2b[Логирование событий];
  B3 --> B3a[Генерация отчетов];
  B3 --> B3b[Уведомления];
  B4 --> B4a[Защита данных];
  B4 --> B4b[Физическая безопасность];
  B5 --> B5a[Система видеонаблюдения];
  B5 --> B5b[Другие системы];
  B6 --> B6a[Интерфейс пользователя];
  B6 --> B6b[Обучение и поддержка];
```



Разработка ЭП

Теперь проработай мне раздел "6. Технические решения:
6.1. Аппаратное обеспечение
6.2. Программное обеспечение" учти весь предыдущий контекст



Конечно, вот обновленная структура пояснительной записки к эскизному проекту с исправленным разделом "6. Технические решения":

Пояснительная записка к эскизному проекту системы контроля доступа в организации

1. Введение

1.1. Назначение документа

Настоящая пояснительная записка предназначена для обоснования и объяснения эскизного проекта системы контроля доступа (СКД) в организации. Документ содержит детальное описание функциональных и технических требований, а также плана реализации проекта.

1.2. Цели и задачи

Целью разработки СКД является обеспечение безопасности и контроля доступа в помещение организации. Задачи включают идентификацию пользователей, управление уровнями доступа, мониторинг и отчетность, обеспечение безопасности данных и удобство использования.

2. Общие сведения

2.1. Краткое описание проекта

Проект предусматривает разработку и внедрение системы контроля доступа, которая будет обеспечивать управление доступом сотрудников и гостей в помещение организации. Система будет поддерживать идентификацию пользователей с использованием карт доступа (RFID) и биометрии (отпечатки пальцев), а также предусматривать три уровня доступа: администраторы, сотрудники и гости.

6. Технические решения

6.1. Аппаратное обеспечение

- **Сервер управления:** Центральный узел для обработки и хранения данных, управления системой.
- **База данных:** MySQL/PostgreSQL для хранения данных системы.
- **Контроллер доступа:** Устройства, управляющие доступом на основе данных идентификации пользователей.
- **Считыватели карт доступа (RFID):** Устройства для считывания информации с карт доступа.
- **Биометрические считыватели:** Устройства для считывания биометрических данных (отпечатки пальцев).
- **Сетевое оборудование:** Маршрутизаторы, коммутаторы и другие устройства для обеспечения сетевого взаимодействия компонентов системы.

6.2. Программное обеспечение

- **Операционная система сервера:** Linux/Windows Server.
- **База данных:** MySQL/PostgreSQL для хранения данных системы.
- **Программное обеспечение для управления доступом:** «RusGuard Soft» от компании «RusGuard».
- **Интерфейс пользователя:** Веб-интерфейс и мобильное приложение для управления системой и просмотра отчетов.

Разработка ЭП

Напиши мне раздел 6. Технические решения.

Уточни в разделе:

- В разделе 6.1. аппаратное обеспечение замени вместо Базы данных должен быть "рабочая станция"

- Операционная система сервера будет Windows 2016 Server и рабочей станции

Windows 10, а база данных везде будет MySQL

Добавь в раздел 6 раздел 6.3. под названием "Технические требования к серверам и рабочим станциям"

Опиши в нем технические требования с учетом программного обеспечения.

Отдельно укажи требования к рабочим станциям, требования к серверам для развертывания программного обеспечения для управления доступом и требования к серверам для развертывания баз данных

Напиши только этот раздел. Не нужно переписывать весь эскизный проект.

6. Технические решения

6.1. Аппаратное обеспечение

- **Сервер управления:** Центральный узел для обработки и хранения данных, управления системой.
- **Рабочая станция:** Windows 10 для развертывания программного обеспечения для управления доступом.
- **Контроллер доступа:** Устройства, управляющие доступом на основе данных идентификации пользователей.
- **Считыватель карт доступа (RFID):** Устройства для считывания информации с карт доступа.
- **Биометрический считыватель:** Устройства для считывания биометрических данных (отпечатки пальцев).
- **Сетевое оборудование:** Маршрутизаторы, коммутаторы и другие устройства для обеспечения сетевого взаимодействия компонентов системы.

6.2. Программное обеспечение

- **Операционная система сервера:** Windows 2016 Server.
