УДК 004.738
Doi: 10.31772/2712-8970-2025-26-1-8-20

Для цитирования: Исаева О. С., Кулясов Н. В., Исаев С. В. Инфраструктура сбора данных и имитации угроз безопасности сети интернета вещей // Сибирский аэрокосмический журнал. 2025. Т. 26, № 1. С. 8–20. Doi: 10.31772/2712-8970-2025-26-1-8-20.

For citation: Isaeva O. S., Kulyasov N. V., Isaev S. V. [Infrastructure for collecting data and simulating security threats in the internet of things network]. *Siberian Aerospace Journal.* 2025, Vol. 26, No. 1, P. 8–20. Doi: 10.31772/2712-8970-2025-26-1-8-20.

Инфраструктура сбора данных и имитации угроз безопасности сети интернета вещей

О. С. Исаева*, Н. В. Кулясов, С. В. Исаев

Институт вычислительного моделирования СО РАН –
обособленное подразделение ФИЦ КНЦ СО РАН
Российская Федерация, 660036, г. Красноярск, ул. Академгородок, 50/44
*E-mail: isaeva@icm.krasn.ru

Аннотация. Внедрение технологии интернета вещей (internet of things, IoT) на предприятиях ракетно-космической отрасли требует обеспечения повышенных мер безопасности информационно-коммуникационных процессов. Существующие системы обнаружения вторжений не способны учитывать гетерогенность структуры сети и масштабность циркулирующей между устройствами информации. Для решения этой проблемы системы обнаружения вторжений используют метод аномалий, для применения которого требуется большое число репрезентативных данных. Авторами выполнен обзор публичных наборов данных, на основе которых может быть построена система выявления аномалий. Они содержат информацию из искусственных имитационных сред или изолированных окружений с имитацией устройств, включают примеры, которые напрямую не связаны с интернетом вещей, и не учитывают динамический характер изменения трафика.

В данной статье мы представляем новую инфраструктуру, которая позволит избежать указанных недостатков. Она собирает данные функционирования реальной сети интернета вещей и позволяет выполнять её тестирование на устойчивость к характерным атакам. Мы используем прикладной протокол MQTT (message queuing telemetry transport) и программные платформы, поддерживающие информационное взаимодействие на основе шаблона «издатель – подписчик». Инфраструктура содержит устройства, осуществляющие мониторинг технологических помещений с телекоммуникационным оборудованием, сервера с различными настройками политик безопасности, приложения для контроля и анализа данных, программные агенты сбора сетевого трафика и имитаторы угроз, выполняющие атаки на узлы сети с одиночных источников или в распределённой среде. Исследователи смогут, применяя собираемые в инфраструктуре данные для анализа кибербезопасности, создавать надёжные решения на базе интернета вещей, необходимые для внедрения этой технологии в наукоёмкие производства космических систем.

Ключевые слова: кибербезопасность, интернет вещей, протокол MQTT, брокер данных, базы данных вторжений, имитация угроз безопасности.

Infrastructure for collecting data and simulating security threats in the internet of things network

O. S. Isaeva*, N. V. Kulyasov, S. V. Isaev

Institute of Computational Modelling of the Siberian Branch of the SB RAS – subdivision Federal Research Center "Krasnoyarsk Scientific Center of the SB RAS"
50/44, Akademgorodok St., Krasnoyarsk, 660036, Russian Federation
*E-mail: isaeva@icm.krasn.ru

Abstract. The implementation of the internet of things technologies in the rocket-space industry requires increased security measures for information and communication processes. Existing intrusion detection systems are unable to take into account the heterogeneity of the network structure and the scale of information circulating between devices. To solve this problem, intrusion detection systems use an anomaly method, which requires a large number of representative data sets. The authors have reviewed public datasets that can be used to build an anomaly detection system. They contain information from artificial simulation medium or isolated environments with simulated devices, include examples that are not directly related to the internet of things, and do not take into account the dynamic nature of traffic changes.

In this paper, we present a new infrastructure that will avoid these drawbacks. It collects data on the functioning of a real Internet of Things network and allows testing its stability to typical attacks. We use the MQTT (message queuing telemetry transport) application protocol and software platforms that support information interaction based on the publisher-subscriber pattern. The infrastructure contains devices that monitor technological rooms with telecommunications equipment, brokers with various security policy settings, applications for data control and analysis, software agents for collecting network traffic and threat simulators that perform attacks on network nodes from single sources or in a distributed environment. Researchers will be able to use the data collected in the infrastructure for cybersecurity analysis to create reliable IoT-based solutions needed to implement this technology in knowledge-intensive space systems production.

Keywords: cybersecurity, internet of things, protocol MQTT, data broker, intrusion databases, simulated security threats.

Введение

Инновации, определяемые концепцией интернета вещей, согласно рекомендациям Международного союза электросвязи [1], отражают современные тренды, направленные на построение инфраструктур, объединяющих физические и виртуальные объекты на основе функционально-совместимых информационно-коммуникационных технологий. Потребность предприятий ракетно-космической отрасли в подобных решениях определяется не только современными требованиями к цифровизации производств, но и необходимостью их оперативной трансформации, отвечающей запросам потребителей продукции, а также ресурсным и технологическим возможностям [2]. Внедрение цифровых технологий позволяет осуществлять постоянный контроль качества выпускаемой продукции, выявлять эксплуатационные риски, прогнозировать отказы технических систем, обеспечивая повышение эффективности производственных процессов [3]. Однако неоспоримые преимущества от применения технологий интернета вещей на предприятиях ракетно-космической отрасли нивелируются необходимостью обеспечения повышенных мер безопасности и надёжности всех информационно-коммуникационных процессов.

Сети интернета вещей вызывают интерес для киберпреступников как из-за характера устройств, облегчённости протоколов их подключения, так и из-за ценности и масштабности информации, которую можно получить при получении к ним доступа. Основной целью кибератак является искажение генерируемых данных, определяющих действия пользователей или автоматизированных систем, нарушение текущих процессов (отказ в обслуживании), раскрытие информации, которая может быть использована с целью получения конкурентных преимуществ [4].

