УДК 004.738.5

ПРОЕКТИРОВАНИЕ ВЕБ-ПРИЛОЖЕНИЯ «КОРПОРАТИВНЫЙ МЕССЕНДЖЕР»

Домбровский Я.А.
старший преподаватель
Калужский государственный университет им. К.Э. Циолковского, Калуга, Россия

Суходольский А.В.
студент
Калужский государственный университет им. К.Э. Циолковского, Калуга, Россия

Комаров К.А.
магистрант
Калужский государственный университет им. К.Э. Циолковского, Калуга, Россия

Аннотация.
В статье рассматривается проектирование веб-приложения корпоративного мессенджера как средства внутренней коммуникации сотрудников с акцентом на контролируемую безопасность и развёртывание на выделенной инфраструктуре предприятия. На основе анализа предметной области и приложений-аналогов сформулированы функциональные и нефункциональные требования: регистрация через администратора, аутентификация и авторизация, личные и групповые чаты, передача файлов, административные функции, простота интерфейса и кроссплатформенность. Предложены модели системы и ключевых бизнес-процессов обмена сообщениями и авторизации с использованием IDEF0, DFD и BPMN. Обоснован выбор технологического стека: серверная часть на

Python (Django/FastAPI), клиентская часть на React, обмен данными в реальном времени через WebSocket, хранение данных в СУБД PostgreSQL/MS SQL Server и применение сквозного шифрования (E2EE) для защиты содержания сообщений.

Ключевые слова: корпоративный мессенджер, веб-приложение, проектирование, IDEF0, DFD, BPMN, WebSocket, E2EE, React, Django, FastAPI, информационная безопасность.

DESIGN OF THE WEB APPLICATION "CORPORATE MESSENGER"

Dombrovsky Y.A.
Senior Lecturer
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia

Sukhodolskiy A.V.
Student
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia

Komarov K.A.
Master's student
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia

Abstract.
The paper addresses the design of a web-based corporate messenger intended for internal employee communications with an emphasis on controllable security and on-premise deployment. Based on domain analysis and existing solutions, the functional

and non-functional requirements are defined: administrator-driven registration, authentication and authorization, one-to-one and group chats, file transfer, administrative tools, usability, and cross-platform access. The system is described using IDEF0, BPMN, and DFD models. A technology stack is justified: Python backend (Django/FastAPI), React frontend, real-time data exchange via WebSocket, data storage in PostgreSQL/MS SQL Server, and end-to-end encryption (E2EE) to protect message content.
Keywords: corporate messenger, web application, system design, IDEF0, DFD, BPMN, WebSocket, E2EE, React, Django, FastAPI, information security.

Обмен сообщениями стал базовым механизмом коммуникации в организациях, особенно в условиях удалённой и гибридной работы. При использовании публичных мессенджеров часть корпоративного трафика обрабатывается инфраструктурой третьих сторон, что может противоречить требованиям по защите информации и внутренним регламентам [6]. Кроме того, при передаче сведений о работниках и клиентах необходимо учитывать требования законодательства о персональных данных [7]. Поэтому актуальным направлением является разработка корпоративных средств коммуникации, развёртываемых на инфраструктуре предприятия и обеспечивающих управляемую безопасность.

Цель работы – спроектировать веб-приложение «Корпоративный мессенджер», предназначенное для защищённого обмена сообщениями и файлами между сотрудниками организации. Стадийность проектирования и формирование технического задания соотнесены с требованиями комплекса стандартов ГОСТ 34 [1,2].

Корпоративный мессенджер ориентирован на рабочие коммуникации и отличается от массовых решений наличием организационного контроля: управляемая регистрация пользователей, разграничение прав доступа,

возможность размещения на собственных серверах и интеграции с корпоративными сервисами. Требования к контролю доступа и управлению рисками ИБ целесообразно формировать в логике СУИБ [3, 4].

К функциональным требованиям отнесены: регистрация пользователей через администратора, аутентификация и авторизация, личные и групповые чаты, передача файлов, просмотр истории сообщений, а также административные операции (управление пользователями и чатами).

