Модель обеспечения информационной безопасности в мессенджерах, разрабатываемых на основе протокола Matrix

К.З. Билятдинов, С.И. Киселев, А.А. Петухова

***Аннотация* — представлены методологические и технологические решения по созданию защищенных децентрализованных мессенджеров для ведомственных и корпоративных систем связи.**

Предлагается модель обеспечения информационной безопасности в мессенджерах, разрабатываемых на основе открытого протокола Matrix, обеспечивающая сквозное шифрование коммуникаций, голосовую и видеосвязь, а также федеративное взаимодействие.

Модель реализована в виде модульной архитектуры, построенной на принципах микросервисов и контейнеризации, с использованием стека технологий, включающего Synapse, PostgreSQL, LiveKit, lk-jwt-service, Nginx и Docker Compose. Особенностью модели является ориентация на развертывание на периферийных сетевых устройствах под управлением OpenWRT, что обеспечивает полный контроль над инфраструктурой и исключает зависимость от внешних платформ.

Верификация соответствия требованиям информационной безопасности проведена в соответствии с ГОСТ Р 56939-2024. Практическая значимость работы подтверждена успешным развертыванием функционирующего прототипа, демонстрирующего устойчивую работу в различных условиях эксплуатации.

Основной положительный эффект заключается в существенном снижении трудоемкости развертывания и сопровождения мессенджера при обеспечении требований к конфиденциальности и суверенности функционирования.

***Ключевые слова* — децентрализованные мессенджеры, протокол Matrix, информационная безопасность, сквозное шифрование, контейнеризация, микросервисная архитектура, суверенные системы связи, OpenWRT.**

I. Введение

В современных условиях обеспечение информационной безопасности пользователей мессенджеров становится важнейшей задачей в связи с ростом требований к защите персональных коммерческих и профессиональных данных (врачебной, адвокатской и нотариальной тайны и других сведений) а также необходимостью предотвращения утечек критической информации и промышленного шпионажа. Дополнительный фактор риска связан с усложнением кибератак, нацеленных на компрометацию каналов коммуникации.

В связи с этим в процессе разработки мессенджеров особую значимость приобретают технологические решения по обеспечению отказоустойчивости и суверенности мессенджеров, функционирующих автономно от глобальных коммерческих платформ.

Отказоустойчивость — свойство системы сохранять полную или частичную работоспособность при отказах её элементов [1].

Суверенность решения подразумевает полный технологический и административный контроль над инфраструктурой, исключающий зависимость от внешних поставщиков [3].

Актуальность исследования определяется необходимостью разработки инновационных методологических, технических и технологических решений (далее – Решений) в сфере обеспечения сквозной конфиденциальности и аутентичности передаваемых данных в распределённых информационных системах в режиме реального времени. Под термином «сквозная конфиденциальность» (англ. End-to-End Confidentiality) понимается принцип защиты информации, при котором криптографическое преобразование данных выполняется на устройстве отправителя, а обратное преобразование — на устройстве получателя, что исключает возможность доступа к данным в открытом виде на промежуточных узлах [8].

Таким образом, комплексная научно-техническая задача заключается в создании инфраструктуры, гарантирующей бесперебойную и защищенную коммуникацию вне зависимости от внешних факторов. Решения данной задачи основываются на криптографии, теории связи и информационных систем.

В настоящее время наблюдается усиление актуальности исследований в этой предметной области, поскольку процессы тотальной цифровизации всех сфер общественной жизни, включая критическую информационную инфраструктуру, дистанционное образование и телемедицину, многократно увеличивают возможности для потенциальных кибератак, а сами

К.З. Билятдинов – д.т.н., профессор ГУАП (email: k74b@mail.ru).
С.И. Киселев – студент ГУАП (email: svyatoslavkiselev@yandex.ru).
А.А. Петухова – студент ГУАП (email: petukhova20040501@mail.ru).

коммуникационные платформы превращаются из инструмента общения в критически важный ресурс, отказ или компрометация которого влечёт значительные социально-экономические потери. Для корпоративных и ведомственных систем связи это трансформируется в требование полного контроля над каналом передачи данных и его максимальной устойчивости.