Компрометация любого отдельного устройства может распространиться на все системы предприятия и нарушить его критические функции [5]. Сообщения о взломах устройств интернета вещей, позволяющих перехватывать удалённое управление и выполнять проникновение в корпоративные сети, или объединении таких устройств в ботнеты появляются регулярно [6].

Системы обнаружения вторжений, согласно методикам проведения исследований, делятся на сигнатурные (позволяют идентифицировать атаки, эксплуатирующие сетевые уязвимости), основанные на правилах (выявляют действия, несоответствующие легитимным пользователям), и исследующие аномалии (применяют методы машинного обучения для обнаружения нетипичного поведения или статистических расхождений) [7]. Сигнатурные и основанные на правилах решения по безопасности не предназначены для поддержки сетей интернета вещей, которые отличаются гетерогенностью структуры, ограниченной вычислительной мощностью взаимосвязанных устройств, многоплатформенностью используемых протоколов подключения, большим объёмом сетевого трафика, разнородностью событий безопасности и нехваткой точных данных о поведении атак [8]. Для интернета вещей предпочтительным является подход на основе аномалий. Но его применение требует создания репрезентативных наборов данных и надёжных методов оценки, учитывающих свойства реальных сетей.

Методы машинного обучения позволяют формировать шаблоны на основе вредоносного сетевого трафика, полученного во время заражения, которые используют для выявления подобных атак в будущем [9]. В отличие от других областей, где широко используется машинное обучение, область обнаружения вторжений предполагает постоянное изменение в характеристиках трафика открытого мира с точки зрения его содержимого, методов обслуживания, сценариев атак и их результатов, меняющихся в зависимости от развития средств уклонения [10]. Вследствие этого нельзя ожидать, что поведение сетевого трафика, продемонстрированное в обучающем наборе данных, с течением времени будет в какой-либо степени соответствовать его поведению в производственной среде [11]. Системы на основе аномалий, использующие методы машинного обучения, должны иметь значительное количество примеров реального сетевого трафика со всеми видами атак и обычным поведением пользователей, а также полезной нагрузкой, которые будут актуальными и охватывающими длительные периоды наблюдения [12].

В данной статье мы представляем новую инфраструктуру сбора данных интернета вещей, предназначенную для накопления информации о сетевом трафике и имитации угроз безопасности. Исследование выполнено в корпоративной сети Красноярского научного центра СО РАН, включающей устройства интернета вещей и программное обеспечение, выполняющее сбор и анализ данных [13]. Для выделения параметров, характеризующих состояние сети и процессы, происходящие в ней, используется построенная в [14] онтология. Предложена концепция организации инфраструктуры сбора данных, которая позволит выделять особенности среды функционирования интернета вещей и учитывать динамический характер событий безопасности, что расширит область применения методов машинного обучения в системе обнаружения вторжений.

Обзор публичных наборов данных

Для разработки и тестирования решений по информационной безопасности и сетевому взаимодействию устройств интернета вещей создаются публичные наборы данных, описывающие различные инфраструктуры киберпространства и сценарии, нарушающие их надёжность и производительность. Для того чтобы определить функции создаваемой инфраструктуры, состав показателей для анализа безопасности были рассмотрены популярные наборы данных (dataset), широко применяемые при построении систем обнаружения вторжений.

Наборы данных KDD99 [15] и NSL-KDD [16] являются одними из наиболее часто упоминаемых, которые содержат нормальные и агрессивные сценарии трафика, полученного на испытательном стенде, созданном в лаборатории Массачусетского технологического института. Исследователи, применяющие эти данные, столкнулись с их избыточностью и недостаточной

балансировкой выборок для обучения. К настоящему времени эти наборы устарели и не отражают динамики современных сетевых систем.

Ещё один широко используемый набор данных – CICIDS2017 Intrusion Detection Evaluation Dataset [17], разработанный Канадским институтом кибербезопасности (CIC), представляет сетевой трафик, формируемый в изолированной среде путём моделирования действий легальных пользователей и нарушителей. Набор содержит более 50 Гб исходных данных и файлов с размеченными сессиями и выделенными признаками в разные дни наблюдений. Популярность этого набора позволила исследователям получить исчерпывающие данные о содержавшихся в нём ошибках. В [18] выполнен анализ признаков сетевых сессий из исходных файлов и их сопоставление с размеченными данными. Выявлены значительные расхождения при выделении сессий, ошибки при расчётах значений признаков и их дублирование, некорректное завершение сессий, отнесение граничных пакетов к следующей сессии, неверный расчёт длин пакетов, которые могут оказать существенное влияние на результаты машинного обучения. Наш опыт применения инструмента обработки пакетов CICFlowMeter [19], на котором построен CICIDS2017, к собственным сырым данным подтвердил вышеуказанные проблемы. В NTLFlowLyzer [20] эти проблемы исправлены.

Перечисленные наборы данных не учитывают специфику сетей и протоколов интернета вещей. В нашем исследовании для выявления аномалий мы объединяем характеристики трафика транспортного уровня с показателями, описывающими прикладные протоколы интернета вещей. Для их выявления рассмотрены наборы данных, получаемые в рамках реализации такого рода сетей.

Комплексный набор данных TON IoT 2021 [21] включает информацию систем интернета вещей, собранную в виде файлов журналов от 10 датчиков телеметрии. Предобработка сырых данных выполнялась с помощью инструмента ZEEK (Bro). Для операционной системы Linux данные собирались с помощью входящего в неё инструмента трассировки, выполняющего мониторинг активности процессора, памяти и сети. В Windows использовался сборщик данных производительности операционной системы. Набор включает 9 различных угроз безопасности.