К нефункциональным требованиям относятся: безопасность передачи и хранения данных (шифрование, контроль доступа, резервное копирование), удобство интерфейса, высокая скорость отклика и кроссплатформенность (работа в браузере на ПК и мобильных устройствах). Указанные меры согласуются с практиками управления информационной безопасностью и требованиями по защите персональных данных [3–5, 7].

Сравнение корпоративных решений-аналогов показывает востребованность следующих возможностей: групповые коммуникации и каналы, поиск по чатам, развитые права доступа, интеграции через API, а также расширения в виде ботов и конференцсвязи. В рамках проектирования целесообразно выделить минимально достаточное ядро (чаты, файлы, администрирование, безопасность) и предусмотреть расширяемость архитектуры (таблица 1).

Таблица 1 – Соответствие ключевых требований проектируемого мессенджера проектным решениям

Требование	**Проектное решение**
Контролируемая регистрация	Регистрация через администратора; ведение списка сотрудников.
Аутентификация и сессии	Проверка логина и пароля на сервере, выдача токена сессии.
Обмен в реальном времени	Двунаправленная доставка сообщений через WebSocket.
Защита содержания	Сквозное шифрование (E2EE) для сообщений/вложений.
Разграничение прав	Роли (администратор/пользователь), управление групповыми чатами.

Хранение и резервирование	СУБД PostgreSQL или MS SQL Server, регулярные бэкапы.
Кроссплатформенность	Веб-клиент на React; работа в современных браузерах.

Для формализации требований и описания функционирования мессенджера использованы нотации IDEF0 (функциональная модель) (рисунок 1 и 2), BPMN (моделирование бизнес-процессов) (рисунок 3) и DFD (потоки данных) (рисунок 4). Такой набор нотаций позволяет связать пользовательские сценарии с потоками данных и точками контроля безопасности (рисунок 1).