При этом эффективность функционирования мессенджеров в различных условиях напрямую зависит от рационального синтеза и корректной реализации трёх факторов:

1. Криптографической стойкости применяемых протоколов шифрования.
2. Способности поддерживать связь в условиях нестабильных или ограниченных каналов связи.
3. Эргономичности пользовательского интерфейса, который должен обеспечивать безопасность по умолчанию.

Дополнительным критерием для корпоративного и ведомственного применения является простота развертывания и сопровождения мессенджеров.

II. Основы исследования и постановка задачи

Актуальность темы исследования и разнообразие функционального предназначения современных мессенджеров, которые эволюционировали от простого обмена сообщениями до критической инфраструктуры для бизнеса, государственного управления и социального взаимодействия, предопределяют необходимость применения системного и междисциплинарного подходов к анализу существующих Решений и теоретических основ.

В перспективе такой анализ необходим для построения комплексной методологии моделирования процессов обеспечения и оценки устойчивости разрабатываемой децентрализованной системы к широкому спектру угроз — от классических атак на конфиденциальность до целевых компрометаций метаданных.

Кроме того, с точки зрения системного подхода в процессе разработки мессенджеров важно учитывать возможные ограничения вычислительных ресурсов и энергопотребления. Рассматривать разрабатываемую модель не как изолированный программный продукт, а как описание киберфизической системы, тесно интегрированной с сетевым оборудованием.

Сегодня одним из направлений обеспечения требуемого уровня информационной безопасности при разработке мессенджеров является применение протокола Matrix.

Выбор в качестве базового протокола открытого стандарта Matrix, с его изначально децентрализованной архитектурой и поддержкой сквозного шифрования по умолчанию, является основным архитектурным решением, которое позволяет реализовать данный подход. Он предоставляет открытый API (от англ. Application Programming Interface) для интеграции и стандартизированный механизм федерации, под которой в контексте коммуникационных систем понимается способ взаимодействия независимых серверов, позволяющий пользователям различных доменов обмениваться данными в рамках единой децентрализованной сети [7], что позволяет оптимизировать размещение сервисов для минимизации задержек при обеспечении их доступности пользователям.

Вышеизложенное предопределяет необходимость дальнейшей разработки методологии эффективного применения современных научно-технических достижений и открытых стандартов при совершенствовании сквозных процедур — от принятия управленческих решений о выборе стека технологий до автоматизированной обработки информации в реальном времени, в том числе динамического моделирования сетевой нагрузки и комплексной оценки устойчивости системы. По сути, сегодня уже сформирована основа для создания самодостаточных и самоуправляемых коммуникационных экосистем, обладающих свойствами адаптивности.

Однако существуют определенные пробелы в описании и систематизации в достаточной степени универсальных Решений по развертыванию защищенного комплекса связи, а также для реализации стандартных компетенций в области администрирования и наиболее рационального применения типового серверного оборудования в зависимости от заданных условий.

Таким образом, постановка задачи исследования заключается в разработке модели обеспечения информационной безопасности в мессенджерах, разрабатываемых на основе протокола Matrix (далее – Модель) в интересах рационального развертывания и эксплуатации суверенной системы передачи данных, текстовой и голосовой связи, характеризующейся повышенной отказоустойчивостью и независимостью от внешних платформ.

III. Назначение, допущения, ограничения и схема модели обеспечения информационной безопасности в мессенджерах, разрабатываемых на основе протокола Matrix

Результаты современных научных исследований [1, 2, 3, 5, 7] дают возможность разработки Модели путем унификации и применения системного подхода к применению протокола Matrix для обеспечения информационной безопасности (далее – ИБ) пользователей мессенджеров.

Назначение Модели (рис. 1): описание и систематизация в достаточной степени универсальных технологических решений и методических рекомендаций для обеспечения ИБ в мессенджерах, разрабатываемых на основе протокола Matrix.

Ограничения при применении Модели заключаются в строгом выполнении требований, изложенных в законодательстве и требованиях ГОСТ Р 56939-2024. «Защита информации. Разработка безопасного программного обеспечения. Общие требования» в части разработки программного обеспечения (рис. 1).