Набор данных UQ-IOT-IDS-2021 [22] получен в реальной среде разнородной сети Интернета вещей, включающей различные устройства, такие как смартфоны, смарт-телевизоры, IP-камеры, смарт-колонки и т. п.

В наборе MQTT-IoT-IDS-2020 [23] содержится трафик имитируемой сети, состоящей из 12 датчиков и брокера, взаимодействующих между собой по протоколу MQTT (Message Queuing Telemetry Transport) и источников угроз (4-х типов). В данные включены флаги протокола, описывающие состояние сессии и уровень качества обслуживания. В своё исследование мы включили аналогичные флаги и показатели, обобщающие характеристики сессий протокола MQTT.

CIC EVSE2024 [24] содержит безопасный трафик, сетевые атаки и атаки, направленные на зарядное устройство электромобилей. Аномальный трафик представляет атаки сбора данных (Reconnaissance) и отказ в обслуживании (DoS), направленные атаки типа Backdoor и Cryptojacking. Эти наборы данных демонстрируют возможности использования полезной нагрузки для выявления аномального поведения устройств интернета вещей.

Особенности публичных наборов состоят в неоднородности предоставляемых данных, различиях в способах имитации событий безопасности и подходов к сбору и предобработке информации, что может оказывать огромное влияние на эффективность обнаружения аномалий. Назначение, функции и вид устройств определяют допустимые границы измерений, получаемые от них в качестве полезной нагрузки. Для выявления аномалий в трафике необходимо исследовать результаты функционирования именно тех устройств, безопасность которых мы планируем обеспечивать. Большая часть наборов включает не только сетевой трафик, связанный с интернетом вещей, но и данные сторонних служб, систем и протоколов, что затрудняет их применение для локализации угроз, направленных на функционирование устройств интернета

вещей. Кроме того, практически все наборы данных получены в искусственной имитационной среде или изолированных окружениях с имитацией устройств. В них рассматриваются угрозы, характерные не только для систем интернета вещей, но и любых других информационных систем, перегружая тем самым источники данных для машинного обучения лишними, не встречаемыми в исследуемых сетях примерами. В таких условиях оправданным является разработка собственной инфраструктуры сбора и накопления данных, учитывающей существующий опыт создания публичных данных и позволяющей актуализировать данные при изменении условий функционирования сети.

Структура корпоративной сети интернета вещей

В Красноярском научном центре технология интернета вещей применяется для контроля показателей температуры и влажности помещений, в которых расположены сервера, поддерживающие работу сетевых и почтовых служб [25]. Структура сети приведена на рис. 1.

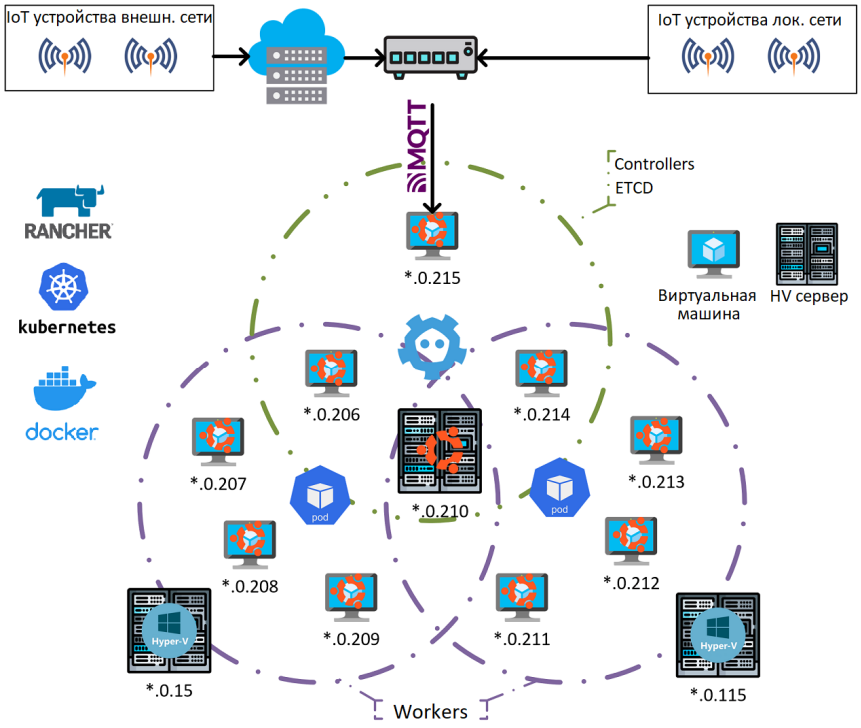

Рис. 1. Структура сети интернета вещей

Fig. 1. Structure of the internet of things network

При построении наборов данных для анализа аномалий необходимо учитывать не только структуру сети, но и свойства протоколов, используемых на отдельных уровнях межмашинного взаимодействия. В табл. 1 приведены примеры протоколов, распределённые по уровням сети (в контексте стека протоколов TCP/IP и эталонной сетевой модели OSI).

При построении сети интернета вещей необходимо выбрать, какие протоколы будут работать на канальном уровне, а какие будут выполнять обмен данными между устройствами и приложениями на прикладном уровне. Требования к этим протоколам заключаются в обеспечении надёжной и эффективной связи между распределёнными устройствами, синхронизации данных в режиме реального времени, возможности асинхронной передачи при нестабильном соединении и в условиях низкой пропускной способности сети [26].

Например, к протоколам канального уровня относятся Ethernet, Modbus, Zigbee, WiFi, LoRaWAN. В нашем случае используются протоколы Ethernet, WiFi, что определяется функ-

циональными возможностями корпоративной сети, в которую встраиваются устройства интернета вещей. Протоколы прикладного уровня выполняют функции по упаковке, форматированию и доставке данных, обеспечивая контроль их целостности и качество обслуживания. К протоколам прикладного уровня относятся MQTT, CoAP, AMQP. В построенной сети для прикладного уровня выбран протокол MQTT – открытый стандарт, разработанный специально для малых вычислительных возможностей устройств [27] и являющийся на сегодняшний день одним из наиболее часто используемых протоколов межмашинного взаимодействия интернета вещей. Его работа основана на шаблоне «издатель – подписчик» (рис. 2).