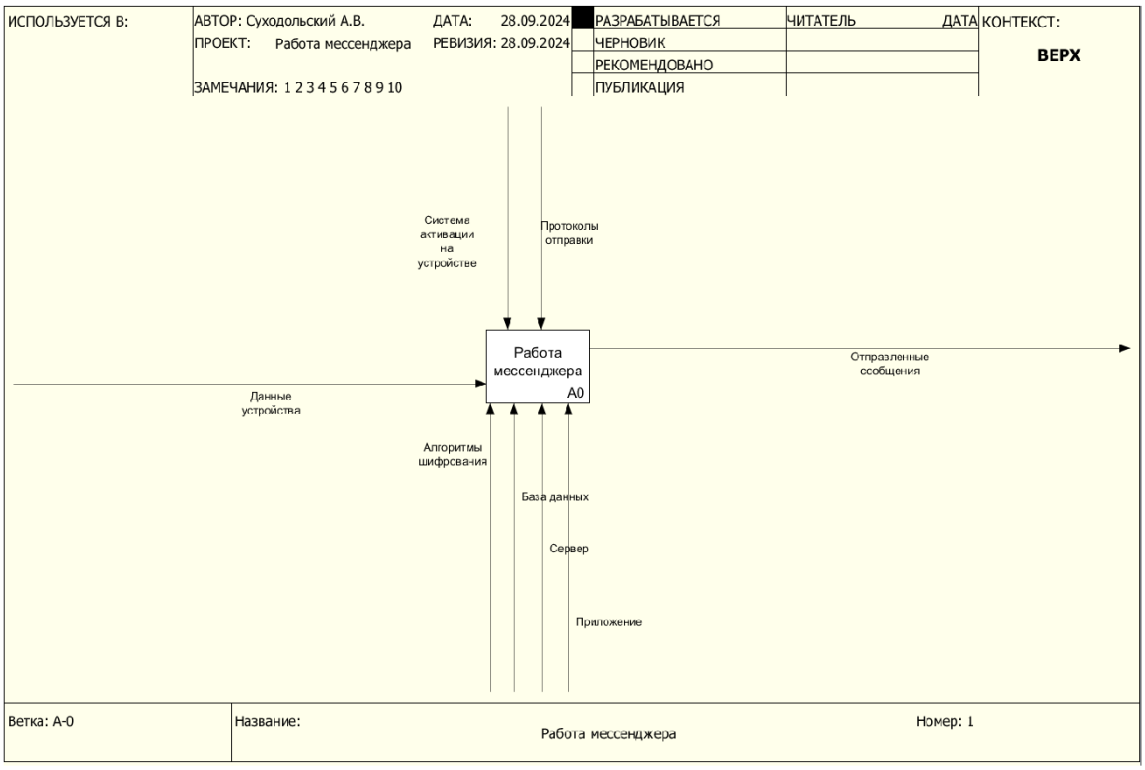

Рис. 1 – Контекстная диаграмма IDEF0 «Работа мессенджера» (составлено авторами)

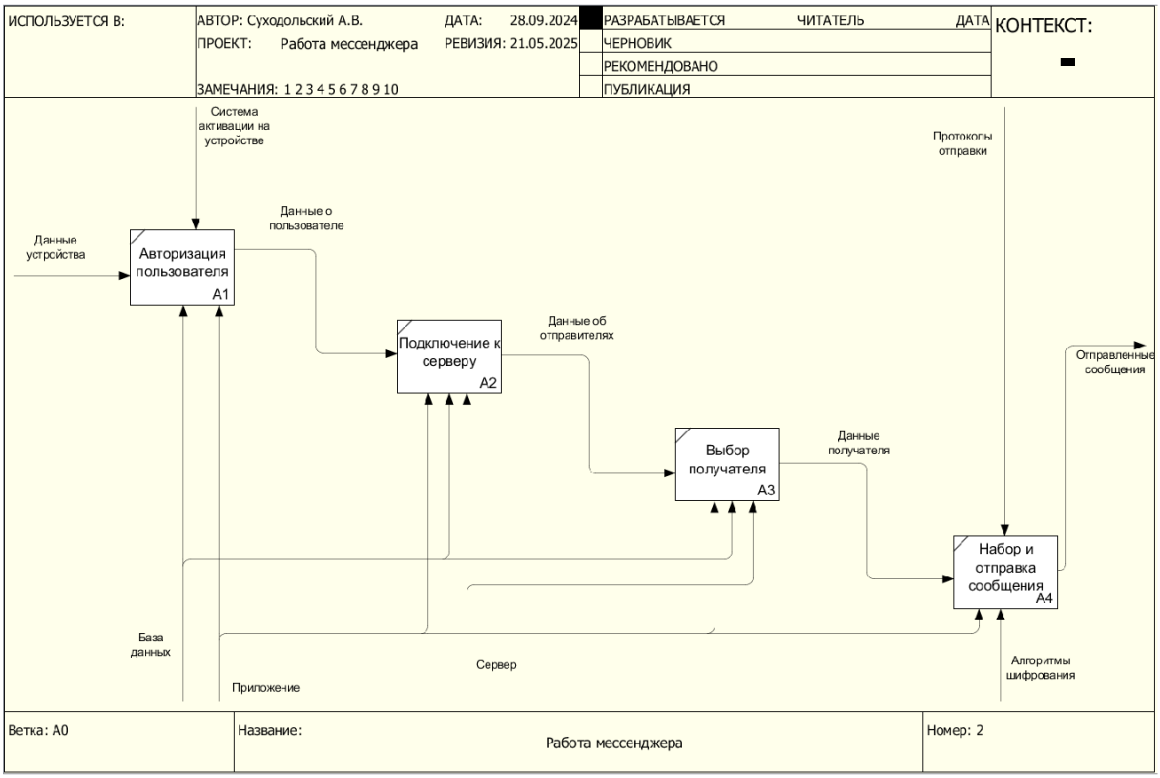

Рис. 2 – Декомпозиция IDEF0 процесса «Работа мессенджера» (составлено авторами)

Процесс авторизации описан в BPMN-диаграмме (рисунок 3). Пользователь вводит учётные данные, далее выполняется проверка логина и хэша пароля по данным базы. При успешной проверке формируется и возвращается токен сессии, при ошибке – сообщение об отказе. При реализации следует учитывать рекомендации по безопасному хранению паролей и ограничению попыток входа. Особое внимание уделяется обработке ошибок, ведению журналов событий и ограничению попыток входа в соответствии с требованиями к мерам защиты информации при обработке персональных данных в информационных системах [5].