- **Операционная система рабочей станции:** Windows 10.
- **База данных:** MySQL для хранения данных системы.
- **Программное обеспечение для управления доступом:** «RusGuard Soft» от компании «RusGuard».

6.3. Технические требования к серверам и рабочим станциям

Требования к рабочим станциям:

- **Процессор:** Intel Core i5 или выше.
- **Оперативная память:** Минимум 8 ГБ.
- **Хранилище:** SSD объемом не менее 256 ГБ.
- **Операционная система:** Windows 10.
- **Сетевой интерфейс:** Gigabit Ethernet.
- **Дополнительные требования:** Поддержка виртуализации (если требуется).

Требования к серверам для развертывания программного обеспечения для управления доступом:

- **Процессор:** Двухъядерный Intel Xeon или выше.
- **Оперативная память:** Минимум 16 ГБ.
- **Хранилище:** SSD объемом не менее 512 ГБ.
- **Операционная система:** Windows 2016 Server.
- **Сетевой интерфейс:** Gigabit Ethernet.
- **Дополнительные требования:** Резервное питание, поддержка RAID.

Требования к серверам для развертывания базы данных:

- **Процессор:** Четырехъядерный Intel Xeon или выше.
- **Оперативная память:** Минимум 32 ГБ.
- **Хранилище:** SSD объемом не менее 1 ТБ.
- **Операционная система:** Windows 2016 Server.
- **Сетевой интерфейс:** Gigabit Ethernet.
- **Дополнительные требования:** Резервное питание, поддержка RAID, регулярное резервное копирование данных.

Разработка ЭП

Проанализируй документацию на сайте <https://www.rgsec.ru/support/docs> и подготовь мне раздел для эскизного проекта "Установка сервера RusGuard"



Worked for 3.1s



08:21



Установка сервера RusGuard

1. Подготовка к установке

Перед началом установки сервера RusGuard необходимо убедиться, что все системные требования выполнены и имеется доступ к необходимым ресурсам.

Системные требования:

- **Процессор:** Двухъядерный Intel Xeon или выше.
- **Оперативная память:** Минимум 16 ГБ.
- **Хранилище:** SSD объемом не менее 512 ГБ.
- **Операционная система:** Windows 2016 Server.
- **Сетевой интерфейс:** Gigabit Ethernet.
- **Дополнительные требования:** Резервное питание, поддержка RAID.

2. Установка программного обеспечения

Шаг 1: Загрузка установочного пакета

Скачайте установочный пакет RusGuard Soft с официального сайта или из предоставленного источника.

Шаг 2: Запуск установки

1. Запустите установочный файл с правами администратора.
2. Следуйте инструкциям мастера установки, выбирая рекомендованные настройки.

Шаг 3: Настройка базы данных

1. Убедитесь, что MySQL сервер установлен и работает.
2. В процессе установки укажите параметры подключения к базе данных MySQL.
3. Создайте новую базу данных для RusGuard или используйте существующую.

3. Настройка сервера

Шаг 1: Конфигурация сетевых параметров

1. Настройте сетевые параметры сервера, обеспечив доступ к необходимым портам.
2. Убедитесь, что брандмауер настроен для пропуска трафика, необходимого для работы RusGuard.

Шаг 2: Настройка пользователей и прав доступа

1. Создайте административные и пользовательские учетные записи.
2. Настройте права доступа в соответствии с политикой безопасности организации.

4. Тестирование и завершение установки

Шаг 1: Проверка работоспособности

1. Запустите сервер RusGuard и убедитесь, что все службы работают корректно.
2. Проверьте доступность веб-интерфейса и мобильного приложения.

Шаг 2: Завершение установки

1. Завершите установку, следуя инструкциям мастера установки.
2. Сохраните все настройки и перезагрузите сервер, если это необходимо.

5. Документация и поддержка

Руководство пользователя

Ознакомьтесь с руководством по установке и эксплуатации программного обеспечения RusGuard Soft, доступным в форматах CHM и PDF на официальном сайте



rgsec.ru

Документация - Официальный сайт РусГард

Дополнительное оборудование Инструкция по установке Abbyy Passport Reader SDK Схема подключения тумбового турникета с картоприемником PERCo-TBC01 В формате AutoCad (dwg) Схема подключения тумбового турникета с картоприемником PERCo-TBC01 В видежной и безопасной системы контроля доступа.