Таблица 1

Распределение сетевых протоколов по уровням моделей OSI и TCP/IP

OSI модель	*TCP/IP*	*Примеры*
Прикладной	Прикладной	HTTP, HTTPS, FTP, MQTT, CoAP, AMQP
Представления		
Сеансовый		
Транспортный	Транспортный	TCP, UDP
Сетевой	Межсетевой	IPv4, IPv6, ICMP
Канальный	Канальный	Ethernet, Wi-Fi, BLE, Zigbee, Z-Wave LoRaWan
Физический		

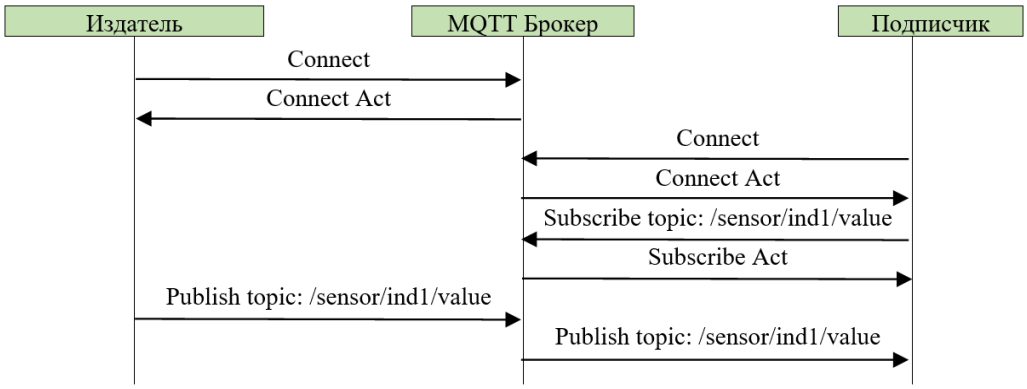

Рис. 2. Шаблон «издатель – подписчик»

Fig. 2. Template “publish – subscribe”

В обмене данными участвуют: издатель (Publisher) – устройство, собирающее информацию или выполняющее измерения; подписчик (Subscriber) – клиент, который в процессе своей работы получает и использует эту информацию; брокер (Broker) – посредник, который получает данные от издателя и раздаёт их по подпискам на темы, определяющие вид и источник информации. Механизмы информационного взаимодействия в разработанной сети интернета вещей учитывают цикличность анализируемых процессов, что позволяет сокращать нагрузку на потребителей информации и используемые сети [28].

Несмотря на то, что подключение устройств интернета вещей к корпоративной сети не было анонсировано в публичном пространстве, наблюдается неуклонный рост нелигитимных запросов соединений. Происходит постоянное сканирование различных сервисов по портам протокола MQTT.

На рис. 3 приведён пример распределения запросов по странам-источникам. Показатели, характеризующие динамику роста запросов к устройствам корпоративной сети интернета вещей рассмотрены в [29].

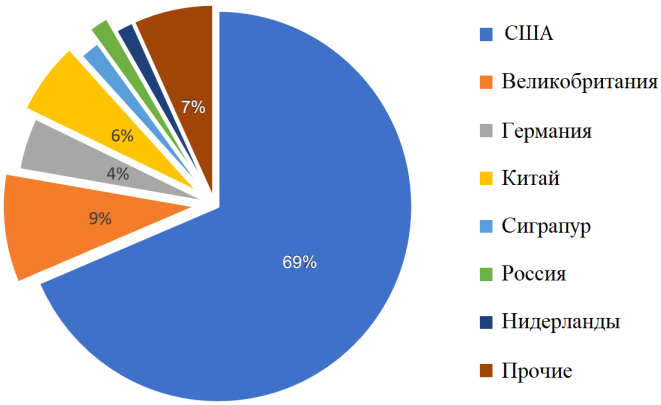

Рис. 3. Распределение запросов по странам (статистика за 6 месяцев)

Fig. 3. Distribution of requests by country (6 months statistics)

Рост интереса к устройствам интернета вещей со стороны нелигитимных пользователей и сканирование сетевых портов протокола MQTT показывают актуальность контроля безопасности построенной структуры и создания инструментов обнаружения сетевых аномалий. Для исследования разработана инфраструктура, обеспечивающая сбор и актуализацию данных.

Построение инфраструктуры сбора данных

Инфраструктура сбора данных и имитации угроз безопасности размещается в рамках существующей сети организации, без дополнительной оптимизации и изоляции. Показанная ранее структура сети интернета вещей дополнена различными реализациями брокеров данных, программными агентами, собирающими информацию на ключевых точках корпоративной сети, и имитаторами угроз, характерными для интернета вещей.

Выбор программной платформы для реализации брокеров определяется требованиями обеспечения производительности, уменьшения задержек передачи данных, поддержки кластеризации, ограничения потребления ресурсов и пр. Как правило, публичные наборы данных не акцентируют внимание на используемых брокерах и их конфигурации, что не позволяет выявить возможные особенности функционирования реализующих их функции программных платформ. Для учёта особенностей различных брокеров в дополнение Eclipse Mosquitto установлены брокеры EMQX, NanoMQ, VerneMQ [30]. Настроены конфигурации брокеров, которые различаются используемыми программными платформами и настройками способа авторизации, шифрования (протокол TLS – Transport Layer Security или без шифрования) и доступа (из внутренней или внешней сети). Примеры условных обозначений брокеров приведены в табл. 2.