Допущения: наличие специалистов и инфраструктуры для развертывания и эксплуатации децентрализованного

мессенджера при использовании протокола Matrix.

IV. Основные компоненты модели обеспечения информационной безопасности в мессенджерах, разрабатываемых на основе протокола Matrix

Применение Модели (рис. 1) обеспечивает создание защищенного децентрализованного мессенджера для установки на периферийных сетевых устройствах.

В Модели децентрализованный мессенджер — система обмена сообщениями, в которой отсутствует единый центральный сервер, а взаимодействие между пользователями осуществляется через распределенную сеть узлов [7].

Особенностью Модели является направленность на выполнение заданных в техническом задании на разработку конкретного мессенджера требований, обусловленных спецификой его применения в ведомственных и корпоративных системах связи.

При этом основным требованием является обеспечение суверенности функционирования — полного контроля над инфраструктурой и данными, без зависимости от внешних платформ и рисков трансграничной передачи информации.

Важным условием является реализация сквозного шифрования по умолчанию для всех видов коммуникаций, включая текстовые сообщения, метаданные, голосовой и видеотрафик, что соответствует современным стандартам криптографической защиты.

Архитектура системы должна поддерживать принцип федеративности, обеспечивая безопасное взаимодействие с другими серверами, построенными на открытых стандартах, необходимое для создания распределённых коммуникационных экосистем. Система должна обладать свойствами отказоустойчивости и способностью к автономной работе в условиях нестабильного или полностью отсутствующего подключения к глобальной сети.

Условием практической реализуемости является простота развертывания и управления, достигаемая за счет автоматизации процессов оркестрации и контейнеризации, позволяющей внедрять решение силами специалистов без углубленной подготовки в области распределённых систем.

Оркестрация контейнеров — автоматизация развертывания, управления, масштабирования и обеспечения сетевого взаимодействия контейнерных приложений [6].

В Модели (рис. 1 и 2) для решения поставленной задачи предлагается модульная архитектура, построенная на принципах микросервисов и контейнеризации [5, 6].

Микросервисная архитектура — стиль проектирования, при котором приложение состоит из небольших независимых сервисов, взаимодействующих через хорошо определенные API [5].

Ядром системы выбран открытый децентрализованный протокол коммуникаций Matrix [7], предоставляющий стандартизированный API, встроенную поддержку сквозного шифрования и механизм федерации.

Архитектурные компоненты и их взаимодействие:

1. Сервер Matrix (Homeserver): реализован на базе Synapse — эталонного сервера протокола Matrix. Homeserver отвечает за хранение и синхронизацию данных пользователей, федеративное взаимодействие с другими серверами, маршрутизацию сообщений, управление комнатами, идентификацию пользователей и криптографические операции [7].

2. Система управления базами данных: используется PostgreSQL — объектно-реляционная СУБД, обеспечивающая надежность, целостность данных и работу с большими объемами информации. Она выполняет роль внешней базы данных для сервера Synapse, поддерживая сохранность и согласованность всех пользовательских данных и истории сообщений.

3. Сервис голосовой и видеосвязи: связь в реальном времени организуется с помощью стека LiveKit — открытой платформы, функционирующей как SFU (от англ. Selective Forwarding Unit) и включающей встроенный TURN-сервер. WebRTC (от англ. Web Real-Time Communication) обеспечивает потоковую передачу аудио и видео между браузерами и приложениями [9]. LiveKit работает как отдельный микросервис, устанавливая медиасессии, обрабатывая трафик и поддерживая работу в сложных сетевых условиях.

4. Сервис аутентификации (lk-jwt-service): специализированный микросервис-шлюз для выдачи JWT (от англ. JSON Web Tokens). Он реализует авторизацию клиентов при подключении к LiveKit, интегрируя систему идентификации Matrix с RTC-стеком и гарантируя безопасный доступ к функционалу звонков.

5. Обратный прокси (Nginx): выполняет роль единой точки входа, осуществляет терминацию TLS (от англ. Transport Layer Security) соединений для всех доменов системы, маршрутизацию запросов к сервисам и публикацию статических файлов конфигурации через механизм «well-known» [9].