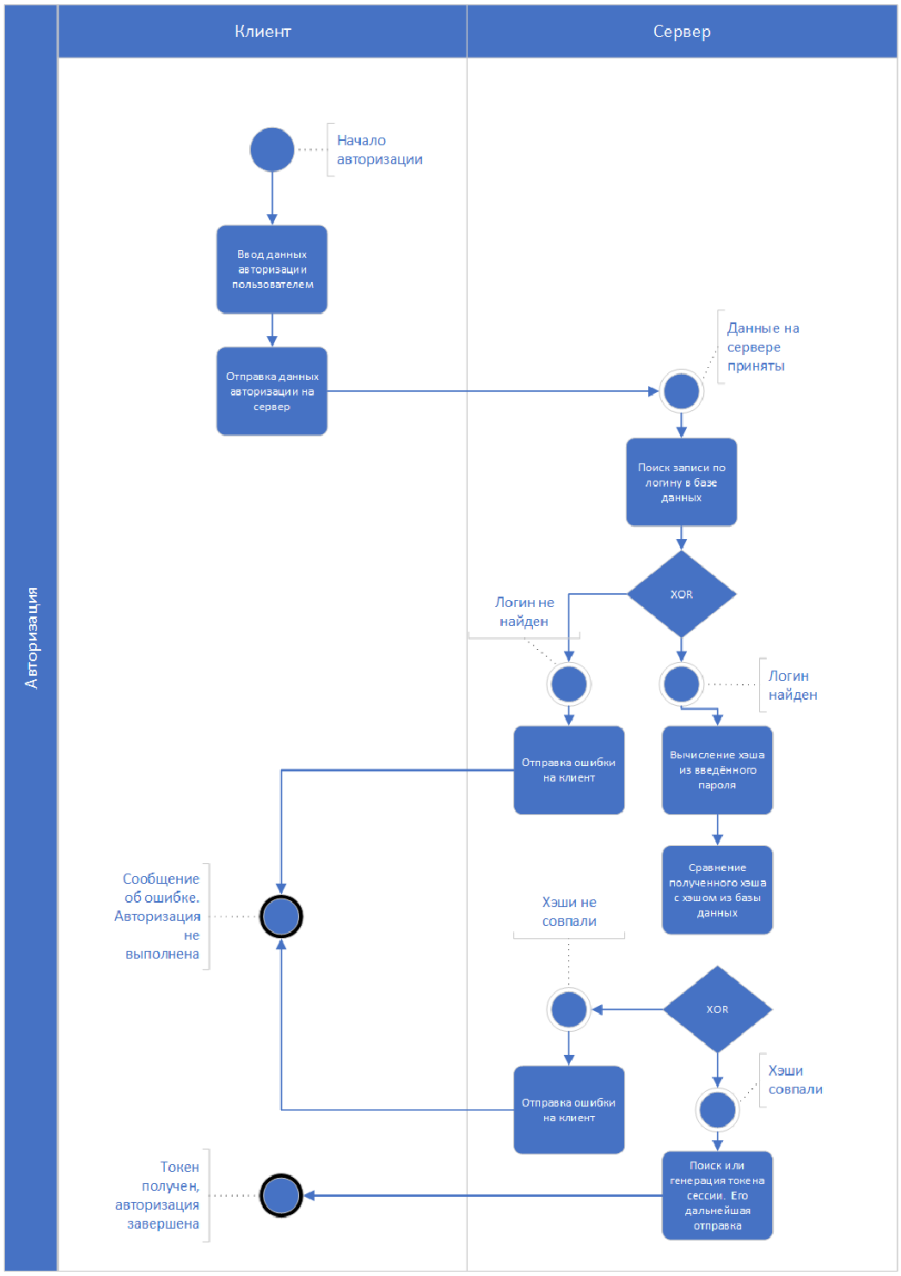

Рис. 3 – BPMN-модель процесса авторизации пользователя (составлено авторами)