Таблица 2

Конфигурация параметров безопасности

Обозначение на схеме	Авторизация	Шифрование
auth_priv	Логин/Пароль	Без шифрования
anon_priv	Без авторизации	Без шифрования
auth_priv_tls	Логин/Пароль	TLS
anon_priv_tls	Без авторизации	TLS

Концептуальная схема инфраструктуры сбора данных и имитации угроз безопасности приведена на рис. 4. В инфраструктуру входят 16 независимых брокеров и реплицирующий брокер для распределения данных с издателей, а также программные агенты, которые собирают информацию о взаимодействии устройств интернета вещей с внешним миром и внутри сети.

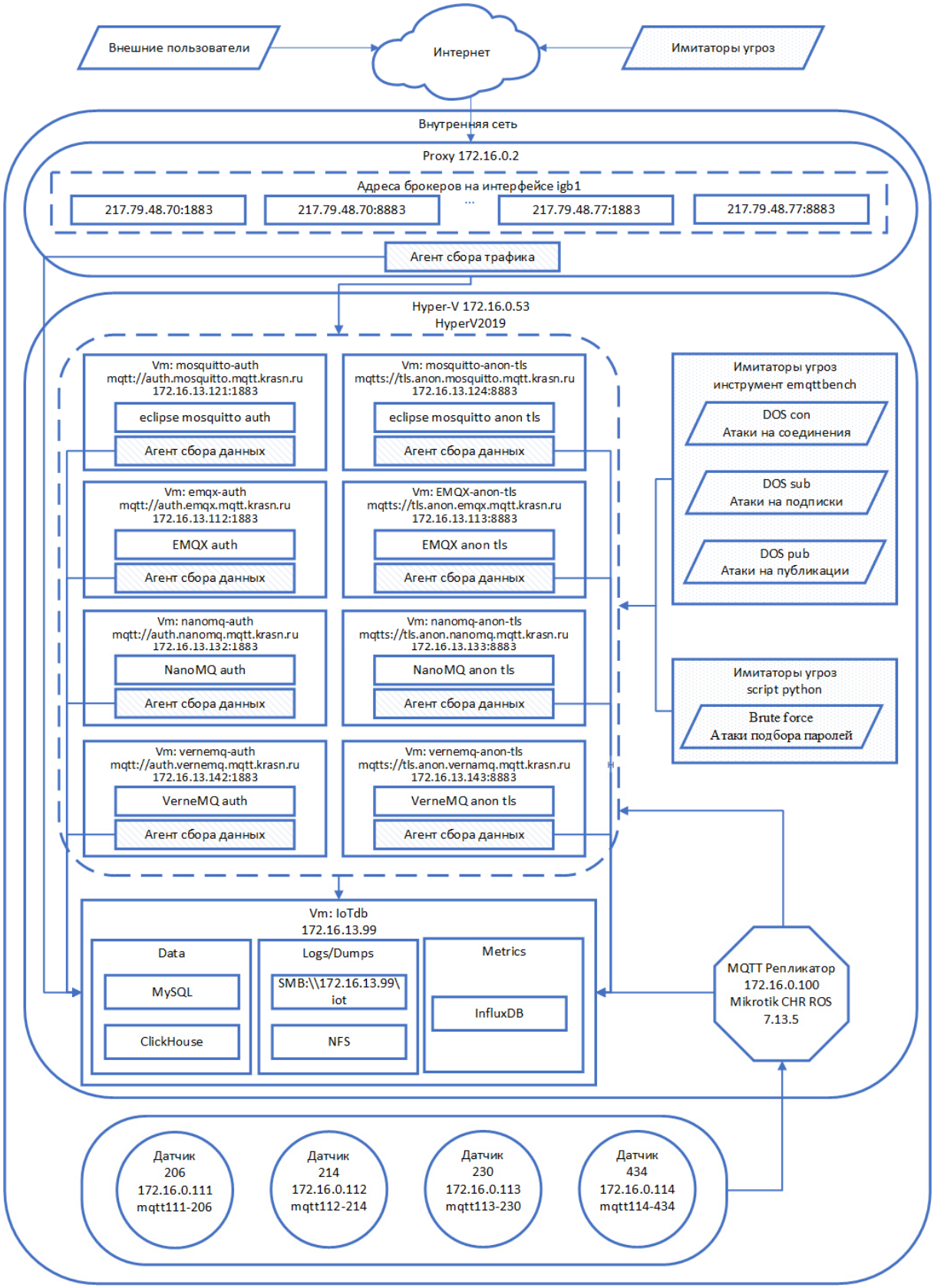

Рис. 4. Схема инфраструктуры сбора данных

Fig. 4. Scheme of the data collection infrastructure

Программные агенты, работающие на брокерах, собирают как внешний, так и внутренний сетевой трафик, приходящий на стандартные и шифрованные порты протокола MQTT. Кроме того, собираются метрики серверов и показатели, предоставляемые программным обеспечением брокера. От серверов получаем процентные характеристики ресурсов системы (процессора, памяти, загруженности сетевого канала), необходимых для выполнения работы, количество выполняемых операций ввода/вывода и другие. От брокеров – количество активных клиентов, полученных и отправленных сообщений, их объём, статические показатели, полученные после анализа сетевого трафика. Исследование данных позволит выбирать брокера и его параметры так, чтобы сохранить баланс между доступностью сервисов и целостностью информации при одинаковых сценариях использования без потери функциональности и в условиях ограниченности потребления ресурсов.

Агенты сбора сетевого трафика расположены также и на Proxy-сервере (устройстве, обслуживающем информационные потоки между пользователями и веб-ресурсами). Собираемые там данные содержат сведения обо всех внешних источниках угрозах.

Для сбора данных, возникающих во время сетевых атак на ресурсы интернета вещей, настроены имитаторы угроз безопасности (применяется инструмент для тестирования производительности eMQTT-Bench). На текущий момент собирается трафик с имитацией следующих угроз:

– DOS con, выполняется большое количество запросов к брокеру на подключение за короткий промежуток времени;

– DOS sub, выполняется большое количество запросов к брокеру на подписки за короткий промежуток времени;

– DOS pub, выполняется большое количество запросов к брокеру на публикацию сообщений за короткий промежуток времени.