Предлагаемое технологическое решение обеспечивает безопасный и централизованный доступ ко всем компонентам системы для клиентов и федеративных серверов.

6. Оркестрация контейнеров (Docker): все компоненты инкапсулированы в отдельные контейнеры и управляются платформой Docker.

Процесс развертывания автоматизирован с помощью Docker Compose, что обеспечивает воспроизводимость, переносимость и минимизирует ручные настройки [6].

Схема применения и взаимодействия технологий представлена на рисунке 2.

Все компоненты функционируют на базе операционной системы OpenWRT, образующей базовую платформу развертывания (пунктирная область на схеме). Блоки, выделенные голубым цветом, представляют собой контейнеризованные сервисы, оркестрируемые Docker Compose.

Внешние подключения из интернета взаимодействуют с Nginx, LiveKit и системными

компонентами OpenWRT (ACME, Network, Firewall). Nginx маршрутизирует запросы к серверу Matrix Synapse и сервису аутентификации lk-jwt-service.

Рис. 1 — Схема модели обеспечения информационной безопасности в мессенджерах, разрабатываемых на основе протокола Matrix

Сервер Synapse взаимодействует с PostgreSQL для хранения сообщений и пользовательских данных, а также с LiveKit для организации голосовой и видеосвязи.

Сервис LiveKit, в свою очередь, интегрирован с lk-jwt-service для аутентификации клиентов и с компонентами OpenWRT для обеспечения сетевого взаимодействия.

В результате проведенной работы реализована и развернута Модель защищенного мессенджера, соответствующая поставленным задачам.

Практическим результатом стала система связи, поддерживающая обмен сообщениями и голосовую связь при полном контроле над данными.

Основным достижением является обеспечение требуемого уровня конфиденциальности и безопасности за счет реализации сквозного шифрования на основе протоколов Matrix.

Суверенность функционирования достигнута через локальное развертывание всех компонентов системы, что исключает риски, связанные с использованием облачных сервисов третьих сторон.

Совместимость системы с открытым стандартом Matrix гарантирует возможность применения широкого спектра клиентских приложений и обеспечивает функционал федерации, позволяющий устанавливать безопасные соединения с другими серверами.

Использование контейнерной оркестрации и автоматизированных скриптов развертывания подтвердило выполнение требований к эффективности внедрения и сопровождения, снизив трудоемкость административных операций.

Таким образом, разработанная Модель продемонстрировала практическую состоятельность как прикладное решение для построения суверенных систем ведомственной или корпоративной связи.

Оценка соответствия требованиям информационной безопасности проведена в соответствии с ГОСТ Р 56939-2024 [15].

Верификация включала тестирование архитектурных решений и практической реализации системы.

В ходе функционального тестирования подтверждена корректная работа базового функционала: доставка текстовых сообщений, установка голосовых и видеовызовов, функционирование федеративных соединений.

На рис. 3 представлена архитектурно значимая часть скрипта развертывания, демонстрирующая ключевые этапы инициализации системы:

1. Инициализацию и валидацию параметров окружения.
2. Формирование структуры каталогов для изолированного хранения данных компонентов.
3. Проверку целостности TLS-сертификатов для обеспечения безопасного обмена данными.
4. Подготовку инфраструктуры для последующей генерации конфигурационных файлов сервисов.

Представленный фрагмент (рис. 3) иллюстрирует принцип последовательной подготовки окружения, предшествующей оркестрации микросервисов средствами Docker Compose, согласно предлагаемой Модели (рис. 1 и 2).

Тестирование безопасности показало соответствие требованиям к криптографической защите информации: реализовано сквозное шифрование текстовой коммуникации и защита медиатрафика современными протоколами.