Для определения состава хранилищ и интерфейсов взаимодействия клиента и сервера построена DFD-диаграмма (рисунок 4), отражающая регистрацию, авторизацию, получение списков чатов и обмен сообщениями. Модель используется при проектировании REST/WS API и структуры базы данных (таблицы пользователей, чатов, сообщений и вложений).

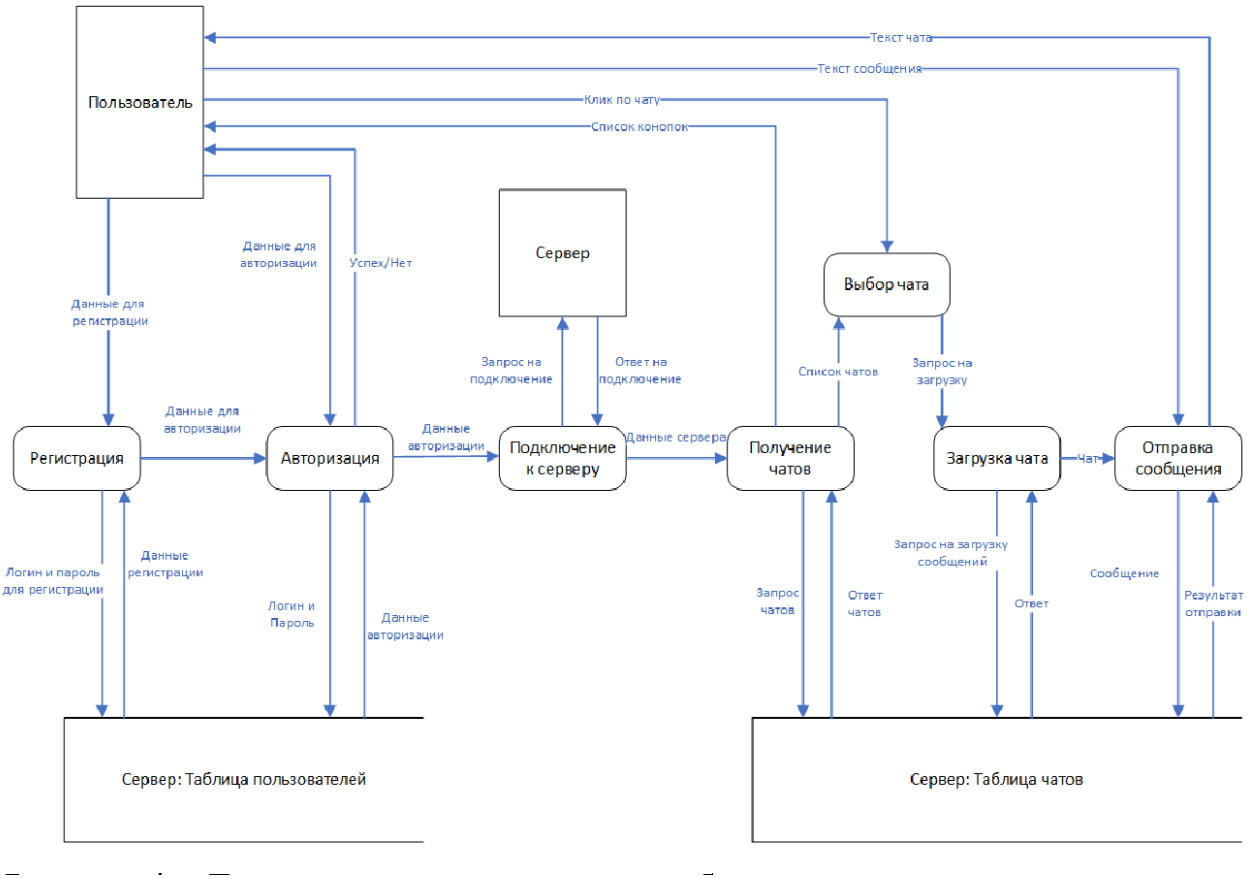

Рис. 4 – DFD-диаграмма потоков данных в корпоративном мессенджере (составлено авторами)

Архитектура проектируемого приложения строится по клиент-серверной модели. Веб-клиент обеспечивает интерфейс, управление состоянием диалогов и отправку запросов на сервер. Сервер реализует бизнес-логику, контроль прав доступа, доставку сообщений и хранение данных.