Перечисленные атаки выполняются как с одного источника, так и имитируются распределённые варианты угроз из многих источников. Дополнительно реализована атака на пароли, выполняющая подбор пары логин/пароль для брокеров с настроенной аутентификацией. Собираемые агентами данные в большой степени не структурированы и для их использования необходима предобработка, выполняющая деление трафика на сессии и расчёт параметров полученных сессий.

Выбор состава анализируемых показателей основан на проведённом обзоре популярных наборов данных. Мы объединили показатели, аналогичные используемым в публичных источниках, характеризующие различные уровни сети. По аналогии с CICIDS2017 мы рассчитываем характеристики сессий: дата – время, идентификатор потока, IP источника и приёмника, протокол, продолжительность потока, его скорость, среднее значение межпакетного интервала, суммарная длина пакетов, переданных в прямом и обратном направлении и другие. Дополняем их показателями, формируемыми в CIC EVSE2024 и не входящими в первый источник данных, например, количество флагов SYN (ACK, FIN и др.) в прямом или обратном направлении. Для исследования особенностей работы протокола MQTT рассчитываем характеристики, обобщающие флаги его сессий, аналогичные используемым в наборе MQTT-IoT-IDS-2020, например, флаг текущей сессии, соединения, удержания, очистки сеанса, уровень качества обслуживания (запрошенный и предоставленный), тип сообщения, его длина и прочее. Таким образом, структурные элементы публичных источников данных используются нами в качестве словарей, что обеспечивает сопоставимость с ними наших метаданных и позволяет выполнять сравнение результатов работы методов машинного обучения, настроенных на наших данных, с другими работами, использующими публичные наборы.

Построенная инфраструктура позволяет собирать трафик интернета вещей и выполнять тестирование сети на устойчивость к нескольким видам атак, характерным для таких сетей. Имитация атак инструментами, входящими в брокер данных, обеспечит их соответствие принятым стандартам.

Заключение

В работе описана инфраструктура сбора данных сетевой активности и имитации угроз безопасности интернета вещей, развёрнутая в рамках корпоративной сети Красноярского научного центра. В нее включены: датчики, выполняющие измерение температуры, влажности и т. д.; брокеры, работающие по протоколу MQTT; подписчики, расположенные в локальной сети или осуществляющие доступ к данным через интернет; агенты, собирающие информацию; имитаторы угроз, позволяющие выполнять атаки, характерные для интернета вещей и используемых сетевых протоколов.

Сбор информации производится в распределённой среде, учитывающей особенности используемых протоколов взаимодействия со всеми устройствами на различных участках сети. Выполняется упорядоченная обработка и перенос собираемых данных к информационным системам внутри сети, а также обеспечивается доступ пользователям, расположенным вне локальной сети.

Инфраструктура позволяет оперативно получать новые наборы данных с актуализированными сценариями атак, учитывая влияние дрейфа атакующих концепций. Её применение позволяет сформировать набор данных для создания и верификации новых методов и инструментов обнаружения угроз информационной безопасности, направленных на работу в реальных сетях интернета вещей. Дальнейшее развитие темы исследования заключается в построении системы идентификации и блокирования киберугроз на основе анализа сетевых аномалий.

Библиографические ссылки

1. Recommendation ITU-T Y.2060. Series Y: Global information infrastructure, internet protocol aspects and next-generation networks. Next generation networks – Frameworks and functional architecture models. Overview of the Internet of things – Switzerland, Geneva: International telecommunication union, 2013. 22 p. [Электронный ресурс]. URL: https://handle.itu.int/11.1002/ 1000/11559 (дата обращения: 10.01.2025).

2. Абрашкин М. С., Афанасьев В. Я., Бускин Н. С. Цифровизация предприятий ракетно-космической промышленности в условиях новой промышленной революции // Russian journal of management. 2024. № 12(2). С. 369–389.

3. Internet of things: Vision, applications and research challenges / D. Miorandi, S. Sicari, F. Pellegrini, I. Chlamtac // Ad Hoc Networks, 2012. Vol. 10(7). P. 1497–1516.

4. A survey of network-based intrusion detection data sets / M. Ring, S. Wunderlich, D. Scheuring, D. Landes, A. Hotho // Computers & Security, 2019. Vol. 86. P. 147–167.

5. Al-Hawawreh M., Sitnikova E., Aboutorab N. X-IIoTID: A Connectivity- and Device-agnostic Intrusion Dataset for Industrial Internet of Things // IEEE Internet of Things Journal. 2021. No. 99. P. 1-1. DOI: 10.1109/JIOT.2021.3102056.

6. Шмелев Я., Моргунов В. Обзор угроз для IoT-устройств в 2023 году [Электронный ресурс]. URL: https://securelist.ru/iot-threat-report-2023/108088/ (дата обращения: 30.09.2024).

7. Jabez J., Muthukumar B. Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach // Procedia Computer Science, 2015. Vol. 48. P. 338–346.

8. Security, privacy and trust in Internet of Things: The road ahead / S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini // Computer Networks, 2015. Vol. 76. P. 146–164.

9. Botnet attacks detection in IoT environment using machine learning techniques / M. AL-Akhrasa, A. Alshunaybirb, H. Omarc, S. Alhazmib // International Journal of Data and Network Science, 2023. Vol. 7. P. 1683–1706.

10. Paxson V., Floyd S. Wide area traffic: the failure of Poisson modeling // IEEE/ACM Transactions on Networking, 1995. Vol. 3(3). P. 226–244.

11. Viegas E. K., Santin A. O., Oliveira L. S. Toward a reliable anomaly-based intrusion detection in real-world environments // Computer Networks, 2017. Vol. 127. P. 200–216.

12. Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling / W. Haider, J. Hu, J. Slay, B. P. Turnbull, Y. Xie // Journal of Network and Computer Applications, 2017. Vol. 87. P. 185–192.