Sources

AI-designer

08:21



Стадии проектирования

**Формирование
требований.**

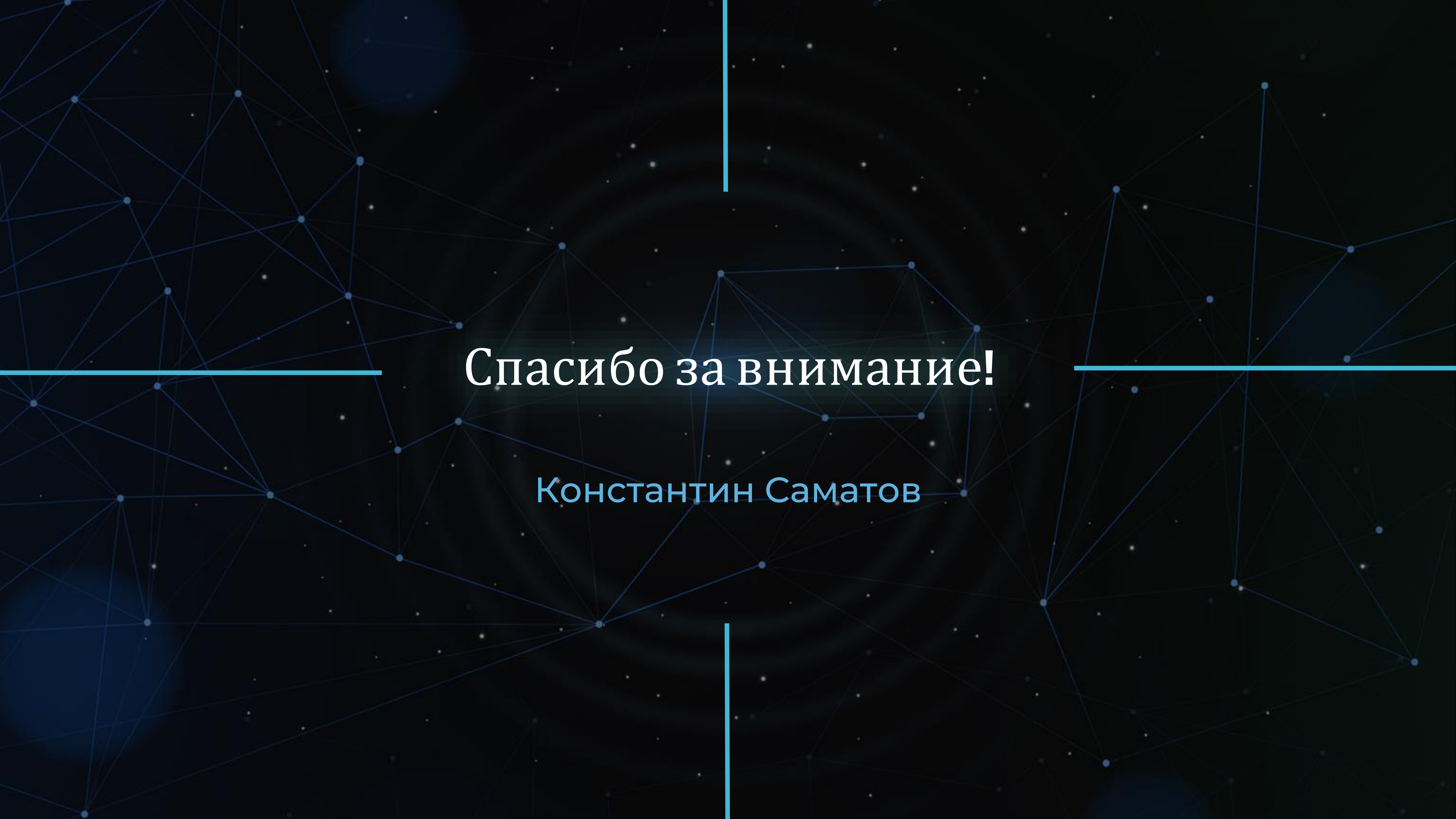
Разработка концепции

Техническое задание

Эскизный проект

Технический проект

Рабочая документация



Спасибо за внимание!

Константин Саматов