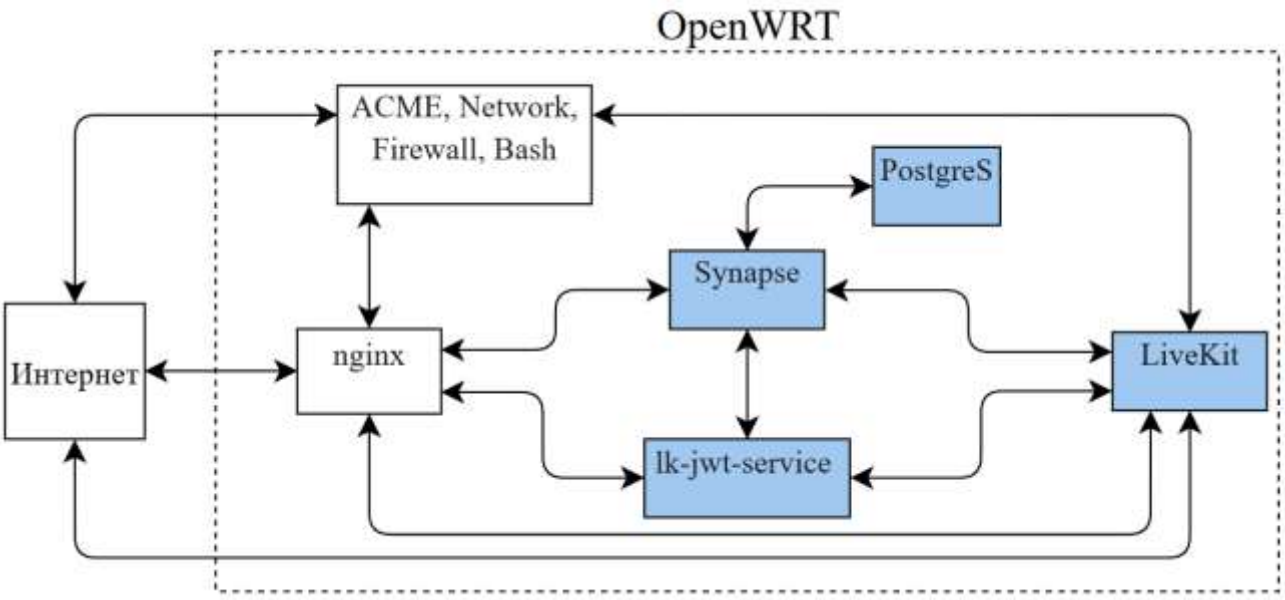

Рис. 2 — Схема применения и взаимодействия технологий в предлагаемой Модели

```
# Matrix Synapse + LiveKit + lk-jwt-service bootstrap for OpenWRT

set -Eeuo pipefail
LOG() { printf '[%(%Y-%m-%d %H:%M:%S)T] %s\n' -1 "$*"; }

# Загрузка конфигурации
ENV_FILE="./.env"

# Load env
if [[ ! -f "${ENV_FILE}" ]]; then
  LOG "ERROR: .env not found at ${ENV_FILE}"
  exit 1
fi
set -a && . "${ENV_FILE}" && set +a

# Создание структуры каталогов
mkdir -p \
  "${WELLKNOWN_ROOT}/.well-known/matrix" \
  "${MATRIX_DIR}/livekit" \
  "$(dirname "${SYNAPSE_CONFIG_PATH}")" \
  "${SYNAPSE_DATA_DIR}"

mkdir -p "${MATRIX_DIR}/postgres"
chown -R 991:991 "${MATRIX_DIR}/synapse"
chmod 0750 "${MATRIX_DIR}/synapse"

# Проверка TLS-сертификатов
for f in "${ACME_CHAIN}" "${ACME_KEY}"; do
  [[ -s "$f" ]] || { LOG "ERROR: certificate file missing: $f"; exit 1; }
done

# [Далее следует генерация конфигурационных файлов...]
# [Конфигурация Synapse → LiveKit → Nginx → Docker Compose]
```

Рис. 3 — Фрагмент кода автоматизированного развертывания мессенджера

Анализ архитектуры системы подтвердил соответствие принципам безопасной разработки: обеспечена изоляция компонентов средствами контейнеризации Docker, реализован принцип минимальных привилегий, применено разделение ответственности между микросервисами.

Нагрузочное тестирование выявило устойчивую работу системы в условиях типовых эксплуатационных нагрузок, при этом подтверждена оптимизация компонентов для работы на ресурсо-ограниченных периферийных устройствах.