13. Исаева О. С. Построение цифрового профиля устройств Интернета вещей // Информационные и математические технологии в науке и управлении, 2023. № 2(30). С. 36–44.

14. Исаева О. С. Построение онтологии для систематизации характеристик сети Интернета вещей // Онтология проектирования, 2024. Т. 14, № 2(52). С. 243–255.

15. KDD Cup 1999 Data [Электронный ресурс]. URL: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (дата обращения: 20.01.2025).

16. Mohi-ud-din G. NSL-KDD // IEEE Dataport, 2018. doi: 10.21227/425a-3e55.

17. Xinpeng C. CICIDS2017 and UNBSW-NB15 // IEEE Dataport, 2023. DOI: 10.21227/ykpn-jx78.

18. Moustafa N. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets // Sustainable Cities and Society, 2021, Vol. 72. P. 102994.

19. Lashkari A. H. CICFlowmeter-V4.0 (formerly known as ISCXFlowMeter) is a network traffic Bi-flow generator and analyser for anomaly detection. [Электронный ресурс]. URL: https://github.com/ISCX/CICFlowMeter.10.13140/RG.2.2.13827.20003 (дата обращения: 20.01.2025).

20. Методика сбора обучающего набора данных для модели обнаружения компьютерных атак / А. И. Гетьман, М. Н. Горюнов, А. Г. Мацкевич, Д. А. Рыболовлев // Труды ИСП РАН, 2021. № 33(5). С. 83–104.

21. Shafi M. M., Lashkari A. H., Roudsari A. H. NLFlowLyzer: Toward generating an intrusion detection dataset and intruders behavior profiling through network layer traffic analysis and pattern extraction // Computers & Security. 2024. Vol. 148, No. 1. P. 104160. DOI:10.1016/j.cose.2024.104160.

22. UQ IoT IDS dataset / H. Ke, K. Dan, Z. Zhien, G. Mengmeng, L. Ulysses, Y. Jiaqi // The University of Queensland. Data Collection, 2022.

23. MQTT-IoT-IDS2020: MQTT Internet of Things Intrusion Detection Dataset / H. Hindy, C. Tachtatzis, R. Atkinson, E. Bayne, X. Bellekens // IEEE Dataport, 2020.

24. CIC EV charger attack dataset 2024 (CICEVSE2024) [Электронный ресурс]. URL: https://www.unb.ca/cic/datasets/evse-dataset-2024.html (дата обращения: 15.10.2024).

25. Isaeva O. S., Kulyasov N. V., Isaev S. V. Creation of a simulation stand for studying of the internet of things' technologies // AIP Conference Proceedings, 2022. № 2647. P. 040030-1–040030-5.

26. A survey of intrusion detection in Internet of Things / B. B. Zarpelão, R. S. Miani, C. T. Kawakani, S. C. de Alvarenga // Journal of Network and Computer Applications, 2017. Vol. 84. P. 25–37.

27. MQTT: The Standard for IoT Messaging [Электронный ресурс]. URL: https://mqtt.org/ (дата обращения: 14.08.2024).

28. Исаева О. С., Исаев С. В., Кулясов Н. В. Формирование адаптивных рассылок брокера данных интернета вещей // Информационно-управляющие системы, 2022. № 5(120). С. 23–31.

29. Исаева О. С., Кулясов Н. В., Исаев С. В. Создание инструментов сбора данных для анализа аспектов безопасности Интернета вещей // Информационные и математические технологии в науке и управлении, 2022. № 3(27). С.113–125.

30. A scalable and low-cost MQTT broker clustering system / P. Jutadhamakorn, T. Pillavas, V. Visoottiviseth, R. Takano, J. Haga, D. Kobayashi // 2nd International Conference on Information Technology (November 2017, Thailand). IEEE. 2017. P. 1–5.

References

1. Recommendation ITU-T Y.2060. Series Y: Global information infrastructure, internet protocol aspects and next-generation networks. Next generation networks – Frameworks and functional archi-

tecture models. Overview of the Internet of things. *International telecommunication union*. 2013. 22 p. Available at: https://handle.itu.int/11.1002/1000/11559 (accessed: 10.01.2025).

2. Abrashkin M. S., Afanas'ev V. Ya., Buskin N. S. [Digitalization of rocket-space industry enterprises in the context of the new industrial revolution]. *Russian journal of management.* 2024, No. 12(2), P. 369–389 (In Russ.).

3. Miorandi D., Sicari S., Pellegrini F., Chlamtac I. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 2012, Vol. 10(7), P. 1497–1516.

4. Ring M., Wunderlich S., Scheuring D., Landes D., Hotho A. A survey of network-based intrusion detection data sets. *Computers & Security*, 2019, Vol. 86, P. 147–167.

5. Al-Hawawreh M., Sitnikova E., Aboutorab N. X-IIoTID: A connectivity and device agnostic intrusion dataset for industrial Internet of Things. *IEEE Internet of Things Journal*. 2021, No. 99, P. 1-1. DOI:10.1109/JIOT.2021.3102056.

6. Shmelev Ya., Morgunov V. [IoT threat landscape in 2023]. (In Russ.). Available at: https://securelist.ru/iot-threat-report-2023/108088/ (accessed 30.09.2024).

7. Jabez J., Muthukumar B. Intrusion detection system (IDS): anomaly detection using outlier detection approach. *Procedia Computer Science*, 2015, Vol. 48, P. 338–346.

8. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead. *Computer Networks*, 2015, Vol. 76, P. 146–164.

9. AL-Akhrasa M., Alshunaybirb A., Omarc H., Alhazmib S. Botnet attacks detection in IoT environment using machine learning techniques. *International Journal of Data and Network Science*, 2023, Vol. 7, P. 1683–1706.

10. Paxson V., Floyd S. Wide area traffic: the failure of Poisson modeling. *IEEE ACM Transactions on Networking*, 1995, Vol. 3(3), P. 226–244.