Серверную часть целесообразно реализовать на Python с использованием Django или FastAPI. Django предоставляет развитую экосистему и удобную административную панель, а FastAPI – высокую производительность и поддержку асинхронной обработки запросов. Клиентскую часть рационально реализовать на React как компонентном фреймворке, упрощающем построение интерактивных интерфейсов.

Для передачи сообщений в реальном времени предлагается использовать WebSocket-протокол, позволяющий поддерживать устойчивое двустороннее соединение между клиентом и сервером. Данные долговременного хранения (учётные записи, чаты, сообщения, метаданные файлов) размещаются в реляционной СУБД PostgreSQL или MS SQL Server. Для защиты конфиденциальности содержимого сообщений предусматривается применение сквозного шифрования (E2EE), при котором шифрование выполняется на стороне отправителя, а расшифрование — на стороне получателя. Организационные и технические меры защиты информации и персональных данных рекомендуется определять с опорой на ГОСТ Р ИСО/МЭК 27001–2021, ГОСТ Р ИСО/МЭК 27002–2021 и требования ФСТЭК России [3,4,5].

Интерфейс корпоративного мессенджера должен обеспечивать минимальную когнитивную нагрузку и предсказуемую навигацию. В проекте выделены следующие принципы: лаконичные UX-тексты, подсказки в местах потенциальной неоднозначности, единообразные иконки и визуальные паттерны, подтверждение необратимых действий (удаление сообщений или чатов). В качестве основных экранов предусматриваются: список диалогов/групп, область переписки, поле ввода сообщения, панель для прикрепления файлов, а также административная часть для управления пользователями и группами.

В работе выполнено проектирование веб-приложения «Корпоративный мессенджер»: сформулированы требования, проведён анализ решений-аналогов, построены модели IDEF0, BPMN и DFD, определены принципы интерфейса и выбран технологический стек. Полученные результаты формируют основу для реализации MVP и дальнейшего расширения функциональности (поиск по сообщениям, интеграции, боты, конференц-связь) при сохранении управляемой безопасности и возможности развёртывания на инфраструктуре предприятия.

Библиографический список:

1. ГОСТ 34.601–90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. – Текст : электронный. – URL: https://docs.cntd.ru/document/1200006921 (дата обращения: 20.12.2025).

2. ГОСТ 34.602–89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. – Текст : электронный. – URL: https://docs.cntd.ru/document/1200006924 (дата обращения: 21.12.2025).

3. ГОСТ Р ИСО/МЭК 27001–2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Текст : электронный. – URL: https://protect.gost.ru/document1.aspx?control=31&id=242006 (дата обращения: 18.12.2025).

4. ГОСТ Р ИСО/МЭК 27002–2021. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. – Текст : электронный. – URL: https://protect.gost.ru/document1.aspx?control=31&id=240766 (дата обращения: 20.12.2025).

5. Приказ ФСТЭК России от 18.02.2013 № 21. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. – Текст : электронный. – URL: https://www.consultant.ru/document/cons_doc_LAW_146520/ (дата обращения: 20.12.2025).

6. Федеральный закон от 27.07.2006 № 149-ФЗ. Об информации, информационных технологиях и о защите информации. – Текст : электронный. –

URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 20.12.2025).

7. Федеральный закон от 27.07.2006 № 152-ФЗ. О персональных данных. – Текст : электронный. – URL: https://pravo.gov.ru/proxy/ips/?docbody=&nd=102108261 (дата обращения: 18.12.2025).