Однако, в качестве существенного недостатка Модели следует отметить ограниченную устойчивость созданной системы к целевым DDoS (от англ. Distributed Denial of Service) атакам, данный показатель соответствует типовым характеристикам оборудования этого класса и не противоречит установленным требованиям для ведомственных систем связи [16, 17].

V. Заключение

Таким образом, в результате проведенного исследования разработана и практически реализована модель обеспечения информационной безопасности для децентрализованных мессенджеров на основе технологии Matrix.

На основе Модели (рис. 1 и 2) разработан программно-аппаратный комплекс, реализующий сквозное шифрование коммуникаций, голосовую и видеосвязь, а также федеративное взаимодействие в условиях автономного развертывания на периферийных сетевых устройствах.

Практическая значимость работы подтверждена успешным развертыванием функционирующего прототипа системы с использованием современных технологий контейнеризации и оркестрации.

Архитектура комплекса, построенная на принципах микросервисов и модульности, обеспечивает соответствие требованиям суверенности функционирования, отказоустойчивости и простоты развертывания.

Верификация работоспособности системы проведена в соответствии с требованиями ГОСТ Р 56939-2024, что подтверждает достижение заданных показателей информационной безопасности.

Основной положительный эффект от внедрения Модели заключается в создании полнофункциональной альтернативы коммерческим мессенджерам с полным контролем над инфраструктурой и данными.

Значительное снижение трудоемкости развертывания и сопровождения за счет автоматизации процессов оркестрации делает решение доступным для применения в ведомственных и специальных системах связи, включая возможность привлечения специалистов, обладающих начальным уровнем знаний и компетенций в области связи и автоматизации.

Перспективными направлениями дальнейших исследований являются:

1. Интеграция системы с платформами мониторинга и управления инцидентами информационной безопасности.
2. Разработка механизмов автоматического масштабирования компонентов системы в условиях переменных нагрузок.
3. Создание специализированных модулей аудита и анализа защищенности коммуникационных сессий.

Таким образом, Модель представляет практическую ценность для создания суверенных систем связи в органах государственного управления, критической информационной инфраструктуре и корпоративных сетях связи, где предъявляются повышенные требования к конфиденциальности и контролю над информационными потоками.

Библиография

[1] Дорф Р. Современные системы управления. — М.: Лаборатория базовых знаний, 2012. — 832 с.

[2] Jabbour K., Poisson J. Cyber Risk Assessment in Distributed Information Systems // The Cyber Defense Review. — 2016. — Vol. 1, № 1. — P. 91—112.

[3] Trevino M. Cyber Physical Systems: The Coming Singularity // PRISM. — 2019. — Vol. 8, № 3. — P. 2—13.

[4] Downes C. Strategic Blind-Spots on Cyber Threats, Vectors and Campaigns // The Cyber Defense Review. — 2018. — Vol. 3, № 1. — P. 79—104.

[5] Richards M., Ford N. Fundamentals of Software Architecture. — O'Reilly Media, 2020. — 400 p.

[6] Burns B., et al. Designing Distributed Systems: Patterns and Paradigms for Scalable, Reliable Services. — O'Reilly Media, 2018. — 165 p.

[7] Matrix.org Foundation. The Matrix Specification [Электронный ресурс]. — URL: https://spec.matrix.org/v1.9/ (дата обращения: 21.09.2024).

[8] Olm: A Cryptographic Ratchet [Электронный ресурс]. — URL: https://gitlab.matrix.org/matrix-org/olm/-/blob/master/docs/olm.md (дата обращения: 21.09.2024).

[9] MSC4143: VoIP FOCI (Framework for Ongoing Conferencing with Identity) [Электронный ресурс]. — URL: https://github.com/matrix-org/matrix-spec-proposals/pull/4143 (дата обращения: 21.09.2024).

[10] ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. — М.: Стандартинформ, 2006. — 8 с.

[11] ГОСТ Р IEC 61508-1-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. — М.: Стандартинформ, 2012. — 51 с.

[12] ГОСТ Р 56939-2024. Защита информации. Разработка безопасного программного обеспечения. Общие требования. — М.: Стандартинформ, 2024. — 45 с.