11. Viegas E. K., Santin A. O., Oliveira L. S. Toward a reliable anomaly-based intrusion detection in real-world environments. *Computer Networks*, 2017, Vol. 127, P. 200–216.

12. Haider W., Hu J., Slay J., Turnbull B. P., Xie Y. Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. *Journal of Network and Computer Applications*, 2017, Vol. 87, P. 185–192.

13. Isaeva O. S. [Building a digital profile of IoT devices]. *Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii*, 2023, No. 2(30), P. 36–44 (In Russ.).

14. Isaeva O. S. [Building an ontology to systematize the characteristics of the Internet of Things network], 2024, Vol. 14, No. 2(52), P. 243–255 (In Russ.).

15. KDD Cup 1999 Data. Available at: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed 20.01.2025).

16. Mohi-ud-din G. NSL-KDD. *IEEE Dataport*, 2018. doi: 10.21227/425a-3e55.

17. Xinpeng C. CICIDS2017 and UNBSW-NB15. *IEEE Dataport*, 2023. doi: 10.21227/ykpn-jx78.

18. Moustafa N. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. *Sustainable Cities and Society*, 2021, Vol. 72, P. 102994.

19. Lashkari A. H. CICFlowmeter-V4.0 (formerly known as ISCXFlowMeter) is a network traffic Bi-flow generator and analyser for anomaly detection. Available at: https://github.com/ISCX/CICFlowMeter.10.13140/RG.2.2.13827.20003 (accessed 20.01.2025).

20. Getman A. I., Goryunov M. N., Matskevich A. G., Rybolovlev D. A. [Methodology for collecting training dataset for computer intrusion detection model]. *Trudy ISP RAN*, 2021, No. 33(5), P. 83–104 (In Russ.).

21. Shafi M. M., Lashkari A. H., Roudsari A. H. NLFlowLyzer: Toward generating an intrusion detection dataset and intruders behavior profiling through network layer traffic analysis and pattern extraction. *Computers & Security*. 2024, Vol. 148, No. 1, P. 104160. DOI:10.1016/j.cose.2024.104160.

22. Ke H., Dan K., Zhien Z., Mengmeng G., Ulysses L., Jiaqi Y. UQ IoT IDS dataset. *The University of Queensland. Data Collection*, 2022.

23. Hindy H., Tachtatzis C., Atkinson R., Bayne E., Bellekens X. MQTT-IoT-IDS2020: MQTT Internet of Things intrusion detection dataset. *IEEE Dataport*, 2020.

24. CIC EV charger attack dataset 2024 (CICEVSE2024) Available at: https://www.unb.ca/cic/ datasets/evse-dataset-2024.html (accessed 15.10.2024).

25. Isaeva O. S., Kulyasov N. V., Isaev S. V. Creation of a simulation stand for studying of the internet of things' technologies. *AIP Conference Proceedings*, 2022, No. 2647, P. 040030-1–040030-5.

26. Zarpelão B. B., Miani R. S., Kawakani C. T., Alvarenga S. C. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, 2017, Vol. 84, P. 25–37.

27. MQTT: The Standard for IoT Messaging [Электронный ресурс]. URL: https://mqtt.org/ (дата обращения: 14.08.2024).

28. Isaeva O. S., Isaev S. V., Kulyasov N. V. [Formation of adaptive publications from the Internet of Things data broker]. *Informatsionno-upravliaiushchie sistemy*, 2022, No. 5(120), P. 23–31 (In Russ.).

29. Isaeva O. S., Kulyasov N. V., Isaev S. V. [Creating data collection tools to analyze security aspects Internet of Things]. *Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii*, 2022. No. 3(27). P. 113–125 (In Russ.).

30. Jutadhamakorn P., Pillavas T., Visoottiviseth V., Takano R., Haga J., Kobayashi D. A scalable and low-cost MQTT broker clustering system. *2nd International Conference on Information Technology,* IEEE, 2017, P. 1–5.

Исаева Ольга Сергеевна – доктор технических наук, старший научный сотрудник; Институт вычислительного моделирования СО РАН – обособленное подразделение ФИЦ КНЦ СО РАН. E-mail: isaeva@icm.krasn.ru. https://orcid.org/0000-0002-5061-6765.

Кулясов Никита Владимирович – программист; Институт вычислительного моделирования СО РАН – обособленное подразделение ФИЦ КНЦ СО РАН. E-mail: razor@icm.krasn.ru.

Исаев Сергей Владиславович – кандидат технических наук, доцент, заместитель директора по научной работе; Институт вычислительного моделирования СО РАН – обособленное подразделение ФИЦ КНЦ СО РАН. E-mail: si@icm.krasn.ru. https://orcid.org/0000-0002-6678-0084.

Isaeva Olga Sergeevna – Doct. Sc., Senior Researcher; Institute of Computational Modelling of the Siberian Branch of the SB RAS – subdivision Federal Research Center "Krasnoyarsk Scientific Center of the SB RAS". E-mail: isaeva@icm.krasn.ru. https://orcid.org/0000-0002-5061-6765.

Kulyasov Nikita Vladimirovich – programmer; Institute of Computational Modelling of the Siberian Branch of the SB RAS – subdivision Federal Research Center "Krasnoyarsk Scientific Center of the SB RAS". E-mail: razor@icm.krasn.ru.

Isaev Sergey Vladislavovich – Cand. Sc., Associate Professor, Deputy Director for Research; Institute of Computational Modelling of the Siberian Branch of the SB RAS – subdivision Federal Research Center "Krasnoyarsk Scientific Center of the SB RAS". E-mail: si@icm.krasn.ru. https://orcid.org/0000-0002-6678-0084.

Статья поступила в редакцию 09.12.2024; принята к публикации 16.01.2025; опубликована 11.04.2025
The article was submitted 09.12.2024; accepted for publication 16.01.2025; published 11.04.2025