[13] PostgreSQL Documentation [Электронный ресурс]. — URL: https://www.postgresql.org/docs/ (дата обращения: 21.09.2024).

[14] ГОСТ Р 59162-2020. Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. — М.: Стандартинформ, 2020. — 32 с.

[15] ГОСТ Р 53110-2008. Система обеспечения информационной безопасности сети связи общего пользования. — М.: Стандартинформ, 2008. — 28 с.

Information security model for messengers based on Matrix protocol

K.Z. Bilyatdinov, S.I. Kiselev, A.A. Petukhova

Abstract — methodological and technological solutions for the creation of secure decentralized messengers for departmental and corporate communication systems are presented. A model for ensuring information security in messengers developed based on the Matrix open protocol is proposed, providing end-to-end encryption of communications, voice and video communications, as well as federated interaction. The model is implemented as a modular architecture based on the principles of microservices and containerization, using a technology stack including Synapse, PostgreSQL, LiveKit, lk-jwt-service, Nginx and Docker Compose. A special feature of the model is its focus on deployment on peripheral network devices running OpenWRT, which provides full control over the infrastructure and eliminates dependence on external platforms. Verification of compliance with information security requirements was carried out in accordance with GOST R 56939-2024. The practical significance of the work is confirmed by the successful deployment of a functioning prototype demonstrating stable operation in various operating conditions. The main positive effect is to significantly reduce the complexity of deploying and maintaining the messenger while ensuring the requirements for confidentiality and sovereignty of functioning.

Key words — decentralized messengers, Matrix protocol, information security, end-to-end encryption, containerization, microservice architecture, sovereign communication systems, OpenWRT.

REFERENCES

[1] Dorf R. Modern Control Systems. Moscow: Laboratory of Basic Knowledge, 2012. 832 p. (in Russian)
[2] Jabbour K., Poisson J. Cyber Risk Assessment in Distributed Information Systems. The Cyber Defense Review, 2016, vol. 1, no. 1, pp. 91—112.
[3] Trevino M. Cyber Physical Systems: The Coming Singularity. PRISM, 2019, vol. 8, no. 3, pp. 2—13.
[4] Downes C. Strategic Blind-Spots on Cyber Threats, Vectors and Campaigns. The Cyber Defense Review, 2018, vol. 3, no. 1, pp. 79—104.
[5] Richards M., Ford N. Fundamentals of Software Architecture. O'Reilly Media, 2020. 400 p.
[6] Burns B., et al. Designing Distributed Systems: Patterns and Paradigms for Scalable, Reliable Services. O'Reilly Media, 2018. 165 p.
[7] Matrix.org Foundation. The Matrix Specification. Available at: https://spec.matrix.org/v1.9/ (accessed: 21.09.2024).
[8] Olm: A Cryptographic Ratchet. Available at: https://gitlab.matrix.org/matrix-org/olm/-/blob/master/docs/olm.md (accessed: 21.09.2024).
[9] MSC4143: VoIP FOCI (Framework for Ongoing Conferencing with Identity). Available at: https://github.com/matrix-org/matrix-spec-proposals/pull/4143 (accessed: 21.09.2024).
[10] GOST R 50922-2006. Information Protection. Basic Terms and Definitions. Moscow: Standartinform, 2006. 8 p. (in Russian)
[11] GOST R IEC 61508-1-2012. Functional Safety of Electrical, Electronic, Programmable Electronic Safety-Related Systems. Moscow: Standartinform, 2012. 51 p. (in Russian)
[12] GOST R 56939-2024. Information Protection. Secure Software Development. General Requirements. Moscow: Standartinform, 2024. 45 p. (in Russian)
[13] PostgreSQL Documentation. Available at: https://www.postgresql.org/docs/ (accessed: 21.09.2024).
[14] GOST R 59162-2020. Information Technology. Security Techniques. Network Security. Moscow: Standartinform, 2020. 32 p. (in Russian)
[15] GOST R 53110-2008. Public Communication Network Information Security System. Moscow: Standartinform, 2008. 28 p. (in Russian)